Nouveau cours de mathématiques
Tome 5

Jean-Marie MONIER

ALGÈBRE 1

cours et 600 exercices corrigés

1re année

MPSI . PCSI . PTSI

j'intègre

PRÉPAS SCIENTIFIQUES

DUNOD

Cours de mathématiques - 5

ALGÈBRE 1

cours et
600 exercices corrigés

1re année MPSI . PCSI . PTSI

Cours de mathématiques - 5

ALGÈBRE 1

cours et 600 exercices corrigés

1re année MPSI . PCSI . PTSI

Jean-Marie Monier
Professeur en classe de Spéciales
au lycée la Martinière-Monplaisir à Lyon

DUNOD

Ce pictogramme mérite une explication. Son objet est d'alerter le lecteur sur la menace que représente pour l'avenir de l'écrit, particulièrement dans le domaine de l'édition technique et universitaire, le développement massif du **photocopillage**.

Le Code de la propriété intellectuelle du 1er juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée dans les établissements d'enseignement supérieur, provoquant une baisse brutale des achats de livres et de revues, au point que la possibilité même pour les auteurs de créer des œuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée.

Nous rappelons donc que toute reproduction, partielle ou totale, de la présente publication est interdite sans autorisation du Centre français d'exploitation du droit de copie (**CFC**, 3 rue Hautefeuille, 75006 Paris).

ISBN 2 10 002974-6

Avant-propos

Ce nouveau Cours de Mathématiques avec exercices corrigés s'adresse aux élèves des classes préparatoires aux grandes écoles (1re et 2e années, toutes filières), aux étudiants du premier cycle universitaire scientifique et aux candidats aux concours de recrutement de professeurs.

Le plan en est le suivant :

Tome 1 : Analyse 1
Tome 2 : Analyse 2
} Analyse en 1re année (2e édition, juin 1996)

Tome 3 : Analyse 3
Tome 4 : Analyse 4
} Analyse en 2e année (2e édition, juin 1997)

Tome 5 : Algèbre 1 : Algèbre en 1re année.

Tome 6 : Algèbre 2 : Algèbre en 2e année.

Tome 7 : Géométrie : Géométrie en 1re année et 2e années (à paraître fin 1997).

Pour vérifier sa bonne compréhension du cours, le lecteur trouvera dans chaque chapitre des exercices tous résolus et dont les solutions sont regroupées en fin de volume et qui sont, à de rares exceptions près, différents de ceux figurant dans les recueils d'exercices déjà parus.

Des questions situées à la limite du programme sont traitées, en fin de chapitre, sous forme de compléments corrigés.

J'accueillerai avec reconnaissance les critiques et suggestions que le lecteur voudra bien me faire parvenir aux bons soins de Dunod, éditeur, 15, rue Gossin, 92513 Montrouge Cedex.

Jean-Marie Monier

Remerciements

Je tiens ici à exprimer ma gratitude aux nombreux collègues qui ont accepté de réviser des parties du manuscrit ou de la saisie : Robert AMBLARD, Bruno ARSAC, Chantal AURAY, Henri BAROZ, Alain BERNARD, Jean-Philippe BERNE, Mohamed BERRAHO, Isabelle BIGEARD, Jacques BLANC, Gérard BOURGIN, Gérard-Pierre BOUVIER, Gérard CASSAYRE, Gilles CHAFFARD, Jean-Paul CHRISTIN, Yves COUTAREL, Gilles DEMEUSOIS, Catherine DONY, Hermin DURAND, Jean FEYLER, Marguerite GAUTHIER, Daniel GENOUD, Christian GIRAUD, André GRUZ, André LAFFONT, Jean-Marc LAPIERRE, Annie MICHEL, Rémy NICOLAÏ, Michel PERNOUD, Jean REY, Sophie RONDEAU, René ROY, Nathalie et Philippe SAUNOIS, Patrice SCHWARTZ, Gérard SIBERT, Mimoun TAÏBI.

Une pensée émue accompagne le regretté Alain GOURET.

Enfin, je remercie vivement les Éditions Dunod, Gisèle Maïus et Michel Mounic, dont la compétence et la persévérance ont permis la réalisation de ces volumes.

Jean-Marie Monier

Table des matières du tome 5

Première partie – Cours

Cours

Chapitre 1

Vocabulaire de la théorie des ensembles

Le but est ici d'exposer un vocabulaire et des propriétés utilisables et utilisés dans tous les domaines des Mathématiques, sans masquer inutilement la puissance de leur généralité, mais également sans développement stérile.

Nous supposons connues du lecteur les propriétés élémentaires de l'ensemble $\mathbb{N} = \{0,1,2,\ldots\}$ des entiers naturels.

1.1 Ensembles

1.1.1 Eléments de logique

Une **assertion** (ou : **propriété**) p peut être vraie ou fausse (l'un des deux, mais pas les deux simultanément). Une **table de vérité** consigne ces deux possibilités :

p
V
F

Un **théorème** (ou : **proposition**) est une assertion vraie.

La **négation** d'une assertion p est l'assertion notée non p (ou : $\rceil p$), définie par la table de vérité ci-contre.

p	non p
V	F
F	V

Les **connecteurs logiques** et **(conjonction)**, ou **(disjonction)**, $\Longrightarrow$ **(implication)**, $\Longleftrightarrow$ **(équivalence logique)** sont définis par :

p	q	p et q	p ou q	$p \Longrightarrow q$	$p \Longleftrightarrow q$
V	V	V	V	V	V
V	F	F	V	F	F
F	V	F	V	V	F
F	F	F	F	V	V

«et» peut se noter : $\wedge$; «ou» peut se noter : $\vee$. Il peut être commode de noter $\begin{cases} p \\ q \end{cases}$ au lieu de : p et q.

Dans l'implication $p \Longrightarrow q$, p s'appelle l'**hypothèse**, q la **conclusion**.
L'implication $q \Longrightarrow p$ s'appelle la **réciproque** de l'implication $p \Longrightarrow q$.
On peut exprimer $p \Longrightarrow q$ de l'une des façons suivantes :

pour que p, il faut que q
pour que q, il suffit que p
si p, alors q
p est une condition suffisante pour q
q est une condition nécessaire de p.

L'équivalence logique $p \Longleftrightarrow q$ peut s'exprimer par :

pour que p, il faut et il suffit que q
p est une condition nécessaire et suffisante (CNS) pour q
p si et seulement si q.

Un **théorème de logique** (appelé aussi **tautologie**) est une assertion vraie quelles que soient les valeurs de vérité des éléments qui la composent. En voici des exemples parmi les plus utiles :

p ou p
p et p
p ou (non p) : tiers exclu
non (p et (non p))
$p \Longrightarrow p$
$p \Longleftrightarrow p$
non (non p) $\Longleftrightarrow p$
(p et ($p \Longrightarrow q$)) $\Longrightarrow q$: **règle d'inférence**, ou syllogisme
($p \Longrightarrow q$) $\Longleftrightarrow$ ((non p) ou q)
($p \Longrightarrow q$) $\Longleftrightarrow$ ((non q) $\Longrightarrow$ (non p)) : **principe de contre-apposition**
(non (p ou q)) $\Longleftrightarrow$ ((non p) et (non q))
(non (p et q)) $\Longleftrightarrow$ ((non p) ou (non q))
(non ($p \Longrightarrow q$)) $\Longleftrightarrow$ (p et (non q))
((p et q) et r) $\Longleftrightarrow$ (p et (q et r)) : associativité du et
((p ou q) ou r) $\Longleftrightarrow$ (p ou (q ou r)) : associativité du ou
((p et q) ou r) $\Longleftrightarrow$ ((p ou r) et (q ou r)) : distributivité de ou sur et
((p ou q) et r) $\Longleftrightarrow$ ((p et r) ou (q et r)) : distributivité de et sur ou
(($p \Longrightarrow q$) et ($q \Longrightarrow r$)) $\Longrightarrow$ ($p \Longrightarrow r$) : transitivité de l'implication.

Par convention, on écrit $p \Longrightarrow q \Longrightarrow r$ au lieu de : ($p \Longrightarrow q$) et ($q \Longrightarrow r$).
A titre d'exemple, montrons le théorème relatif à la négation d'une implication :

p	q	$p \Rightarrow q$	non $(p \Rightarrow q)$	non q	p et (non q)	(non $(p \Rightarrow q)$) $\Leftrightarrow$ (p et (non q))
V	V	V	F	F	F	V
V	F	F	V	V	V	V
F	V	V	F	F	F	V
F	F	V	F	V	F	V

Raisonnement par l'absurde

Pour établir que $p \Longrightarrow q$ est vraie, on suppose que p est vraie et q est fausse, et on montre que cela entraîne une contradiction.

Ceci revient à montrer que (p et (non q)) est fausse, c'est-à-dire que (non p) ou q est vraie, ce qui est bien $p \Longrightarrow q$.

Exercice

◇ **1.1.1** Montrer les théorèmes de logique suivants :

a) $(p \Longleftrightarrow q) \Longleftrightarrow (q \Longleftrightarrow p)$

b) $\begin{cases} p \Longrightarrow q \\ q \Longrightarrow r \\ r \Longrightarrow p \end{cases} \Longrightarrow \begin{cases} p \Longleftrightarrow q \\ p \Longleftrightarrow r \\ q \Longleftrightarrow r \end{cases}$

c) $(p \Longrightarrow (q \Longrightarrow r)) \Longleftrightarrow ((p \text{ et } q) \Longrightarrow r)$

d) $((p \text{ ou } q) \Longrightarrow r) \Longleftrightarrow ((p \Longrightarrow r) \text{ et } (q \Longrightarrow r))$.

1.1.2 Ensembles

Nous nous contenterons d'une notion naïve (intuitive) des **ensembles**, sans aborder la notion de relation «collectivisante». Un ensemble est une collection d'objets, par exemple $\{0,1,3\}$, $\{x \in \mathbb{R};\ x \geqslant 2\}$. La notation $x \in E$ signifie : x **appartient à** (ou : **est élément de**) E ; sa négation est notée $x \notin E$. On note $\varnothing$ l'**ensemble vide**, qui n'a aucun élément.

Un ensemble ayant un élément x et un seul est appelé **singleton**, et noté $\{x\}$.

Le **quantificateur universel** $\forall$ se lit «pour tout» ou «quel que soit».

Le **quantificateur existentiel** $\exists$ se lit «il existe au moins un élément». La notation $\exists!$ signifie : il existe un et un seul élément.

La lettre affectée par un quantificateur est muette; elle peut être remplacée par n'importe quelle lettre (n'ayant pas, par ailleurs, déjà une signification) :

$$\big(\forall x \in E, P(x)\big) \Longleftrightarrow \big(\forall y \in E, P(y)\big)$$
$$\big(\exists x \in E, P(x)\big) \Longleftrightarrow \big(\exists y \in E, P(y)\big).$$

Négation d'une phase quantifiée

On a : $\begin{cases} \big(\text{non } \big(\forall x \in E, P(x)\big)\big) \Longleftrightarrow \big(\exists x \in E, \text{ non } P(x)\big) \\ \big(\text{non } \big(\exists x \in E, P(x)\big)\big) \Longleftrightarrow \big(\forall x \in E, \text{ non } P(x)\big). \end{cases}$

Toute phrase quantifiée commençant par $\exists x \in \varnothing$ est fausse. Toute phrase quantifiée commençant par $\forall x \in \varnothing$ est vraie.

Dans une phrase quantifiée, on ne peut pas, a priori, modifier l'ordre des quantificateurs.

Par exemple : $(\forall x \in \mathbb{N}, \exists y \in \mathbb{N}, x \leqslant y)$ est vraie, mais $(\exists y \in \mathbb{N}, \forall x \in \mathbb{N}, x \leqslant y)$ est fausse.

Cependant, si les ensembles E, E' sont fixés :

$$\big(\forall x \in E, \forall x' \in E', P(x,x')\big) \iff \big(\forall x' \in E', \forall x \in E, P(x,x')\big)$$

et :

$$\big(\exists x \in E, \exists x' \in E', P(x,x')\big) \iff \big(\exists x' \in E', \exists x \in E, P(x,x')\big).$$

1.1.3 Inclusion

◆ **Définition** Etant donnés deux ensembles E, F, on dit que E **est inclus dans** F (ou : E est une **partie** de F ; ou : F **contient** E), et on note $E \subset F$ (ou : $F \supset E$), si et seulement si : $\forall x \in E, x \in F$.

On note $\mathfrak{P}(E)$ l'ensemble des parties de E.

EXEMPLES :

- $\mathfrak{P}(\varnothing) = \{\varnothing\}$
- $\mathfrak{P}(\{0,1\}) = \{\varnothing, \{0\}, \{1\}, \{0,1\}\}$.

Remarques :

1) $A \in \mathfrak{P}(E) \iff A \subset E$

2) $\{x\} \in \mathfrak{P}(E) \iff x \in E$.

On note $E \underset{\neq}{\subset} F$ pour : $E \subset F$ et $E \neq F$.

On note $E \not\subset F$ la négation de $E \subset F$, c'est-à-dire : $\exists x \in E, x \notin F$.

On a : $E = F \iff (E \subset F$ et $F \subset E)$.

Et donc : $E \neq F \iff \left| \begin{array}{l} E \not\subset F \\ \text{ou} \\ F \not\subset E \end{array} \right. \iff \left| \begin{array}{l} (\exists x \in E, x \notin F) \\ \text{ou} \\ (\exists y \in F, y \notin E) \end{array} \right.$.

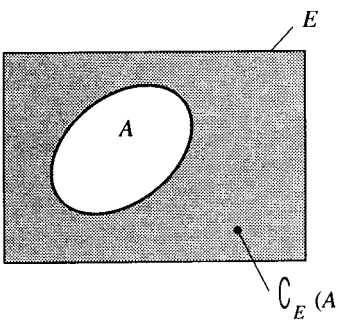
Les propriétés suivantes, pour tous ensembles E, F, G, sont immédiates :

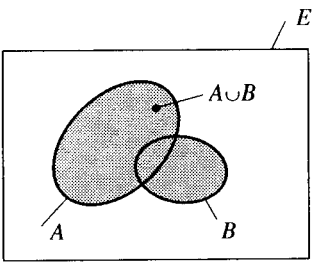
- $\varnothing \subset E$, $E \subset E$
- $\left\{ \begin{array}{l} E \subset F \\ F \subset G \end{array} \right. \Longrightarrow E \subset G$ (transitivité de l'inclusion).

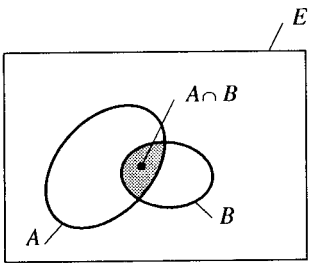
1.1.4 Opérations dans $\mathfrak{P}(E)$

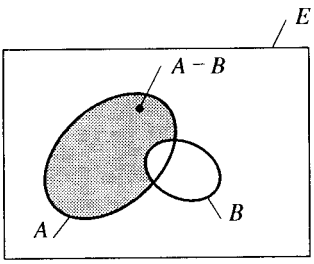
◆ **Définition 1** Soient E un ensemble, $A, B \in \mathfrak{P}(E)$. On définit les parties suivantes de E :

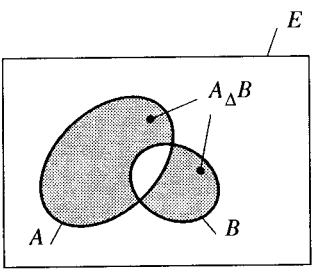
- $\complement_E(A) = \{x \in E ; x \notin A\}$, **complémentaire de A dans E**
- $A \cup B = \{x \in E ; x \in A \text{ ou } x \in B\}$, **réunion de A et B**
- $A \cap B = \{x \in E ; x \in A \text{ et } x \in B\}$, **intersection de A et B**
- $A - B = \{x \in E ; x \in A \text{ et } x \notin B\}$, **différence A moins B**
- $A_\Delta B = (A - B) \cup (B - A)$, **différence symétrique de A et B.**











Pour éviter une éventuelle confusion avec un autre sens de « − » (dans les groupes abéliens, les espaces vectoriels,...) on peut noter $A \setminus B$ au lieu de $A - B$.

Il peut être commode de noter $\overline{A}$ au lieu de $\complement_E(A)$, s'il n'y a pas risque de confusion.

On admettra que la Définition peut s'étendre au cas où A et B ne sont pas «directement» des parties d'un même ensemble E. Par exemple, si F, G sont deux ensembles, on admet qu'on peut définir $F \cup G$, $F \cap G$, $F - G$, $F_\triangle G$ de façon analogue à celle vue ci-dessus.

Deux ensembles F, G sont dits **disjoints** si et seulement si $F \cap G = \varnothing$.

Le lecteur pourra établir, à titre d'exercice, les propriétés suivantes, pour toutes parties A, B, C d'un ensemble E :

- $\complement_E(\varnothing) = E, \complement_E(E) = \varnothing, \complement_E\left(\complement_E(A)\right) = A$

- $A \cup \varnothing = \varnothing \cup A = A$ ($\varnothing$ est neutre pour $\cup$)
  $A \cup A = A$ (tout élément de $\mathfrak{P}(E)$ est idempotent pour $\cup$)
  $A \cup E = E$ (E est absorbant pour $\cup$)
  $A \cup B = B \iff A \subset B$
  $A \cup B = B \cup A$ ($\cup$ est commutative)
  $(A \cup B) \cup C = A \cup (B \cup C)$ ($\cup$ est associative)

- $A \cap \varnothing = \varnothing \cap A = \varnothing$ ($\varnothing$ est absorbant pour $\cap$)
  $A \cap A = A$ (tout élément de $\mathfrak{P}(E)$ est idempotent pour $\cap$)
  $A \cap E = A$ (E est neutre pour $\cap$)
  $A \cap B = A \iff A \subset B$
  $A \cap B = B \cap A$ ($\cap$ est commutative)
  $(A \cap B) \cap C = A \cap (B \cap C)$ ($\cap$ est associative)

- $\complement_E(A \cup B) = \complement_E(A) \cap \complement_E(B), \complement_E(A \cap B) = \complement_E(A) \cup \complement_E(B)$
  (lois de De Morgan)

- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (distributivité de $\cap$ par rapport à $\cup$)
  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (distributivité de $\cup$ par rapport à $\cap$)
  $A \cap (A \cup B) = A \cup (A \cap B) = A$ (égalités modulaires)

- $\complement_E(A) = E - A, \quad A - \varnothing = A$
  $A - B = \varnothing \iff A \subset B$
  $A - B = A \cap \complement_E(B) = A - (A \cap B)$

- $A_\triangle B = B_\triangle A$ ($\triangle$ est commutative)
  $A_\triangle \varnothing = A$ ($\varnothing$ est neutre pour $\triangle$)
  $A_\triangle A = \varnothing$ (tout élément de $\mathfrak{P}(E)$ est son symétrique pour $\triangle$)
  $A_\triangle B = (A \cup B) - (A \cap B)$.

◆ **Définition 2** Soient E un ensemble, $\mathcal{P}$ une partie de $\mathfrak{P}(E)$. On dit que $\mathcal{P}$ est une **partition** de E si et seulement si :

(i) $\forall A \in \mathcal{P}, A \neq \varnothing$

(ii) $\forall A \in \mathcal{P}, \forall B \in \mathcal{P}, (A \neq B \Longrightarrow A \cap B = \varnothing)$

(iii) $\forall x \in E, \exists A \in \mathcal{P}, x \in A$.

EXEMPLES :

1) Pour tout ensemble non vide E, $\{E\}$ et $\{\{x\}; x \in E\}$ sont des partitions de E.

2) Pour tout ensemble E et toute partie A de E autre que $\varnothing$ et E, $\{A, \complement_E(A)\}$ est une partition de E.

3) $\{\mathbb{R}^*_-, \{0\}, \mathbb{R}^*_+\}$ est une partition de $\mathbb{R}$.

Exercices

◇ **1.1.2** Soit E un ensemble. Montrer, pour toutes parties A, B, C, D de E :

a) $A \subset B \Longleftrightarrow \complement_E(A) \supset \complement_E(B) \Longleftrightarrow A \cup B = B$
$\Longleftrightarrow A \cup B = A \Longleftrightarrow A - B = \varnothing \Longleftrightarrow \complement_E(A) \cup B = E$

b) $A \cap B \subset (A \cap C) \cup (B \cap \complement_E(C))$

c) $A \cup B = A \cap C \Longleftrightarrow B \subset A \subset C$

d) $\begin{cases} A \cap B = A \cap C \\ A \cup B = A \cup C \end{cases} \Longleftrightarrow B = C$

e) $(A - B) \cup (A - C) = A - (B \cap C)$

f) $(A - B) - (A - C) = (A - B) \cap C = (A \cap C) - B$

g) $\begin{cases} A \cap C \subset B \cap C \\ A - C \subset B - C \end{cases} \Longleftrightarrow A \subset B$

h) $A \cup \big(B \cap (A \cup C)\big) = A \cup (B \cap C)$

i) $A \cap \big(B \cup (A \cap C)\big) = A \cap (B \cup C)$

j) $A \cap B = C \cap D \Longrightarrow \big(A \cup (B \cap C)\big) \cap \big(A \cup (B \cap D)\big) = A$

k) $(A \cap B = C \cap D, C \cup D = E, C \subset A, D \subset B) \Longrightarrow (C = A, D = B)$.

◇ **1.1.3** Soient E un ensemble, $X, Y, Z, X', Y', Z' \in \mathfrak{P}(E)$. On suppose :

$$\begin{cases} X \cup Y \cup Z = E \\ X \cap Y = X' \cap Y', X \cap Z = X' \cap Z', Y \cap Z = Y' \cap Z' \\ X \subset X', Y \subset Y', Z \subset Z'. \end{cases}$$

Etablir : $X = X', Y = Y', Z = Z'$.

◇ **1.1.4** Soient E un ensemble, $A, B \in \mathfrak{P}(E)$. Résoudre dans $\mathfrak{P}(E)$ les équations suivantes :

a) $X \cup A = B$

b) $X \cap A = B$

c) $X - A = B$

d) $X_{\triangle} A = B$.

◇ **1.1.5** Soient E un ensemble, $\mathcal{P}$ une partition de E, $\mathcal{A}$ une partie de $\mathcal{P}$, $\mathcal{B} = \complement_{\mathcal{P}}(\mathcal{A})$. On note :

$$F = \{x \in E ; \exists A \in \mathcal{A}, x \in A\}, \qquad G = \{x \in E ; \exists B \in \mathcal{B}, x \in B\}.$$

a) Montrer que $\mathcal{A}$ (resp. $\mathcal{B}$) est une partition de F (resp. G).

b) Etablir : $G = \complement_E(F)$.

◇ **1.1.6** Soient E un ensemble, $n \in \mathbb{N}^*$, $A_0, \ldots, A_n$ des parties de E telles que :

$$\varnothing = A_0 \underset{\neq}{\subset} A_1 \underset{\neq}{\subset} A_2 \ldots \underset{\neq}{\subset} A_n = E.$$

On note $B_1 = A_1 - A_0, \ldots, B_n = A_n - A_{n-1}$.
Montrer que $\{B_1, \ldots, B_n\}$ est une partition de E.

1.2 Relations

1.2.1 Généralités

◆ **Définition 1** Pour deux éléments x,y, on appelle **couple** (x,y) l'ensemble $\{\{x\},\{x,y\}\}$.

Il s'agit d'un artifice pour définir (x,y) comme la donnée de deux éléments x,y (non nécessairement distincts) dans un certain ordre : x d'abord, puis y.

◆ **Proposition 1** Pour tous éléments x,y,x',y', on a :

$$(x,y) = (x',y') \Longleftrightarrow \begin{cases} x = x' \\ y = y' \end{cases}.$$

Preuve :

• L'implication $\Longleftarrow$ est évidente.

• Supposons $(x,y) = (x',y')$, c'est-à-dire : $\{\{x\},\{x,y\}\} = \{\{x'\},\{x',y'\}\}$.

Supposons $x \neq x'$. Alors $\{x\} \neq \{x'\}$, donc $\{x\} = \{x',y'\}$ et $\{x,y\} = \{x'\}$, d'où $x = y'$ et $x' = y$. Mais alors $\{\{x\},\{x,x'\}\} = \{\{x'\},\{x',x\}\}$, d'où $\{x\} = \{x'\}$, $x = x'$, contradiction.
On a donc $x = x'$, puis $\{x,y\} = \{x',y'\} = \{x,y'\}$, et donc $y = y'$. ■

On peut dire que le couple (x,y) est la donnée de x et y, «dans cet ordre».

◆ **Définition 2** Soient E,F deux ensembles. On appelle **produit cartésien de E et F** l'ensemble des couples (x,y) tels que $x \in E$ et $y \in F$:

$$E \times F = \{(x,y);\ x \in E \text{ et } y \in F\}.$$

L'ensemble $E \times E$ est souvent noté E^2.

En pratique, au lieu d'écrire $\forall (x,y) \in E^2, \ldots$, on peut noter : $\forall x,y \in E, \ldots$
La proposition suivante est immédiate :

◆ **Proposition 2** Pour tous ensembles E,F,G :

1) $E \times F = \varnothing \Longleftrightarrow (E = \varnothing \text{ ou } F = \varnothing)$

2) $E \times F = F \times E \Longleftrightarrow (E = \varnothing \text{ ou } F = \varnothing \text{ ou } E = F)$

3) $(E \times F) \cup (E \times G) = E \times (F \cup G)$

4) $(E \times F) \cup (G \times F) = (E \cup G) \times F$

5) $(E \times F) \cap (G \times H) = (E \cap G) \times (F \cap H)$.

Remarque :

Il se peut que $(E \times F) \cup (G \times H) \neq (E \cup G) \times (F \cup H)$, comme le montre l'exemple : $E = F = \{0\}$, $G = H = \{1\}$. ■

Soient $n \in \mathbb{N}^*$, $E_1,\ldots,E_n$ des ensembles. Pour tout x_1 de $E_1,\ldots,x_n$ de E_n, on note $(x_1,\ldots,x_n) = (\ldots((x_1,x_2),x_3),\ldots,x_n)$, appelé ***n*-uplet**, et on note $\prod_{i=1}^{n} E_i$ (ou $E_1 \times \ldots \times E_n$), appelé **produit cartésien de** $E_1,\ldots,E_n$, l'ensemble des n-uplets $(x_1,\ldots,x_n)$ où $x_1 \in E_1,\ldots,x_n \in E_n$. Un 3-uplet est appelé un **triplet**. Il est clair que, pour tout $(x_1,\ldots,x_n)$ et tout $(y_1,\ldots,y_n)$ de $\prod_{i=1}^{n} E_i$, on a :

$$(x_1,\ldots,x_n) = (y_1,\ldots,y_n) \iff (\forall i \in \{1,\ldots,n\}, x_i = y_i).$$

◆ **Définition 3** Soient E, F deux ensembles.

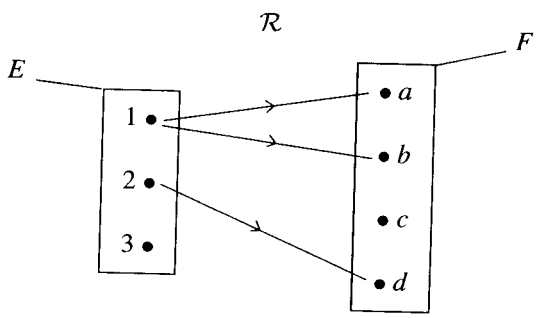
On appelle **relation** (ou : **correspondance**) de E vers F tout triplet (E,Γ,F) où Γ est une partie de $E \times F$. On note $x\mathcal{R}y$ au lieu de $(x,y) \in \Gamma$.

E s'appelle l'**ensemble de départ** de $\mathcal{R}$

F s'appelle l'**ensemble d'arrivée** de $\mathcal{R}$

Γ s'appelle le **graphe** de $\mathcal{R}$.

On peut représenter une relation par un **diagramme (sagittal)** dans lequel une flèche va de x vers y si et seulement si $x\mathcal{R}y$. Exemple :



Le graphe de $\mathcal{R}$ est : $\{(1,a),(1,b),(2,d)\}$. ■

Deux relations $\mathcal{R},\mathcal{S}$ sont égales si et seulement si :

$$\begin{cases} \mathcal{R} \text{ et } \mathcal{S} \text{ ont le même ensemble de départ, noté } E \\ \mathcal{R} \text{ et } \mathcal{S} \text{ ont le même ensemble d'arrivée, noté } F \\ \forall (x,y) \in E \times F, \quad (x\mathcal{R}y \iff x\mathcal{S}y). \end{cases}$$ ■

Si $\mathcal{R}$ est une relation de E vers F, on note $\not\mathcal{R}$ (ou : non $\mathcal{R}$) la relation de E vers F définie par :

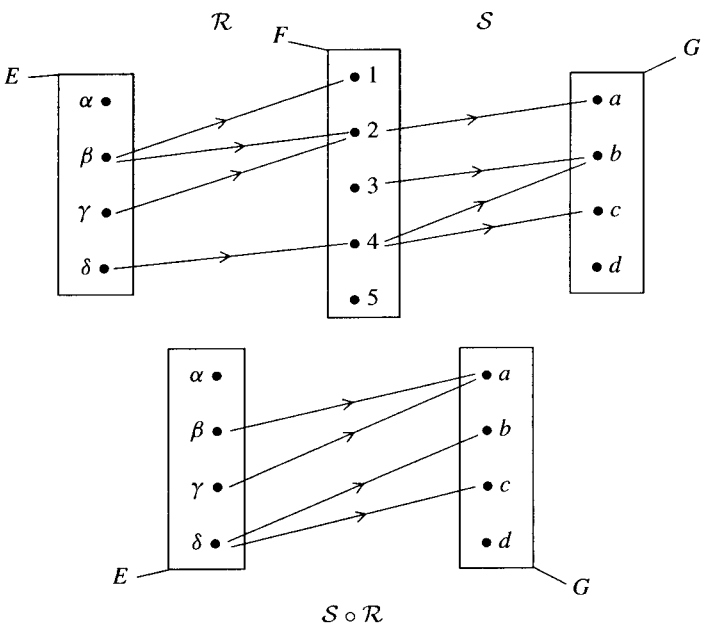
$$\forall (x,y) \in E \times F, \quad \big(x\not\mathcal{R}y \iff (\text{non}(x\mathcal{R}y))\big).$$

◆ **Définition 4** Soient E, F, G trois ensembles, $\mathcal{R}$ (resp. $\mathcal{S}$) une relation de E vers F (resp. de F vers G). On définit la relation **composée** de $\mathcal{R}$ et $\mathcal{S}$, notée $\mathcal{S} \circ \mathcal{R}$, de E vers G par :

$$\forall (x,z) \in E \times G, \quad \left(x \ \mathcal{S} \circ \mathcal{R} \ z \Longleftrightarrow \left(\exists y \in F, \begin{cases} x \mathcal{R} y \\ y \mathcal{S} z \end{cases} \right) \right).$$

EXEMPLES :

1)



2) $E = F = G$ est l'ensemble des droites d'un plan affine euclidien

$\mathcal{R} = \mathcal{S} = \perp$, orthogonalité.

Alors $\mathcal{S} \circ \mathcal{R} = //$ (parallélisme) car pour toutes droites D, D'' de E :

$$D // D'' \Longleftrightarrow \left(\exists D' \in E, \begin{cases} D \perp D' \\ D' \perp D'' \end{cases} \right).$$

On peut donc écrire ici : $\perp \circ \perp = //$.

◆ **Proposition 3** **(Associativité de la composition des relations)**

Soient E, F, G, H des ensembles, $\mathcal{R}$ (resp. $\mathcal{S}$, resp. $\mathcal{T}$) une relation de E vers F (resp. F vers G, resp. G vers H). On a alors :

$$(\mathcal{T} \circ \mathcal{S}) \circ \mathcal{R} = \mathcal{T} \circ (\mathcal{S} \circ \mathcal{R}).$$

Preuve :

D'abord, $(\mathcal{T}\circ\mathcal{S})\circ\mathcal{R}$ et $\mathcal{T}\circ(\mathcal{S}\circ\mathcal{R})$ ont le même ensemble de départ (E) et le même ensemble d'arrivée (H).

Soit $(x,t)\in E\times H$. On a :

$$x\ (\mathcal{T}\circ\mathcal{S})\circ\mathcal{R}\ t \iff \left(\exists y\in F\begin{cases} x\mathcal{R}y \\ y\ \mathcal{T}\circ\mathcal{S}\ t\end{cases}\right) \iff \left(\exists y\in F,\exists z\in G,\begin{cases} x\mathcal{R}y \\ y\mathcal{S}z \\ z\mathcal{T}t\end{cases}\right)$$
$$\iff \left(\exists z\in G\begin{cases} x\ \mathcal{S}\circ\mathcal{R}\ z \\ z\,\mathcal{T}\,t\end{cases}\right) \iff x\ \mathcal{T}\circ(\mathcal{S}\circ\mathcal{R})\ t.$$

◆ **Définition 5** Soient E,F deux ensembles, $\mathcal{R}$ une relation de E vers F. On définit la **relation réciproque** de $\mathcal{R}$, notée $\mathcal{R}^{-1}$, de F vers E, par :

$$\forall(x,y)\in E\times F,\quad (y\mathcal{R}^{-1}x \iff x\mathcal{R}y).$$

Par exemple, la relation réciproque de $\leqslant$ dans $\mathbb{N}$ est $\geqslant$.

◆ **Proposition 4**

1) Pour toute relation $\mathcal{R}$: $(\mathcal{R}^{-1})^{-1}=\mathcal{R}$.

2) Soient E,F,G des ensembles, $\mathcal{R}$ (resp. $\mathcal{S}$) une relation de E vers F (resp. F vers G). On a :

$$(\mathcal{S}\circ\mathcal{R})^{-1}=\mathcal{R}^{-1}\circ\mathcal{S}^{-1}.$$

Preuve :

1) Immédiat.

2) Pour tout (x,z) de $E\times G$:

$$z\ (\mathcal{S}\circ\mathcal{R})^{-1}\ x \iff x\ \mathcal{S}\circ\mathcal{R}\ z \iff \left(\exists y\in F,\begin{cases} x\mathcal{R}y \\ y\mathcal{S}z\end{cases}\right)$$
$$\iff \left(\exists y\in F,\begin{cases} z\mathcal{S}^{-1}y \\ y\mathcal{R}^{-1}x\end{cases}\right) \iff z\ \mathcal{R}^{-1}\circ\mathcal{S}^{-1}\ x.$$

◆ **Définition 6** Une relation $\mathcal{R}$ de E vers F est appelée **relation binaire** si et seulement si $F=E$. On dit alors que $\mathcal{R}$ est une relation binaire dans E.

La plupart des relations utilisées en Mathématiques sont des relations binaires ($\leqslant$ dans $\mathbb{R}$, divisibilité dans $\mathbb{N}$ ou $\mathbb{Z}$, inclusion dans $\mathfrak{P}(E)$), ou des applications (voir 1.3 p. 23 plus loin).

◆ **Définition 7** Soient E un ensemble, $\mathcal{R}$ une relation binaire dans E, $A\in\mathfrak{P}(E)$. La relation binaire dans A, notée $\mathcal{R}_A$, définie par :

$$\forall(x,y)\in A^2,\quad (x\mathcal{R}_A y \iff x\mathcal{R}y)$$

est appelée **relation induite par** $\mathcal{R}$ **sur** (ou : **dans**) A.

EXEMPLE :

La relation induite sur l'ensemble $\mathcal{P}$ des nombres premiers ($\mathcal{P} = \{2,3,5,7,11,\ldots\}$) par la divisibilité dans $\mathbb{Z}$ est l'égalité.

◆ **Définition 8** Une relation binaire $\mathcal{R}$ dans un ensemble E est dite :

réflexive si et ssi : $\forall x \in E,\ x\mathcal{R}x$

symétrique si et ssi : $\forall (x,y) \in E^2,\ (x\mathcal{R}y \Longrightarrow y\mathcal{R}x)$

antisymétrique si et ssi : $\forall (x,y) \in E^2,\ \left(\begin{cases} x\mathcal{R}y \\ y\mathcal{R}x \end{cases} \Longrightarrow x = y\right)$

transitive si et ssi : $\forall (x,y,z) \in E^3,\ \left(\begin{cases} x\mathcal{R}y \\ y\mathcal{R}z \end{cases} \Longrightarrow x\mathcal{R}z\right)$.

EXEMPLES :

1) La relation $\leqslant$ dans $\mathbb{N}$ est réflexive, non symétrique, antisymétrique, transitive.

2) La relation $\perp$ dans l'ensemble des droites du plan affine euclidien est symétrique, mais n'est ni réflexive, ni antisymétrique, ni transitive.

1.2.2 Relations d'équivalence

◆ **Définition 1** Soit $\mathcal{R}$ une relation binaire dans un ensemble E.

On dit que $\mathcal{R}$ est une **relation d'équivalence** si et seulement si : $\mathcal{R}$ est réflexive, symétrique et transitive.

◆ **Définition 2** Soit $\mathcal{R}$ une relation d'équivalence dans un ensemble E.

Pour tout x de E, on appelle **classe d'équivalence** de x (**modulo** $\mathcal{R}$) l'ensemble, noté $\mathrm{cl}_{\mathcal{R}}(x)$ (ou $\widehat{x}$, ou $\overline{x}$, ou $\dot{x}$) défini par :

$$\mathrm{cl}_{\mathcal{R}}(x) = \{y \in E;\ x\mathcal{R}y\}.$$

Tout élément de $\mathrm{cl}_{\mathcal{R}}(x)$ est appelé **un représentant de** $\mathrm{cl}_{\mathcal{R}}(x)$.

On appelle **ensemble-quotient** de E par $\mathcal{R}$, et on note $E/\mathcal{R}$, l'ensemble des classes d'équivalence modulo $\mathcal{R}$, c'est-à-dire :

$$E/\mathcal{R} = \{\mathrm{cl}_{\mathcal{R}}(x);\ x \in E\}.$$

EXEMPLES :

1) La relation d'égalité dans un ensemble quelconque E est une relation d'équivalence. Pour tout x de E, on a $\mathrm{cl}_{=}(x) = \{x\}$, et $E/_{=} = \{\{x\};\ x \in E\}$.

2) Dans un ensemble E, la relation $\mathcal{R}$ définie par : $\forall (x,y) \in E^2,\quad x\mathcal{R}y$

est une relation d'équivalence. Pour tout x de E, on a $\mathrm{cl}_{\mathcal{R}}(x) = E$, et $E/\mathcal{R} = \{E\}$.

3) Pour tout n de $\mathbb{N}^*$, la relation «est congru à... modulo n», définie par :

$$\forall (x,y) \in \mathbb{Z}^2, \quad (x \equiv y\ [n] \iff n \mid x-y)$$

est une relation d'équivalence (voir plus loin, 4.1.2 Prop. 1 p. 101). Pour tout x de $\mathbb{Z}$, la classe de x est appelée classe de x modulo n et notée $\widehat{x}$ (ou $\overline{x}$, ou $\dot{x}$), et : $\widehat{x} = \{x + kn;\ k \in \mathbb{Z}\}$.

4) Dans l'ensemble d des droites affines d'un plan affine P, la relation de parallélisme est une relation d'équivalence. Pour toute D de d, la classe de D modulo le parallélisme est appelée la direction de D.

◆ **Proposition** Soit E un ensemble.

1) Pour toute relation d'équivalence $\mathcal{R}$ dans E, l'ensemble quotient $E/\mathcal{R}$ est une partition de E.

2) Pour toute partition $\mathcal{P}$ de E, la relation $\mathcal{R}$ définie dans E par :

$$\forall (x,y) \in E^2, \left(x\mathcal{R}y \iff \left(\exists P \in \mathcal{P}, \begin{cases} x \in P \\ y \in P \end{cases}\right)\right)$$

est une relation d'équivalence dans E, et $\mathcal{P} = E/\mathcal{R}$.

Preuve :

1) Soit $\mathcal{R}$ une relation d'équivalence dans E.

- $(\forall x \in E, \mathrm{cl}_{\mathcal{R}}(x) \neq \varnothing)$, car $x \in \mathrm{cl}_{\mathcal{R}}(x)$.
- Soit $(x,y) \in E^2$ tel que $\mathrm{cl}_{\mathcal{R}}(x) \cap \mathrm{cl}_{\mathcal{R}}(y) \neq \varnothing$.

Il existe donc $z \in \mathrm{cl}_{\mathcal{R}}(x) \cap \mathrm{cl}_{\mathcal{R}}(y)$. On a alors $x\mathcal{R}z$ et $y\mathcal{R}z$, d'où (par symétrie et transitivité) $x\mathcal{R}y$. On en déduit $\mathrm{cl}_{\mathcal{R}}(x) \subset \mathrm{cl}_{\mathcal{R}}(y)$. En effet, soit $t \in \mathrm{cl}_{\mathcal{R}}(x)$; on a $x\mathcal{R}t$ et $x\mathcal{R}y$, d'où $y\mathcal{R}t$, c'est-à-dire $t \in \mathrm{cl}_{\mathcal{R}}(y)$. Puis, x et y jouant des rôles symétriques : $\mathrm{cl}_{\mathcal{R}}(x) = \mathrm{cl}_{\mathcal{R}}(y)$.

- Comme $(\forall x \in E, x \in \mathrm{cl}_{\mathcal{R}}(x))$, la réunion des éléments de $E/\mathcal{R}$ est E.

2) Réciproquement, soient $\mathcal{P}$ une partition de E et $\mathcal{R}$ la relation définie dans E par :

$$\forall (x,y) \in E^2, \left(x\mathcal{R}y \iff \left(\exists P \in \mathcal{P}, \begin{cases} x \in P \\ y \in P \end{cases}\right)\right).$$

a) • Comme $(\forall x \in E, \exists P \in \mathcal{P}, x \in P)$, on a : $\forall x \in E, x\mathcal{R}x$, et donc $\mathcal{R}$ est réflexive.

- Pour tout (x,y) de E^2 :

$$x\mathcal{R}y \iff \left(\exists P \in \mathcal{P}, \begin{cases} x \in P \\ y \in P \end{cases}\right) \iff \left(\exists P \in \mathcal{P}, \begin{cases} y \in P \\ x \in P \end{cases}\right) \iff y\mathcal{R}x,$$

et donc $\mathcal{R}$ est symétrique.

- Soit $(x,y,z) \in E^3$ tel que $x\mathcal{R}y$ et $y\mathcal{R}z$. Il existe $P, Q \in \mathcal{P}$ tels que : $\begin{cases} x \in P \\ y \in P \end{cases}$ et $\begin{cases} y \in Q \\ z \in Q \end{cases}$.

Comme $P \cap Q \neq \varnothing$ et que $\mathcal{P}$ est une partition, on a $P = Q$ et donc $\begin{cases} x \in P \\ z \in P \end{cases}$, d'où $x\mathcal{R}z$. Ainsi, $\mathcal{R}$ est transitive.

b) α) Soit $x \in E$. Il existe $P \in \mathcal{P}$ tel que $x \in P$, et on a alors $\mathrm{cl}_{\mathcal{R}}(x) = P$. En effet :

- Pour tout y de P, $\begin{cases} x \in P \\ y \in P \end{cases}$ donc $x\mathcal{R}y$
- Pour tout y de $\mathrm{cl}_{\mathcal{R}}(x)$, il existe $Q \in \mathcal{P}$ tel que $\begin{cases} x \in Q \\ y \in Q \end{cases}$, puis $Q = P$ (car $P \in \mathcal{P}$, $Q \in \mathcal{P}$, $P \cap Q \neq \varnothing$), donc $y \in P$.

Ceci prouve : $E/\mathcal{R} \subset \mathcal{P}$.

β) Réciproquement, soit $P \in \mathcal{P}$. Il existe $x \in P$ et on a alors $\mathrm{cl}_{\mathcal{R}}(x) = P$, d'après α). Ceci montre : $\mathcal{P} \subset E/\mathcal{R}$.

Remarques :

1) Si $\mathcal{R}$ est une relation d'équivalence dans E, alors, pour tout (x,y) de E^2 :

$$x\mathcal{R}y \iff \mathrm{cl}_{\mathcal{R}}(x) = \mathrm{cl}_{\mathcal{R}}(y) \iff x \in \mathrm{cl}_{\mathcal{R}}(y) \iff y \in \mathrm{cl}_{\mathcal{R}}(x).$$

2) La proposition précédente met en évidence une bijection (cf. 1.3.2 Déf. 1 p. 26) entre l'ensemble des relations d'équivalence sur E et l'ensemble des partitions de E.

Exercices

◇ **1.2.1** Soient E un ensemble, $\mathcal{R}$ une relation réflexive dans E telle que :

$$\forall (x,y,z) \in E^3,\ \left(\begin{cases} x\mathcal{R}y \\ y\mathcal{R}z \end{cases} \Longrightarrow z\mathcal{R}x \right).$$

Vérifier que $\mathcal{R}$ est une relation d'équivalence.

◇ **1.2.2** Soient E un ensemble, $\mathcal{R}$ une relation réflexive et transitive dans E, $\mathcal{S}$ la relation définie dans E par :

$$x\mathcal{S}y \iff (x\mathcal{R}y \text{ et } y\mathcal{R}x).$$

Vérifier que $\mathcal{S}$ est une relation d'équivalence.

◇ **1.2.3** Dans $\mathbb{R}$, on considère la relation $\mathcal{R}$ définie par :

$$x\mathcal{R}y \iff x^2 - y^2 = x - y.$$

a) Vérifier que $\mathcal{R}$ est une relation d'équivalence.

b) Pour tout x de $\mathbb{R}$, calculer $\mathrm{cl}_{\mathcal{R}}(x)$.

◇ **1.2.4** Soit $\mathcal{R}$ la relation définie dans $\mathbb{R}$ par :

$$(x^3 + 2)(y^2 + 1) = (y^3 + 2)(x^2 + 1).$$

a) Vérifier que $\mathcal{R}$ est une relation d'équivalence.

b) Pour tout x de $\mathbb{R}$, préciser le nombre d'éléments de $\mathrm{cl}_{\mathcal{R}}(x)$.

1.2.3 Relations d'ordre

1) Généralités

◆ **Définition 1** Soit $\mathcal{R}$ une relation binaire dans un ensemble E.
On dit que $\mathcal{R}$ est une **relation d'ordre** si et seulement si : $\mathcal{R}$ est réflexive, antisymétrique et transitive.

On dit souvent **ordre** au lieu de : relation d'ordre. Une relation d'ordre est souvent notée $\leqslant$ (par exemple, $\leqslant$ usuel dans $\mathbb{R}$), ou $\preccurlyeq$.
Un **ensemble ordonné** est un couple $(E, \preccurlyeq)$ où $\preccurlyeq$ est un ordre sur E.

◆ **Définition 2** Soit $(E, \preccurlyeq)$ un ensemble ordonné.

1) Deux éléments x, y de E sont dits **comparables** (pour $\preccurlyeq$) si et seulement si :

$$x \preccurlyeq y \quad \text{ou} \quad y \preccurlyeq x.$$

2) On dit que $\preccurlyeq$ est une **relation d'ordre totale** (ou : est un **ordre total**) si et seulement si les éléments de E sont tous comparables deux à deux, c'est-à-dire :

$$\forall (x,y) \in E^2, \quad (x \preccurlyeq y \text{ ou } y \preccurlyeq x).$$

EXEMPLES :

1) $\leqslant$ usuel dans $\mathbb{R}$ est un ordre total.

2) Si E est un ensemble ayant au moins deux éléments, l'inclusion dans $\mathfrak{P}(E)$ est un ordre non total. ■

Soit $(E, \preccurlyeq)$ un ensemble ordonné. On définit dans E une relation, notée $\prec$, appelée **ordre strict associé à** $\preccurlyeq$, définie par :

$$\forall (x,y) \in E^2, \quad \left(x \prec y \iff \begin{cases} x \preccurlyeq y \\ x \neq y \end{cases}\right).$$

On remarquera que (si E n'est pas vide), $\prec$ n'est pas une relation d'ordre, puisqu'elle n'est pas réflexive.

La relation réciproque (cf. 1.2.1 Déf. 5 p. 14) d'un ordre $\preccurlyeq$ dans E est un ordre, noté $\succcurlyeq$; autrement dit :

$$\forall (x,y) \in E^2, \quad (x \succcurlyeq y \iff y \preccurlyeq x).$$

Si $\preccurlyeq$ est un ordre sur E, pour toute partie A de E, la relation induite par $\preccurlyeq$ dans A (cf. 1.2.1 Déf. 7 p. 14) est un ordre, appelé **ordre induit** par $\preccurlyeq$ dans A.

2) Eléments remarquables d'un ensemble ordonné

◆ **Définition 1** Soit $(E, \preccurlyeq)$ un ensemble ordonné.

1) Soient $A \in \mathfrak{P}(E)$, $x \in E$. On dit que x est **un majorant** (resp. **minorant**) de A dans E si et seulement si :

$$\forall a \in A,\ a \preccurlyeq x \quad (\text{resp.} \quad \forall a \in A,\ x \preccurlyeq a).$$

2) Soit $A \in \mathfrak{P}(E)$. On dit que A est **majorée** (resp. **minorée**) dans E si et seulement si A admet au moins un majorant (resp. minorant) dans E, c'est-à-dire :

$$\exists x \in E, \forall a \in A,\ a \preccurlyeq x \quad (\text{resp.} \quad \exists x \in E, \forall a \in A,\ x \preccurlyeq a).$$

3) Soient $A \in \mathfrak{P}(E)$, $\alpha \in E$. On dit que α est un **plus grand** (resp. **petit**) élément de A si et seulement si :

$$\begin{cases} \alpha \in A \\ \forall a \in A, \quad a \preccurlyeq \alpha \end{cases} \quad \left(\text{resp.} \quad \begin{cases} \alpha \in A \\ \forall a \in A, \quad \alpha \preccurlyeq a \end{cases}\right).$$

4) Soient $A \in \mathfrak{P}(E)$, $x \in A$. On dit que x est **un élément maximal** (resp. **minimal**) de A si et seulement si :

$$\forall a \in A,\ (x \preccurlyeq a \Longrightarrow x = a) \quad (\text{resp.} \quad \forall a \in A,\ (a \preccurlyeq x \Longrightarrow x = a)).$$

On peut noter $\mathrm{Maj}_E(A)$ (resp. $\mathrm{Min}_E(A)$) l'ensemble des majorants (resp. minorants) de A dans E. Pour $(a,b) \in E^2$, on dit que b est **un majorant de** a (ou que a est **un minorant de** b) si et seulement si $a \preccurlyeq b$.

Remarques :

1) Si α, β sont des plus grands éléments de A, alors $\alpha \preccurlyeq \beta$ (car $\alpha \in A$ et β est un plus grand élément de A), et de même $\beta \preccurlyeq \alpha$, d'où $\alpha = \beta$. Ainsi, une partie A de E admet au plus un plus grand élément. Si A admet un plus grand (resp. petit) élément, celui-ci est noté $\mathrm{pge}(A)$ ou $\mathrm{Max}(A)$ (resp. $\mathrm{ppe}(A)$, $\mathrm{Min}(A)$).

2) Une partie A de E peut avoir ou ne pas avoir de plus grand élément. Par exemple, dans $(\mathbb{R}, \leqslant)$, $\mathbb{R}_-$ admet un plus grand élément (qui est 0), mais $\mathbb{R}_+$ n'a pas de plus grand élément.

3) Une partie A de E peut ne pas avoir d'élément maximal, ou en avoir un ou plus d'un. Par exemple :

- dans $(\mathbb{R}, \leqslant)$, $\mathbb{R}_+$ n'a pas d'élément maximal
- dans $(\mathbb{R}, \leqslant)$, $[0; 1]$ admet un élément maximal et un seul, qui est 1 et qui est aussi le plus grand élément de $[0; 1]$
- dans $(\mathbb{N} - \{0,1\}, |)$, $\mathbb{N} - \{0,1\}$ admet une infinité d'éléments minimaux, qui sont les nombres premiers.

4) Si $(E,\preccurlyeq)$ est totalement ordonné, alors E admet au plus un élément maximal, qui est alors aussi le plus grand élément de E. En effet, si x est un élément maximal de E, comme $\preccurlyeq$ est total dans E, on a

$$\forall a \in E, \quad (a \preccurlyeq x \text{ ou } x \preccurlyeq a)$$

et donc : $\forall a \in E$, $(a \preccurlyeq x$ ou $x = a)$, c'est-à-dire : $\forall a \in E, a \preccurlyeq x$.

La notion d'élément maximal n'a donc d'intérêt que dans le cas où $\preccurlyeq$ est non total.

◆ **Définition 2** Soient $(E,\preccurlyeq)$ un ensemble ordonné, $A \in \mathfrak{P}(E)$.

1) Si l'ensemble $\mathrm{Maj}_E(A)$ des majorants de A dans E admet un plus petit élément M, M est appelé **la borne supérieure de** A **(dans** E**)** et est noté $\mathrm{Sup}_E(A)$, ou $\mathrm{Sup}(A)$.

2) Si l'ensemble $\mathrm{Min}_E(A)$ des minorants de A dans E admet un plus grand élément m, m est appelé **la borne inférieure de** A **(dans** E**)** et est noté $\mathrm{Inf}_E(A)$, ou $\mathrm{Inf}(A)$.

Lorsque A est formé de deux éléments x,y, ou d'une famille d'éléments $(x_i)_{i\in I}$, on note $\mathrm{Sup}_E(x,y)$, $\mathrm{Inf}_E(x,y)$, $\sup_{i\in I} x_i$, $\inf_{i\in I} x_i$ au lieu de $\mathrm{Sup}_E(A)$, $\mathrm{Inf}_E(A)$.

Remarque :

Soient $(E,\preccurlyeq)$ un ensemble ordonné, $A \in \mathfrak{P}(E)$, $M \in E$. Pour que M soit la borne supérieure (si elle existe) de A dans E, il faut et il suffit que :

$$\begin{cases} \forall a \in A, & a \preccurlyeq M \\ \forall x \in E, & \big((\forall a \in A, a \preccurlyeq x) \Longrightarrow M \preccurlyeq x\big). \end{cases}$$

EXEMPLES :

1) $E = \mathbb{R}$, $\leqslant$ usuel, $A = [0;1[$.

On a : • $\mathrm{Maj}_E(A) = [1;+\infty[$, donc $\mathrm{Sup}_E(A)$ existe et $\mathrm{Sup}_E(A) = 1$

• $\mathrm{Min}_E(A) =]-\infty;0]$, donc $\mathrm{Inf}_E(A)$ existe et $\mathrm{Inf}_E(A) = 0$.

On remarque, d'après cet exemple, que la borne supérieure (resp. inférieure) de A dans E, si elle existe, peut ne pas appartenir à A.

2) $E = \mathbb{Q}$, $\leqslant$ usuel, $A = \{x \in \mathbb{Q}_+ ; x^2 < 2\}$.

On a : $\mathrm{Maj}_E(A) = \{x \in \mathbb{Q}_+ ; x^2 \geqslant 2\} = \{x \in \mathbb{Q}_+ ; x^2 > 2\}$, qui n'a pas de plus petit élément (cela revient à : $\sqrt{2} \notin \mathbb{Q}$); donc A n'admet pas de borne supérieure dans E.

3) $E = \mathfrak{P}(F)$ où F est un ensemble, $\subset$ est l'inclusion. Pour tout (X,Y) de E^2, on a :

$$\mathrm{Sup}_{\mathfrak{P}(F)}(X,Y) = X \cup Y \quad \text{et} \quad \mathrm{Inf}_{\mathfrak{P}(F)}(X,Y) = X \cap Y.$$

4) $E = \mathbb{N} - \{0,1\}$, $|$ est la divisibilité. Pour tout (x,y) de E^2, on a (cf. 4.2.2 Prop. 3 p. 109) :

$$\mathrm{Sup}(x,y) = x \vee y = \mathrm{ppcm}(x,y), \quad \mathrm{Inf}(x,y) = x \wedge y = \mathrm{pgcd}(x,y).$$

Remarques :

1) • $\mathrm{Sup}_E(\varnothing)$ est le plus petit élément de E (s'il existe)

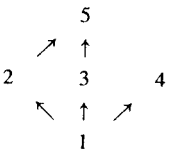
• $\mathrm{Inf}_E(\varnothing)$ est le plus grand élément de E (s'il existe).

2) Pour toute partie non vide A de E, si $\mathrm{Inf}_E(A)$ et $\mathrm{Sup}_E(A)$ existent, alors :

$$\mathrm{Inf}_E(A) \leqslant \mathrm{Sup}_E(A).$$

Exercices

◇ **1.2.5** Soient $E = \{1,2,3,4,5\}$, $\mathcal{R}$ la relation d'ordre définie dans E par le diagramme ci-contre (ne contenant pas la réflexivité ni la transitivité, par convention), $A = \{2,3\}$, $B = \{2,4\}$, $C = \{1,2,5\}$.



Pour chacune des parties A, B, C, étudier l'existence et la valeur éventuelle de l'ensemble de ses majorants dans E, de l'ensemble de ses éléments maximaux, de sa borne supérieure, et de son plus grand élément.

◇ **1.2.6** *a)* Soient $(E, \preccurlyeq)$ un ensemble ordonné, A, B deux parties de E telles que $A \subset B$. Montrer que, si A et B admettent des bornes supérieures dans E, alors $\mathrm{Sup}_E(A) \preccurlyeq \mathrm{Sup}_E(B)$.

b) Donner trois exemples d'ensembles ordonnés $(E, \preccurlyeq)$ et de parties A, B de E telles que $A \subset B$ et telles que :

1) $\begin{cases} A \text{ admet une borne supérieure dans } E \\ B \text{ n'admet pas de borne supérieure dans } E \end{cases}$

2) $\begin{cases} A \text{ n'admet pas de borne supérieure dans } E \\ B \text{ admet une borne supérieure dans } E \end{cases}$

3) $\begin{cases} A \text{ et } B \text{ admettent des bornes supérieures dans } E \\ \mathrm{Sup}_E(A) \neq \mathrm{Sup}_E(B). \end{cases}$

◇ 1.2.7 Ordre produit

Soient $(E,\preccurlyeq)$, $(F,\preccurlyeq)$ deux ensembles ordonnés, $\mathcal{P}$ la relation définie dans $E \times F$ par :

$$(x,y)\mathcal{P}(x',y') \iff \begin{cases} x \preccurlyeq x' \\ y \preccurlyeq y' \end{cases}.$$

a) Montrer que $\mathcal{P}$ est un ordre sur $E \times F$, appelé *ordre produit* des ordres de E et F.

b) On prend ici $E = F = \mathbb{R}$ muni de son ordre usuel.

α) Préciser, pour tout (x,y) de $\mathbb{R}^2$, l'ensemble des majorants de (x,y) dans $\mathbb{R}^2$ pour $\mathcal{P}$.

β) L'ordre $\mathcal{P}$ est-il total dans $\mathbb{R}^2$?

γ) Quel est l'ensemble des éléments maximaux de $A = \{(x,y) \in \mathbb{R}^2 ; x + y \geqslant 0\}$ pour l'ordre $\mathcal{P}$?

δ) Est-ce que $(\mathbb{R}_-^*)^2$ admet une borne supérieure dans $\mathbb{R}^2$ pour $\mathcal{P}$, et si oui, quelle est-elle ?

◇ 1.2.8 Ordre lexicographique

Soient $(E,\preccurlyeq)$, $(F,\preccurlyeq)$ deux ensembles ordonnés, $\mathcal{L}$ la relation définie dans $E \times F$ par :

$$(x,y)\mathcal{L}(x',y') \iff \begin{vmatrix} x \prec x' \\ \text{ou} \\ (x = x' \text{ et } y \preccurlyeq y') \end{vmatrix}.$$

a) Montrer que $\mathcal{L}$ est un ordre sur $E \times F$, appelé *ordre lexicographique* (des ordres de E et F).

b) Montrer que si $\preccurlyeq$ de E et de F sont totaux, alors $\mathcal{L}$ est total.

c) On prend ici $E = F = \mathbb{R}$ muni de son ordre usuel.

α) Préciser, pour tout (x,y) de $\mathbb{R}^2$, l'ensemble des majorants de (x,y) dans $\mathbb{R}^2$ pour $\mathcal{L}$.

β) Est-ce que $\mathbb{R}_-^* \times \mathbb{R}$ admet une borne supérieure dans $\mathbb{R}^2$ pour $\mathcal{L}$, et si oui, quelle est-elle ?

1.3 Applications

1.3.1 Définitions

◆ **Définition 1** Soient E, F deux ensembles.

On appelle **fonction de E vers F** toute relation f de E vers F telle que :

$$\forall (x,y,y') \in E \times F \times F, \quad \left(\begin{cases} x\ f\ y \\ x\ f\ y' \end{cases} \Longrightarrow y = y' \right).$$

On note alors plutôt $y = f(x)$ que $x\ f\ y$.

On appelle **ensemble** (ou **domaine**) **de définition** de la fonction f, et on note $\mathrm{Def}(f)$ l'ensemble des éléments x de E tels qu'il existe $y \in F$ tel que $y = f(x)$.

Pour tout x de E, l'élément y de F tel que $y = f(x)$, s'il existe, est appelé **l'image de x par f**.

Pour tout y de F, tout élément x de E tel que $y = f(x)$ (il peut ne pas en exister, en exister un, en exister plus d'un) est appelé un **antécédent de y par f.**

Ainsi, une relation est une fonction si et seulement si tout élément du départ est en relation avec au plus un élément de l'arrivée.

◆ **Proposition 1** Si f est une fonction de E vers F et g une fonction de F vers G, alors la relation $g \circ f$ (cf. 1.2.1 Déf. 4 p. 13) est une fonction de E vers G.

Preuve :

Soit $(x,z,z') \in E \times G \times G$ tel que : $\begin{cases} x\ (g \circ f)\ z \\ x\ (g \circ f)\ z' \end{cases}$. Il existe $(y,y') \in F^2$ tel que : $\begin{cases} x\ f\ y \quad \text{et} \quad y\ g\ z \\ x\ f\ y' \quad \text{et} \quad y'\ g\ z' \end{cases}$.

Comme $\begin{cases} x\ f\ y \\ x\ f\ y' \end{cases}$ et que f est une fonction, on a $y = y'$. Puis, comme $\begin{cases} y\ g\ z \\ y\ g\ z' \end{cases}$, et que g est une fonction, on conclut $z = z'$.

◆ **Définition 2** Une fonction f de E vers F est appelée **application** si et seulement si $\mathrm{Def}(f) = E$. L'ensemble des applications de E dans F est noté F^E.

Autrement dit, une relation $\mathcal{R}$ de E vers F est une application si et seulement si, pour tout x de E, il existe un et un seul élément y de F tel que $x\mathcal{R}y$. La notation F^E sera justifiée plus loin (3.5.1 p. 91).

Une application f de E vers F est notée $f : E \underset{x \longmapsto f(x)}{\longrightarrow} F$, où la lettre x est muette.

Remarque :

Deux applications f, g sont égales si et seulement si elles ont même ensemble de départ (noté E), même ensemble d'arrivée, et : $\forall x \in E, \quad f(x) = g(x)$.

◆ **Proposition 2** Si $f : E \longrightarrow F, g : F \longrightarrow G$ sont deux applications, alors la fonction composée $g \circ f$ est une application.

Preuve :

D'après Prop. 1 p. 23, $g \circ f$ est déjà une fonction. Soit $x \in E$. Puisque f est une application, il existe $y \in F$ tel que $y = f(x)$. Puis, comme g est une application, il existe $z \in G$ tel que $z = g(y)$. On a alors, par définition de $g \circ f$, $z = (g \circ f)(x)$.

Remarque :

Si $f : E \longrightarrow F, g : F \longrightarrow G$ sont deux applications, on a :

$$\forall x \in E, \quad (g \circ f)(x) = g(f(x)).$$

◆ **Proposition 3** **(Associativité de la composition des applications)**

Pour toutes applications $f : E \longrightarrow F, g : F \longrightarrow G, h : G \longrightarrow H$, on a :

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

Preuve :

C'est un cas particulier de 1.2.1 Prop. 3 p. 13.

Remarque :

La composition des applications n'est pas commutative, c'est-à-dire qu'il se peut que $g \circ f \neq f \circ g$. Par exemple, $f : \underset{x \longmapsto x+1}{\mathbb{R} \longrightarrow \mathbb{R}}$ et $g : \underset{y \longmapsto y^2}{\mathbb{R} \longrightarrow \mathbb{R}}$ ne commutent pas pour $\circ$ car :

$$\forall x \in \mathbb{R}, \quad \begin{cases} (g \circ f)(x) = g(x+1) = (x+1)^2 \\ (f \circ g)(x) = f(x^2) = x^2 + 1 \end{cases},$$

et en particulier $(g \circ f)(1) \neq (f \circ g)(1)$. ■

EXEMPLES :

1) Pour tout ensemble E, on note $\mathrm{Id}_E : \underset{x \longmapsto x}{E \longrightarrow E}$, appelée **application identique** (ou : **identité**) de E.

2) Soient E un ensemble, $A \in \mathfrak{P}(E)$; on appelle **inclusion canonique de A dans E** l'application, notée $\mathrm{i}_{A,E}$ (ou i_A) définie par :

$$\mathrm{i}_{A,E} : \underset{x \longmapsto x}{A \longrightarrow E}.$$

3) Soient E un ensemble, $f : E \longrightarrow E$ une application. On note $f^0 = \mathrm{Id}_E$, $f^1 = f$, et, pour tout n de $\mathbb{N} - \{0,1\}$, $f^n = f \circ f^{n-1}$, s'il n'y a pas de risque de confusion avec d'autres opérations (f^{-1} pourrait désigner $\frac{1}{f}$, $f^{(n)}$ pourrait désigner la dérivée $n^{\text{ième}}$ de f...).

4) Soient E, F deux ensembles, $a \in F$. On appelle **application constante** a l'application, souvent notée encore a définie par : $a : \underset{x \longmapsto a}{E \longrightarrow F}$.

5) Soit E un ensemble. Pour toute partie A de E, on définit la **fonction caractéristique** (ou : **fonction indicatrice**) de A, notée χ_A (ou : φ_A) par :

$$\chi_A : E \longrightarrow \{0,1\}, \quad x \longmapsto \begin{cases} 1 \text{ si } x \in A \\ 0 \text{ si } x \in \complement_E(A) \end{cases}.$$

6) Soient $n \in \mathbb{N}^*$, $E_1, \ldots, E_n$ des ensembles. Pour chaque i de $\{1, \ldots, n\}$, on définit la $i^{\text{ème}}$ **projection canonique**, notée p_i par :

$$\begin{array}{rcl} p_i : E_1 \times \ldots \times E_n & \longrightarrow & E_i \,. \\ (x_1, \ldots, x_n) & \longmapsto & x_i \end{array}$$

Par exemple, pour $n = 2$:

$$\begin{array}{rcl} p_1 : E_1 \times E_2 & \longrightarrow & E_1 \\ (x_1, x_2) & \longmapsto & x_1 \end{array} \quad \text{et} \quad \begin{array}{rcl} p_2 : E_1 \times E_2 & \longrightarrow & E_2 \,. \\ (x_1, x_2) & \longmapsto & x_2 \end{array}$$

Remarque :

Pour toute application $f : E \longrightarrow F$, on a :

$$f \circ \mathrm{Id}_E = f \quad \text{et} \quad \mathrm{Id}_F \circ f = f.$$

◆ **Définition 3** Une partie A d'un ensemble E est dite **stable par** une application $f : E \longrightarrow E$ si et seulement si : $\forall a \in A,\ f(a) \in A$.

Exercices

◇ **1.3.1** Soit E un ensemble. Pour toute partie A de E, on note $\varphi_A : E \longrightarrow \{0,1\}$ la fonction

$$x \longmapsto \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \in \overline{A} \end{cases}$$

caractéristique de A (cf. Exemple *5)* p. 24), où $\overline{A} = \complement_E(A)$.

Montrer les formules suivantes, pour toutes parties A, B de E :

1) $A \subset B \Longleftrightarrow \varphi_A \leqslant \varphi_B$

2) $A = B \Longleftrightarrow \varphi_A = \varphi_B$

3) $\varphi_A^2 = \varphi_A$

4) $\varphi_{A \cap B} = \varphi_A \varphi_B$

5) $\varphi_{\overline{A}} = 1 - \varphi_A$

6) $\varphi_{A \cup B} = \varphi_A + \varphi_B - \varphi_A \varphi_B$

7) $\varphi_{A - B} = \varphi_A (1 - \varphi_B)$

8) $\varphi_{A \triangle B} = \varphi_A + \varphi_B - 2\varphi_A \varphi_B = (\varphi_A - \varphi_B)^2 = |\varphi_A - \varphi_B|$.

◇ **1.3.2** Soient E, F deux ensembles, $\mathcal{U}$ l'ensemble des couples (X, f) formés d'une partie non vide X de E et d'une application f de X dans F. On définit dans $\mathcal{U}$ une relation, notée $\mathcal{R}$, par :

$$(X, f)\mathcal{R}(X', f') \Longleftrightarrow \begin{cases} X \subset X' \\ \forall x \in X, \quad f(x) = f'(x). \end{cases}$$

a) Montrer que $\mathcal{R}$ est une relation d'ordre dans $\mathcal{U}$.

b) Quels sont les éléments maximaux (resp. minimaux) de $\mathcal{U}$ pour $\mathcal{R}$?

◇ **1.3.3** Soient E, F, G, E', F', G' des ensembles, $\begin{array}{ccc} E & \xrightarrow{f} & F \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle v} \\ E' & \xrightarrow[f']{} & F' \end{array}$, $\begin{array}{ccc} F & \xrightarrow{g} & G \\ {\scriptstyle v}\downarrow & & \downarrow{\scriptstyle w} \\ F' & \xrightarrow[g']{} & G' \end{array}$

des *diagrammes commutatifs*, c'est-à-dire tels que $v \circ f = f' \circ u$ et $w \circ g = g' \circ v$.

Montrer que le diagramme $\begin{array}{ccc} E & \xrightarrow{g\circ f} & G \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle w} \\ E' & \xrightarrow[g'\circ f']{} & G' \end{array}$ est commutatif.

◇ **1.3.4 Factorisations d'une application**

Soient E, F, G trois ensembles non vides.

a) Soient $f : E \longrightarrow F, g : E \longrightarrow G$ deux applications. Montrer que, pour qu'il existe $h : F \longrightarrow G$ telle que le diagramme $\begin{array}{ccc} E & \xrightarrow{g} & G \\ {\scriptstyle f}\downarrow & \nearrow h & \\ F & & \end{array}$ soit commutatif (c'est-à-dire : $h \circ f = g$), il faut et il suffit que : $\forall (x,x') \in E^2, (f(x) = f(x') \Longrightarrow g(x) = g(x'))$.

b) Soient $g : E \longrightarrow G, h : F \longrightarrow G$ deux applications. Montrer que, pour qu'il existe $f : E \longrightarrow F$ telle que le diagramme $\begin{array}{ccc} E & \xrightarrow{g} & G \\ {\scriptstyle f}\downarrow & \nearrow h & \\ F & & \end{array}$ soit commutatif (c'est-à-dire : $h \circ f = g$), il faut et il suffit que : $\forall x \in E, \ \exists y \in F, \ g(x) = h(y)$.

1.3.2 Injectivité, surjectivité, bijectivité

◆ **Définition 1** Une application $f : E \longrightarrow F$ est dite :

- **injective** si et ssi : $\forall (x,x') \in E^2, (f(x) = f(x') \Longrightarrow x = x')$
- **surjective** si et ssi : $\forall y \in F, \exists x \in E, y = f(x)$
- **bijective** si et ssi : f est surjective et injective, c'est-à-dire : $\forall y \in F, \exists ! x \in E, y = f(x)$.

On dit aussi **injection** (resp. **surjection**, resp. **bijection**) au lieu d'application injective (resp. application surjective, resp. application bijective).

Remarques :

1) Une application $f : E \longrightarrow F$ est injective si et seulement si :

$$\forall (x,x') \in E^2, \quad (x \neq x' \Longrightarrow f(x) \neq f(x')).$$

Autrement dit, $f : E \longrightarrow F$ est injective si et seulement si tout élément de F admet *au plus* un antécédent par f dans E.

2) Une application $f : E \longrightarrow F$ est surjective si et seulement si tout élément de F admet *au moins* un antécédent par f dans E.

EXEMPLES :

1) Si $A \subset E$, l'inclusion canonique $i_A : \begin{array}{ccc} A & \longrightarrow & E \\ x & \longmapsto & x \end{array}$ est une injection, appelée aussi **injection canonique** de A dans E.

2) Soient E un ensemble, $\mathcal{R}$ une relation d'équivalence dans E. L'application $s : \begin{array}{ccc} E & \longrightarrow & E/\mathcal{R} \\ x & \longmapsto & \mathrm{cl}_{\mathcal{R}}(x) \end{array}$ est une surjection, appelée **surjection canonique de E sur $E/\mathcal{R}$**.

◆ **Définition 2**

1) On appelle **permutation** de E toute bijection de E dans E.

2) On appelle **involution** (ou : **application involutive**) de E toute application $f : E \longrightarrow E$ telle que $f \circ f = \mathrm{Id}_E$.

◆ **Proposition 1** La composée de deux injections (resp. surjections, resp. bijections) est une injection (resp. surjection, resp. bijection).

Preuve :

Soient $f : E \longrightarrow F$, $g : F \longrightarrow G$ deux applications.

1) Supposons f et g injectives.

On a, pour tout (x,x') de E^2 :

$$(g \circ f)(x) = (g \circ f)(x') \Longleftrightarrow g(f(x)) = g(f(x')) \Longrightarrow f(x) = f(x') \Longrightarrow x = x',$$

et donc $g \circ f$ est injective.

2) Supposons f et g surjectives.

Soit $z \in G$. Puisque g est surjective, il existe $y \in F$ tel que $z = g(y)$. Puis, comme f est surjective, il existe $x \in E$ tel que $y = f(x)$. On a donc $z = g(f(x)) = (g \circ f)(x)$, ce qui montre que $g \circ f$ est surjective.

3) (f et g bijectives) $\Longrightarrow \left\{ \begin{array}{l} f \text{ et } g \text{ injectives} \\ f \text{ et } g \text{ surjectives} \end{array} \right. \Longrightarrow \left\{ \begin{array}{l} g \circ f \text{ injective} \\ g \circ f \text{ surjective} \end{array} \right. \Longrightarrow (g \circ f \text{ bijective}).$

◆ **Proposition 2** Soient $f : E \longrightarrow F$, $g : F \longrightarrow G$.

1) Si $g \circ f$ est injective, alors f est injective.

2) Si $g \circ f$ est surjective, alors g est surjective.

Preuve :

1) Supposons $g \circ f$ injective. On a, pour tout (x,x') de E^2 :

$$f(x) = f(x') \Longrightarrow g(f(x)) = g(f(x')) \Longleftrightarrow (g \circ f)(x) = (g \circ f)(x') \Longrightarrow x = x',$$

ce qui montre que f est injective.

2) Supposons $g \circ f$ surjective. Soit $z \in G$; il existe $x \in E$ tel que $z = (g \circ f)(x) = g(f(x))$. Ceci montre que g est surjective.

◆ **Proposition 3** Soit $f : E \longrightarrow F$ une application. Pour que la relation réciproque de f soit une application, il faut et il suffit que f soit bijective. De plus, si f est bijective, l'application réciproque f^{-1} de f est une bijection.

Preuve :

1) Rappelons que la relation réciproque f^{-1} de f est définie (cf. 1.2.1 Déf. 5 p. 14) par :

$$\forall (x,y) \in E \times F, \quad y\, f^{-1}\, x \Longleftrightarrow x\, f\, y \Longleftrightarrow y = f(x).$$

On a : $(f$ bijective$) \Longleftrightarrow (\forall y \in F, \exists ! x \in E,\ y = f(x))$

$$\Longleftrightarrow (\forall y \in F, \exists ! x \in E,\ y\, f^{-1}\, x) \Longleftrightarrow (f^{-1} \text{ est une application}).$$

2) Si f est bijective, alors f^{-1} est une application (ci-dessus) et, comme $(f^{-1})^{-1} = f$ est une application, f^{-1} est bijective.

◆ **Proposition 4** Si $f : E \longrightarrow F$ et $g : F \longrightarrow G$ sont bijectives, alors $g \circ f : E \longrightarrow G$ est bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Preuve : Résulte de Prop. 1 p. 27 et 1.2.1 Prop. 4 p. 14.

Remarque :

Dorénavant, nous n'utiliserons guère de réciproque de relation autrement que dans le cas où la relation est une bijection. La notation f^{-1} désignera donc l'application réciproque de f, ce qui suppose que f soit bijective. Cependant, nous emploierons la notation $f^{-1}(A')$ (image réciproque d'une partie A' de l'arrivée) pour une application f quelconque, cf. 1.3.5 Déf. p. 32.

◆ **Proposition 5** Soit $f : E \longrightarrow F$ une application. Pour que f soit bijective, il faut et il suffit qu'il existe une application $g : F \longrightarrow E$ telle que :

$$\begin{cases} g \circ f = \mathrm{Id}_E \\ f \circ g = \mathrm{Id}_F \end{cases}.$$

De plus, sous ces hypothèses, on a : $g = f^{-1}$.

Preuve :

1) Si f est bijective, alors f^{-1} existe en tant qu'application, et il est clair que :

$$\begin{cases} f^{-1} \circ f = \mathrm{Id}_E \\ f \circ f^{-1} = \mathrm{Id}_F \end{cases}.$$

2) Réciproquement, s'il existe $g : F \longrightarrow E$ telle que $\begin{cases} g \circ f = \mathrm{Id}_E \\ f \circ g = \mathrm{Id}_F \end{cases}$, alors, d'après Prop. 2 p. 27, comme Id_E est injective et Id_F est surjective, on déduit que f est injective et surjective, donc bijective. De même pour g. Enfin :

$$g = g \circ (f \circ f^{-1}) = (g \circ f) \circ f^{-1} = \mathrm{Id}_E \circ f^{-1} = f^{-1}.$$

◆ **Corollaire** Une application $f : E \longrightarrow E$ est involutive si et seulement si :

$$\begin{cases} f \text{ est bijective} \\ f^{-1} = f \end{cases}.$$

Exercices

◇ **1.3.5** Soient E, F deux ensembles, $f : E \longrightarrow F$, $g : F \longrightarrow E$ deux applications telles que $f \circ g \circ f$ soit bijective. Montrer que f et g sont bijectives.

◇ **1.3.6** Soient E, F, G des ensembles, $f : E \longrightarrow F$, $g : F \longrightarrow G$ des applications. Montrer :

a) si $g \circ f$ est injective et f surjective, alors g est injective

b) si $g \circ f$ est surjective et g injective, alors f est surjective.

◇ **1.3.7** Soient E, F deux ensembles non vides, $f : E \longrightarrow F$. Montrer (en utilisant l'exercice 1.3.4 p. 26) :

a) f est injective si et seulement s'il existe une application surjective $h : F \longrightarrow E$ telle que $h \circ f = \mathrm{Id}_E$

b) f est surjective si et seulement s'il existe une application injective $g : F \longrightarrow E$ telle que $f \circ g = \mathrm{Id}_F$.

◇ **1.3.8** Soient E, F deux ensembles non vides. Montrer que les deux propriétés suivantes sont équivalentes :

(i) il existe une injection de E dans F

(ii) il existe une surjection de F dans E.

◇ **1.3.9** Soient $f : \begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{N} \\ x & \longmapsto & 2x \end{array}$ et $g : \mathbb{N} \longrightarrow \mathbb{N}$, $y \longmapsto \begin{cases} \dfrac{y}{2} & \text{si } y \text{ est pair} \\ \dfrac{y-1}{2} & \text{si } y \text{ est impair.} \end{cases}$

a) Etudier l'injectivité, la surjectivité, la bijectivité de f et de g.

b) Préciser $g \circ f$ et $f \circ g$.

◇ **1.3.10** **Produit de deux relations d'équivalence**

Soient E, F deux ensembles, $\mathcal{R}$ (resp. $\mathcal{S}$) une relation d'équivalence dans E (resp. F), $\mathcal{T}$ la relation définie dans $E \times F$ par :

$$(x,y)\ \mathcal{T}\ (x',y') \Longleftrightarrow \begin{cases} x \mathcal{R} x' \\ y \mathcal{S} y' \end{cases}.$$

a) Vérifier que $\mathcal{T}$ est une relation d'équivalence dans $E \times F$.

b) Mettre en évidence une bijection entre $E/\mathcal{R} \times F/\mathcal{S}$ et $(E \times F)/\mathcal{T}$.

◇ **1.3.11*** Dans $E = \mathbb{R}^{\mathbb{R}}$, on définit une relation $\mathcal{R}$ par :

$$f \mathcal{R} g \Longleftrightarrow \left(\exists \varphi \in E, \begin{cases} \varphi \text{ est bijective} \\ \varphi \circ f = g \circ \varphi \end{cases} \right).$$

a) Montrer que $\mathcal{R}$ est une relation d'équivalence dans E.

b) A-t-on ch $\mathcal{R}$ sh (fonctions hyperboliques)? cos $\mathcal{R}$ sin?

c) Former une CNS sur $(p,q) \in \mathbb{R}^2$ pour que $f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 \end{array}$ et $g : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 + px + q \end{array}$ soient équivalentes.

1.3.3 Restrictions et prolongements

◆ **Définition 1** Soient E, F deux ensembles, $f : E \longrightarrow F$ une application, $A \in \mathfrak{P}(E)$. On appelle **restriction de f à A** l'application, notée $f|_A$, définie par :

$$f|_A : \begin{array}{ccc} A & \longrightarrow & F \\ x & \longmapsto & f(x) \end{array}.$$

En notant $\mathrm{i} : A \longrightarrow E$ l'inclusion canonique, on a donc : $f|_A = f \circ \mathrm{i}$.

◆ **Définition 2** Soient E, F deux ensembles, $f : E \longrightarrow F$ une application, E' un ensemble tel que $E \subset E'$. On appelle **prolongement de f à E'** toute application $g : E' \longrightarrow F$ telle que : $\forall x \in E, g(x) = f(x)$.

En notant $\mathrm{i} : E \longrightarrow E'$ l'inclusion canonique, g est un prolongement de f à E' si et seulement si $g \circ \mathrm{i} = f$.

Remarque :
Si $f : E \longrightarrow F$ et E' sont donnés, f admet (sauf exception) plus d'un prolongement à E'. Par exemple $f : \mathbb{R}^* \longrightarrow \mathbb{R}$ admet une infinité de prolongements à $\mathbb{R}$, qui sont les applications $x \longmapsto \frac{\sin x}{x}$

$$\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \begin{cases} \dfrac{\sin x}{x} \text{ si } x \neq 0 \\ \alpha \text{ si } x = 0 \end{cases} \end{array}, \alpha \in \mathbb{R}.$$

Parmi ces prolongements, il y en a un remarquable, $g : \mathbb{R} \longrightarrow \mathbb{R}$, car c'est le seul

$$x \longmapsto \begin{cases} \dfrac{\sin x}{x} \text{ si } x \neq 0 \\ 1 \text{ si } x = 0 \end{cases}$$

qui soit continu en 0.

◆ **Définition 3** Soient E, F deux ensembles, $f : E \longrightarrow F$ une application, $A \in \mathfrak{P}(E)$, $B \in \mathfrak{P}(F)$ telles que :

$$\forall a \in A, \quad f(a) \in B.$$

On appelle **application induite par f sur A (au départ) et B (à l'arrivée)** l'application $\begin{array}{ccc} A & \longrightarrow & B \\ x & \longmapsto & f(x) \end{array}$.

En particulier, soient $f : E \longrightarrow E$ une application et A une partie de E stable par f ; l'application induite par f sur A au départ et A à l'arrivée est appelée **application induite par f sur A** et notée souvent f_A. On a donc $f_A : \begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & f(x) \end{array}$.

1.3.4 Ordre et applications

1) Monotonie

◆ **Définition** Soient $(E,\preccurlyeq)$, $(F,\preccurlyeq)$ deux ensembles ordonnés. Une application $f : E \longrightarrow F$ est dite :

- **croissante** si et ssi : $\forall (x,y) \in E^2, (x \preccurlyeq y \Longrightarrow f(x) \preccurlyeq f(y))$
- **décroissante** si et ssi : $\forall (x,y) \in E^2, (x \preccurlyeq y \Longrightarrow f(y) \preccurlyeq f(x))$
- **monotone** si et ssi : f est croissante ou décroissante
- **strictement croissante** si et ssi : $\forall (x,y) \in E^2, (x \prec y \Longrightarrow f(x) \prec f(y))$
- **strictement décroissante** si et ssi : $\forall (x,y) \in E^2, (x \prec y \Longrightarrow f(y) \prec f(x))$
- **strictement monotone** si et ssi : f est strictement croissante ou strictement décroissante.

EXEMPLES :

1) L'application $f : \begin{array}{ccc} \mathbb{N}^* & \longrightarrow & \mathbb{N}^* \\ x & \longmapsto & x^2 \end{array}$ est strictement croissante, lorsqu'on munit $\mathbb{N}^*$ (départ et arrivée) de l'ordre | (divisibilité).

2) L'application $E : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{Z} \\ x & \longmapsto & \mathrm{E}(x) \end{array}$ (partie entière) est croissante, mais non strictement croissante (pour l'ordre $\leqslant$ usuel).

3) Pour tout ensemble E, l'application $\begin{array}{ccc} \mathfrak{P}(E) & \longrightarrow & \mathfrak{P}(E) \\ X & \longmapsto & \complement_E(X) \end{array}$ est strictement décroissante pour l'inclusion.

4) L'application $\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 \end{array}$ n'est pas monotone (pour l'ordre usuel).

2) Ordre induit sur F^X par un ordre de F

La proposition suivante est immédiate.

◆ **Proposition** Soient X un ensemble, $(F,\preccurlyeq)$ un ensemble ordonné. La relation dans F^X, encore notée $\preccurlyeq$, définie par :

$$f \preccurlyeq g \Longleftrightarrow (\forall x \in X, f(x) \preccurlyeq g(x))$$

est une relation d'ordre sur F^X.

Remarque :

Même si l'ordre de F est total, l'ordre sur F^X peut ne pas être total. Par exemple, pour $X = F = \{0,1\}$ ordonné par $\leqslant$ usuel, les éléments f,g de F^X définis par $f(0) = 0$, $f(1) = 1$, $g(0) = 1$, $g(1) = 0$ ne sont pas comparables pour $\leqslant$.

Exercices

◇ **1.3.12** Soient E un ensemble, $(F,\preccurlyeq)$ un ensemble ordonné, $f : E \longrightarrow F$ une application injective. On définit dans E une relation $\mathcal{R}$ par : $x\mathcal{R}y \iff f(x) \preccurlyeq f(y)$.
Vérifier que $\mathcal{R}$ est une relation d'ordre sur E.

◇ **1.3.13** Soient $(E,\preccurlyeq)$, $(F,\preccurlyeq)$, $(G,\preccurlyeq)$ trois ensembles ordonnés, $f : E \longrightarrow F$, $g : F \longrightarrow G$ deux applications.

a) Si f et g sont monotones (resp. strictement monotones), que dire de $g \circ f$?

b) Donner un exemple où f est croissante et bijective et où f^{-1} n'est pas croissante.

c) Montrer que, si f est croissante et injective, alors f est strictement croissante.

d) Montrer que, si f est strictement croissante et si l'ordre $\preccurlyeq$ de E est total, alors f est injective.

◇ **1.3.14** Soient E un ensemble, $f : \mathfrak{P}(E) \longrightarrow \mathfrak{P}(E)$ une application. Montrer que les deux propriétés suivantes sont équivalentes :
(i) $\forall X,Y \in \mathfrak{P}(E),\ f(X \cup Y) \supset f(f(X)) \cup f(Y) \cup Y$
(ii) $\forall X,Y \in \mathfrak{P}(E),\ \begin{cases} f(X) \supset X \\ f(f(X)) = f(X) \\ X \subset Y \Longrightarrow f(X) \subset f(Y) \end{cases}$.
(Bien noter que $f(X)$ ne désigne pas l'image directe par f d'une partie X, cf. 1.3.5 Déf. ci-dessous, mais désigne l'image d'un élément X du départ de f).

◇ **1.3.15** Soient $(E,\preccurlyeq)$, $(F,\preccurlyeq)$ deux ensembles ordonnés, $f : E \longrightarrow F$, $g : F \longrightarrow E$ croissantes, $A = \{x \in E;\ (g \circ f)(x) = x\}$, $B = \{y \in F;\ (f \circ g)(y) = y\}$.

a) Montrer que $\begin{cases} \forall x \in A,\ f(x) \in B \\ \forall y \in B,\ g(y) \in A \end{cases}$. On note $f' : \begin{array}{ccc} A & \longrightarrow & B \\ x & \longmapsto & f(x) \end{array}$ et $g' : \begin{array}{ccc} B & \longrightarrow & A \\ y & \longmapsto & g(y) \end{array}$.

b) Montrer que f' et g' sont des bijections strictement croissantes et réciproques l'une de l'autre (A et B étant munis des ordres induits par ceux de E et F).

1.3.5 Images directes ou réciproques de parties par une application

◆ **Définition** Soient E,E' deux ensembles, $f : E \longrightarrow E'$ une application.

1) Pour toute partie A de E, on définit **l'image directe de A par f**, notée $f(A)$:

$$f(A) = \{x' \in E';\ \exists a \in A, x' = f(a)\}.$$

2) Pour toute partie A' de E', on définit **l'image réciproque de A' par f**, notée $f^{-1}(A')$:

$$f^{-1}(A') = \{x \in E;\ f(x) \in A'\}.$$

Remarques :

1) On a : • Pour tous A de $\mathfrak{P}(E)$ et x' de E' : $x' \in f(A) \iff (\exists a \in A,\ x' = f(a))$

• Pour tous A' de $\mathfrak{P}(E')$ et x de E : $x \in f^{-1}(A') \iff f(x) \in A'$.

Ceci montre que les images réciproques sont plus «simples» à manipuler que les images directes.

2) La notation $f^{-1}(A')$ (où A' est une partie de E') ne suppose pas que f soit bijective. Le lecteur pourra montrer que, si $f : E \longrightarrow E'$ est bijective, alors, pour toute A' de $\mathfrak{P}(E')$, l'image directe de A' par f^{-1} est aussi l'image réciproque de A' par f.

On pourra établir, à titre d'exercice, les résultats suivants :

◆ **Proposition** Soient E, E' deux ensembles, $f : E \longrightarrow E'$ une application.

1) On a, pour toutes parties A, B de E :

- $A \subset B \Longrightarrow f(A) \subset f(B)$
- $f(A \cup B) = f(A) \cup f(B)$
- $f(A \cap B) \subset f(A) \cap f(B)$.

2) On a, pour toutes parties A', B' de E' :

- $A' \subset B' \Longrightarrow f^{-1}(A') \subset f^{-1}(B')$
- $f^{-1}(A' \cup B') = f^{-1}(A') \cup f^{-1}(B')$
- $f^{-1}(A' \cap B') = f^{-1}(A') \cap f^{-1}(B')$
- $f^{-1}(\complement_{E'}(A')) = \complement_E(f^{-1}(A'))$.

3) • $\forall A \in \mathfrak{P}(E),\ A \subset f^{-1}(f(A))$

• $\forall A' \in \mathfrak{P}(E'),\ f(f^{-1}(A')) \subset A'$.

Exercices

◇ **1.3.16** Soient E, F deux ensembles, $f : E \longrightarrow F$, $g : F \longrightarrow E$ deux applications telles que $f \circ g = \mathrm{Id}_F$. Montrer : $(g \circ f)(E) = g(F)$.

◇ **1.3.17** Soient E, E' deux ensembles, $f : E \longrightarrow E'$. Montrer :

$$\forall A' \in \mathfrak{P}(E'),\ f(f^{-1}(A')) = A' \cap f(E).$$

◇ **1.3.18** Soient E, E' deux ensembles, $f : E \longrightarrow E'$. Montrer que f est bijective si et seulement si : $\forall A \in \mathfrak{P}(E),\ f(\complement_E(A)) = \complement_{E'}(f(A))$.

◇ **1.3.19** Soient E, E' deux ensembles, $f : E \longrightarrow E'$. Montrer que les propriétés suivantes sont équivalentes :

(i) f est surjective

(ii) $\forall y \in E',\ f(f^{-1}(\{y\})) = \{y\}$

(iii) $\forall A' \in \mathfrak{P}(E'),\ f(f^{-1}(A')) = A'$

(iv) $\forall A' \in \mathfrak{P}(E'),\ \big(f^{-1}(A') = \varnothing \Longrightarrow A' = \varnothing\big)$.

◇ **1.3.20** Soient E, E' deux ensembles, $f : E \longrightarrow E'$.

a) Montrer : $\forall A', B' \in \mathfrak{P}(E'),\ f^{-1}(A'_{\triangle} B') = f^{-1}(A')_{\triangle} f^{-1}(B')$.

b) Montrer que f est injective si et seulement si : $\forall A, B \in \mathfrak{P}(E),\ f(A_{\triangle} B) = f(A)_{\triangle} f(B)$.

◇ **1.3.21** Soient E un ensemble, $\mathcal{A}$ une partie de E^E, $\mathcal{F} = \{X \in \mathfrak{P}(E);\ \forall f \in \mathcal{A}, f(X) \subset X\}$. Montrer que toute partie non vide de $\mathcal{F}$ admet une borne supérieure et une borne inférieure dans $\mathcal{F}$ pour l'inclusion.

1.3.6 Familles

◆ **Définition 1** Soit E un ensemble. On appelle **famille d'éléments de** E toute application dont l'ensemble d'arrivée est E.

Une famille d'éléments d'un ensemble E est notée $(x_i)_{i \in I}$ au lieu de $\begin{array}{ccc} I & \longrightarrow & E \\ i & \longmapsto & x(i) \end{array}$; l'ensemble de départ I de la famille est appelé l'ensemble des **indices** de la famille.

Par exemple, une suite est une famille dont l'ensemble des indices est $\mathbb{N}$.

Une famille $(x_i)_{i \in I}$ est dite **finie** si et seulement si I est un ensemble fini. Si $I = \{1, \ldots, p\}$ où $p \in \mathbb{N}^*$, $(x_i)_{i \in I}$ est aussi notée $(x_i)_{1 \leqslant i \leqslant p}$ et considérée comme confondue avec le p-uplet $(x_1, \ldots, x_p)$ (cf. 1.2.1 p. 12).

On appelle **sous-famille** d'une famille $(x_i)_{i \in I}$ d'éléments de E toute famille $(x_j)_{j \in J}$ où J est une partie de I. En notant $\varphi : \begin{array}{ccc} J & \longrightarrow & I \\ j & \longmapsto & j \end{array}$ l'inclusion canonique et f la famille $(x_i)_{i \in I}$ (c'est-à-dire $f : \begin{array}{ccc} I & \longrightarrow & E) \\ i & \longmapsto & x_i \end{array}$, la sous-famille $(x_j)_{j \in J}$ est $f \circ \varphi : \begin{array}{ccc} J & \longrightarrow & E. \\ j & \longmapsto & x_j \end{array}$ Par exemple, une suite extraite d'une suite $(x_n)_{n \in \mathbb{N}}$ est une sous-famille de $(x_n)_{n \in \mathbb{N}}$ dont l'ensemble d'indices soit infini.

◆ **Définition 2** Soient E un ensemble, $(A_i)_{i \in I}$ une famille de parties de E. On définit :

- **la réunion de la famille** $(A_i)_{i \in I}$, notée $\bigcup_{i \in I} A_i$ par :

$$\bigcup_{i \in I} A_i = \{x \in E;\ \exists i \in I, x \in A_i\}$$

- **l'intersection de la famille** $(A_i)_{i \in I}$, notée $\bigcap_{i \in I} A_i$ par :

$$\bigcap_{i \in I} A_i = \{x \in E;\ \forall i \in I, x \in A_i\}.$$

Ainsi, pour tout x de E, on a :

- $x \in \bigcup_{i \in I} A_i \iff (\exists i \in I, x \in A_i)$
- $x \in \bigcap_{i \in I} A_i \iff (\forall i \in I, x \in A_i)$.

D'après la définition, on a en particulier : $\bigcup_{i \in \varnothing} A_i = \varnothing$ et $\bigcap_{i \in \varnothing} A_i = E$.

◆ **Définition 3** Soit E un ensemble. Une famille $(A_i)_{i\in I}$ de parties de E est appelée **partition** de E si et seulement si :

(i) $\forall i \in I, A_i \neq \varnothing$

(ii) $\forall (i,j) \in I^2, (i \neq j \Longrightarrow A_i \cap A_j = \varnothing)$

(iii) $\bigcup_{i\in I} A_i = E.$

Cette définition est cohérente avec celle vue en 1.1.4 Déf. 2 p. 9 car, pour que $(A_i)_{i\in I}$ soit une partition au sens ci-dessus, il faut et il suffit que $\{A_i ; i \in I\}$ soit une partition de E au sens de 1.1.4 Déf. 2 p. 9.

Par exemple, $\{[n; n+1[; n \in \mathbb{Z}\}$ et $([n; n+1[)_{n\in\mathbb{Z}}$ sont des partitions de $\mathbb{R}$.

Exercices

◇ **1.3.22** Soit E un ensemble. Etablir les formules suivantes, pour toutes familles de parties de E et toutes parties de E :

a) $\complement_E\left(\bigcup_{i\in I} A_i\right) = \bigcap_{i\in I} \complement_E(A_i), \quad \complement_E\left(\bigcap_{i\in I} A_i\right) = \bigcup_{i\in I} \complement_E(A_i)$

b) $\left(\bigcup_{i\in I} A_i\right) \cap B = \bigcup_{i\in I} (A_i \cap B), \quad \left(\bigcap_{i\in I} A_i\right) \cup B = \bigcap_{i\in I} (A_i \cup B)$

c) $\left(\bigcup_{i\in I} A_i\right) \cap \left(\bigcup_{j\in J} B_j\right) = \bigcup_{(i,j)\in I\times J} (A_i \cap B_j), \quad \left(\bigcap_{i\in I} A_i\right) \cup \left(\bigcap_{j\in J} B_j\right) = \bigcap_{(i,j)\in I\times J} (A_i \cup B_j)$

d) $(\forall i \in I, A_i \subset B_i) \Longrightarrow \begin{cases} \bigcup_{i\in I} A_i \subset \bigcup_{i\in I} B_i \\ \bigcap_{i\in I} A_i \subset \bigcap_{i\in I} B_i \end{cases}$

e) $\bigcap_{i\in I} (A_i - B_i) = \left(\bigcap_{i\in I} A_i\right) - \left(\bigcup_{i\in I} B_i\right).$

◇ **1.3.23** Soient E, E' deux ensembles, $f : E \longrightarrow E'$ une application.

a) Montrer, pour toute famille $(A'_i)_{i\in I}$ de parties de E' :

$$f^{-1}\left(\bigcup_{i\in I} A'_i\right) = \bigcup_{i\in I} f^{-1}(A'_i), \quad f^{-1}\left(\bigcap_{i\in I} A'_i\right) = \bigcap_{i\in I} f^{-1}(A'_i).$$

b) Montrer, pour toute famille $(A_i)_{i\in I}$ de parties de E :

$$f\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} f(A_i), \quad f\left(\bigcap_{i\in I} A_i\right) \subset \bigcap_{i\in I} f(A_i).$$

c) Etablir que, si f est injective, alors, pour toute famille $(A_i)_{i\in I}$ de parties de E :

$$f\left(\bigcap_{i\in I} A_i\right) = \bigcap_{i\in I} f(A_i).$$

◇ **1.3.24** Soient E un ensemble, $f,g : E \longrightarrow E$.

a) Soit $A \in \mathfrak{P}(E)$.

α) Montrer que, si A est stable par f et par g, alors A est stable par $g \circ f$.

β) En déduire que, si A est stable par f, alors la suite $(f^n(A))_{n\in\mathbb{N}}$ est décroissante, où $f^0 = \mathrm{Id}_E$, $f^1 = f$, $f^n = f \circ \ldots \circ f$ (n facteurs).

γ) Montrer que, si A est stable par f et s'il existe $n \in \mathbb{N}^*$ tel que $f^n(A) = A$, alors $f(A) = A$.

b) Soit $(A_i)_{i\in I}$ une famille de parties de E. Montrer que, si chaque A_i ($i \in I$) est stable par f, alors $\bigcup_{i\in I} A_i$ et $\bigcap_{i\in I} A_i$ sont stables par f.

◇ **1.3.25** *a)* Soient E, E' deux ensembles, $f : E \longrightarrow E'$ une application surjective. Montrer que, pour toute partition $(A'_i)_{i\in I}$ de E', la famille $(f^{-1}(A'_i))_{i\in I}$ est une partition de E.

b) Donner un exemple d'ensembles E, E', d'application surjective $f : E \longrightarrow E'$ et de partition $(A_i)_{i\in I}$ de E telle que $(f(A_i))_{i\in I}$ ne soit pas une partition de E'.

Complément

◇ C 1.1* Compatibilité entre relations d'équivalence et application

A Compatibilité

Soient E, F deux ensembles, $\mathcal{R}$ (resp. $\mathcal{S}$) une relation d'équivalence dans E (resp. F), $f : E \longrightarrow F$ une application. On dit que f est **compatible** avec $\mathcal{R}$ et $\mathcal{S}$ si et seulement si :

$$\forall (x,x') \in E^2, \quad (x \mathcal{R} x' \Longrightarrow f(x) \mathcal{S} f(x')).$$

1) Soient E, F deux ensembles, $\mathcal{R}$ (resp. $\mathcal{S}$) une relation d'équivalence dans E (resp. F), $p : E \longrightarrow E/\mathcal{R}$ (resp. $q : F \longrightarrow F/\mathcal{S}$) la surjection canonique, $f : E \longrightarrow F$ une application.

Montrer que, pour qu'il existe $\varphi : E/\mathcal{R} \longrightarrow F/\mathcal{S}$ telle que le diagramme ci-après soit commutatif (c'est-à-dire : $\varphi \circ p = q \circ f$), il faut et il suffit que f soit compatible avec $\mathcal{R}$ et $\mathcal{S}$ et que, si f est compatible avec $\mathcal{R}$ et $\mathcal{S}$, alors φ est unique.

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle q} \\ E/\mathcal{R} & \xrightarrow[\varphi]{} & F/\mathcal{S} \end{array}$$

Si f est compatible avec $\mathcal{R}$ et $\mathcal{S}$, on note $\widetilde{f}$ l'unique application de $E/\mathcal{R}$ dans $F/\mathcal{S}$ telle que $\widetilde{f} \circ p = q \circ f$; on dit que $\widetilde{f}$ est obtenue à partir de f en **passant aux quotients.**

2) a) Soient E, F, G trois ensembles, $\mathcal{R}$ (resp. $\mathcal{S}$, resp. $\mathcal{T}$) une relation d'équivalence dans E (resp. F, resp. G), $f : E \longrightarrow F$ une application compatible avec $\mathcal{R}$ et $\mathcal{S}$, $g : F \longrightarrow G$ une application compatible avec $\mathcal{S}$ et $\mathcal{T}$. Montrer que $g \circ f : E \longrightarrow G$ est compatible avec $\mathcal{R}$ et $\mathcal{T}$, et que $\widetilde{g \circ f} = \widetilde{g} \circ \widetilde{f}$.

b) Soient E un ensemble et $\mathcal{R}$ une relation d'équivalence dans E. Vérifier que Id_E est compatible avec $\mathcal{R}$ et $\mathcal{R}$, et que $\widetilde{\mathrm{Id}_E} = \mathrm{Id}_{E/\mathcal{R}}$.

B Décomposition canonique d'une application

1) Soient E, F deux ensembles, $f : E \longrightarrow F$ une application.

a) Montrer que la relation $\mathcal{R}_f$ définie dans E par :

$$x \mathcal{R}_f x' \Longleftrightarrow f(x) = f(x')$$

est une relation d'équivalence.

b) On note $i : f(E) \longrightarrow F$ l'injection canonique et $p : E \longrightarrow E/\mathcal{R}_f$ la surjection canonique.

Montrer qu'il existe une application $\widehat{f} : E/\mathcal{R}_f \longrightarrow f(E)$ unique telle que $f = i \circ \widehat{f} \circ p$, et que $\widehat{f}$ est bijective.

On dit que la relation $f = i \circ \widehat{f} \circ p$ constitue la **décomposition canonique** de f.

2) Exemples

a) Déterminer la décomposition canonique de la partie entière $\mathrm{E} : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \mathrm{E}(x) \end{array}$.

b) Soient E un ensemble, $A \in \mathfrak{P}(E)$,

$$f : \begin{array}{ccc} \mathfrak{P}(E) & \longrightarrow & \mathfrak{P}(E) \\ X & \longmapsto & X \cap A \end{array}, \quad g : \begin{array}{ccc} \mathfrak{P}(E) & \longrightarrow & \mathfrak{P}(E) \\ X & \longmapsto & X \cup A \end{array}.$$

Déterminer les décompositions canoniques de f et g.

Chapitre 2

Structures algébriques

2.1 Lois de composition interne

◆ **Définition 1** On appelle **loi de composition interne** (en abrégé : **lci**) sur un ensemble E toute application de $E \times E$ dans E.

Une lci sur E est souvent notée $* : \begin{array}{ccc} E \times E & \longrightarrow & E \\ (x,y) & \longmapsto & x*y \end{array}$, ou $\top$, $\perp$, $+$, $\cdot$, $\circ$, ...

On dit quelquefois **loi** au lieu de loi de composition interne.

EXEMPLES :

1) L'addition et la multiplication sont des lci dans $\mathbb{N}$.

2) Pour tout ensemble X, la réunion et l'intersection sont des lci dans $\mathfrak{P}(X)$.

◆ **Définition 2** On appelle **magma** tout couple $(E,*)$ où E est un ensemble et $*$ une lci dans E.

◆ **Définition 3** Une lci $*$ dans un ensemble E est dite **associative** si et seulement si : $\forall (x,y,z) \in E^3, \quad (x*y)*z = x*(y*z)$.

Au lieu de «$*$ est associative», on dit aussi : le magma $(E,*)$ est associatif.

EXEMPLES :

1) L'addition et la multiplication dans $\mathbb{C}$ sont associatives.

2) La lci $* : \begin{array}{ccc} \mathbb{Q}^2 & \longrightarrow & \mathbb{Q} \\ (x,y) & \longmapsto & \frac{x+y}{2} \end{array}$ n'est pas associative, puisque $((-1)*0)*1 = \frac{1}{4}$ et $(-1)*(0*1) = -\frac{1}{4}$.

◆ **Notation** Soient E un ensemble, $*$ ou $\cdot$ ou $+$ une lci associative dans E, $n \in \mathbb{N}^*$, $x_1, \ldots, x_n \in E$, $x \in E$. On note :

$$\mathop{*}_{i=1}^{n} x_i = x_1 * x_2 * \ldots * x_n,$$

$$\prod_{i=1}^{n} x_i = x_1 x_2 \ldots x_n, \quad \sum_{i=1}^{n} x_i = x_1 + x_2 + \ldots + x_n,$$

$$x^n = x*x*\ldots*x, \quad x^n = xx\ldots x, \quad nx = x + x + \ldots + x$$

(n termes ou facteurs) (en particulier : $x^1 = x$).

On dit que deux éléments x, y d'un magma $(E,*)$ **commutent** (ou : **sont permutables**) si et seulement si : $x * y = y * x$.

◆ **Définition 4** Une lci $*$ dans un ensemble E est dite **commutative** si et seulement si : $\forall (x,y) \in E^2, \quad x * y = y * x$.

EXEMPLES :

1) L'addition et la multiplication dans $\mathbb{C}$ sont commutatives.

2) La soustraction dans $\mathbb{C}$ n'est pas commutative.

On démontre aisément (par des raisonnements par récurrence) la Proposition suivante :

◆ **Proposition 1** Soit E un ensemble muni d'une lci associative et commutative notée $+$. Alors :

1) $\forall n \in \mathbb{N}^*, \forall (x_1,\ldots,x_n) \in E^n, \forall (y_1,\ldots,y_n) \in E^n,$

$$\sum_{i=1}^{n}(x_i + y_i) = \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i$$

2) $\forall (n,p) \in (\mathbb{N}^*)^2, \forall (x_{ij})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant p} \in E^{np}, \sum_{i=1}^{n}\left(\sum_{j=1}^{p} x_{ij}\right) = \sum_{j=1}^{p}\left(\sum_{i=1}^{n} x_{ij}\right).$

3) $\forall n \in \mathbb{N}^*, \forall \sigma \in \mathfrak{S}_n, \forall (x_1,\ldots,x_n) \in E^n, \quad \sum_{i=1}^{n} x_{\sigma(i)} = \sum_{i=1}^{n} x_i.$

(Voir 3.3.1 p. 78 pour le groupe symétrique $\mathfrak{S}_n$).

◆ **Définition 5** Soient $(E,*)$ un magma, $a \in E$.

1) On dit que a est **régulier** (ou : **simplifiable**) **à gauche** pour $*$ si et seulement si :

$$\forall (x,y) \in E^2, \quad (a * x = a * y \Longrightarrow x = y).$$

2) On dit que a est **régulier** (ou **simplifiable**) **à droite** pour $*$ si et seulement si :

$$\forall (x,y) \in E^2, \quad (x * a = y * a \Longrightarrow x = y).$$

3) On dit que a est **régulier** (ou : **simplifiable**) pour $*$ si et seulement si a est régulier à gauche et régulier à droite pour $*$, c'est-à-dire :

$$\forall (x,y) \in E^2, \quad \begin{cases} a * x = a * y \Longrightarrow x = y \\ x * a = y * a \Longrightarrow x = y \end{cases}.$$

EXEMPLES :

1) Dans $\mathbb{C}$, tout élément est régulier pour $+$.

2) Les éléments de $\mathbb{C}$ réguliers pour $\cdot$ sont les complexes $\neq 0$.

3) Pour $n \in \mathbb{N}^*$, les éléments réguliers de $\mathbf{M}_n(\mathbb{C})$ sont les matrices de $\mathbf{M}_n(\mathbb{C})$ de déterminant $\neq 0$ (cf. 9.4 Prop 2) *4)* p. 310).

◆ **Définition 6** Soient $(E,*)$ un magma, $e \in E$.

1) On dit que e est **neutre à gauche** pour $*$ si et seulement si : $\forall x \in E, e*x = x$.

2) On dit que e est **neutre à droite** pour $*$ si et seulement si : $\forall x \in E, x*e = x$.

3) On dit que e est **neutre** pour $*$ si et seulement si e est neutre à gauche et neutre à droite pour $*$, c'est-à-dire : $\forall x \in E, e*x = x*e = x$.

EXEMPLES :

1) 0 est neutre pour $+$ dans $\mathbb{C}$.

2) Pour la lci $* : \mathbb{N}^2 \longrightarrow \mathbb{N}$, $(x,y) \longmapsto y$, tout élément de $\mathbb{N}$ est neutre à gauche et aucun élément de $\mathbb{N}$ n'est neutre à droite.

◆ **Notation** Si $(E,*)$ est un magma admettant un neutre noté e, alors, pour tout x de E, on note : $x^0 = e$.

◆ **Proposition 2** **(Unicité de l'élément neutre, s'il existe)**

Si e,e' sont neutres pour $*$ dans E, alors $e = e'$.

Preuve :

Plus généralement, si e est neutre à gauche et si e' est neutre à droite, alors $e = e'$ car $e*e' = e'$ (e est neutre à gauche) et $e*e' = e$ (e' est neutre à droite).

◆ **Définition 7** On appelle **monoïde** tout magma $(E,*)$ tel que :

$$\begin{cases} * & \text{est associative} \\ E & \text{admet un neutre pour } *. \end{cases}$$

EXEMPLES :

- $(\mathbb{N},+)$ et $(\mathbb{N},\times)$ sont des monoïdes.
- Pour tout ensemble X, $(\mathfrak{P}(X),\cap)$, $(\mathfrak{P}(X),\cup)$ sont des monoïdes.
- Pour tout ensemble X, $(X^X,\circ)$ est un monoïde.

◆ **Définition 8** Soit $(E,*)$ un magma admettant un neutre e.

Un élément x de E est dit **symétrisable** pour $*$ si et seulement s'il existe au moins un élément y de E tel que $x*y = y*x = e$; un tel élément y (s'il en existe) est appelé **un symétrique** de x pour $*$.

◆ **Proposition 3** Soient $(E,*)$ un monoïde, et $x \in E$. Si x est symétrisable pour $*$, alors x admet un et un seul symétrique pour $*$.

Preuve :

Soient $y,z \in E$ tels que $\begin{cases} x*y = y*x = e \\ x*z = z*x = e \end{cases}$.

Alors : $y = y*e = y*(x*z) = (y*x)*z = e*z = z$.

◆ **Notation** Soient $(E,*)$ un monoïde, x un élément de E symétrisable pour $*$. Le symétrique de x est noté $\mathrm{sym}(x)$ ou x^{-1}, et appelé aussi **inverse** de x. Lorsque la loi est notée $+$, le symétrique de x (s'il existe) est noté $-x$ et appelé **opposé** de x.

◆ **Proposition 4** Soient $(E,*)$ un monoïde, $x,y \in E$. Si x et y sont symétrisables pour $*$, alors $x * y$ est symétrisable pour $*$ et :

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Preuve :

$(y^{-1}*x^{-1})*(x*y) = (y^{-1}*(x^{-1}*x))*y = y^{-1}*y = e$ et de même : $(x*y)*(y^{-1}*x^{-1}) = e$.

◆ **Définition 9** Soient E un ensemble, $*,\top$ deux lci dans E.

1) On dit que $\top$ est **distributive à gauche** (resp. **à droite**) **sur** (ou : **pour** ou : **par rapport à**) $*$ si et seulement si :

$$\forall (x,y,z) \in E^3, \quad x\top(y*z) = (x\top y)*(x\top z)$$
$$\big(\text{resp.} \quad (y*z)\top x = (y\top x)*(z\top x)\big).$$

2) On dit que $\top$ est **distributive sur** $*$ si et seulement si $\top$ est distributive à gauche et distributive à droite sur $*$.

EXEMPLES :

1) Dans $\mathbb{R}$, la multiplication est distributive sur l'addition.

2) Pour tout ensemble X, chacune des deux lois $\cup,\cap$ est distributive sur les deux lois $\cup,\cap$ dans $\mathfrak{P}(X)$.

◆ **Définition 10** Etant donné deux magmas $(E,*)$, $(F,\top)$, on appelle **morphisme de magmas** (ou : **morphisme**) de $(E,*)$ dans $(F,\top)$ toute application $f : E \longrightarrow F$ telle que : $\forall (x,y) \in E^2, \quad f(x*y) = f(x)\top f(y)$.

Un **endomorphisme d'un magma** $(E,*)$ est un morphisme de magmas de $(E,*)$ dans $(E,*)$.

Un **isomorphisme de magmas** est un morphisme bijectif de magmas.

Un **automorphisme d'un magma** $(E,*)$ est un endomorphisme bijectif du magma $(E,*)$.

On peut noter $f : (E,*) \longrightarrow (F,\top)$ un morphisme de magmas.

EXEMPLES :

1) L'application $\ln : \begin{array}{ccc} \mathbb{R}_+^* & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \ln x \end{array}$ est un isomorphisme du magma $(\mathbb{R}_+^*,\times)$ sur le magma $(\mathbb{R},+)$.

2) Soient E un ensemble, $*,\top$ deux lci dans E. Pour que $\top$ soit distributive à gauche (resp. droite) sur $*$, il faut et il suffit que, pour tout a de E, l'application $\gamma_a : \underset{x\longmapsto a\top x}{E \longrightarrow E}$ (resp. $\delta_a : \underset{x\longmapsto x\top a}{E \longrightarrow E}$) soit un endomorphisme du magma $(E,*)$.

◆ **Proposition 5**

1) Si $f : (E,*) \longrightarrow (F,\top)$ et $g : (F,\top) \longrightarrow (G,\perp)$ sont deux morphismes de magmas, alors $g \circ f : E \longrightarrow G$ est un morphisme de magmas de $(E,*)$ dans $(G,\perp)$.

2) Pour tout magma $(E,*)$, $\mathrm{Id}_E : \underset{x \longmapsto x}{E \longrightarrow E}$ est un automorphisme du magma $(E,*)$.

3) Si $f : (E,*) \longrightarrow (F,\top)$ est un isomorphisme de magmas, alors $f^{-1} : F \longrightarrow E$ est un isomorphisme du magma $(F,\top)$ sur le magma $(E,*)$.

Preuve :

1) $\forall (x,y) \in E^2, (g \circ f)(x * y) = g(f(x) \top f(y)) = (g \circ f)(x) \perp g \circ f(y)$.

2) Evident.

3) Puisque f est bijective, l'application réciproque $f^{-1} : F \longrightarrow E$ existe, et on a, pour tout (u,v) de F^2 : $u \top v = f(f^{-1}(u)) \top f(f^{-1}(v)) = f(f^{-1}(u) * f^{-1}(v))$,
d'où, en composant par f^{-1} : $f^{-1}(u \top v) = f^{-1}(u) * f^{-1}(v)$.

◆ **Définition 11** Soient X un ensemble, $(E,*)$ un magma. On peut munir E^X d'une lci, encore notée $*$, définie par :

$$\forall f,g \in E^X, \quad \forall x \in X, \quad (f * g)(x) = f(x) * g(x),$$

et appelée **extension** à E^X de la loi $*$ de E.

EXEMPLE :
Si $f,g : \mathbb{R} \longrightarrow \mathbb{R}$, alors $f + g : \underset{x \longmapsto f(x)+g(x)}{\mathbb{R} \longrightarrow \mathbb{R}}$.

◆ **Définition 12** Soit $(E,*)$ un magma. On peut munir $\mathfrak{P}(E)$ d'une lci, encore notée $*$, définie par :

$$\forall A,B \in \mathfrak{P}(E), A*B = \{x \in E; \exists (a,b) \in A \times B, x = a*b\} = \{a*b; (a,b) \in A \times B\},$$

appelée **extension** à $\mathfrak{P}(E)$ de la loi $*$ de E.

EXEMPLE :
Dans $\mathbb{R}$, $\{1,2\} + \{4,9\} = \{5,6,10,11\}$, $]-\infty;0[+]0;\infty[= \mathbb{R}$.
Pour $A \in \mathfrak{P}(E)$ et $a \in A$, on peut noter $a * A$ au lieu de $\{a\} * A$; par exemple, dans $(\mathbb{R},\cdot)$ usuel, pour tout x de $\mathbb{R}$, $x\mathbb{Z} = \{xn; n \in \mathbb{Z}\}$.

◆ **Définition 13** Soit $(E,*)$ un magma. Une partie A de E est dite **stable** pour $*$ si et seulement si $A * A \subset A$, c'est-à-dire : $\forall (x,y) \in A^2, \quad x * y \in A$.
Si A est une partie stable de E pour $*$, la lci dans A définie par : $\underset{(x,y) \longmapsto x*y}{A \times A \longrightarrow A}$
est appelée **lci induite** sur A par $*$ de E, et encore notée $*$.

◆ **Définition 14** On appelle **produit de deux magmas** $(E,\top)$, $(F,\bot)$ le magma $(E\times F,*)$ où $*$ est la lci dans $E\times F$ définie par :

$$\forall (x,y),(x',y')\in E\times F,\quad (x,y)*(x',y')=(x\top x',y\bot y').$$

EXEMPLE :

$\mathbb{R}^2$, muni de la lci + définie par :

$$\forall (x,y),(x',y')\in \mathbb{R}^2,\quad (x,y)+(x',y')=(x+x',y+y')$$

est le produit du magma $(\mathbb{R},+)$ par lui-même.

Exercices

◇ **2.1.1** Soit $*$ la lci définie dans $\mathbb{R}$ par :

$$x*y=xy+(x^2-1)(y^2-1).$$

a) Vérifier que $*$ est commutative, non associative, et admet un neutre.

b) Résoudre les équations suivantes (d'inconnue $x\in\mathbb{R}$) :

1) $2*x=5$ 2) $x*x=1$.

◇ **2.1.2** Soit $*$ une lci dans $\mathbb{R}$ telle que :

$$\forall (a,b,c)\in\mathbb{R}^3,\quad \begin{cases} 0*a=-a \\ a*(b*c)=c*(b*a)\end{cases}.$$

Montrer : $\forall (a,b,c)\in\mathbb{R}^3,\ a*(b*c)=(a*b)*(-c)$.

Donner un exemple de telle loi $*$.

◇ **2.1.3** Soient $(E,*)$ un magma associatif, $a\in E$, $\top$ la lci définie dans E par : $x\top y=x*a*y$. Montrer que $\top$ est associative.

◇ **2.1.4** Soient $(E,\cdot)$ un magma, $(x,y)\in E^2$; on suppose $\cdot$ associative et $xy=yx$. Montrer :

$$\forall (n,p)\in(\mathbb{N}^*)^2,\quad x^n y^p=y^p x^n.$$

◇ **2.1.5** Soit $(E,*)$ un monoïde; montrer que tout élément de E symétrisable pour $*$ est régulier pour $*$. Donner un exemple où la réciproque est fausse.

◇ **2.1.6** Soit $(E,*)$ un magma. Pour tout a de E, on note $\gamma_a : \begin{matrix} E\longrightarrow E \\ x\longmapsto a*x\end{matrix}$ et $\delta_a : \begin{matrix} E\longrightarrow E \\ x\longmapsto x*a\end{matrix}$, appelée respectivement **translation à gauche** et **translation à droite** par a.

a) Montrer que, pour tout a de E, γ_a (resp. δ_a) est injective si et seulement si a est régulier à gauche (resp. à droite).

b) Montrer que $*$ est associative si et seulement si : $\forall (a,b)\in E^2,\ \gamma_a\circ\delta_b=\delta_b\circ\gamma_a$.

◇ **2.1.7** Soit $(E,*)$ un magma associatif fini. On suppose qu'il existe un élément x de E régulier pour $*$. Montrer que $*$ admet un neutre et que x est symétrisable.

◇ **2.1.8** Soit $(E,*)$ un magma. Un élément x de E est dit **idempotent** si et seulement si : $x*x=x$.

a) Montrer que, si $*$ est associative et si x et y sont idempotents et commutent, alors $x*y$ est idempotent.

b) Montrer que, si $*$ est associative, admet un neutre et si x est idempotent et symétrisable, alors x^{-1} est idempotent.

◇ **2.1.9** Soient E un ensemble, $*$ une lci associative dans E, $\top$ une lci dans E distributive sur $*$.

a) Montrer que, si $x,x',y,y' \in E$ sont tels que $x \top x'$ et $y \top y'$ soient réguliers pour $*$, alors $x \top y'$ et $y \top x'$ commutent pour $*$ (calculer $(x*y)\top(x'*y')$ de deux façons différentes).

b) En déduire que, si $\top$ possède un neutre, deux éléments réguliers pour $*$ sont permutables pour $*$.

c) Montrer que, si $\top$ possède un neutre et si tous les éléments de E sont réguliers pour $*$, alors $*$ est commutative.

◇ **2.1.10** *a)* Etudier (associativité, commutativité, existence d'un neutre) la loi $*$ définie dans $]0;+\infty[$ par : $x*y = \sqrt{x^2+y^2}$.

b) Pour $(n,a) \in \mathbb{N}^* \times]0;+\infty[$, calculer $a * \ldots * a$ (n facteurs).

◇ **2.1.11** *a)* Etudier (associativité, commutativité, existence d'un neutre, existence de symétriques) la loi $*$ définie dans $\mathbb{R}$ par : $x*y = x+y-xy$.

b) Pour $(n,a) \in \mathbb{N}^* \times \mathbb{R}$, calculer $a * \ldots * a$ (n facteurs).

◇ **2.1.12** Soient $(E,*)$, $(F,\top)$ deux magmas, $f : E \longrightarrow F$ un morphisme de magmas.

a) Montrer que, si une partie A de E est stable pour $*$, alors $f(A)$ est stable pour $\top$.

b) Montrer que, si une partie B de F est stable pour $\top$, alors $f^{-1}(B)$ est stable pour $*$.

◇ **2.1.13** Soient X un ensemble, $(E,*)$ un magma, $*$ la lci dans E^X définie par (cf. Déf. 11 p. 43) :

$$\forall f,g \in E^X, \forall x \in X, \quad (f*g)(x) = f(x)*g(x).$$

Montrer que, si $*$ (dans E) possède l'une des propriétés suivantes, alors $*$ (dans E^X) possède la même propriété :

1) associativité *2)* commutativité *3)* existence d'un neutre

4) existence d'un neutre et, pour tout élément, existence d'un symétrique.

◇ **2.1.14** Soit $(E,*)$ un magma; on note encore $*$ l'extension de $*$ à $\mathfrak{P}(E)$ (cf. Déf. 12 p. 43).

a) Montrer :

1) $\forall A,B,A',B' \in \mathfrak{P}(E), \begin{cases} A \subset A' \\ B \subset B' \end{cases} \Longrightarrow A*B \subset A'*B'$

2) si $*$ est associative (resp. commutative) dans E, alors $*$ est associative (resp. commutative) dans $\mathfrak{P}(E)$

3) si $*$ admet un neutre e dans E, alors $\{e\}$ est neutre pour $*$ dans $\mathfrak{P}(E)$.

b) Si $*$ admet un neutre et si tout élément de E est symétrisable pour $*$, peut-on affirmer que tout élément de $\mathfrak{P}(E)$ soit symétrisable pour $*$?

◇ **2.1.15** Soient $(E,*)$ un magma associatif, $(a,b) \in E^2$. Montrer que $\{a\}*E$, $E*\{b\}$, $\{a\}*E*\{b\}$, $E*\{a\}*E$ sont stables pour $*$.

◇ **2.1.16** Soit $(E,*)$ un magma. Pour $A,B,C \in \mathfrak{P}(E)$, comparer :

a) $A*(B \cup C)$ et $(A*B) \cup (A*C)$

b) $A*(B \cap C)$ et $(A*B) \cap (A*C)$.

◇ **2.1.17** Soient $(E,*)$ un magma associatif et commutatif, et A l'ensemble des éléments de E non réguliers pour $*$. Montrer $E * A \subset A$; en particulier, A est stable pour $*$.

◇ **2.1.18** Soit $(E,*)$ un magma associatif. Montrer :

a) Pour toute partie stable A, $A * A$ est stable

b) Pour toute partie A de E, le **commutant** de A (défini par : $A^c = \{x \in E ; \forall a \in A, a * x = x * a\}$) est stable.

◇ **2.1.19** Soient $(E,*)$ un magma, $A = \{x \in E ; \quad \forall (y,z) \in E^2, \quad (x * y) * z = x * (y * z)\}$.

a) Montrer que A est stable pour $*$.

b) Montrer que la loi induite par $*$ dans A est associative.

◇ **2.1.20** Soient $(E,*)$ un magma, $C = \{x \in E ; \forall y \in E, \quad x * y = y * x\}$ appelé **centre** de $(E,*)$. On suppose $*$ associative.

a) Montrer que C est stable pour $*$.

b) Montrer que la loi induite par $*$ dans C est commutative.

◇ **2.1.21** Soient $(E,\top)$, $(F,\perp)$ deux magmas, $*$ la loi-produit, définie par (cf. Déf. 14 p. 44) : $(x,y) * (x',y') = (x \top x', y \perp y')$.

Montrer que, si $\top$ et $\perp$ possèdent l'une des propriétés suivantes, alors $*$ possède la même propriété :

1) associativité *2)* commutativité *3)* existence d'un neutre

4) existence d'un neutre et, pour tout élément, existence d'un symétrique.

◇ **2.1.22** Soient X un ensemble, $E = X^X$ muni de la loi $\circ$, $f \in E$. Montrer :

a) f est injective si et seulement si f est régulière à gauche pour $\circ$ dans E

b) f est surjective si et seulement si f est régulière à droite pour $\circ$ dans E.

◇ **2.1.23** Soient $(E,*)$ un magma et $\leqslant$ une relation d'ordre dans E. On suppose que, pour tout (a,b,x) de E^3 :

(i) $a * b \leqslant a$ (ii) $a * b \leqslant b$ (iii) $\left.\begin{matrix} x \leqslant a \\ x \leqslant b \end{matrix}\right\} \Longrightarrow x \leqslant a * b.$

Montrer :

a) $*$ est commutative

b) tout élément de E est idempotent pour $*$ (cf. exercice 2.1.8 p. 44)

c) $\forall (a,b,c) \in E^3, (a \leqslant b \Longrightarrow a * c \leqslant b * c)$

d) $\forall (a,b,c,d) \in E^4, \left(\left\{\begin{matrix} a \leqslant b \\ c \leqslant d \end{matrix}\right. \Longrightarrow a * c \leqslant b * d\right)$

e) $*$ est associative.

2.2 Groupes

2.2.1 Généralités

◆ **Définition 1** On dit qu'un ensemble G muni d'une lci $*$ est un **groupe** si et seulement si :

$$\begin{cases} * \text{ est associative} \\ G \text{ admet un neutre pour } * \\ \text{Tout élément de } G \text{ admet un symétrique pour } *. \end{cases}$$

Si de plus $*$ est commutative, on dit que G est un **groupe abélien** (ou : **groupe commutatif**).

EXEMPLES :

1) $(\mathbb{C},+)$ est un groupe abélien.

2) L'ensemble des isométries vectorielles d'un plan vectoriel euclidien est un groupe pour $\circ$.

Les notations les plus utilisées sont les suivantes :

loi	composé de deux éléments	neutre	symétrique d'un élément	composé $x * \text{sym}(y)$
$*$	$x * y$	$e,1$	$\text{sym}(x)$, x^{-1}	$x * \text{sym}(y)$, $x * y^{-1}$
$\circ$	$x \circ y$	$I,1$	x^{-1}	xy^{-1}
$\cdot$	xy	1	x^{-1}	xy^{-1}
$+$	$x+y$	0	$-x$	$x-y$

◆ **Proposition**

Dans un groupe, tout élément est régulier.

Preuve :

Pour tout (x,y,z) de G^3 :

$(x*y = x*z \Longrightarrow x^{-1}*(x*y) = x^{-1}*(x*z) \Longrightarrow (x^{-1}*x)*y = (x^{-1}*x)*z \Longrightarrow y = z)$, et de même de l'autre côté.

◆ **Définition 2** Si $(G,*)$ est un groupe fini, on appelle **ordre** de G le cardinal de G.

Par exemple, pour tout n de $\mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z},+)$ (cf. 4.1.2 Prop. 3 p. 102) est un groupe fini d'ordre n.

Exercices

◇ **2.2.1** Soit $(G,\cdot)$ un groupe tel que : $\forall x \in G, x^2 = e$. Montrer que G est commutatif.

◇ **2.2.2** Soient $(G,\cdot)$ un groupe fini, A, B deux parties de G telles que :

$$\mathrm{Card}(A) + \mathrm{Card}(B) > \mathrm{Card}(G).$$

Montrer $G = AB$ (c'est-à-dire : $\forall x \in G, \exists (a,b) \in A \times B, x = ab$).

◇ **2.2.3** Soient $(G,\cdot)$ un groupe fini d'ordre pair, S l'ensemble des éléments de G d'ordre 2, c'est-à-dire : $S = \{x \in G;\ x^2 = e \text{ et } x \neq e\}$.

a) Montrer que la relation $\mathcal{R}$ définie dans G par : $x\mathcal{R}y \iff (y = x \text{ ou } y = x^{-1})$ est une relation d'équivalence.

b) En déduire que $\mathrm{Card}(S)$ est impair.

◇ **2.2.4** Montrer que $\mathcal{A} = \{f_{a,b} : \begin{matrix}\mathbb{R} \longrightarrow \mathbb{R} \\ x \longmapsto ax+b\end{matrix} ; (a,b) \in \mathbb{R}^* \times \mathbb{R}\}$ est un groupe pour $\circ$. Est-il commutatif?

2.2.2 Sous-groupes

◆ **Définition 1** Soient $(G,*)$ un groupe, $H \in \mathfrak{P}(G)$. On dit que H est un **sous-groupe** de G si et seulement si :

(i) $\forall (x,y) \in H^2, x * y \in H$

(ii) $e \in H$

(iii) $\forall x \in H, x^{-1} \in H$

(où e est le neutre de G et x^{-1} le symétrique de x dans G).

EXEMPLES :

1) Pour tout n de $\mathbb{N}$, $n\mathbb{Z} = (\{na;\ a \in \mathbb{Z}\})$ est un sous-groupe additif de $\mathbb{Z}$.

2) L'ensemble des isométries vectorielles directes d'un plan vectoriel euclidien P est un sous-groupe du groupe des isométries vectorielles de P, pour $\circ$.

◆ **Proposition 1** Soient $(G,*)$ un groupe, $H \in \mathfrak{P}(G)$. Pour que H soit un sous-groupe de G, il faut et il suffit que l'on ait :

$$\begin{cases} H & \text{est stable pour } * \\ H & \text{est un groupe pour la loi induite par la loi } * \text{ de } G. \end{cases}$$

Preuve :

1) Supposons que H soit un sous-groupe de G. D'après (i), $*$ est interne dans H.

La loi $*$ dans H est associative (car elle l'est dans G), admet e pour neutre (cf. (ii)), et tout élément de H admet un symétrique pour $*$ dans H, d'après (iii). Ainsi, $(H,*)$ est un groupe.

2) Réciproquement, supposons que H soit stable pour $*$ et que $(H,*)$ soit un groupe.

• Il est clair que (i) est satisfaite.

• Notons e' le neutre de H. On a $e' * e' = e' = e' * e$ donc (régularité de e' dans G) $e' = e$. Ainsi, $e \in H$.

• Soit $x \in H$. Puisque $(H,*)$ est un groupe, x admet un symétrique y pour $*$ dans H : $x * y = y * x = e$.

Alors y est symétrique de x pour $*$ dans G, donc (cf. 2.1 Prop. 3 p. 41) $x^{-1} = y \in H$.

◆ **Proposition 2** Soient G un groupe, $(H_i)_{i \in I}$ une famille de sous-groupes de G. Alors $\bigcap_{i \in I} H_i$ est un sous-groupe de G.

Preuve :

Notons $H = \bigcap_{i \in I} H_i$.

1) Pour tout (x,y) de G^2 :
$(x,y) \in H^2 \Longrightarrow (\forall i \in I, (x \in H_i \text{ et } y \in H_i)) \Longrightarrow (\forall i \in I, x * y \in H_i) \Longrightarrow x * y \in H$.

2) $(\forall i \in I, e \in H_i)$, donc $e \in H$.

3) Pour tout x de G : $x \in H \Longrightarrow (\forall i \in I, x \in H_i) \Longrightarrow (\forall i \in I, x^{-1} \in H_i) \Longrightarrow x^{-1} \in H$.

La Proposition précédente permet la Définition suivante :

◆ **Définition 2** Soient $(G,*)$ un groupe, $A \in \mathfrak{P}(G)$. L'intersection de tous les sous-groupes de G contenant A est un sous-groupe de G, appelé **sous-groupe engendré** par A, et noté $< A >$.

On a ainsi : $< A > = \bigcap_{\substack{H \text{ sg de } G \\ A \subset H}} H$.

Pour tout a de G, on peut noter $< a >$ au lieu de $< \{a\} >$.

◆ **Proposition 3** Soient $(G,*)$ un groupe, $A \in \mathfrak{P}(G)$; $< A >$ est (au sens de l'inclusion) le plus petit sous-groupe de G contenant A.

Preuve :

1) D'après la Prop. 2, $< A >$ est un sous-groupe de G contenant A.

2) Soit H un sous-groupe de G contenant A. Par définition de $< A >$, on a : $< A > \subset H$. Ainsi $< A >$ est inclus dans tout sous-groupe de G contenant A.

◆ **Proposition 4** Soient $(G,*)$ un groupe, $A \in \mathfrak{P}(G)$.

1) $< \varnothing > = \{e\}$, où e est le neutre de G.

2) Pour toute partie non vide A de G, $< A >$ est l'ensemble des composés multiples d'éléments de A et de symétriques d'éléments de A.

Preuve :

1) Evident.

2) Notons $A^{-1} = \{y \in G;\ y^{-1} \in A\} = \{x^{-1};\ x \in A\}$, $B = A \cup A^{-1}$, H l'ensemble des composés multiples d'éléments de B, c'est-à-dire :

$$H = \{x \in G;\ \exists n \in \mathbb{N}^*, \exists (b_1,\ldots,b_n) \in B^n,\ x = \overset{n}{\underset{i=1}{*}} b_i\}.$$

Nous allons montrer que H est le plus petit sous-groupe de G contenant A.

a) Montrons que H est un sous-groupe de G.

- Soit $(x,y) \in H^2$. Il existe $n,p \in \mathbb{N}^*$, $b_1,\ldots,b_n,c_1,\ldots,c_p \in B$ tels que $x = \overset{n}{\underset{i=1}{*}} b_i$ et $y = \overset{p}{\underset{j=1}{*}} c_j$. En notant $d_k = \begin{cases} b_k & \text{si } 1 \leqslant k \leqslant n \\ c_{k-n} & \text{si } n+1 \leqslant k \leqslant n+p \end{cases}$, on a :

$$x * y = b_1 * \ldots * b_n * c_1 * \ldots * c_p = d_1 * \ldots * d_n * d_{n+1} * \ldots * d_{n+p} = \overset{n+p}{\underset{k=1}{*}} d_k \in H.$$

- Puisque $A \neq \varnothing$, il existe $a \in A$, et donc $e = a * a^{-1} \in H$.
- Soit $x \in H$. Il existe $n \in \mathbb{N}^*, b_1,\ldots,b_n \in B$ tels que $x = \overset{n}{\underset{i=1}{*}} b_i$. Alors, $b_1^{-1},\ldots,b_n^{-1} \in B$ et $x^{-1} = \overset{n}{\underset{i=1}{*}} b_{n+1-i}^{-1} = b_n^{-1} * \ldots * b_1^{-1} \in H$.

b) $A \subset H$ car $A \subset B \subset H$.

c) Soit L un sous-groupe de G tel que $A \subset L$.

On a alors : $\forall x \in A$, ($x \in L$ et $x^{-1} \in L$), d'où $B \subset L$, puis $H \subset L$.

Puisque H est le plus petit sous-groupe de G contenant A, on conclut (cf. Prop. p. 000) : $H =< A >$.

◆ **Définition 3**

1) Un groupe G est dit **monogène** si et seulement s'il existe $a \in G$ tel que $G =< a >$.

2) Si G est un groupe monogène, on appelle **générateur** de G tout élément a de G tel que $G =< a >$.

3) Un groupe G est dit **cyclique** si et seulement s'il est monogène et fini.

EXEMPLES :

1) $(\mathbb{Z},+)$ est un groupe monogène, dont un générateur est 1 (ou -1).

2) $(\mathbb{Z}/3\mathbb{Z},+)$ est un groupe monogène, dont un générateur est, par exemple, $\hat{2}$.

3) $(\mathbb{R},+)$ n'est pas un groupe monogène.

Nous étudierons plus loin (ex. 4.1.32 p. 106) la classification des groupes monogènes.

Exercices

◇ **2.2.5** Soient G un groupe, H, K deux sous-groupes de G. Montrer :

$$H \cup K = G \Longleftrightarrow (H = G \quad \text{ou} \quad K = G).$$

◇ **2.2.6** Soient $G = \mathbb{R}^* \times \mathbb{R}$ et $*$ la lci dans G définie par : $(x,y) * (x',y') = (xx', xy' + y)$.

a) Montrer que $(G,*)$ est un groupe non commutatif.

b) Montrer que $\mathbb{R}_+^* \times \mathbb{R}$ est un sous-groupe de G.

◇ **2.2.7** Soit $(G,\bullet)$ un groupe. On appelle **centre** de G la partie C de G définie par :

$$C = \{x \in G; \forall y \in G, \quad xy = yx\}.$$

Montrer que C est un sous-groupe de G.

◇ **2.2.8** Soient $G = \mathbb{R}^* \times \mathbb{R}$ et $*$ la lci dans G définie par : $(x,y) * (x',y') = \left(xx', xy' + \dfrac{y}{x'}\right)$.

a) Montrer que $(G,*)$ est un groupe.

b) Quel est le centre (cf. exercice 2.2.7) de G ?

c) Montrer que $\mathbb{R}^* \times \{0\}$, $\{1\} \times \mathbb{R}$, $\mathbb{Q}^* \times \mathbb{Q}$ sont des sous-groupes de G.

d) Montrer que, pour tout k de $\mathbb{R}$, l'ensemble $H_k = \left\{\left(x, k\left(x - \dfrac{1}{x}\right)\right) ; x \in \mathbb{R}^*\right\}$ est un sous-groupe commutatif de G.

◇ **2.2.9** Soit G un groupe fini.

Montrer que, pour tout sous-groupe H de G, si $\text{Card}(H) > \dfrac{1}{2}\text{Card}(G)$, alors $H = G$.

◇ **2.2.10** Soient $(G,\top)$, $(G',\perp)$ deux groupes, $*$ la loi-produit (cf. 2.1 Déf. 14 p. 44) définie dans $G \times G'$ par : $(x,y) * (x',y') = (x \top x', y \perp y')$.

a) Montrer que $(G \times G', *)$ est un groupe.

b) Montrer que, si H (resp. H') est un sous-groupe de G (resp. G'), alors $H \times H'$ est un sous-groupe de $G \times G'$.

◇ **2.2.11*** Soit G un sous-groupe de $(\mathbb{C},+)$ tel que : $\forall x \in [0;1], \quad x + ix^2 \in G$.

Etablir $G = \mathbb{C}$.

2.2.3 Morphismes de groupes

◆ **Définition 1** Soient $(G,*)$, $(G',\top)$ deux groupes, $f : G \longrightarrow G'$ une application. Si f est un morphisme (resp. endomorphisme, resp. isomorphisme, resp. automorphisme) de magmas, f prend le nom de **morphisme** (resp. **endomorphisme**, resp. **isomorphisme**, resp. **automorphisme**) **de groupes**.

◆ **Proposition 1** Soit $f : (G,*) \longrightarrow (G',\top)$ un morphisme de groupes. Alors :

1) $f(e) = e'$

2) $\forall x \in G,\ f(x^{-1}) = (f(x))^{-1}$

où e (resp. e') est le neutre de G (resp. G').

Preuve :

1) $f(e)\top f(e) = f(e*e) = f(e) = f(e)\top e'$, d'où, par régularité de $f(e)$ dans G' : $f(e) = e'$.

2) $\begin{cases} f(x)\top f(x^{-1}) = f(x*x^{-1}) = f(e) = e' \\ f(x^{-1})\top f(x) = f(x^{-1}*x) = f(e) = e' \end{cases}$, d'où $f(x^{-1}) = (f(x))^{-1}$.

◆ **Définition 2** Soient $(G,*)$, $(G',\top)$ deux groupes, $f : (G,*) \longrightarrow (G',\top)$ un morphisme de groupes. On appelle :

- **noyau** de f, et on note $\mathrm{Ker}(f)$:
$$\mathrm{Ker}(f) = \{x \in G;\ f(x) = e'\} = f^{-1}(\{e'\}),$$
où e' est le neutre de G'

- **image** de f, et on note $\mathrm{Im}(f)$:
$$\mathrm{Im}(f) = \{y \in G';\ \exists x \in G,\ y = f(x)\} = f(G).$$

◆ **Proposition 2** Si $f : (G,*) \longrightarrow (G',\top)$ est un morphisme de groupes, alors $\mathrm{Ker}(f)$ (resp. $\mathrm{Im}(f)$ est un sous-groupe de G (resp. G').

Preuve :

1) • Soit $(x,y) \in (\mathrm{Ker}(f))^2$. On a : $f(x*y) = f(x)\top f(y) = e'\top e' = e'$, donc $x*y \in \mathrm{Ker}(f)$.

- $f(e) = e'$, donc $e \in \mathrm{Ker}(f)$.
- Si $x \in \mathrm{Ker}(f)$, alors $f(x^{-1}) = (f(x))^{-1} = e'^{-1} = e'$, et donc $x^{-1} \in \mathrm{Ker}(f)$.

2) • Soit $(x',y') \in (\mathrm{Im}(f))^2$. Il existe $(x,y) \in G^2$ tel que $x' = f(x)$, $y' = f(y)$, d'où :
$$x'\top y' = f(x)\top f(y) = f(x*y) \in \mathrm{Im}(f).$$

- $e' = f(e) \in \mathrm{Im}(f)$.
- Si $x' \in \mathrm{Im}(f)$, alors il existe $x \in G$ tel que $x' = f(x)$, et on a : $x'^{-1} = (f(x))^{-1} = f(x^{-1}) \in \mathrm{Im}(f)$.

Plus généralement, voir exercice 2.2.12 p. 54.

◆ **Définition 3** Un groupe $(G,*)$ est dit **isomorphe à** un groupe $(G',\top)$ si et seulement s'il existe un isomorphisme de groupes de $(G,*)$ sur (G',T).

EXEMPLE :

$(\mathbb{R}_+^*,\times)$ est isomorphe à $(\mathbb{R},+)$ car $\ln : \mathbb{R}_+^* \longrightarrow \mathbb{R}$ est un isomorphisme de groupes.
$x \longmapsto \ln x$

Remarque :

La relation «être isomorphe à» entre groupes est une relation d'équivalence sur tout ensemble de groupes (mais il n'existe pas d'ensemble de tous les groupes).

◆ **Proposition 3 (Transfert de la structure de groupe)**

Soient $(G,*)$ un groupe, $(E,\top)$ un magma. S'il existe un isomorphisme de magmas de $(G,*)$ sur $(E,\top)$, alors $(E,\top)$ est un groupe isomorphe au groupe $(G,*)$.

On dit aussi **transport**, au lieu de transfert.

Preuve :

Supposons qu'il existe un isomorphisme de magmas $f : (G,*) \longrightarrow (E,\top)$. Notons e le neutre de G.

Soient $x,y,z \in E$, $X = f^{-1}(x)$, $Y = f^{-1}(y)$, $Z = f^{-1}(z)$.

$$1)\ (x\top y)\top z = (f(X)\top f(Y))\top f(Z) = f(X*Y)\top f(Z) = f((X*Y)*Z)$$
$$= f(X*(Y*Z)) = f(X)\top f(Y*Z) = f(X)\top(f(Y)\top f(Z)) = x\top(y\top z),$$

et donc $\top$ est associative dans E.

$$2)\ \begin{cases} x\top f(e) = f(X)\top f(e) = f(X*e) = f(X) = x \\ f(e)\top x = f(e)\top f(X) = f(e*X) = f(X) = x \end{cases},$$

et donc $f(e)$ est neutre pour $\top$ dans E.

$$3)\ \begin{cases} x\top f(X^{-1}) = f(X)\top f(X^{-1}) = f(X*X^{-1}) = f(e) \\ f(X^{-1})\top x = f(X^{-1})\top f(X) = f(X^{-1}*X) = f(e) \end{cases},$$

et donc x admet un symétrique pour $\top$ dans E.

EXEMPLE :

Considérons la loi $*$ définie dans $\mathbb{R}$ par :

$$\forall (x,y) \in \mathbb{R}^2, \quad x*y = x\sqrt{1+y^2} + y\sqrt{1+x^2}.$$

Il est clair que l'application sh : $\mathbb{R} \longrightarrow \mathbb{R}$ (sinus hyperbolique) est bijective et vérifie :

$$\forall (u,v) \in \mathbb{R}^2, \quad \operatorname{sh}(u+v) = \operatorname{sh} u * \operatorname{sh} v.$$

Donc $(\mathbb{R},*)$ est un groupe, isomorphe à $(\mathbb{R},+)$, l'application sh étant un isomorphisme de groupes de $(\mathbb{R},+)$ sur $(\mathbb{R},*)$.

Exercices

◇ **2.2.12** Soient $(G,\top)$, $(G',\perp)$ deux groupes, $f : G \longrightarrow G'$ un morphisme de groupes.

a) Montrer que, pour tout sous-groupe H de G, $f(H)$ est un sous-groupe de G'.

b) Montrer que, pour tout sous-groupe H' de G', $f^{-1}(H')$ est un sous-groupe de G.

◇ **2.2.13** Montrer que l'ensemble des automorphismes d'un magma $(E,*)$ est un groupe pour $\circ$.

◇ **2.2.14** Soient G,G' deux groupes, e le neutre de G, $f : G \longrightarrow G'$ un morphisme de groupes. Montrer que f est injectif si et seulement si $\mathrm{Ker}(f) = \{e\}$.

◇ **2.2.15** Soient G un groupe fini, f un automorphisme de G tel que :

$$\mathrm{Card}\{x \in G;\ f(x) = x^{-1}\} > \frac{1}{2}\,\mathrm{Card}(G).$$

Montrer : $f^2 = \mathrm{Id}_G$.

◇ **2.2.16*** Soient $(G,\bullet)$ un groupe, H,K deux sous-groupes finis de G. Montrer que la partie HK de G est finie et que : $\mathrm{Card}(HK) = \dfrac{\mathrm{Card}(H)\cdot\mathrm{Card}(K)}{\mathrm{Card}(H\cap K)}$.

◇ **2.2.17*** Soit $(G,\bullet)$ un groupe tel que $f : \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x^3 \end{array}$ soit un endomorphisme surjectif du groupe G. Démontrer que G est abélien.

◇ **2.2.18** Soit $(G,\bullet)$ un groupe tel qu'il existe $n \in \mathbb{N}^*$ tel que $f_n : \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x^n \end{array}$ soit un endomorphisme surjectif du groupe G. Démontrer :

$$\forall (x,y) \in G^2,\quad x^{n-1}y = yx^{n-1}.$$

◇ **2.2.19** Soient G un groupe monogène (resp. cyclique), $f : G \longrightarrow G'$ un morphisme surjectif de groupes. Montrer que G' est monogène (resp. cyclique).

◇ **2.2.20** Montrer que les groupes $(\mathbb{Q},+)$ et $(\mathbb{Q}_+^*,\times)$ ne sont pas isomorphes.

◇ **2.2.21** Montrer que les groupes $(\mathbb{R}^*,\times)$ et $(\mathbb{C}^*,\times)$ ne sont pas isomorphes.

2.3 Anneaux

2.3.1 Définitions

◆ **Définition** Soit A un ensemble muni de deux lci notées $+,\cdot$.

1) On dit que $(A,+,\cdot)$ (ou : A) est un **pseudo-anneau** si et seulement si :

$$\begin{cases} (A,+) \text{ est un groupe abélien} \\ \cdot \text{ est associative} \\ \cdot \text{ est distributive sur } +. \end{cases}$$

2) On dit que A est un **anneau** si et seulement si :

$$\begin{cases} (A,+,\cdot) \text{ est un pseudo-anneau} \\ A \text{ admet un neutre pour } \cdot \end{cases}$$

3) On dit que A est un **anneau commutatif** si et seulement si :

$$\begin{cases} A \text{ est un anneau} \\ \cdot \text{ est commutative.} \end{cases}$$

EXEMPLES :

1) $(\mathbb{Z},+,.)$ est un anneau commutatif

2) $(K[X],+,.)$ est un anneau commutatif

3) Pour tout n de $\mathbb{N} - \{0,1\}$, $\mathbf{M}_n(K)$ est un anneau non commutatif (cf. 8.1.4 p. 269).

4) Pour tout ensemble X, $(\mathfrak{P}(X),\Delta,\cap)$ est un anneau commutatif (cf. plus loin, ex. 2.3.6 p. 59).

2.3.2 Calculs dans un anneau

Soit $(A,+,\cdot)$ un anneau. On note :

0 le neutre de $+$

$-x$ le symétrique d'un élément x de A pour $+$

1 (ou 1_A) le neutre de $\cdot$.

On montre facilement les formules suivantes :

1) $\forall x \in A, 0 \cdot x = x \cdot 0 = 0$ (on dit que 0 est **absorbant** pour $\cdot$)

2) $\forall x \in A, (-1_A) \cdot x = x \cdot (-1_A) = -x$

3) $\forall (x,y) \in A^2, \begin{cases} (-x)y = x(-y) = -xy \\ (-x)(-y) = xy \end{cases}$

4) $\forall (x,y,z) \in A^3, \begin{cases} (x-y)z = xz - yz \\ z(x-y) = zx - zy \end{cases}$

5) $\forall n \in \mathbb{N}^*, \forall a \in A, \quad (1-a)\sum_{k=0}^{n-1} a^k = \left(\sum_{k=0}^{n-1} a^k\right)(1-a) = 1-a^n$

6) $\forall p \in \mathbb{N}, \forall a \in A, \quad (1+a)\sum_{k=0}^{2p}(-1)^k a^k = \left(\sum_{k=0}^{2p}(-1)^k a^k\right)(1+a) = 1+a^{2p+1}$

7) $\forall a \in A, \forall n \in \mathbb{N}^*, \forall (x_1,\ldots,x_n) \in A^n, \left(\sum_{i=1}^{n} a x_i = a\sum_{i=1}^{n} x_i, \sum_{i=1}^{n} x_i a = \left(\sum_{i=1}^{n} x_i\right)a\right.$

8) $\forall n,p \in \mathbb{N}^*, \forall (x_1,\ldots,x_n), (y_1,\ldots,y_n) \in A^n,$

$$\sum_{i=1}^{n}\left(\sum_{j=1}^{p} x_i y_j\right) = \sum_{j=1}^{p}\left(\sum_{i=1}^{n} x_i y_j\right) = \left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{p} y_j\right).$$

◆ **Notation** Soit $(A,+,\cdot)$ un anneau. Pour tout (n,x) de $\mathbb{Z} \times A$, on note :

$$\begin{cases} nx = x + \ldots + x & (n \text{ termes}) \quad \text{si } n \in \mathbb{N}^* \\ nx = 0 & \text{si } n = 0 \\ nx = -(-n)x & \text{si } n \in \mathbb{Z}_-^*. \end{cases}$$

Le lecteur prouvera facilement les formules suivantes :

1) $\forall (n,p) \in \mathbb{Z}^2, \forall x \in A, \quad (n+p)x = nx + px$

2) $\forall n \in \mathbb{Z}, \forall x \in A, \quad n(-x) = (-n)x = -(nx), \quad$ noté $-nx$

3) $\forall n \in \mathbb{Z}, \forall (x,y) \in A^2, \quad \begin{cases} n(x+y) = nx + ny \\ n(x-y) = nx - ny \end{cases}$

4) $\forall (n,p) \in \mathbb{Z}^2, \forall x \in A, \quad (np)x = n(px)$

5) $\forall n \in \mathbb{Z}, \forall (x,y) \in A^2, \quad n(xy) = (nx)y = x(ny)$

6) $\forall n \in \mathbb{Z}, \forall x \in A, \quad nx = (n1_A)x = x(n1_A).$

On note quelquefois n au lieu de $n1_A$, pour $n \in \mathbb{Z}$, s'il n'en résulte pas de confusion.

◆ **Théorème (Formule du binôme de Newton)**

Soient $(A,+,\cdot)$ un anneau, $n \in \mathbb{N}$, $(x,y) \in A^2$ tel que $xy = yx$. On a :

$$(x+y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k}$$

(où, par convention, $x^0 = y^0 = 1_A$).

Le lecteur, depuis la Classe de Terminale, connaît les coefficients C_n^p, dont l'étude figure plus loin, 3.3.3 p. 79.

Preuve :

1re méthode

Récurrence sur n.

La formule est évidente pour $n = 0$.

Remarquer que les puissances de x et de y commutent entre elles (cf. ex. 2.1.4 p. 44).

Supposons la formule vraie pour n, x, y fixés. On a :

$$\begin{aligned}(x+y)^{n+1} &= (x+y)^n(x+y) = \left(\sum_{k=0}^{n} C_n^k x^k y^{n-k}\right)(x+y)\\ &= \left(\sum_{k=0}^{n} C_n^k x^k y^{n-k}\right)x + \left(\sum_{k=0}^{n} C_n^k x^k y^{n-k}\right)y\\ &= \sum_{k=0}^{n} C_n^k x^{k+1} y^{n-k} + \sum_{k=0}^{n} C_n^k x^k y^{n-k+1}\\ &= \sum_{\substack{l=0\\(l=k+1)}}^{n+1} C_n^{l-1} x^l y^{n+1-l} + \sum_{k=0}^{n+1} C_n^k x^k y^{n+1-k}\\ &= \sum_{k=0}^{n+1}(C_n^{k-1} + C_n^k)x^k y^{n+1-k} = \sum_{k=0}^{n+1} C_{n+1}^k x^k y^{n+1-k}.\end{aligned}$$

2ème méthode

Il est clair «par développement» que $(x+y)^n$ est une somme de termes du type $x^k y^{n-k}$, $0 \leqslant k \leqslant n$; dans cette somme, le nombre de termes $x^k y^{n-k}$, pour $k \in \{0,\ldots,n\}$ fixé, est égal au nombre de k facteurs pris parmi n, donc vaut C_n^k.

Exercices

◇ **2.3.1** Soit A un anneau tel que : $\forall x \in A, x^2 = x$.

a) Montrer : $\forall x \in A, 2x = 0$.

b) En déduire que A est commutatif.

c) Montrer, pour tout (x,y,z) de A^3 : $(x+y)z = 0 \iff \begin{cases} x(y+1)z = 0 \\ (x+1)yz = 0 \end{cases}$.

◇ **2.3.2** Soient $(A,+,\cdot)$ un pseudo-anneau, C **le centre** de A, $C = \{x \in A; \forall a \in A, ax = xa\}$.

On suppose : $\forall x \in A, x^2 - x \in C$.

a) Montrer : $\forall (x,y) \in A^2, xy + yx \in C$.

b) En déduire : $\forall (x,y) \in A^2, xy = yx$.

◇ **2.3.3** Soit A un anneau. Un élément x de A est dit **nilpotent** si et seulement s'il existe $n \in \mathbb{N}^*$ tel que $x^n = 0$.

a) Montrer que, si x, y sont nilpotents et commutent alors $x + y$ est nilpotent.

b) Montrer que, si x est nilpotent et $xy = yx$, alors xy est nilpotent.

c) Soit $x \in A$ nilpotent. Montrer que $1 - x$ est inversible et calculer $(1-x)^{-1}$.

◇ **2.3.4** **Caractéristique d'un anneau**

Soient A un anneau, $E = \{n \in \mathbb{N}^* ; n1_A = 0_A\}$.

Si $E = \varnothing$, on dit que A est de **caractéristique** 0.

Si $E \neq \varnothing$, on appelle **caractéristique** de A le plus petit élément de E.

Autrement dit, la caractéristique de A est le plus petit entier n de $\mathbb{N}^*$ tel que $n1_A = 0_A$, s'il existe, et vaut 0 sinon.

Quelle est la caractéristique de $\mathbb{Z}$? de $\mathbb{Z}/n\mathbb{Z}$ $(n \in \mathbb{N}^*)$?

◇ **2.3.5*** Soient A un anneau, $a \in A$. On suppose que a admet au moins un inverse à gauche et n'admet aucun inverse à droite. Démontrer que a admet une infinité d'inverses à gauche.

2.3.3 Sous-anneaux

◆ **Définition** Soient $(A,+,\cdot)$ un anneau, $B \in \mathfrak{P}(A)$. On dit que B est un **sous-anneau** de A si et seulement si :

$$\begin{cases} B \text{ est un sous-groupe de } (A,+) \\ \forall (x,y) \in B^2, \quad xy \in B \\ 1_A \in B. \end{cases}$$

Remarque :

Si B est un sous-anneau de A, alors B un anneau (pour les lois induites par celles de A) et a le même élément neutre que A pour $\cdot$.

EXEMPLES :

1) $\mathbb{Z}$ est un sous-anneau de l'anneau $(\mathbb{Q},+,\cdot)$.

2) $2\mathbb{Z}$ n'est pas un sous-anneau de $(\mathbb{Z},+,\cdot)$.

◆ **Proposition** Soient $(A,+,\cdot)$ un anneau, $B \in \mathfrak{P}(A)$. Pour que B soit un sous-anneau de A, il faut et il suffit que :

$$\begin{cases} \text{(i)} \quad \forall (x,y) \in B^2, \quad x - y \in B \\ \text{(ii)} \quad \forall (x,y) \in B^2, \quad xy \in B \\ \text{(iii)} \quad 1_A \in B. \end{cases}$$

Preuve :

1) Il est clair que, si B est un sous-anneau de A, les conditions (i), (ii), (iii) sont satisfaites.

2) Réciproquement, supposons (i), (ii), (iii) vérifiées. Alors :

$$0_A = 1_A - 1_A \in B$$
$$\forall x \in B, \quad -x = 0 - x \in B$$
$$\forall (x,y) \in B^2, \quad x + y = x - (-y) \in B$$

et donc B est un sous-groupe de $(A,+)$.

2.3.4 Morphismes d'anneaux

♦ **Définition** Soient A, A' deux anneaux, $f : A \longrightarrow A'$ une application. On dit que f est un **morphisme d'anneaux** si et seulement si :

$$\begin{cases} \forall (x,y) \in A^2, & f(x+y) = f(x) + f(y) \\ \forall (x,y) \in A^2, & f(xy) = f(x)f(y) \\ f(1_A) = 1_B. \end{cases}$$

Un **endomorphisme d'un anneau** $(A,+,\cdot)$ est un morphisme d'anneaux de $(A,+,\cdot)$ dans $(A,+,\cdot)$.

Un **isomorphisme d'anneaux** est un morphisme d'anneaux bijectif.

Un **automorphisme d'un anneau** $(A,+,\cdot)$ est un endomorphisme bijectif de l'anneau $(A,+,\cdot)$.

♦ **Proposition**

1) Si $f : A \longrightarrow A'$ et $g : A' \longrightarrow A''$ sont des morphismes d'anneaux, alors $g \circ f : A \longrightarrow A''$ est un morphisme d'anneaux.

2) $\mathrm{Id}_A : A \longrightarrow A$ est un automorphisme de l'anneau $(A,+,\cdot)$.

3) Si $f : A \longrightarrow A'$ est un isomorphisme d'anneaux, alors $f^{-1} : A' \longrightarrow A$ est un isomorphisme d'anneaux.

Preuve :

Analogue à celle de 2.1 Prop. 5 p. 43.

Exercice

◇ **2.3.6** Soit X un ensemble.

a) Monter que $((\mathbb{Z}/2\mathbb{Z})^X, +, \bullet)$ est un anneau commutatif.

b) Pour toute partie A de X, on note $\theta_A : X \longrightarrow \mathbb{Z}/2\mathbb{Z}$ l'application définie par :

$$\theta_A(x) = \begin{cases} \hat{1} & \text{si } x \in A \\ \hat{0} & \text{si } x \in \complement_X(A) \end{cases}$$

appelée *fonction caractéristique* de A (cf. 1.3.1 Exemple *5)* p. 24).

Montrer que l'application $\theta : \begin{array}{ccc} \mathfrak{P}(X) & \longrightarrow & (\mathbb{Z}/2\mathbb{Z}) \\ A & \longmapsto & \theta_A \end{array}$ est un isomorphisme de $(\mathfrak{P}(X), \Delta, \cap)$ dans $((\mathbb{Z}/2\mathbb{Z})^X, +, \bullet)$, et en déduire que $(\mathfrak{P}(X), \Delta, \cap)$ est un anneau commutatif.

2.3.5 Anneaux intègres

◆ **Définition 1**

Soient A un anneau, $a \in A$.

1) On dit que a est un **diviseur de zéro à gauche** dans A si et ssi :

$$\begin{cases} a \neq 0 \\ \exists b \in A, \quad (b \neq 0 \text{ et } ab = 0) \end{cases}$$

2) On dit que a est **diviseur de zéro à droite** dans A si et ssi :

$$\begin{cases} a \neq 0 \\ \exists c \in A, \quad (c \neq 0 \text{ et } ca = 0) \end{cases}$$

3) On dit que a est un **diviseur de zéro** dans A si et seulement si a est un diviseur de zéro à gauche dans A ou un diviseur de zéro à droite dans A.

EXEMPLES :

1) $\mathbb{Z}$ n'admet aucun diviseur de zéro.

2) Dans $\mathbb{Z}/_{6\mathbb{Z}}$, $\hat{2},\hat{3},\hat{4}$ sont des diviseurs de zéro, et $\hat{0}$, $\hat{1}$, $\hat{5}$ ne sont pas diviseurs de 0.

3) Dans $\mathbf{M}_2(\mathbb{R})$, $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ est un diviseur de zéro à gauche et $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ est un diviseur de zéro à droite, puisque $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = 0$.

4) Dans $\mathbb{R}^{\mathbb{R}}$, $f : \mathbb{R} \longrightarrow \mathbb{R}$, $x \longmapsto \begin{cases} 0 \text{ si } x < 0 \\ x \text{ si } x \geqslant 0 \end{cases}$ et $g : \mathbb{R} \longrightarrow \mathbb{R}$, $x \longmapsto \begin{cases} x \text{ si } x \leqslant 0 \\ 0 \text{ si } x > 0 \end{cases}$ sont des diviseurs de zéro, puisque : $f \neq 0$, $g \neq 0$, $fg = 0$.

◆ **Définition 2** Un anneau A est dit **intègre** si et seulement si :

$$\begin{cases} A & \text{est commutatif} \\ A & \text{n'admet aucun diviseur de zéro} \\ A & \neq \{0\}. \end{cases}$$

EXEMPLES :

1) $(\mathbb{Z},+,\cdot)$ est intègre.

2) $(\mathbb{Z}/_{6\mathbb{Z}},+,\cdot)$ n'est pas intègre.

2.4 Corps

◆ **Définition 1** Un ensemble K muni de deux lois $+,\cdot$ est appelé **corps** si et seulement si :

$$\begin{cases} (K,+,\cdot) \text{ est anneau} \\ 0_K \neq 1_K \\ \text{Tout élément de } K - \{0\} \text{ admet un inverse pour } \cdot \text{ dans } K. \end{cases}$$

Si, de plus, $\cdot$ est commutative dans K, on dit que $(K,+,\cdot)$ est un **corps commutatif**.

EXEMPLES :

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps commutatifs (pour les lois usuelles $+,\cdot$).

Dans le Cours, tous les corps qui interviendront seront commutatifs. D'autre part, on peut montrer (th. de Wedderburn) que tout corps fini est commutatif.

Remarque :

Tout corps commutatif est un anneau intègre.

La réciproque est fausse : $\mathbb{Z}$ est un anneau intègre, et n'est pas un corps.

◆ **Définition 2** Soient $(K,+,\cdot)$ un corps, $L \in \mathfrak{P}(K)$. On dit que L est un **sous-corps** de K si et seulement si : $\left|\begin{array}{l} L \text{ est un sous-anneau de } K \\ \forall x \in L - \{0\}, \quad x^{-1} \in L \end{array}\right|$, c'est-à-dire :

$$\begin{cases} \forall (x,y) \in L^2, \quad x - y \in L \\ \forall (x,y) \in L^2, \quad xy \in L \\ 1_K \in L \\ \forall x \in L - \{0\}, \quad x^{-1} \in L. \end{cases}$$

EXEMPLES :

$\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, et $\mathbb{R}$ est un sous-corps de $\mathbb{C}$ (pour les lois usuelles $+,\cdot$).

Remarque :

Tout sous-corps d'un corps K est un corps pour les lois induites, et les neutres de L pour $+$ et $\cdot$ sont ceux de K.

◆ **Définition 3** Soient K, K' deux corps, $f : K \longrightarrow K'$ une application. Si f est un morphisme (resp. endomorphisme, resp. isomorphisme, resp. automorphisme) d'anneaux, f prend le nom de **morphisme** (resp. **endomorphisme**, resp. **isomorphisme**, resp. **automorphisme**) **de corps**.

EXEMPLES :

$\mathrm{Id}_{\mathbb{C}} : \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & z \end{array}$ et la conjugaison $\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \overline{z} \end{array}$ sont des automorphismes du corps $\mathbb{C}$ (pour les lois usuelles).

Remarque : Si $f : K \longrightarrow K'$ est un morphisme de corps, alors, pour tout x de $K - \{0\}$:

$$f(x) \neq 0 \quad \text{et} \quad (f(x))^{-1} = f(x^{-1}).$$

Exercices

◇ **2.4.1** Soient K un corps, $(x,y) \in (K-\{0\})^2$ tels que $x+y=-1$ et $x^{-1}+y^{-1}=1$. Montrer : $xy=-1$ et $x^4+y^4=7$.

(On a ici noté n au lieu de $n1_K$, pour $n \in \mathbb{Z}$, cf. 2.3.2 p. 57).

◇ **2.4.2** Soit K un corps. Montrer que la caractéristique de l'anneau K (cf. exercice 2.3.4 p. 58) est 0 ou un nombre premier. Quelle est la caractéristique de $\mathbb{Q}$? de $\mathbb{Z}/p\mathbb{Z}$ (p premier) ?

◇ **2.4.3*** Soit K un corps commutatif fini. Montrer :

$$\forall x \in K, \quad \exists (a,b) \in K^2, \quad x = a^2 + b^2.$$

(Utiliser l'exercice 2.2.2 p. 48).

◇ **2.4.4*** Existe-t-il un corps K tel que les groupes $(K,+)$ et $(K-\{0\},\times)$ soient isomorphes ?

Compléments

◇ C 2.1 Classes à gauche dans un groupe, théorème de Lagrange

Soit $(G,\bullet)$ un groupe, de neutre noté e.

1) Soit $\mathcal{R}$ une relation d'équivalence dans G, compatible à gauche avec la loi de G, c'est-à-dire telle que :

$$\forall (x,x',y) \in G^3, \quad (x\mathcal{R}x' \Longrightarrow yx\mathcal{R}yx').$$

Pour $x \in G$, on note $\overline{x}$ la classe de x modulo $\mathcal{R}$.

a) Montrer que $\overline{e}$ est un sous-groupe de G.

b) Etablir : $\forall (x,x') \in G^2$, $(x\mathcal{R}x' \Longleftrightarrow x^{-1}x' \in \overline{e})$. Ainsi : $\forall x \in G, \overline{x} = x\overline{e}$.

*2)*Réciproquement, soient H un sous-groupe de G, et $\mathcal{R}_H$ la relation définie dans G par :

$$\forall (x,x') \in G^2, \quad (x\mathcal{R}_H x' \Longleftrightarrow x^{-1}x' \in H).$$

a) Montrer que $\mathcal{R}_H$ est une relation d'équivalence dans G, compatible à gauche avec la loi de G, et que H est la classe $\overline{e}$ de e modulo $\mathcal{R}_H$.

b) Montrer que, pour tout x de G, l'application $y \longmapsto xy$ est une bijection de $\overline{e}$ sur $\overline{x}$.

3) **Théorème de Lagrange**

Montrer que, si G est un groupe fini, alors, pour tout sous-groupe H de G, le cardinal de H divise celui de G.

4) Exemples d'utilisations du théorème de Lagrange

a) Dans un groupe fini à 24 éléments, peut-il exister des sous-groupes de 10 éléments?

b) Soient G un groupe, de neutre noté e, H, K deux sous-groupes finis de G tels que pgcd (Card(H), Card(K)) = 1 (cf. 4.2.1 Prop-Déf. p. 107). Montrer : $H \cap K = \{e\}$.

◇ C 2.2* Sous-groupes distingués, groupes-quotients

I Sous-groupes distingués

Soit $(G,\cdot)$ un groupe, de neutre noté e.

1) Soit $\mathcal{R}$ une relation d'équivalence dans G compatible à gauche et à droite avec la loi de G, c'est-à-dire telle que (cf. C 2.1 *1)*) :

$$\forall (x,x',y) \in G^3, \quad \left(x\mathcal{R}x' \Longrightarrow \begin{cases} yx\mathcal{R}yx' \\ xy\mathcal{R}x'y \end{cases}\right).$$

Pour $x \in G$, on note $\overline{x}$ la classe de x modulo $\mathcal{R}$.

Montrer que $\overline{e}$ est un sous-groupe de G, et que : $\forall x \in G, \forall y \in \overline{e}, xyx^{-1} \in \overline{e}$.

2) Un sous-groupe H de G est **distingué** dans G et on note $H \lhd G$ si et seulement si :

$$\forall x \in H, \forall y \in G, \quad yxy^{-1} \in H.$$

Soit H un sous-groupe distingué de G. On note $\mathcal{R}_H$ la relation dans G définie par :

$$\forall (x,x') \in G^2, \quad (x\mathcal{R}_H x') \Longleftrightarrow x^{-1}x' \in H).$$

Montrer que $\mathcal{R}_H$ est une relation d'équivalence dans G, compatible à gauche et à droite avec la loi de G, et que H est la classe de e modulo $\mathcal{R}_H$.

3) a) Montrer que, si G est commutatif, alors tout sous-groupe de G est distingué dans G.

b) Donner un exemple d'un groupe G et d'un sous-groupe H de G tel que H ne soit pas distingué dans G.

4) Soient G, G' deux groupes, $f : G \longrightarrow G'$ un morphisme de groupes.

a) Montrer que, pour tout sous-groupe distingué H' de G', $f^{-1}(H')$ est un sous-groupe distingué de G. En particulier, $\mathrm{Ker}(f)$ est un sous-groupe distingué de G.

b) Donner un exemple de groupes G, G' de morphisme de groupes $f : G \longrightarrow G'$, et de sous-groupe H distingué dans G tel que $f(H)$ ne soit pas un sous-groupe distingué de G'.

c) Montrer que, si $H \lhd G$ et si f est surjective, alors $f(H) \lhd G'$.

5) a) Soient $(G, \cdot)$ un groupe, $C(G)$ le **centre** de G, défini par :

$$C(G) = \{a \in G;\ \forall x \in G,\ ax = xa\}.$$

Montrer $C(G) \lhd G$.

b) Soit G un groupe fini de cardinal pair $2n$ ($n \in \mathbb{N}^*$). Montrer que tout sous-groupe de G de cardinal n est distingué dans G.

II Groupes-quotients

Soient G un groupe, H un sous-groupe distingué de G. On note $\mathcal{R}_H$ la relation d'équivalence dans G définie par :

$$\forall (x, x') \in G^2, \quad (x \mathcal{R}_H x' \Longleftrightarrow x^{-1}x' \in H).$$

Pour $x \in G$, on note $\overline{x}$ la classe de x modulo $\mathcal{R}_H$. On note G/H au lieu de $G/\mathcal{R}_H$.

1) Montrer : $\forall (x, x', y, y') \in G^4, \quad \left(\begin{cases} x \mathcal{R} x' \\ y \mathcal{R} y' \end{cases} \Longrightarrow xy \mathcal{R} x'y' \right)$.

2) En déduire qu'on peut définir une loi de composition interne sur G/H, encore notée $\cdot$, par :

$$\forall (x, y) \in G^2, \quad \overline{x}\,\overline{y} = \overline{xy}.$$

3) Montrer que $(G/H, \cdot)$ est un groupe, appelé **groupe-quotient** de G par le sous-groupe distingué H.

4) a) **Factorisation d'un morphisme de groupes**

Soient G (resp. G') un groupe, H (resp. H') un sous-groupe distingué de G (resp. G'), $f : G \longrightarrow G'$ un morphisme de groupes tel que $f(H) \subset H'$. Montrer que f est compatible avec les relations d'équivalence $\mathcal{R}_H$ dans G et $\mathcal{R}_{H'}$ dans G' (cf. C 1.1 *A* p. 37).

Il existe donc (cf. C 1.1 *A* 1) p. 37) une application $\widetilde{f} : G/H \longrightarrow G'/H'$ unique telle que le diagramme $\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p'} \\ G/H & \xrightarrow[\widetilde{f}]{} & G'/H' \end{array}$ soit commutatif, où p, p' sont les surjections canoniques. Montrer que $\widetilde{f}$ est un morphisme de groupes.

b) **Décomposition canonique d'un morphisme de groupes**

Soient G, G' deux groupes, $f : G \longrightarrow G'$ un morphisme de groupes. Montrer qu'il existe un morphisme de groupes unique $\widehat{f} : G/\mathrm{Ker}(f) \longrightarrow \mathrm{Im}(f)$ tel que $f = i \circ \widehat{f} \circ p$ (où $\mathrm{Ker}(f) = \{x \in G;\ f(x) = e'\}$, $\mathrm{Im}(f) = \{x' \in G';\ \exists x \in G, x' = f(x)\}$, $i : \mathrm{Im}(f) \longrightarrow G'$ est l'injection canonique, $p : G \longrightarrow G/\mathrm{Ker}(f)$ la surjection canonique), et que $\widehat{f}$ est un isomorphisme de groupes.

Exemple (cf. 4.1.2 p. 101) : Déterminer $i, \widehat{f}, p$ lorsque $G = \mathbb{Z}$, $G' = \mathbb{Z}/n\mathbb{Z}$ ($n \in \mathbb{N}^*$), $f : \begin{array}{ccc} G & \longrightarrow & G' \\ k & \longmapsto & \overline{k} \end{array}$ (où $\overline{k}$ est la classe de k modulo n).

◊ C 2.3 Anneaux booléiens finis

Un anneau A est dit **booléien** si et seulement si : $\forall x \in A, x^2 = x$.

I 1) Un exemple

Soit E un ensemble.

a) Montrer que $((\mathbb{Z}/2\mathbb{Z})^E, +, \cdot)$ est un anneau booléien (où $\mathbb{Z}/2\mathbb{Z} = \{\hat{0}, \hat{1}\}$ est muni de l'addition et de la multiplication modulo 2, cf. 4.1.2 Prop. 3 p. 102).

b) Etablir que $(\mathfrak{P}(E), \Delta, \cap)$ est un anneau booléien isomorphe à $((\mathbb{Z}/2\mathbb{Z})^E, +, \cdot)$.

2) Soit A un anneau booléien.

a) Etablir : $\forall x \in A, x + x = 0$.

b) Montrer que A est commutatif.

c) Montrer : $\forall (x, y) \in A^2, xy(x + y) = 0$.

d) On suppose, dans cette question *I 2) d)* seulement, que A est intègre. Démontrer que A est isomorphe à $\{0\}$ ou à $\mathbb{Z}/2\mathbb{Z}$ (utiliser *c)*).

II Soit A un anneau booléien.

1) Montrer que la relation $\leqslant$ dans A définie par : $\forall (x, y) \in A^2, \quad (x \leqslant y \iff xy = x)$

est une relation d'ordre dans A.

2) a) Etablir que, pour tout (x, y) de A^2, $\mathrm{Inf}(x, y)$ et $\mathrm{Sup}(x, y)$ existent et valent respectivement xy et $x + y + xy$.

b) En notant $x \wedge y = \mathrm{Inf}(x, y)$ et $x \vee y = \mathrm{Sup}(x, y)$, montrer que les lois internes $\wedge$ et $\vee$ sont associatives, commutatives, et distributives chacune pour l'autre.

3) a) Montrer que A admet un plus petit élément, qui est 0.

b) Montrer que, pour tout x de A, il existe un unique élément de A, que l'on notera x^*, tel que $\begin{cases} x \wedge x^* = 0 \\ x \vee x^* = 1 \end{cases}$, et calculer x^* en fonction de x.

c) Prouver les formules suivantes, pour tout (x, y) de A^2 :

1) $0^* = 1$ et $1^* = 0$

2) $x^{**} = x$

3) $(x \vee y)^* = x^* \wedge y^*$ et $(x \wedge y)^* = x^* \vee y^*$

4) $x \leqslant y \iff y^* \leqslant x^*$

5) $x \leqslant y \iff x \wedge y^* = 0 \iff x^* \vee y = 1$.

4) On suppose dans cette question *4)* que A est *fini*. On note M l'ensemble des éléments maximaux de $A - \{1\}$ (cf. 1.2.3 *2)* Déf. 1 *4)* p. 19), et $\phi : A \longrightarrow \mathfrak{P}(M)$ l'application définie par :

$$\forall x \in A, \quad \phi(x) = \{m \in M; \quad \mathrm{Non}(x \leqslant m)\}.$$

a) Etablir, pour tout (x, m) de $A \times M$:

$$\big(\mathrm{non}(x \leqslant m)\big) \longleftrightarrow mx \neq x \iff x^* \leqslant m \iff (1 + m)(1 + x) = 0.$$

b) Montrer, pour tout (x,y,m) de $A \times A \times M$: $x \wedge y \leqslant m \iff (x \leqslant m \text{ ou } y \leqslant m)$.

c) En déduire, pour tout (x,y) de A^2 :

1) $\phi(x) = \varnothing \iff x = 0$

2) $\phi(x^*) = \complement_M(\phi(x))$

3) $\phi(x \wedge y) = \phi(x) \cap \phi(y)$

4) $\phi(x \vee y) = \phi(x) \cup \phi(y)$.

d) Démontrer que ϕ est un isomorphisme d'anneaux.

Chapitre 3

Nombres entiers, nombres rationnels

3.1 Propriétés de $\mathbb{N}$

3.1.1 Structure de $\mathbb{N}$

Nous rappelons ici les propriétés usuelles de l'ensemble $\mathbb{N}$ des **entiers naturels**, supposées connues. Le lecteur intéressé trouvera une construction de $\mathbb{N}$ (axiomatique de Péano) dans le Cours de J.-M. Arnaudiès et H. Fraysse, Tome 1, pp. 41-54.

L'ensemble $\mathbb{N} = \{0,1,2,3,\ldots\}$ est muni de deux lois de composition interne $+$ (addition) et $\cdot$ (multiplication), qui vérifient :

$+$ est associative, $+$ est commutative, $+$ admet un neutre, noté 0

Tout élément de $\mathbb{N}$ est régulier pour $+$

$\cdot$ est associative, $\cdot$ est commutative, $\cdot$ admet un neutre, noté 1

$\cdot$ est distributive sur $+$

Tout élément de $\mathbb{N}^*$ $(= \mathbb{N} - \{0\})$ est régulier pour $\cdot$.

L'ensemble $\mathbb{N}$ est muni d'une relation d'ordre total $\leqslant$ vérifiant :

Toute partie non vide de $\mathbb{N}$ admet un plus petit élément (on dit que $\mathbb{N}$ est **bien ordonné**)

Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément

$\leqslant$ est compatible avec $+$, c'est-à-dire : $\forall (a,b,c) \in \mathbb{N}^3$, $(a \leqslant b \Longrightarrow a+c \leqslant b+c)$

$\leqslant$ est compatible avec $\cdot$, c'est-à-dire : $\forall (a,b,c) \in \mathbb{N}^3$, $(a \leqslant b \Longrightarrow ac \leqslant bc)$.

On déduit les propriétés élémentaires suivantes :

$$\forall (a,b,c,d) \in \mathbb{N}^4, \quad \left(\begin{cases} a \leqslant b \\ c \leqslant d \end{cases} \Longrightarrow a+c \leqslant b+d\right)$$

$$\forall (a,b,c) \in \mathbb{N}^3, \quad (a+c \leqslant b+c \Longrightarrow a \leqslant b)$$

$$\forall (a,b,c,d) \in \mathbb{N}^4, \quad \left(\begin{cases} a \leqslant b \\ c \leqslant d \end{cases} \Longrightarrow ac \leqslant bd\right)$$

$$\forall (a,b,c) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}^*, \quad (ac \leqslant bc \Longrightarrow a \leqslant b)$$

$$\forall (a,b,n) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}^*, \quad (a \leqslant b \Longleftrightarrow a^n \leqslant b^n).$$

Enfin, si une partie E de $\mathbb{N}$ est telle que : $\left\{\begin{array}{l} 0 \in E \\ \forall n \in E, \quad n+1 \in E \end{array}\right.$,

alors $E = \mathbb{N}$ **(principe de récurrence)**.

3.1.2 Le principe de récurrence

Le principe de récurrence vu ci-dessus en 3.1.1 peut s'exprimer aussi de la façon suivante :

Soient $n_0 \in \mathbb{N}$ et $P(n)$ une propriété portant sur un entier n tel que $n \geqslant n_0$. Pour que $P(n)$ soit vraie pour tout n de $\mathbb{N}$ tel que $n \geqslant n_0$, il faut et il suffit que l'on ait :

$\left\{\begin{array}{l} \bullet \ P(n_0) \text{ est vraie} \\ \bullet \ \text{Pour tout } n \text{ de } \mathbb{N} \text{ tel que } n \geqslant n_0, \text{ si } P(n) \text{ est vraie, alors } P(n+1) \text{ est vraie.} \end{array}\right.$

EXEMPLE :

Montrer : $\forall n \in \mathbb{N}^*, 2\sum_{k=1}^{n} k = n(n+1)$.

La formule est évidente pour $n = 1$. Si $2\sum_{k=1}^{n} k = n(n+1)$, alors :

$$2\sum_{k=1}^{n+1} k = \left(2\sum_{k=1}^{n} k\right) + 2(n+1) = n(n+1) + 2(n+1) = (n+1)(n+2).$$

Remarquons que la formule demandée peut aussi être obtenue en additionnant :

$$\left\{\begin{array}{l} \displaystyle\sum_{k=1}^{n} k = 1 + 2 + \ldots + (n-1) + n \\ \displaystyle\sum_{k=1}^{n} k = n + (n-1) + \ldots + 2 + 1. \end{array}\right.$$

En anticipant sur les fractions (cf. 3.7 p. 96), on a : $\boxed{\forall n \in \mathbb{N}^*, \quad \displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}}$.

Le lecteur pourra de même montrer, par récurrence, les formules classiques suivantes, pour tout n de $\mathbb{N}^*$: $\displaystyle\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$, $\displaystyle\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$.

Plus généralement, pour le calcul de $\displaystyle\sum_{k=1}^{n} k^p$, voir exercice 3.3.19 p. 83. ∎

Il peut arriver que, dans un raisonnement par récurrence, pour déduire $P(n+1)$, on ait besoin non seulement de $P(n)$ mais aussi des $P(k)$ pour $n_0 \leqslant k \leqslant n$. En appliquant le principe de récurrence à la propriété $Q(n)$ définie par :

$$Q(n) \Longleftrightarrow (\forall k \in \{n_0, \ldots, n\}, \quad P(k)),$$

on voit que, pour que $P(n)$ soit vraie pour tout n de $\mathbb{N}$ tel que $n \geqslant n_0$, il faut et il suffit que l'on ait :

- $P(n_0)$ est vraie
- Pour tout n de $\mathbb{N}$ tel que $n \geqslant n_0$, si $P(k)$ est vraie pour tout k de $\{n_0, \ldots, n\}$, alors $P(n+1)$ est vraie.

Dans ce cas, on dit qu'il s'agit d'une **récurrence forte**.

3.1.3 Divisibilité dans $\mathbb{N}$

♦ **Définition 1** Soit $(a,b) \in \mathbb{N}^2$. On dit que a **divise** b (dans $\mathbb{N}$), et on note $a|b$, si et seulement s'il existe $c \in \mathbb{N}$ tel que $b = ac$.

Un entier naturel n est dit **pair** (resp. **impair**) si et seulement si $2|n$ (resp. $2|n+1$).

Remarques :

1) $\forall a \in \mathbb{N}, \quad a|0$.

2) $\forall b \in \mathbb{N}, \quad (0|b \Longleftrightarrow b = 0)$.

♦ **Proposition**

La relation $|$ est une relation d'ordre non total dans $\mathbb{N}$.

Preuve :

1) La réflexivité est évidente.

2) Supposons $a|b$ et $b|a$. Il existe $c,d \in \mathbb{N}$ tels que $b = ac$ et $a = bd$; on déduit $b = bcd$.
Si $b \neq 0$, alors $cd = 1$, donc $c = d = 1$, $a = b$.
Si $b = 0$, alors $a = 0$, donc $a = b$.
Ainsi, $|$ est antisymétrique.

3) Supposons $a|b$ et $b|c$. Il existe $d,e \in \mathbb{N}$ tels que $b = ad$ et $c = be$, d'où $c = a(de)$ et $de \in \mathbb{N}$, donc $a|c$. Ainsi, $|$ est transitive.

4) $2 \not| 3$ et $3 \not| 2$, donc $|$ n'est pas totale.

On montre aisément les propriétés suivantes, qui seront reprises dans l'arithmétique de $\mathbb{Z}$ (4.1.1 Prop. 2 p. 100) :

1) $\forall (a,b,c) \in \mathbb{N}^3,\ (a \mid b \Longrightarrow a \mid bc)$

2) $\forall (a,b,c) \in \mathbb{N}^3,\ \left(\begin{cases} a \mid b \\ a \mid c \end{cases} \Longrightarrow a \mid b+c \right)$

3) $\forall (a,b,\alpha,\beta) \in \mathbb{N}^4,\ \left(\begin{cases} a \mid b \\ \alpha \mid \beta \end{cases} \Longrightarrow a\alpha \mid b\beta \right)$

4) $\forall (a,b,n) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}^*,\ (a \mid b \Longrightarrow a^n \mid b^n)$.

Pour des raisons de commodité, si $a \mid b$ et $a \neq 0$, on pourra noter $\dfrac{b}{a}$ l'unique élément c de $\mathbb{N}$ tel que $b = ac$, par anticipation sur l'étude de $\mathbb{Q}$ (3.7 p. 96).

◆ **Définition 2** Un élément p de $\mathbb{N}$ est dit **premier** si et seulement si :

$$\begin{cases} p \geqslant 2 \\ \forall a \in \mathbb{N},\ \big(a \mid p \Longrightarrow (a = 1 \text{ ou } a = p)\big). \end{cases}$$

Nous montrerons plus loin (4.4.3 Th. 2 p. 124) que l'ensemble $\mathcal{P} = \{2,3,5,7,11,\ldots\}$ des nombres premiers est infini.

Exercices

◇ **3.1.1** Montrer : $\forall (a,b,c) \in (\mathbb{N}^*)^3, (ab < c \Longrightarrow a + b \leqslant c)$.

◇ **3.1.2** Résoudre dans $\mathbb{N}^3$: $10x + 15y + 6z = 133$.

◇ **3.1.3** Montrer, pour tout n de $\mathbb{N}$:
(i) $1^{2n} + 2^{2n} + 3^{2n} \geqslant 2 \cdot 7^n$
(ii) $1^{2n+1} + 2^{2n+1} + 3^{2n+1} \geqslant 6^{n+1}$,
et étudier les cas d'égalité.

Les exercices 3.1.4 *et* 3.1.5 *illustrent le principe de récurrence*

◇ **3.1.4** Montrer :

a) $\forall n \in \mathbb{N} - \{0,1\}, \quad \displaystyle\sum_{k=1}^{n} \frac{1}{k^2} > \frac{3n}{2n+1}$

b) $\forall n \in \mathbb{N}^*, \quad 4^n (n!)^3 < (n+1)^{3n}$

c) $\forall n \in \mathbb{N}^*, \quad 1!3! \ldots (2n+1)! \geqslant ((n+1)!)^{n+1}$

d) $\forall n \in \mathbb{N}^*, \quad \sqrt{\dfrac{3}{4n+3}} < \displaystyle\prod_{k=1}^{n} \frac{4k+1}{4k+3} < \sqrt{\frac{5}{4n+5}}$.

◇ **3.1.5** Soient $n \in \mathbb{N} - \{0,1\}$, E un ensemble, $(A_i)_{1 \leqslant i \leqslant n}$ une famille de parties de E. Montrer que $\overset{n}{\underset{i=1}{\triangle}} A_i$ (où $\triangle$ est la différence symétrique) est l'ensemble des éléments de E qui appartiennent exactement à un nombre impair des A_i.

◇ **3.1.6** Montrer que $f : \begin{array}{ccc} \mathbb{N} \times \mathbb{N}^* & \longrightarrow & \mathbb{N} \\ (x,y) & \longmapsto & (x+y)^2 + y \end{array}$ est injective.

◇ **3.1.7** Trouver les couples d'applications (f,g) de $\mathbb{N}^*$ dans $\mathbb{N}^*$ tels que :
$$\forall (x,y) \in (\mathbb{N}^*)^2, \quad (f(x))^{g(y)} + (f(y))^{g(x)} = x + y.$$

◇ **3.1.8** Trouver tous les triplets d'applications (f,g,h) de $\mathbb{N}^*$ dans $\mathbb{N}^*$ tels que :
$$\forall (x,y,z) \in (\mathbb{N}^*)^3, \quad (f(x))^{g(y)} + (g(y))^{h(z)} + (h(z))^{f(x)} = x + y + z.$$

◇ **3.1.9*** Trouver toutes les applications $f : \mathbb{N} \longrightarrow \mathbb{N}$ strictement croissantes telles que :
$$\begin{cases} f(2) = 2 \\ \forall (p,q) \in \mathbb{N}^2, \quad f(pq) = f(p) f(q). \end{cases}$$

◇ **3.1.10** Calculer $\displaystyle\sum_{k=1}^{n} k(n+1-k)$, pour $n \in \mathbb{N}^*$.

◇ **3.1.11*** Pour $(n,p) \in \mathbb{N}^* \times \mathbb{N}$, on note $S_p(n) = \displaystyle\sum_{k=1}^{n} k^p$. Trouver tous les triplets (p,q,r) de $(\mathbb{N}^*)^3$ tels que : $r \geqslant 2$ et : $\forall n \in \mathbb{N}^*, S_p(n) = (S_q(n))^r$.

3.2 Ensembles finis, ensembles infinis

Notre propos n'est pas ici de construire une théorie des cardinaux, mais seulement de dégager les propriétés élémentaires des ensembles finis. La plupart de ces propriétés peuvent être considérées comme intuitivement évidentes.

Nous n'abordons pas la question de la *dénombrabilité* (équipotence avec $\mathbb{N}$), pour laquelle le lecteur pourra se référer au Cours de J.-M. Arnaudiès et H. Fraysse (Tome 1, pp. 59-61).

3.2.1 Equipotence

◆ **Définition** On dit qu'un ensemble E est **équipotent** à un ensemble F si et seulement s'il existe une bijection de E sur F.

EXEMPLES :

1) $\{2,4\}$ est équipotent à $\{1,2\}$.

2) $\mathbb{N}^*$ est équipotent à $\mathbb{N}$ car l'application $\begin{array}{c}\mathbb{N}^* \longrightarrow \mathbb{N} \\ n \longmapsto n-1\end{array}$ est une bijection.

◆ **Proposition** La relation «être équipotent à» est une relation d'équivalence entre ensembles.

Preuve :

1) Pour tout ensemble E, $\mathrm{Id}_E : E \longrightarrow E$ est une bijection.

2) Si $f : E \longrightarrow F$ est une bijection, alors f^{-1} est une bijection de F sur E (cf. 1.3.2 Prop. 3 p. 28).

3) Si $f : E \longrightarrow F$, $g : F \longrightarrow G$ sont des bijections, alors $g \circ f : E \longrightarrow G$ est une bijection (cf. 1.3.2 Prop. 1 p. 27).

On note $E \simeq F$ pour : E est équipotent à F.

3.2.2 Ensembles finis

On note ici $F_0 = \varnothing$ et, pour tout n de $\mathbb{N}^*$, $F_n = \{1,\ldots,n\} = \{k \in \mathbb{N};\ 1 \leqslant k \leqslant n\}$.

Le lecteur pourra aussi rencontrer la notation $[\![1; n]\!]$ pour F_n.

◆ **Définition 1** Un ensemble E est dit **fini** si et seulement s'il existe $n \in \mathbb{N}$ tel que E soit équipotent à F_n.

◆ **Proposition 1** Si un ensemble E est fini, tout ensemble E' équipotent à E est fini.

Preuve :

Si $E \simeq F_n$ et $E' \simeq E$, alors $E' \simeq F_n$, car $\simeq$ est transitive.

On peut considérer la Proposition suivante comme intuitive :

♦ **Proposition 2** Soit $(n,p) \in \mathbb{N}^2$.

1) Il existe une injection de F_n dans F_p si et seulement si $n \leqslant p$.

2) Il existe une surjection de F_n sur F_p si et seulement si $n \geqslant p$.

3) Il existe une bijection de F_n sur F_p si et seulement si $n = p$.

D'après le *3)* de la Prop. 2 ci-dessus, on peut donner la Déf. suivante :

♦ **Définition 2** Soit E un ensemble fini. Il existe un entier n de $\mathbb{N}$ unique tel que E soit équipotent à F_n ; n s'appelle le **cardinal** de E et est noté $\mathrm{Card}(E)$ ou $\#(E)$.

On déduit de la Prop. 2 la Prop. 3 suivante :

♦ **Proposition 3** Soient E, E' deux ensembles.

1) Si E' est fini, alors il existe une injection de E dans E' si et seulement si :
$$E \text{ est fini} \quad \text{et} \quad \#(E) \leqslant \#(E').$$

2) Si E est fini, alors il existe une surjection de E sur E' si et seulement si :
$$E' \text{ est fini} \quad \text{et} \quad \#(E) \geqslant \#(E').$$

3) Si E ou E' est fini, alors il existe une bijection de E sur E' si et seulement si : E et E' sont finis et $\#(E) = \#(E')$.

♦ **Proposition 4** Si E est un ensemble fini, toute partie F de E est finie, et on a : $\#(F) \leqslant \#(E)$.

Preuve :
Il suffit d'appliquer Prop. 3 *1)* à l'injection canonique $F \longrightarrow E$.

♦ **Proposition 5** Si E, F sont deux ensembles finis, alors $E \cup F$ est fini et :
$$\#(E \cup F) + \#(E \cap F) = \#(E) + \#(F).$$

Preuve :

1) Soient A, B deux ensembles finis disjoints; notons $a = \#(A)$, $b = \#(B)$. Il existe une bijection $\alpha : F_a \longrightarrow A$ et une bijection $\beta : F_b \longrightarrow B$. Il est clair que l'application $\gamma : F_{a+b} \longrightarrow B$ définie par : $\forall n \in F_{a+b}$, $\gamma(n) = \begin{cases} \alpha(n) & \text{si } 1 \leqslant n \leqslant a \\ \beta(n-a) & \text{si } a+1 \leqslant n \leqslant a+b \end{cases}$
est une bijection. Il en résulte que $A \cup B$ est fini et que : $\#(A \cup B) = \#(A) + \#(B)$.

2) En appliquant *1)* à $(E, F - E)$ au lieu de (A, B), on conclut que $E \cup F$ est fini et :

$$\#(E \cup F) + \#(E \cap F) = \#(E \cup (F - E)) + \#(E \cap F) = (\#(E) + \#(F - E)) + \#(E \cap F)$$
$$= \#(E) + (\#(F - E) + \#(E \cap F)) = \#(E) + \#(F).$$

Pour une généralisation à n ensembles finis (**formule du crible**), voir l'exercice 3.2.7 p. 77.

◆ **Corollaire 1** Soient E un ensemble fini, $F \in \mathfrak{P}(E)$. Si $\#(F) = \#(E)$, alors $F = E$.

Preuve :

Si $\#(F) = \#(E)$, comme $\#(E) = \#(F) + \#(E - F)$, on déduit $\#(E - F) = 0$, $E - F = \emptyset$, $F = E$.

◆ **Corollaire 2** Soient $n \in \mathbb{N}^*$ et $E_1, \ldots, E_n$ des ensembles finis. Si $E_1, \ldots, E_n$ sont deux à deux disjoints, alors : $\#\left(\bigcup_{i=1}^{n} E_i\right) = \sum_{i=1}^{n} \#(E_i)$.

Preuve :

Récurrence sur n.

La propriété est vraie pour $n = 1$, $n = 2$ (cf. Prop. 5).

Si elle est vraie pour n, et si $E_1, \ldots, E_{n+1}$ sont des ensembles finis deux à deux disjoints, alors $E_1, \ldots, E_n$ sont deux à deux disjoints et $\left(\bigcup_{i=1}^{n} E_i\right) \cap E_{n+1} = \emptyset$, d'où :

$$\#\left(\bigcup_{i=1}^{n+1} E_i\right) = \#\left(\bigcup_{i=1}^{n} E_i\right) + \#(E_{n+1}) = \sum_{i=1}^{n} \#(E_i) + \#(E_{n+1}) = \sum_{i=1}^{n+1} \#(E_i).$$

◆ **Proposition 6** Soient E, E' deux ensembles finis de même cardinal, et $f : E \longrightarrow E'$ une application. Les propriétés suivantes sont équivalentes :

(i) f est injective (ii) f est surjective (iii) f est bijective.

Preuve :

1) (i) $\Longrightarrow$ (ii), et (i) $\Longrightarrow$ (iii) :

Si f est injective, alors $\widetilde{f} : E \longrightarrow f(E)$, $x \longmapsto f(x)$ est bijective, donc $\#(f(E)) = \#(E) = \#(E')$, d'où $f(E) = E'$ (cf. Prop. 5 p. 73), f est surjective, et donc f est bijective.

2) (ii) $\Longrightarrow$ (i), et (ii) $\Longrightarrow$ (iii) :

Supposons f surjective et non injective. Il existe $x_1, x_2 \in E$ tels que : $x_1 \neq x_2$ et $f(x_1) = f(x_2)$.

L'application $g : E - \{x_2\} \longrightarrow E'$, $x \longmapsto f(x)$ est surjective, donc (cf. Prop. 3 *2)* p. 73) :

$$\#(E - \{x\}) \geqslant \#(E').$$

Mais $\#(E - \{x_2\}) = \#(E) - 1$ et $\#(E') = \#(E)$, d'où une contradiction.

Ainsi f est injective, puis bijective.

3) (iii) $\Longrightarrow$ (i) et (iii) $\Longrightarrow$ (ii), trivialement.

♦ **Proposition 7** Si E, F sont deux ensembles finis, alors $E \times F$ est fini et $\#(E \times F) = \#(E) \cdot \#(F)$.

Preuve :

En notant $n = \#(E)$, $p = \#(F)$, il est clair que $F_n \times F_p$ est fini, de cardinal np, et que $E \times F$ est équipotent à $F_n \times F_p$.

On peut aussi remarquer $E \times F = \bigcup_{f \in F} (E \times \{f\})$, et appliquer le Cor. 2 p. 74. ■

Il en résulte facilement (par récurrence sur n) que, pour tout n de $\mathbb{N}^*$ et tous ensembles finis $E_1, \ldots, E_n$, l'ensemble $\prod_{i=1}^{n} E_i$ est fini et que : $\#\left(\prod_{i=1}^{n} E_i\right) = \prod_{i=1}^{n} \#(E_i)$. ■

En particulier, pour tout n de $\mathbb{N}^*$ et tout ensemble fini E, E^n est fini et :

$$\#(E^n) = (\#(E))^n.$$

♦ **Corollaire** Si E, F sont deux ensembles finis, alors F^E est fini et :

$$\#(F^E) = (\#(F))^{\#(E)}.$$

Preuve :

Il suffit de remarquer que F^E est équipotent à $F^{\#(E)}$ et d'appliquer le résultat précédent.

Remarques :

1) La formule précédente «justifie» la notation générale F^E pour désigner l'ensemble des applications de E dans F.

2) Si $E = \varnothing$, alors F^E est formé d'une application et d'une seule, l'application vide, de graphe $\varnothing$, et donc $\#(F^E) = 1$; on retrouve bien $(\#(F))^{\#(E)} = (\#(F))^0 = 1$. En particulier : $0^0 = 1$.

On veillera à ne pas confondre la notation algébrique 0^0 avec une éventuelle limite.

3.2.3 Ensembles infinis

◆ **Définition** Un ensemble est dit **infini** si et seulement s'il n'est pas fini.

En raisonnant par contre-apposition, ou à l'aide d'un raisonnement par l'absurde, on déduit du 3.2.2 les résultats suivants.

◆ **Proposition 1** Si un ensemble E est infini, tout ensemble E' équipotent à E est infini.

◆ **Proposition 2** Soient E, E' deux ensembles.

1) Si E est infini et s'il existe une injection de E dans E', alors E' est infini.

2) Si E' est infini et s'il existe une surjection de E sur E', alors E est infini.

◆ **Proposition 3** Tout ensemble admettant au moins une partie infinie est lui-même infini.

◆ **Proposition 4** Si E est infini et F non vide, alors $E \times F$ est infini.

Enfin, on peut considérer les résultats suivants comme «naturels» :

◆ **Proposition 5** $\mathbb{N}$ est infini.

◆ **Proposition 6** Si E est infini, alors il existe une injection de $\mathbb{N}$ dans E.

Exercices

◊ **3.2.1** Soit E un ensemble fini. Montrer que $\mathfrak{P}(E)$ est fini et que : $\#(\mathfrak{P}(E)) = 2^{\#(E)}$.

◊ **3.2.2** Soit E un ensemble. Montrer que, si $\mathfrak{P}(E)$ est fini, alors E est fini.

◊ **3.2.3** Montrer que toute suite décroissante à termes dans $\mathbb{N}$ est stationnaire.

◊ **3.2.4** Soient E, F deux ensembles, $f : E \longrightarrow F$ une application.

a) Soit A une partie finie de E ; montrer que $f(A)$ est finie et : $\#(f(A)) \leqslant \#(A)$.

b) Soit B une partie finie de F ; peut-on affirmer que $f^{-1}(B)$ soit finie ? Examiner le cas où f est injective.

◊ **3.2.5** Soit E un ensemble, $f : E \longrightarrow E$ une involution, $A = \{x \in E ; f(x) \neq x\}$. On suppose A fini ; montrer que $\#(A)$ est pair.

◊ **3.2.6** Etablir que $f : \mathbb{N}^2 \longrightarrow \mathbb{N}$ définie par :

$$f(x,y) = \frac{(x+y)(x+y+1)}{2} + x$$

est bijective (on peut supposer connue l'étude élémentaire de $\mathbb{Q}$).

◊ **3.2.7*** **Formule du crible**

Soient $n \in \mathbb{N}^*$, $E_1, \ldots, E_n$ des ensembles finis. Etablir :

$$\#\left(\bigcup_{i=1}^{n} E_i\right) = \sum_{k=1}^{n} (-1)^{k-1} \sum_{I \in \mathfrak{P}_k(\{1,\ldots,n\})} \#\left(\bigcap_{i \in I} E_i\right),$$

où $\mathfrak{P}_k(\{1,\ldots,n\})$ désigne l'ensemble des parties à k éléments de $\{1,\ldots,n\}$. Par exemple :

$$\#(E_1 \cup E_2 \cup E_3) = \#(E_1) + \#(E_2) + \#(E_3) - \Big(\#(E_1 \cap E_2) + \#(E_1 \cap E_3) + \#(E_2 \cap E_3)\Big) + \#(E_1 \cap E_2 \cap E_3).$$

◊ **3.2.8** Soient E un ensemble fini, $n = \#(E)$, $\mathcal{R}$ une relation d'équivalence dans E, $N = \#(E/\mathcal{R})$, ν le nombre de couples (x,y) de E^2 tels que $x \mathcal{R} y$.

a) En notant $E_1, \ldots, E_N$ les éléments de $E/\mathcal{R}$, montrer : $\nu = \sum_{i=1}^{N} (\#(E_i))^2$.

b) En déduire : $n^2 \leqslant N\nu$.

◊ **3.2.9*** Soient $(a_n)_{n \in \mathbb{N}}$, $(b_n)_{n \in \mathbb{N}}$ deux suites à termes dans $\mathbb{N}$. Montrer :

$$\exists (p,q) \in \mathbb{N}^2, \quad (p \neq q,\ a_p \leqslant a_q,\ b_p \leqslant b_q).$$

◊ **3.2.10** Soient $(n,p) \in \mathbb{N}^2$, tel que $n \geqslant p^2 + 1$, $(x_1, \ldots, x_n) \in \mathbb{N}^n$. Montrer :

au moins $p+1$ des nombres $x_1, \ldots, x_n$ sont égaux

ou

au moins $p+1$ des nombres $x_1, \ldots, x_n$ sont deux à deux différents.

◊ **3.2.11*** Soit E un ensemble. Démontrer que, pour que E soit fini, il faut et il suffit que toute partie non vide de $\mathfrak{P}(E)$ admette au moins un élément maximal (pour l'inclusion).

3.3 Analyse combinatoire

On note ici $F_n = \{1,\ldots,n\}$, pour $n \in \mathbb{N}^*$.

3.3.1 Permutations

Rappelons qu'on appelle permutation de F_n toute bijection de F_n dans F_n (1.3.2 Déf. 2 p. 27).

◆ **Notation** On note $\mathfrak{S}_n$ l'ensemble des permutations de $\{1,\ldots,n\}$.

La donnée d'un élément σ de $\mathfrak{S}_n$ est définie par les données successives de $\sigma(1)$ ($\sigma(1) \in F_n$), $\sigma(2)$ ($\sigma(2) \in F_n - \{\sigma(1)\}$),..., $\sigma(n)$. On en déduit : $\text{Card}(\mathfrak{S}_n) = n(n-1)\ldots 1$.

Le produit $\prod_{k=1}^{n} k$ est appelé **factorielle** (de) n, et noté $n!$.

On obtient ainsi : $\text{Card}(\mathfrak{S}_n) = n!$

3.3.2 Arrangements

◆ **Définition** Soient $n, p \in \mathbb{N}^*$ tels que $p \leqslant n$. On appelle **arrangement** de p éléments de F_n tout p-uplet $(x_1,\ldots,x_p)$ de $(F_n)^p$ tel que $x_1,\ldots,x_p$ soient deux à deux distincts.

EXEMPLES :

1) (1,4,2) est un arrangement de trois éléments de F_5.

2) (3,2,2,5) n'est pas un arrangement (car 2 est répété).

La donnée d'un arrangement de p éléments de F_n revient à la donnée d'une application injective de F_p dans F_n. Plus précisément, l'application $f \longmapsto (f(1),\ldots,f(p))$ est une bijection de l'ensemble des applications injectives de F_p dans F_n sur l'ensemble des arrangements de p éléments de F_n.

La donnée d'un arrangement $(x_1,\ldots,x_p)$ revient aux données successives de x_1 (dans F_n), x_2 (dans $F_n - \{x_1\}$),..., x_p (dans $F_n - \{x_1,\ldots,x_{p-1}\}$). On en déduit que le nombre d'arrangements de p éléments de F_n est : $n(n-1)\cdot\ldots\cdot(n-p+1)$.

On note $A_n^p = n(n-1)\cdot\ldots\cdot(n-p+1) = \dfrac{n!}{(n-p)!}$, qui est le nombre d'arrangements de p éléments de F_n ; par convention : $A_n^p = 0$ si $p > n$.

En particulier : $A_n^n = n!$.

Remarque :

Nous venons de dénombrer, par une formule simple, les injections de F_p dans F_n ($p \leqslant n$). En revanche, il n'y a pas de formule «simple» pour le nombre de surjections de F_n sur F_p ($n \geqslant p$), cf. exercice 3.3.18 p. 83.

3.3.3 Combinaisons

♦ **Définition** Soit $(n,p) \in \mathbb{N}^2$. On appelle **combinaison** de p éléments de F_n (ou : **p-bloc** de F_n) toute partie de F_n de cardinal p.

Supposons $p \leqslant n$. Notons ici $\mathcal{A}(n,p)$ l'ensemble des arrangements de p éléments de F_n, et $\mathcal{C}(n,p)$ l'ensemble des combinaisons de p éléments de F_n. L'application $\theta : \begin{array}{ccc} \mathcal{A}(n,p) & \longrightarrow & \mathcal{C}(n,p) \\ (x_1,\ldots,x_p) & \longmapsto & \{x_1,\ldots,x_p\} \end{array}$ est surjective, et tout élément $\{x_1,\ldots,x_p\}$ de $\mathcal{C}(n,p)$ admet exactement $p!$ antécédents, obtenus en permutant $(x_1,\ldots,x_p)$.

On en déduit : $\text{Card}(\mathcal{A}(n,p)) = p!\,\text{Card}(\mathcal{C}(n,p))$, d'où la Proposition suivante.

♦ **Proposition-Définition 1** Soit $(n,p) \in \mathbb{N}^2$. Si $p \leqslant n$, le nombre de combinaisons de p éléments de $\{1,\ldots,n\}$, noté C_n^p (ou : $\binom{n}{p}$) vaut

$$\frac{n(n-1)\cdot\ldots\cdot(n-p+1)}{p!}.$$

Ainsi, pour tout (n,p) de $\mathbb{N}^2$ tel que $p \leqslant n$: $\boxed{C_n^p = \dfrac{n!}{p!(n-p)!}}$

Remarque :

1) D'après sa définition, C_n^p est un entier naturel non nul (pour $0 \leqslant p \leqslant n$), et donc $p!$ divise A_n^p.

2) Si $p > n$, alors $C_n^p = 0$.

3) On prolonge la définition des C_n^p par : $C_n^p = 0$ si $(n,p) \in \mathbb{N} \times \mathbb{Z}_-^*$.

4) $\forall n \in \mathbb{N}$, $C_n^0 = C_n^n = 1$.

♦ **Proposition 2**

1) $\forall (n,p) \in \mathbb{N} \times \mathbb{Z}$, $C_n^p = C_n^{n-p}$.

2) $\forall (n,p) \in \mathbb{N} \times \mathbb{Z}$, $C_n^p + C_n^{p+1} = C_{n+1}^{p+1}$ **(formule fondamentale)**

Preuve :

1) • Si $0 \leqslant p \leqslant n$: $C_n^{n-p} = \dfrac{n!}{(n-p)!p!} = C_n^p$.

• Si $p < 0$ ou $p > n$: $C_n^p = 0$ et $C_n^{n-p} = 0$.

2) • Si $0 \leqslant p \leqslant n-1$:

$$C_n^p + C_n^{p+1} = \frac{n!}{p!(n-p)!} + \frac{n!}{(p+1)!(n-p-1)!} = \frac{n!}{(p+1)!(n-p)!}\Big((p+1)+(n-p)\Big)$$
$$= \frac{(n+1)!}{(p+1)!\Big((n+1)-(p+1)\Big)!} = C_{n+1}^{p+1}.$$

- Si $p < -1$ ou $p > n$: $C_n^p = C_n^{p+1} = C_{n+1}^{p+1} = 0$.
- Si $p = -1$: $C_n^p + C_n^{p+1} = C_n^0 = 1$ et $C_{n+1}^{p+1} = C_{n+1}^0 = 1$.
- Si $p = n$: $C_n^p + C_n^{p+1} = C_n^n = 1$ et $C_{n+1}^{p+1} = C_{n+1}^{n+1} = 1$. ∎

On dispose les C_n^p en un triangle, appelé **triangle de Pascal**, dans lequel C_n^p se trouve à la $n^{\text{ème}}$ ligne et $p^{\text{ème}}$ colonne (pour $0 \leqslant p \leqslant n$) :

n \ p	0	1	2	3	4	5	...	p	$p+1$	...
1	1	1								
2	1	2	1							
3	1	3	3	1			⋮			
4	1	4	6	4	1					
5	1	5	10	10	5	1				
⋮			...							
n								C_n^p	C_n^{p+1}	
$n+1$									C_{n+1}^{p+1}	

◆ **Théorème (Formule du binôme de Newton)**

Soient $n \in \mathbb{N}$, A un anneau, $(x,y) \in A^2$ tel que $xy = yx$. On a :

$$(x+y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k}$$

(où $x^0 = y^0 = 1$).

Preuve :

Récurrence sur n, cf. 2.3.2 Th. p. 56. ∎

En appliquant la formule du binôme de Newton à $(x,y) = (1,1)$ ou $(x,y) = (1,-1)$, on obtient :

◆ **Corollaire**

$$\forall n \in \mathbb{N}\ , \quad \sum_{k=0}^{n} C_n^k = 2^n$$

$$\forall n \in \mathbb{N}^*, \quad \sum_{k=0}^{n} (-1)^k C_n^k = 0.$$

La formule du binôme de Newton sera utilisée pour des nombres x, y réels, complexes, mais aussi pour des matrices carrées x, y commutant (cf. par exemple, ex. 8.1.9 p. 271).

♦ **Proposition 3** Pour tout ensemble fini E, $\mathfrak{P}(E)$ est fini et :
$$\mathrm{Card}(\mathfrak{P}(E)) = 2^{\mathrm{Card}(E)}.$$

Preuve :

En notant $n = \mathrm{Card}(E)$, on a

$$\mathfrak{P}(E) = \bigcup_{k\in\{0,\dots,n\}} \mathfrak{P}_k(E),$$

où $$\mathfrak{P}_k(E) = \{F \in \mathfrak{P}(E);\ \mathrm{Card}(F) = k\},$$

donc $\mathfrak{P}(E)$ est fini et :

$$\mathrm{Card}(\mathfrak{P}(E)) = \sum_{k=0}^{n} \mathrm{Card}(\mathfrak{P}_k(E)) = \sum_{k=0}^{n} \mathrm{C}_n^k = 2^n.$$

Voir aussi l'exercice 3.2.1 p. 77. ■

Anticipons enfin sur l'étude des polynômes (ch. 5. p. 139), pour obtenir une identité sur les coefficients binômiaux.

Soient $n, p, q \in \mathbb{N}$ tels que $n \leqslant p+q$. D'après la formule du binôme de Newton, le coefficient de X^n dans $(X+1)^p(X+1)^q$ est $\sum_{k=0}^{n} \mathrm{C}_p^k \mathrm{C}_q^{n-k}$, par développement du produit de $(X+1)^p$ par $(X+1)^q$. D'autre part, toujours d'après la formule du binôme de Newton, le coefficient de X^n dans $(X+1)^{p+q}$ est C_{p+q}^n.

On conclut : $\displaystyle\sum_{k=0}^{n} \mathrm{C}_p^k \mathrm{C}_q^{n-k} = \mathrm{C}_{p+q}^n$.

Exercices

◇ **3.3.1** Soit $n \in \mathbb{N}$ tel que $n \geqslant 4$. Montrer :
$$\mathrm{C}_{\mathrm{C}_n^2}^2 = 3\mathrm{C}_{n+1}^4.$$

◇ **3.3.2** Soit $(n,p) \in (\mathbb{N}^*)^2$ tel que $n > p$. Résoudre l'équation $\mathrm{C}_n^p = \mathrm{C}_{n-1}^p + \mathrm{C}_{n-x}^{p-x}$, d'inconnue $x \in \mathbb{N}^*$.

◇ **3.3.3** Calculer, pour $n \in \mathbb{N}^*$, $\displaystyle\sum_{k=0}^{n-1} (k+1)\frac{\mathrm{C}_n^{k+1}}{\mathrm{C}_n^k}$.

◇ **3.3.4** En notant $P_n = \displaystyle\prod_{k=0}^{n} \mathrm{C}_n^k$, montrer, pour tout n de $\mathbb{N}^*$: $\dfrac{P_n}{P_{n-1}} = \dfrac{n^{n-1}}{(n-1)!} = \dfrac{n^n}{n!}$.

◇ **3.3.5** Calculer, pour $(p,q) \in (\mathbb{N}^*)^2$, $\displaystyle\sum_{k=0}^{q} \frac{p}{p+q-k} \cdot \frac{\mathrm{C}_q^k}{\mathrm{C}_{p+q}^k}$.

◇ **3.3.6** Montrer, pour tout $(p,q) \in \mathbb{N}^2$ tel que $1 \leqslant p \leqslant q$: $\displaystyle\sum_{k=1}^{p} \frac{C_p^k}{C_q^k} = \frac{p}{q-p+1}$.

◇ **3.3.7** Prouver : $\forall n \in \mathbb{N}^*$, $(n!)^{(n-1)!} \mid (n!)!$.

◇ **3.3.8** Montrer : $\forall (p,q) \in (\mathbb{N}^*)^2$, $\displaystyle\sum_{k=0}^{q-1} (p-2k) C_p^k = q C_p^q$.

◇ **3.3.9** Soit $(n,p,q) \in \mathbb{N}^3$ tel que $p \geqslant n+q+1$. Etablir : $\displaystyle\sum_{k=0}^{n} C_{p-k}^q = C_{p+1}^{q+1} - C_{p-n}^{q+1}$.

◇ **3.3.10** Calculer, pour $(n,p) \in (\mathbb{N}^*)^2$, $\displaystyle\sum_{k=1}^{n} \left(\prod_{i=0}^{p-1} (i+j) \right)$.

◇ **3.3.11** Calculer, pour $n \in \mathbb{N}^*$, $\displaystyle\sum_{k=0}^{E(\frac{n}{2})} C_n^{2k}$ et $\displaystyle\sum_{k=0}^{E(\frac{n}{2})} C_n^{2k+1}$.

◇ **3.3.12** Soit $(n,p) \in (\mathbb{N}^*)^2$ tel que $n \geqslant 2p$. Calculer $\displaystyle\sum_{k=0}^{p} C_n^{p-k} C_n^{p+k}$.

◇ **3.3.13** Etablir : $\forall (n,p,q) \in \mathbb{N}^3$, $\displaystyle\sum_{k=0}^{n} (n-k) C_p^{n-k} C_q^k = \frac{np}{p+q} C_{p+q}^n$.

◇ **3.3.14** *a)* Montrer, pour tout (n,p) de $\mathbb{N}^2$ tel que $n \geqslant p$: $\displaystyle\sum_{k=0}^{n} (-1)^{n-k} C_n^k C_k^p = \begin{cases} 1 & \text{si } n = p \\ 0 & \text{si } n > p \end{cases}$.

b) Soient A un anneau, $(x_n)_{n\in\mathbb{N}}$ une suite dans A, $(y_n)_{n\in\mathbb{N}}$ la suite définie par :

$$\forall n \in \mathbb{N}, \quad y_n = \sum_{k=0}^{n} C_n^k x_k.$$

Montrer : $\forall n \in \mathbb{N}$, $x_n = \displaystyle\sum_{k=0}^{n} (-1)^{n-k} C_n^k y_k$.

◇ **3.3.15** *a)* Etablir, pour tout (n,p,q) de $\mathbb{N}^3$ tel que $n \leqslant p+q$: $\displaystyle\sum_{k=0}^{p} C_p^k C_q^{n-k} = C_{p+q}^n$.

*b)** En déduire : $\forall n \in \mathbb{N}^*$, $\displaystyle\sum_{k=0}^{E(\frac{n-1}{2})} \left(\frac{n-2k}{n} C_n^k \right)^2 = \frac{1}{n} C_{2n-2}^{n-1}$.

◇ **3.3.16** Soit $(k,n) \in \mathbb{N}^2$ tel que $3k \leqslant n+1$.

a) Montrer : $\forall i \in \{0,\ldots,k\}$, $C_n^i \leqslant \dfrac{1}{2^{k-i}} C_n^k$.

b) En déduire : $\displaystyle\sum_{i=0}^{k} C_n^i \leqslant 2C_n^k$.

◇ **3.3.17*** Soit $n \in \mathbb{N}$; déterminer le nombre d'entiers impairs parmi les C_n^k, $0 \leqslant k \leqslant n$ (on fera intervenir l'écriture de n en base 2).

◇ **3.3.18** Soit $(n,p) \in (\mathbb{N}^*)^2$ tel que $n \geqslant p$. On note S_n^p le nombre de surjections de $\{1,\ldots,n\}$ sur $\{1,\ldots,p\}$. Montrer : $\displaystyle\sum_{k=1}^{p} C_p^k S_n^k = p^n$.

En déduire les valeurs de S_5^p pour $p \in \{1,\ldots,5\}$.

◇ **3.3.19** Pour $(n,p) \in \mathbb{N}^2$, on note $S_p(n) = \displaystyle\sum_{k=0}^{n} k^p$.

a) Montrer : $\forall (n,p) \in \mathbb{N}^2,\quad S_{p+1}(n+1) = \displaystyle\sum_{k=0}^{p+1} C_{p+1}^k S_k(n)$.

b) En déduire : $\forall (n,p) \in \mathbb{N}^2,\quad (n+1)^{p+1} = \displaystyle\sum_{k=0}^{p} C_{p+1}^k S_k(n)$.

c) Retrouver ainsi les valeurs des sommes classiques $\displaystyle\sum_{k=1}^{n} k$, $\displaystyle\sum_{k=1}^{n} k^2$, $\displaystyle\sum_{k=1}^{n} k^3$.

◇ **3.3.20** Soient $(p,q) \in \mathbb{N}^2$, $E = \{0,1\}^{p+q+1}$,

$$A = \left\{ (x_1,\ldots,x_{p+q+1}) \in E;\ \sum_{i=1}^{p+q+1} x_i \geqslant p+1 \right\},$$

$$B = \complement_E(A).$$

a) Pour chaque k de $\{0,\ldots,q\}$ soit A_k l'ensemble des éléments $(x_1,\ldots,x_{p+1})$ de E tels que :

$$\sum_{i=1}^{p+k} x_i = p \quad \text{et} \quad x_{p+k+1} = 1.$$

Montrer : $\mathrm{Card}(A_k) = C_{p+k}^p 2^{q-k}$.

b) En déduire $\mathrm{Card}(A)$, puis $\mathrm{Card}(B)$.

c) Montrer : $\displaystyle\sum_{k=0}^{q} \frac{C_{p+k}^p}{2^{p+k}} + \sum_{k=0}^{p} \frac{C_{q+k}^q}{2^{q+k}} = 2$.

d) En déduire : $\forall p \in \mathbb{N},\quad \displaystyle\sum_{i=0}^{p} 2^i C_{2p-i}^p = 2^{2p}$.

◇ **3.3.21*** Etablir, pour tout n de $\mathbb{N}$: $\displaystyle\sum_{k=0}^{n} \frac{1}{C_n^k} = \frac{n+1}{2^{n+1}} \sum_{k=1}^{n+1} \frac{2^k}{k}$.

3.4 Le groupe symétrique

Cette étude sera surtout utilisée dans la théorie des déterminants (ch. 9 p. 301).

Rappelons (cf. 3.3.1 p. 78) que, pour $n \in \mathbb{N}^*$, $\mathfrak{S}_n$ désigne l'ensemble des permutations de $\{1,\ldots,n\}$ et que $\text{Card}(\mathfrak{S}_n) = n!$.

3.4.1 Structure de $\mathfrak{S}_n$

◆ | **Proposition** $\mathfrak{S}_n$ est un groupe pour la loi $\circ$, appelé **groupe symétrique**.

Preuve :

1) $\forall \rho,\sigma \in \mathfrak{S}_n, \sigma \circ \rho \in \mathfrak{S}_n$ (cf. 1.3.2 Prop. 1 p. 27).

2) $\circ$ est associative.

3) $\text{Id}_{\{1,\ldots,n\}} \in \mathfrak{S}_n$.

4) Pour tout σ de $\mathfrak{S}_n$, σ est bijective et $\sigma^{-1} \in \mathfrak{S}_n$.

Par commodité, nous noterons e l'identité de $\{1,\ldots,n\}$. ■

Une permutation σ de $\mathfrak{S}_n$ sera notée : $\begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n-1) & \sigma(n) \end{pmatrix}$.

3.4.2 Transpositions

On suppose ici $n \geqslant 2$.

Définition 1 Pour tout (i,j) de $\{1,\ldots,n\}^2$ tel que $i < j$, on appelle **transposition** échangeant i et j, et on note $\tau_{i,j}$ (ou : τ_{ij}, ou : (i,j)) la permutation de $\{1,\ldots,n\}$ définie par :

$$\tau_{i,j}(i) = j, \quad \tau_{i,j}(j) = i, \quad \tau_{i,j}(k) = k \text{ pour tout } k \text{ de } \{1,\ldots,n\} - \{i,j\}.$$

EXEMPLE :

Pour $n = 5$, $\tau_{2,4} = (2,4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$.

Remarques :

1) $\mathfrak{S}_n$ contient exactement C_n^2 transpositions.

2) Toute transposition est involutive.

◆ | **Théorème 1** Les transpositions de $\{1,\ldots,n\}$ engendrent le groupe $\mathfrak{S}_n$.

Autrement dit, toute permutation de $\{1,\ldots,n\}$ est décomposable (d'au moins une façon) en un produit de (plusieurs) transpositions.

Preuve :

Récurrence sur n.

$\mathfrak{S}_2 = \{e, \tau_{1,2}\}$ et $e = \tau_{1,2}^2$, donc $\{\tau_{1,2}\}$ engendre $\mathfrak{S}_2$.

Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$. Supposons que les transpositions de $\{1,\ldots,n\}$ engendrent $\mathfrak{S}_n$, et soit $\sigma \in \mathfrak{S}_{n+1}$.

1er cas : $\sigma(n+1) = n+1$.

Comme σ est bijective, $\{1,\ldots,n\}$ est alors stable par σ et l'application induite $\sigma' : \{1,\ldots,n\} \longrightarrow \{1,\ldots,n\}$, $k \longmapsto \sigma(k)$ est une permutation de $\{1,\ldots,n\}$. D'après l'hypothèse de récurrence, il existe $N \in \mathbb{N}^*$ et des transpositions $t'_1,\ldots,t'_N$ de $\{1,\ldots,n\}$ telles que :

$$\sigma' = t'_1 \circ \ldots \circ t'_N.$$

En notant, pour chaque r de $\{1,\ldots,N\}$, $t_r : \{1,\ldots,n+1\} \longrightarrow \{1,\ldots,n+1\}$ l'application définie par : $t_r(k) = \begin{cases} t'_r(k) & \text{si } 1 \leqslant k \leqslant n \\ n+1 & \text{si } k = n+1 \end{cases}$, il est clair que $t_1,\ldots,t_N$ sont des transpositions de $\{1,\ldots,n+1\}$, et que $\sigma = t_1 \circ \ldots \circ t_N$.

2ème cas : $\sigma(n+1) \neq n+1$.

Considérons $\rho = \tau_{n+1,\sigma(n+1)} \circ \sigma$. On a $\rho \in \mathfrak{S}_{n+1}$ et $\rho(n+1) = \tau_{n+1,\sigma(n+1)}(\sigma(n+1)) = n+1$. D'après l'étude du 1er cas, il existe $N \in \mathbb{N}^*$ et des transpositions $t_1,\ldots,t_N$ de $\{1,\ldots,n+1\}$ telles que $\rho = t_1 \circ \ldots \circ t_N$. Alors $\sigma = \tau_{n+1,\sigma(n+1)} \circ t_1 \circ \ldots \circ t_N$ et donc σ est un produit de transpositions de $\{1,\ldots,n+1\}$. ■

La preuve précédente fournit un algorithme permettant de décomposer une permutation quelconque en un produit de transpositions : on remet les éléments $1,\ldots,n$ dans l'ordre, en en mettant un à sa place (au moins) à chaque étape.

Par exemple, soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 3 & 7 & 4 & 8 & 1 & 5 & 2 \end{pmatrix}$

1	2	3	4	5	6	7	8	
6	3	7	4	[8]	1	5	[2]	σ
6	3	[7]	4	2	1	[5]	8	$\tau_{2,8}$
[6]	3	5	4	2	[1]	7	8	$\tau_{5,7}$
1	3	[5]	4	[2]	6	7	8	$\tau_{1,6}$
1	[3]	[2]	4	5	6	7	8	$\tau_{2,5}$
1	2	3	4	5	6	7	8	$\tau_{2,3}$

Dans chaque ligne, on a encadré les deux éléments qui vont être échangés pour obtenir la ligne suivante.

On a donc $\tau_{2,3} \circ \tau_{2,5} \circ \tau_{1,6} \circ \tau_{5,7} \circ \tau_{2,8} \circ \sigma = e$, d'où $\sigma = \tau_{2,8} \circ \tau_{5,7} \circ \tau_{1,6} \circ \tau_{2,5} \circ \tau_{2,3}$.

Remarque :

L'algorithme précédent montre que toute permutation de $\{1,\ldots,n\}$ est décomposable, d'au moins une façon, en un produit d'au plus n transpositions.

◆ **Définition 2** Soit $\sigma \in \mathfrak{S}_n$.

On dit qu'un couple $(\sigma(i),\sigma(j))$ **présente une inversion pour** σ (ou : **est une inversion de** σ) si et seulement si : $i < j$ et $\sigma(i) > \sigma(j)$.

On note $I(\sigma)$ le nombre d'inversions de σ, et on appelle **signature** de σ le nombre, noté $\varepsilon(\sigma)$, défini par : $\varepsilon(\sigma) = (-1)^{I(\sigma)}$.

On dit que σ est **paire** (resp. **impaire**) si et seulement si $\varepsilon(\sigma) = 1$ (resp. $\varepsilon(\sigma) = -1$).

Ainsi : • σ paire $\iff \varepsilon(\sigma) = 1 \iff I(\sigma)$ pair.

• σ impaire $\iff \varepsilon(\sigma) = -1 \iff I(\sigma)$ impair.

◆ **Proposition 1** Pour toute σ de $\mathfrak{S}_n$: $\displaystyle\varepsilon(\sigma) = \prod_{\{i,j\}\in\mathfrak{P}_2(n)} \frac{\sigma(j)-\sigma(i)}{j-i}$,

où $\mathfrak{P}_2(n)$ désigne l'ensemble des paires de $\{1,\ldots,n\}$.

Nous anticipons ici sur la notion de nombre rationnel (cf. 3.7 p. 96), par commodité.

Preuve :

1) Puisque σ est une permutation de $\{1,\ldots,n\}$ l'application $\sigma_2 : \begin{array}{ccc}\mathfrak{P}_2(n) & \longrightarrow & \mathfrak{P}_2(n) \\ \{i,j\} & \longmapsto & \{\sigma(i),\sigma(j)\}\end{array}$

est une permutation de $\mathfrak{P}_2(n)$, et donc :

$$\prod_{\{i,j\}\in\mathfrak{P}_2(n)} |\sigma(j)-\sigma(i)| = \prod_{\{i,j\}\in\mathfrak{P}_2(n)} |j-i|,$$

ce qui montre : $\displaystyle\left|\prod_{\{i,j\}\in\mathfrak{P}_2(n)} \frac{\sigma(j)-\sigma(i)}{j-i}\right| = 1.$

2) Le nombre de paires $\{i,j\}$ de $\{1,\ldots,n\}$ telles que $\dfrac{\sigma(j)-\sigma(i)}{j-i} < 0$ est $I(\sigma)$, donc $\displaystyle\prod_{\{i,j\}\in\mathfrak{P}_2(n)} \frac{\sigma(j)-\sigma(i)}{j-i}$ est du même signe que $\varepsilon(\sigma)$.

Remarque :

On a aussi : $\displaystyle\varepsilon(\sigma) = \prod_{1\leqslant i<j\leqslant n} \frac{\sigma(j)-\sigma(i)}{j-i}$.

◆ **Théorème 2** L'application signature $\varepsilon : \mathfrak{S}_n \longrightarrow \{-1,1\}$ est un morphisme du groupe $(\mathfrak{S}_n,\circ)$ sur le groupe multiplicatif $\{-1,1\}$.

Preuve :

Soient $\rho,\sigma \in \mathfrak{S}_n$. On a :

$$\begin{aligned}\varepsilon(\sigma\circ\rho) &= \prod_{\{i,j\}\in\mathfrak{P}_2(n)} \frac{(\sigma\circ\rho)(j)-(\sigma\circ\rho)(i)}{j-i} \\ &= \prod_{\{i,j\}\in\mathfrak{P}_2(n)} \frac{\sigma(\rho(j))-\sigma(\rho(i))}{\rho(j)-\rho(i)} \cdot \prod_{\{i,j\}\in\mathfrak{P}_2(n)} \frac{\rho(j)-\rho(i)}{j-i}.\end{aligned}$$

L'application $\{i,j\} \longmapsto \{\rho(i),\rho(j)\}$ étant une permutation de $\mathfrak{P}_2(n)$, on obtient :

$$\varepsilon(\sigma \circ \rho) = \prod_{\{k,l\} \in \mathfrak{P}_2(n)} \frac{\sigma(l) - \sigma(k)}{l - k} \cdot \prod_{\{i,j\} \in \mathfrak{P}_2(n)} \frac{\rho(j) - \rho(i)}{j - i} = \varepsilon(\sigma)\varepsilon(\rho).$$

D'autre part, il est clair que $\{-1,1\}$ est un groupe pour la multiplication.

♦ **Proposition-Définition 2**

Le noyau de ε est un sous-groupe de $\mathfrak{S}_n$, appelé **groupe alterné**, et noté $\mathcal{A}_n$.

Preuve :

On sait (2.2.3 Prop. 2 p. 52) que le noyau d'un morphisme de groupes est un sous-groupe.■

Ainsi, $\mathcal{A}_n = \varepsilon^{-1}(\{1\}) = \{\sigma \in \mathfrak{S}_n ; \varepsilon(\sigma) = 1\}$, c'est-à-dire que $\mathcal{A}_n$ est l'ensemble des permutations paires de $\{1,\ldots,n\}$.

EXEMPLE :

Pour $n = 3$, $\mathfrak{S}_3 = \{e,\tau_{1,2},\tau_{1,3},\tau_{2,3},c,c'\}$ où $c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ et $c' = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = c^2$,

et $\mathcal{A}_3 = \{e,c,c'\}$

$\circ$ ↗	e	c	c'	τ_{12}	τ_{13}	τ_{23}
e	e	c	c'	τ_{12}	τ_{13}	τ_{23}
c	c	c'	e	τ_{13}	τ_{23}	τ_{12}
c'	c'	e	c	τ_{23}	τ_{12}	τ_{13}
τ_{12}	τ_{12}	τ_{23}	τ_{13}	e	c'	c
τ_{13}	τ_{13}	τ_{12}	τ_{23}	c	e	c'
τ_{23}	τ_{23}	τ_{13}	τ_{12}	c'	c	e

♦ **Proposition 3**

Toute transposition de $\{1,\ldots,n\}$ est impaire.

Preuve :

Soit $(i,j) \in \{1,\ldots,n\}^2$ tel que $i < j$. Puisque

$$\tau_{i,j} = \begin{pmatrix} 1 & \ldots & i-1 & i & i+1 & \ldots & j-1 & j & j+1 & \ldots & n \\ 1 & \ldots & i-1 & j & i+1 & \ldots & j-1 & i & j+1 & \ldots & n \end{pmatrix},$$

les couples présentant une inversion (sur la 2$^{\text{eme}}$ ligne) sont :

$$(j,i+1), (j,i+2),\ldots,(j,j-1), (j,i) (i+1,i), (i+2,i),\ldots,(j-1,i),$$

qui sont au nombre de $2(j-i)-1$.

Donc $\mathrm{I}(\tau_{i,j})$ est impair, $\varepsilon(\tau_{i,j}) = -1$, $\tau_{i,j}$ est impaire.

◆ **Corollaire** Soient $\sigma \in \mathfrak{S}_n$, $N \in \mathbb{N}^*$, $t_1,\ldots,t_N$ des transpositions de $\{1,\ldots,n\}$ telles que $\sigma = t_1 \circ \ldots \circ t_N$. On a : $\varepsilon(\sigma) = (-1)^N$.

Ainsi, une permutation paire (resp. impaire) ne peut être décomposée qu'en un produit d'un nombre pair (resp. impair) de transpositions.

3.4.3 Cycles

On suppose ici $n \geqslant 2$.

◆ **Définition** Soit $p \in \mathbb{N}$ tel que $2 \leqslant p \leqslant n$. On appelle ***p*-cycle** de $\{1,\ldots,n\}$ toute permutation σ de $\{1,\ldots,n\}$ telle qu'il existe $x_1,\ldots,x_p \in \{1,\ldots,n\}$, deux à deux distincts, tels que :

$$\begin{cases} \sigma(x_1) = x_2,\ \sigma(x_2) = x_3,\ldots,\sigma(x_{p-1}) = x_p,\ \sigma(x_p) = x_1 \\ \forall k \in \{1,\ldots,n\} - \{x_1,\ldots,x_p\}, \quad \sigma(k) = k. \end{cases}$$

L'ensemble $\{x_1,\ldots,x_p\}$ (qui est à l'évidence unique pour un p-cycle σ donné) est appelé le **support** de σ, et on note $\sigma = (x_1,\ldots,x_p)$.

Une permutation σ de $\{1,\ldots,n\}$ est appelée **cycle** si et seulement s'il existe $p \in \{2,\ldots,n\}$ tel que σ soit un p-cycle.

EXEMPLE :
$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}$ est le 3-cycle (2, 5, 3).

Remarques :

1) $(x_1,\ldots,x_p) = (x_2,\ldots,x_p,x_1) = \ldots = (x_p,x_1,\ldots,x_{p-1})$.

2) Les 2-cycles sont les transpositions.

3) e n'est pas un cycle.

◆ **Théorème** Toute permutation de $\{1,\ldots,n\}$ est décomposable en un produit de cycles à supports deux à deux disjoints, de façon unique à l'ordre près des cycles.

On peut convenir que e est décomposable en un produit vide de cycles.

Preuve : (pouvant être omise en première lecture)

1) Existence

Récurrence sur n.

La propriété est triviale pour $n = 2$.

Soient $n \in \mathbb{N}$ tel que $n \geqslant 2$, et $\sigma \in \mathfrak{S}_{n+1}$.

1^er cas : $\sigma(n+1) = n+1$.

On raisonne comme dans la preuve de Th. 1 de 3.4.2 p. 85. Comme σ est bijective, $\{1,\ldots,n\}$ est alors stable par σ et l'application induite $\sigma' : \{1,\ldots,n\} \longrightarrow \{1,\ldots,n\}$, $k \longmapsto \sigma(k)$ est une permutation de $\{1,\ldots,n\}$. D'après l'hypothèse de récurrence, il existe $\nu \in \mathbb{N}^*$ et des cycles $c'_1,\ldots,c'_\nu$ de $\{1,\ldots,n\}$, à supports deux à deux disjoints, tels que $\sigma' = c'_1 \circ \ldots \circ c'_\nu$. En notant, pour chaque r de $\{1,\ldots,\nu\}$, $c_r : \{1,\ldots,n+1\} \longrightarrow \{1,\ldots,n+1\}$ l'application définie par $c_r(k) = \begin{cases} c'_r(k) & \text{si } 1 \leqslant k \leqslant n \\ n+1 & \text{si } k = n+1 \end{cases}$, il est clair que $c_1,\ldots,c_\nu$ sont des cycles de $\{1,\ldots,n+1\}$ à supports deux à deux disjoints, et que $\sigma = c_1 \circ \ldots \circ c_\nu$.

2^ème cas : $\sigma(n+1) \neq n+1$.

Comme les $n+2$ entiers $n+1$, $\sigma(n+1),\ldots,\sigma^{n+1}(n+1)$ sont dans $\{1,\ldots,n+1\}$, il existe $(k,l) \in \{0,\ldots,n+1\}^2$ tel que : $k < l$ et $\sigma^k(n+1) = \sigma^l(n+1)$. En notant $m = l-k$, on a : $m \in \{1,\ldots,n+1\}$ et $\sigma^m(n+1) = n+1$.

Ainsi, l'ensemble $\{q \in \{1,\ldots,n+1\};\ \sigma^q(n+1) = n+1\}$ est une partie non vide de $\mathbb{N}^*$, donc admet un plus petit élément, noté p.

On a alors : $\sigma^p(n+1) = n+1$.

D'autre part, les p entiers $n+1, \sigma(n+1),\ldots,\sigma^{p-1}(n+1)$ sont deux à deux distincts car, s'il existait $(k,l) \in \{0,\ldots,p-1\}^2$ tel que $(k < l$ et $\sigma^k(n+1) = \sigma^l(n+1))$, alors on aurait, en notant $q = l-k$: $q \in \{1,\ldots,n+1\}$, $\sigma^q(n+1) = n+1$, $q \leqslant p-1$,

ce qui contredirait la définition de p.

Notons c le p-cycle $c = (n+1, \sigma(n+1),\ldots,\sigma^{p-1}(n+1))$, et $\rho = c^{-1} \circ \sigma$, de sorte que $\rho(n+1) = c^{-1}(\sigma(n+1)) = n+1$.

D'après l'étude du 1^er cas, il existe $\nu \in \mathbb{N}$ et des cycles $c_1,\ldots,c_\nu$ de $\{1,\ldots,n+1\}$ à supports deux à deux disjoints, tels que $\rho = c_1 \circ \ldots \circ c_\nu$.

Comme : $\rho(n+1) = n+1$, $\rho(\sigma(n+1)) = \sigma(n+1),\ldots,\rho(\sigma^{p-1}(n+1)) = \sigma^{p-1}(n+1)$, les supports des cycles $c_1,\ldots,c_\nu$ ne contiennent aucun des éléments $n+1, \sigma(n+1),\ldots,\sigma^{p-1}(n+1)$. Finalement, $\sigma = c \circ c_1 \circ \ldots \circ c_\nu$ où $c, c_1,\ldots,c_\nu$ sont des cycles de $\{1,\ldots,n+1\}$ à supports deux à deux disjoints.

2) Unicité

Soient $\sigma = c_1 \circ \ldots \circ c_\nu = d_1 \circ \ldots \circ d_{\nu'}$ deux décompositions de σ en cycles à supports deux à deux disjoints.

Remarquons d'abord que $c_1,\ldots,c_\nu$ commutent entre eux deux à deux, et que $d_1,\ldots,d_{\nu'}$ commutent entre eux deux à deux.

Le cas $\sigma = e$ est immédiat; supposons $\sigma \neq e$.

Il existe donc $i \in \{1,\ldots,n\}$ tel que $\sigma(i) \neq i$, puis $r \in \{1,\ldots,\nu\}$ et $r' \in \{1,\ldots,\nu'\}$ tels que i soit dans le support de c_r et dans le support de $d_{r'}$.

Comme dans 1) ci-dessus, il existe $p \in \mathbb{N}^*$ tel que : $\begin{cases} i, \sigma(i),\ldots,\sigma^{p-1}(i) & \text{sont deux à deux distincts} \\ \sigma^p(i) = i. \end{cases}$

On a alors $c_r = d_{r'} = (i, \sigma(i),\ldots,\sigma^{p-1}(i))$.

En réitérant, on en déduit $\nu' = \nu$ et $\{c_1,\ldots,c_\nu\} = \{d_1,\ldots,d_{\nu'}\}$. ∎

EXEMPLE :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 6 & 9 & 1 & 5 & 8 & 2 & 7 & 10 & 3 \end{pmatrix} = (1,4) \circ (2,6,8,7) \circ (3,9,10).$$

Exercices

◇ **3.4.1** Montrer que $\mathfrak{S}_n$ est non commutatif dès que $n \geqslant 3$.

◇ **3.4.2** Pour $n \in \mathbb{N}^*$, déterminer la signature de $\sigma : \{1,\ldots,n\} \longrightarrow \{1,\ldots,n\}$, $i \longmapsto n+1-i$

◇ **3.4.3** Pour $n \in \mathbb{N}^*$, déterminer la signature de

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n & n+1 & n+2 & \ldots & 2n \\ 2 & 4 & 6 & \ldots & 2n & 1 & 3 & \ldots & 2n-1 \end{pmatrix}.$$

◇ **3.4.4** Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 7 & 1 & 5 & 12 & 6 & 3 & 9 & 4 & 2 & 11 & 8 & 10 \end{pmatrix}$.

a) Déterminer le nombre d'inversions et la parité de σ.

b) Décomposer σ (d'au moins une façon) en un produit de transpositions.

c) Décomposer σ en un produit de cycles à supports disjoints. Retrouver ainsi la valeur de $\varepsilon(\sigma)$.

◇ **3.4.5** Soit $n \in \mathbb{N}$ tel que $n \geqslant 3$.

a) Vérifier, pour tout couple (i,j) de $\{1,\ldots,n\}^2$ tel que $2 \leqslant i < j \leqslant n$:

$$\tau_{ij} = \tau_{1i} \circ \tau_{1j} \circ \tau_{1i}.$$

En déduire que $\{\tau_{1i};\ 2 \leqslant i \leqslant n\}$ engendre le groupe $\mathfrak{S}_n$.

b) Vérifier, pour tout couple (i,j) de $\{2,\ldots,n\}^2$ tel que $i \neq j$: $(1,i,j) = \tau_{1j} \circ \tau_{1i}$.
En déduire que $\{(1,i,j);\ (i,j) \in \{2,\ldots,n\}^2, i \neq j\}$ engendre le sous-groupe $\mathcal{A}_n$.

c) Vérifier, pour tout $k \in$ de $\{3,\ldots,n\}$:

$$\tau_{1k} \circ \tau_{12} = \gamma_k \quad \text{et} \quad \tau_{12} \circ \tau_{1k} = \gamma_k^2, \text{ où } \gamma_k = (1,2,k).$$

En déduire, pour tout (i,j) de $\{3,\ldots,n\}^2$: $\tau_{1i} \circ \tau_{1j} = \gamma_i \circ \gamma_j^2$.
En déduire que $\{(1,2,i);\ 3 \leqslant i \leqslant n\}$ engendre le sous-groupe $\mathcal{A}_n$.

3.5 Dénombrements

Dénombrer un ensemble fini, c'est calculer son cardinal.

3.5.1 Dénombrements classiques

Rappelons (3.2.2 pp. 73-75, 3.3.3 p. 81) que, si E, F sont des ensembles finis, alors $E \cup F$, $E \times F$, F^E, $\mathfrak{P}(E)$ sont finis et :

$$\begin{aligned} \#(E \cup F) + \#(E \cap F) &= \#(E) + \#(F) \\ \#(E \times F) &= \#(E) \cdot \#(F) \\ \#(F^E) &= (\#(F))^{\#(E)} \\ \#(\mathfrak{P}(E)) &= 2^{\#(E)}. \end{aligned}$$

On a vu (cf. 3.3.2 p. 78) que, si E et F sont finis, alors le nombre d'injections de F dans E est $A_n^p = \dfrac{n!}{(n-p)!}$, où $n = \#(E)$, $p = \#(F)$, $p \leqslant n$.

En particulier (cf. 3.3.1 p. 78) le nombre de permutations d'un ensemble fini à n éléments est $n!$.

3.5.2 Exemples de dénombrements

1) Soient E, F deux ensembles finis, $n = \#(E)$, $p = \#(F)$.

a) Le nombre de relations de E vers F est 2^{np} car l'application qui, à une relation de E vers F, associe son graphe est une bijection de l'ensemble des relations de E vers F sur l'ensemble des parties de $E \times F$.

b) Le nombre de lois de composition interne dans E est n^{n^2} car il s'agit du nombre d'applications de $E \times E$ dans E.

2) Combien y a-t-il de nombres entiers dont l'écriture décimale comporte exactement n chiffres ($n \geqslant 3$) dont deux chiffres 8 exactement ?

Soit N un nombre de n chiffres exactement (donc le 1$^{\text{er}}$ chiffre à gauche n'est pas 0) et comportant exactement deux 8.

1$^{\text{er}}$ cas Un des deux 8 peut être le 1$^{\text{er}}$ chiffre de N, ce qui donne $n-1$ possibilités de placer le 2$^{\text{ème}}$ 8, les $n-2$ autres chiffres étant quelconques, distincts de 8. Il y a ainsi exactement $(n-1)9^{n-2}$ nombres N de ce premier type. Par exemple, pour $n = 6$, on peut choisir $N = 841182$.

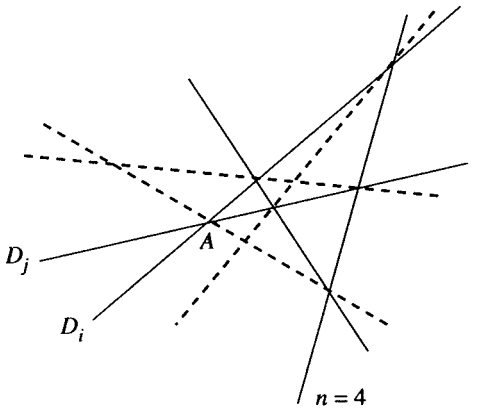
2$^{\text{ème}}$ cas Aucun des deux 8 n'est le 1$^{\text{er}}$ chiffre de N, ce qui donne C_{n-1}^2 possibilités de placer les deux 8, le 1$^{\text{er}}$ chiffre étant quelconque parmi 1, 2, 3, 4, 5, 6, 7, 9, et les $n-3$ autres chiffres quelconques distincts de 8. Il y a ainsi exactement $\dfrac{(n-1)(n-2)}{2} \cdot 8 \cdot 9^{n-3}$ nombres N de ce deuxième type.

Finalement, le nombre demandé est : $(n-1)9^{n-2} + 4(n-1)(n-2)9^{n-3}$, c'est-à-dire $(4n+1)(n-1)9^{n-3}$.

3) On donne, dans le plan, n droites distinctes «en position générale» ($n \geqslant 4$).

a) En combien de points ces droites se coupent-elles?

b) Combien de nouvelles droites sont déterminées par les points d'intersection précédents?



a) Il y autant de points cherchés que de paires de droites parmi $D_1, \ldots, D_n$; il y en a donc C_n^2.

Par exemple, pour $n = 4$, il y a 6 points d'intersection deux à deux des droites D_1, D_2, D_3, D_4.

b) Considérons un point A obtenu en *a)*. Il existe exactement deux droites D_i, D_j $(i < j)$ passant par A (parmi $D_1, \ldots, D_n$). Sur D_i (comme sur D_j), il y a, en plus de A, exactement $n - 2$ points du *a)*. Les points à joindre à A pour obtenir de nouvelles droites sont donc au nombre de $C_n^2 - 1 - 2(n-2)$, c'est-à-dire $\dfrac{(n-2)(n-3)}{2}$. Comme chaque nouvelle droite joint deux points du *a)*, le nombre de nouvelles droites est : $\dfrac{1}{2} C_n^2 \dfrac{(n-2)(n-3)}{2}$, c'est-à-dire $\dfrac{1}{8} n(n-1)(n-2)(n-3)$.

Par exemple, pour $n = 4$, il y a 3 nouvelles droites.

4) Soient E un ensemble fini à n éléments, A une partie de E à p éléments $(0 \leqslant p \leqslant n)$. Dénombrer les couples (X, Y) de parties de E telles que : $X \cup Y = E$ et $X \cap Y = A$.

Notons $B = \complement_E(A)$.

Il est clair que l'application $(X', Y') \longmapsto (X' \cup A, Y' \cup A)$ est une bijection de

$\{(X', Y') \in (\mathfrak{P}(B))^2;\ X' \cup Y' = B\}$ sur $\{(X, Y) \in (\mathfrak{P}(E))^2;\ X \cup Y = E \text{ et } X \cap Y = A\}$.

De plus : $\forall (X', Y') \in (\mathfrak{P}(B))^2$, $\left(X' \cup Y' = B \iff \complement_B(X') \subset Y'\right)$. Ainsi, le cardinal demandé est aussi celui de $\{(X'', Y') \in (\mathfrak{P}(B))^2;\ X'' \subset Y'\}$. Pour $Y' \in \mathfrak{P}(B)$ fixée, de cardinal noté y', le cardinal de $\{X'' \in \mathfrak{P}(B);\ X'' \subset Y'\}$ est $2^{y'}$. Le cardinal cherché est donc $\displaystyle\sum_{y'=0}^{n-p} 2^{y'} C_{n-p}^{y'}$, c'est-à-dire 3^{n-p}.

Exercices

◊ **3.5.1** Combien y a-t-il de fonctions d'un ensemble E à n éléments dans un ensemble F à p éléments ?

◊ **3.5.2** On note P_n le nombre de partitions de $\{1,\dots,n\}$, pour $n \in \mathbb{N}^*$. Montrer :

$$\forall n \in \mathbb{N}, \quad P_{n+1} = \sum_{k=0}^{n} \mathrm{C}_n^k P_k$$

(où $P_0 = 1$).

En déduire P_n pour $0 \leqslant n \leqslant 5$.

◊ **3.5.3** Pour $(n,p) \in (\mathbb{N}^*)^2$, on note $P_{n,p}$ le nombre de partitions de $\{1,\dots,n\}$ en p ensembles.

a) Montrer, pour tout (n,p) de $(\mathbb{N}^*)^2$:

$$P_{n+1,p+1} = P_{n,p} + (p+1)P_{n,p+1}.$$

b) En déduire $P_{n,p}$ pour $(n,p) \in \{1,\dots,5\}^2$.

c) Montrer, pour tout n de $\mathbb{N}^*$:

$$P_{n+1,n} = \mathrm{C}_{n+1}^2, \qquad P_{n+1,2} = 2^n - 1, \qquad P_{n+1,3} = \frac{3^n - 2^{n+1} + 1}{2}.$$

◊ **3.5.4** Soient E un ensemble fini, $n = \mathrm{Card}(E)$, et, pour tout k de $\mathbb{N}$:

$$A_{n,k} = \{f : E \longrightarrow \mathbb{N} : \sum_{x \in E} f(x) \leqslant k\},$$

$$B_{n,k} = \{f : E \longrightarrow \mathbb{N} : \sum_{x \in E} f(x) = k\},$$

$$a_{n,k} = \#(A_{n,k}), \quad b_{n,k} = \#(B_{n,k}).$$

a) Montrer, pour tout (n,k) de $(\mathbb{N}^*)^2$:

$$b_{n,k} = a_{n-1,k}, \qquad a_{n,k} = b_{n,k} + a_{n,k-1}.$$

b) En déduire, pour tout (n,k) de $\mathbb{N}^2$:

$$a_{n,k} = \mathrm{C}_{n+k}^k, \qquad b_{n,k} = \mathrm{C}_{n+k-1}^k \quad (\text{si } n \geqslant 1).$$

3.6 Propriétés de $\mathbb{Z}$

Nous rappelons ici les propriétés usuelles de l'ensemble $\mathbb{Z}$ des **entiers relatifs**, supposées connues. Le lecteur intéressé trouvera une construction de $\mathbb{Z}$ (symétrisation du demi-groupe $(\mathbb{N},+)$) dans le Cours de J.-M. Arnaudiès et H. Fraysse, Tome 1, pp. 70-73.

L'ensemble $\mathbb{Z} = \{\ldots,-3,-2,-1,0,1,2,3,\ldots\}$ est muni d'une addition $+$, d'une multiplication $\cdot$, et d'une relation d'ordre total $\leqslant$, prolongeant celles de $\mathbb{N}$ et vérifiant :

$(\mathbb{Z},+,\cdot)$ est un anneau commutatif intègre

$\{x \in \mathbb{Z};\ 0 \leqslant x\} = \mathbb{N}$

$\forall (a,b,c) \in \mathbb{Z}^3,\ (a \leqslant b \iff a+c \leqslant b+c)$

$\forall (a,b,c,d) \in \mathbb{Z}^4,\ \left(\begin{cases} a \leqslant b \\ c \leqslant d \end{cases} \Longrightarrow a+c \leqslant b+d\right)$

$\forall (a,b,c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{N}^*,\ (a \leqslant b \iff ac \leqslant bc)$

Toute partie non vide et majorée (resp. minorée) de $\mathbb{Z}$ admet un plus grand (resp. petit) élément.

On prolonge à $\mathbb{Z}$ la définition de la divisibilité dans $\mathbb{N}$:

◆ **Définition** Soit $(a,b) \in \mathbb{Z}^2$. On dit que a **divise** b (dans $\mathbb{Z}$) et on note $a|b$ si et seulement s'il existe $c \in \mathbb{Z}$ tel que $b = ac$.

Remarques :

1) $\forall a \in \mathbb{Z},\quad a|0.$

2) $\forall b \in \mathbb{Z},\quad (0|b \iff b = 0).$

3) La relation $|$ est réflexive et transitive dans $\mathbb{Z}$, mais n'est pas antisymétrique puisque, par exemple, $2|(-2)$, $(-2)|2$, $2 \neq -2$. Cependant, on montre facilement :

$$\forall (a,b) \in \mathbb{Z}^2,\quad \left(\begin{cases} a|b \\ b|a \end{cases} \iff (b = a \text{ ou } b = -a)\right).$$

◆ **Théorème-Définition** **(Division euclidienne dans $\mathbb{Z}$)**

Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$. Il existe un couple unique (q,r) de $\mathbb{Z}^2$ tel que : $\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$.

On dit que q (resp. r) est le **quotient** (resp. **reste**) de la division euclidienne de a par b.

Preuve :

1) Existence

Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$. Considérons $E = \{p \in \mathbb{Z};\ a \geqslant bp\}$.

- $E \neq \varnothing$ car : $\begin{cases} \text{si } a \geqslant 0, \text{ alors } 0 \in E \\ \text{si } a < 0, \text{ alors } a \in E. \end{cases}$
- E est majorée car : $\begin{cases} \text{si } a \geqslant 0, \text{ alors } (\forall p \in E, p \leqslant a) \\ \text{si } a < 0, \text{ alors } (\forall p \in E, p \leqslant -a). \end{cases}$

La partie E de $\mathbb{Z}$ étant non vide et majorée admet un plus grand élément, noté q.

Notons $r = a - bq$; déjà : $r \in \mathbb{Z}$.

Puisque $q \in E$, on a $a \geqslant bq$, donc $r \geqslant 0$.

Puisque $q + 1 \notin E$, on a $a < b(q + 1)$, donc $r < b$.

2) Unicité

Soient $(q,r),(q',r')$ dans Z^2 tels que : $\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$ et $\begin{cases} a = bq' + r' \\ 0 \leqslant r' < b. \end{cases}$

Alors $b(q - q') = r' - r$ et $-b < r' - r < b$, d'où $-1 < q - q' < 1$, et donc $q' = q, r' = r$.

3.7 Propriétés de $\mathbb{Q}$

Nous rappelons ici les propriétés usuelles de l'ensemble $\mathbb{Q}$ des **nombres rationnels**, supposées connues. Le lecteur intéressé trouvera une construction de $\mathbb{Q}$ (corps des fractions de l'anneau intègre $\mathbb{Z}$) dans le Cours de J.-M. Arnaudiès et H. Fraysse, Tome 1, pp. 78-80.

L'ensemble $\mathbb{Q}$ est muni d'une addition $+$, d'une multiplication $\cdot$, et d'une relation d'ordre total $\leqslant$, vérifiant :

$\mathbb{Z} \subset \mathbb{Q}$ (en confondant $\frac{a}{1}$ et a, pour $a \in \mathbb{Z}$)

$(\mathbb{Q},+,\cdot)$ est un corps commutatif

$\forall x \in \mathbb{Q}, \exists (p,q) \in \mathbb{Z} \times \mathbb{N}^*, qx = p$ (on note : $x = \frac{p}{q}$)

$\forall (a,b,c) \in \mathbb{Q}^3, (a \leqslant b \iff a + c \leqslant b + c)$

$\forall (a,b,c,d) \in \mathbb{Q}^4, \left(\begin{cases} a \leqslant b \\ c \leqslant d \end{cases} \Longrightarrow a + c \leqslant b + d \right)$

$\forall (a,b,c) \in \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}_+^*, (a \leqslant b \iff ac \leqslant bc)$

en notant $\mathbb{Q}^+ = \{x \in \mathbb{Q}; x \geqslant 0\}$, $\mathbb{Q}_- = \{x \in \mathbb{Q}; x \leqslant 0\}$, $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, $\mathbb{Q}_+^* = \mathbb{Q}_+ - \{0\}$, $\mathbb{Q}_-^* = \mathbb{Q}_- - \{0\}$.

On définit l'application **valeur absolue** $|\cdot| : \mathbb{Q} \longrightarrow \mathbb{Q}$ (qui a déjà été utilisée dans le cadre plus général des nombres réels, cf. Tome 1 ch. 1).

$$x \longmapsto \begin{cases} x \text{ si } 0 \leqslant x \\ -x \text{ si } x \leqslant 0 \end{cases}$$

◆ **Proposition 1** $\mathbb{Q}$ est **archimédien**, c'est-à-dire :

$$\forall \varepsilon \in \mathbb{Q}_+^*, \forall A \in \mathbb{Q}_+^*, \exists N \in \mathbb{N}^*, N\varepsilon > A.$$

Preuve :

Soit $(\varepsilon, A) \in (\mathbb{Q}_+^*)^2$. Il existe $(\alpha,\beta,a,b) \in (\mathbb{N}^*)^4$ tel que : $\varepsilon = \frac{\alpha}{\beta}$ et $A = \frac{a}{b}$.

On a, pour tout N de $\mathbb{N}^*$: $N\varepsilon > A \iff N\alpha b > a\beta$.

Comme $\alpha b \geqslant 1$, il suffit donc de prendre $N = a\beta + 1$.

◆ **Proposition 2** $\mathbb{Q}$ est **dense**, c'est-à-dire :

$$\forall (x,y) \in \mathbb{Q}^2, \quad \big(x < y \Longrightarrow (\exists z \in \mathbb{Q}, x < z < y)\big).$$

Preuve :

Il suffit de prendre $z = \frac{1}{2}(x + y)$.

◆ **Proposition-Définition 3** Pour tout x de $\mathbb{Q}$, il existe un élément n de $\mathbb{Z}$ et un seul tel que $n \leqslant x < n + 1$; cet élément n s'appelle la **partie entière** de x, et est noté $\mathrm{E}(x)$.

Preuve :

Soit $x \in \mathbb{Q}$. En appliquant la Prop. 1 avec $\varepsilon = 1$, on voit que $\{n \in \mathbb{Z}; n \leqslant x\}$ est une partie majorée et non vide de $\mathbb{Z}$, donc admet un plus grand élément. ∎

Nous avions déjà défini plus généralement la partie entière d'un réel (Tome 1, 1.2.3, *3)* Prop-Déf.).

Remarque :

Pour tout (a,b) de $\mathbb{Z} \times \mathbb{N}^*$, la partie entière de $\frac{a}{b}$ est le quotient de la division euclidienne de a par b (cf. 3.6 Th-Déf. p. 94).

Chapitre 4

Arithmétique dans $\mathbb{Z}$

4.1 Divisibilité

4.1.1 Généralités

Rappelons (cf. 3.6 p. 94) :

◆ **Définition** Soit $(a,b) \in \mathbb{Z}^2$. On dit que a **divise** b (**dans** $\mathbb{Z}$), et on note $a|b$ si et seulement s'il existe $c \in \mathbb{Z}$ tel que $b = ac$.

Au lieu de a divise b, on dit aussi : a est **un diviseur de** b, ou : b est **un multiple de** a.

On note $\mathrm{Div}(a)$ l'ensemble des diviseurs de a (pour $a \in \mathbb{Z}$), et $\mathrm{Div}(a_1,\ldots,a_n)$ l'ensemble des diviseurs communs à $a_1,\ldots,a_n$ (pour $n \in \mathbb{N}^*$ et $(a_1,\ldots,a_n) \in \mathbb{Z}^n$) :

$$\mathrm{Div}(a_1,\ldots,a_n) = \{x \in \mathbb{Z};\quad \forall i \in \{1,\ldots,n\},\ x|a_i\}\,.$$

Remarques :

1) $\forall a \in \mathbb{Z},\quad a|0.$

2) $\forall b \in \mathbb{Z},\quad (0|b \iff b = 0).$

3) En notant, pour tout a de $\mathbb{Z}$, $a\mathbb{Z} = \{b \in \mathbb{Z};\ \exists c \in \mathbb{Z},\ b = ac\}$ on a :

$$\forall (a,b) \in \mathbb{Z}^2,\quad (a|b \iff a\mathbb{Z} \supset b\mathbb{Z}).$$

◆ **Proposition 1**

1) $\forall a \in \mathbb{Z},\quad a|a$

2) $\forall (a,b) \in \mathbb{Z}^2,\quad \left(\begin{cases} a|b \\ b|a \end{cases} \iff |a| = |b|\right)$

3) $\forall (a,b,c) \in \mathbb{Z}^3, \left(\begin{cases} a|b \\ b|c \end{cases} \implies a|c\right).$

Preuve :

1) Evident.

2) Supposons $a|b$ et $b|a$. Il existe $(d,e) \in \mathbb{Z}^2$ tel que $b = ad$ et $a = be$, d'où $b = b(de)$.
Si $b = 0$, alors $a = b = 0$.
Si $b \neq 0$, alors $de = 1$, donc $|d| = |e| = 1$, puis $|b| = |a|\,|d| = |a|$.
Réciproquement, si $|b| = |a|$, il existe $\varepsilon \in \{-1,1\}$ tel que $b = \varepsilon a$ (donc $a = \varepsilon b$), d'où $a|b$ et $b|a$.

3) Supposons $a|b$ et $b|c$. Il existe $(d,e) \in \mathbb{Z}^2$ tel que $b = ad$ et $c = be$, d'où $c = a(de)$ et $de \in \mathbb{Z}$, donc $a|c$.

◆ **Proposition 2**

1) $\forall (a,b,c) \in \mathbb{Z}^3, \quad (a|b \Longrightarrow a|bc)$

2) $\forall (a,b,c) \in \mathbb{Z}^3, \quad \left(\begin{cases} a|b \\ a|c \end{cases} \Longrightarrow a \mid b+c\right)$

3) $\forall (a,b,\alpha,\beta) \in \mathbb{Z}^4, \quad \left(\begin{cases} a|b \\ \alpha|\beta \end{cases} \Longrightarrow a\alpha|b\beta\right)$

4) $\forall (a,b,n) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{N}^*, \quad (a|b \Longrightarrow a^n|b^n)$.

Preuve :

1) Si $a|b$, il existe $d \in \mathbb{Z}$ tel que $b = ad$, d'où $bc = a(cd)$ et $cd \in \mathbb{Z}$, donc $a|bc$.

2) Si ($a|b$ et $a|c$), il existe $(d,e) \in \mathbb{Z}^2$ tel que $b = ad$ et $c = ae$, d'où $b + c = a(d+e)$ et $d + e \in \mathbb{Z}$, donc $a \mid b + c$.

3) Si ($a|b$ et $\alpha|\beta$), il existe $(c,\gamma) \in \mathbb{Z}^2$ tel que $b = ac$ et $\beta = \alpha\gamma$, d'où $b\beta = (a\alpha)(c\gamma)$ et $c\gamma \in \mathbb{Z}$, donc $a\alpha|b\beta$.

4) Se déduit de *3)* par récurrence sur n (ou des règles de calcul sur les puissances). ■

Rappelons le théorème de division euclidienne dans $\mathbb{Z}$ (cf. 3.6 p. 94) :

◆ **Théorème - Définition**

Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$. Il existe un couple unique (q,r) de $\mathbb{Z}^2$ tel que :

$$\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases} .$$

On dit que q (resp. r) est le **quotient** (resp. **reste**) de la **division euclidienne** de a par b.

Remarque :

Pour tout (a,b) de $\mathbb{Z} \times \mathbb{N}^*$, a divise b si et seulement si le reste de la division euclidienne de b par a est nul.

4.1.2 Congruences

♦ **Définition** Soient $n \in \mathbb{N}^*$, $(a,b) \in \mathbb{Z}^2$; on dit que a est **congru à b modulo n**, et on note $a \equiv b\ [n]$ (ou : $a \underset{[n]}{\equiv} b$) si et seulement si n divise $b - a$.

Ainsi : $$a \equiv b\ [n] \iff n \mid b - a.$$

♦ **Proposition 1** Pour tout n de $\mathbb{N}^*$, la relation $\equiv\ [n]$ est une relation d'équivalence dans $\mathbb{Z}$.

Preuve :

1) La réflexivité est évidente.

2) On a, pour tout (a,b) de $\mathbb{Z}^2$:

$a \equiv b\ [n] \iff n \mid b - a \iff n \mid a - b \iff b \equiv a\ [n]$, ce qui prouve la symétrie.

3) Pour tout (a,b,c) de $\mathbb{Z}^3$:

$$\begin{cases} a \equiv b\ [n] \\ b \equiv c\ [n] \end{cases} \iff \begin{cases} n \mid b - a \\ n \mid c - b \end{cases} \Longrightarrow n \mid (b-a) + (c-b) \iff n \mid c - a \iff a \equiv c\ [n].$$

♦ **Notation**

Pour tout n de $\mathbb{N}^*$, on note $\mathbb{Z}/_{n\mathbb{Z}}$ au lieu de $\mathbb{Z}/_{\equiv\ [n]}$.

Autrement dit , $\mathbb{Z}/_{n\mathbb{Z}}$ est l'ensemble-quotient de $\mathbb{Z}$ par la relation (d'équivalence) de congruence modulo n.

Pour tout x de $\mathbb{Z}$, on note $\widehat{x}$ (ou $\overline{x}$, ou $\dot{x}$) la classe de x dans $\mathbb{Z}/_{n\mathbb{Z}}$:

$$\widehat{x} = \{y \in \mathbb{Z};\ \ x \equiv y\ [n]\} = \{x + \lambda n;\ \lambda \in \mathbb{Z}\}.$$

On peut aussi noter x mod n la classe de x modulo n.

Il est alors clair (à l'aide de la division euclidienne par n) que $\mathbb{Z}/_{n\mathbb{Z}}$ est un ensemble fini, à n éléments, et que : $\mathbb{Z}/_{n\mathbb{Z}} = \{\widehat{0}, \widehat{1}, \ldots, \widehat{n-1}\}$.

Par exemple, $\mathbb{Z}/_{6\mathbb{Z}} = \{\widehat{0}, \widehat{1}, \widehat{2}, \widehat{3}, \widehat{4}, \widehat{5}\}$.

Afin de diminuer l'ordre de grandeur dans des calculs dans $\mathbb{Z}/_{n\mathbb{Z}}$, il pourra être intéressant de répartir autour de 0 les représentants choisis; par exemple : $\mathbb{Z}/_{6\mathbb{Z}} = \{\widehat{-2}, \widehat{-1}, \widehat{0}, \widehat{1}, \widehat{2}, \widehat{3}\}$.

♦ **Proposition 2**

Soit $n \in \mathbb{N}^*$. On a pour tout (a,b,c,d) de $\mathbb{Z}^4$:

$$\begin{cases} a \equiv b\ [n] \\ c \equiv d\ [n] \end{cases} \Longrightarrow \begin{cases} a + c \equiv b + d\ [n] \\ ac \equiv bd\ [n]. \end{cases}$$

Preuve :

Supposons $a \equiv b\ [n]$ et $c \equiv d\ [n]$. Il existe $(\lambda,\mu) \in \mathbb{Z}^2$ tel que $b-a = \lambda n$ et $d-c = \mu n$. On a :

1) $(b+d)-(a+c) = (b-a)+(d-c) = (\lambda+\mu)n$ et $\lambda+\mu \in \mathbb{Z}$, donc $a+c \equiv b+d\ [n]$.

2) $bd - ac = (a+\lambda n)(c+\mu n) - ac = (\lambda c + a\mu + \lambda\mu n)n$ et $\lambda c + a\mu + \lambda\mu n \in \mathbb{Z}$, donc $ac \equiv bd\ [n]$. ∎

Ainsi, la relation d'équivalence $\equiv [n]$ est *compatible* avec les lois de composition $+$ et $\cdot$ dans $\mathbb{Z}$. ∎

◆ **Corollaire**

$$\forall (a,b) \in \mathbb{Z}^2,\quad \forall k \in \mathbb{N}^*,\quad \Big(a \equiv b\ \ [n] \implies a^k \equiv b^k\ \ [n]\Big).$$ ∎

Soit $n \in \mathbb{N}^*$.

Soit $(\xi,\zeta) \in \left(\mathbb{Z}/_{n\mathbb{Z}}\right)^2$; il existe $(x,y) \in \mathbb{Z}^2$ tel que $\xi = \widehat{x}$ et $\zeta = \widehat{y}$.

Si $(x',y') \in \mathbb{Z}^2$ est un (autre) couple tel que $\xi = \widehat{x'}$ et $\zeta = \widehat{y'}$, alors (cf. Prop. 2) :

$$\widehat{x+y} = \widehat{x'+y'} \quad \text{et} \quad \widehat{xy} = \widehat{x'y'}.$$

On peut donc définir deux lois de composition interne dans $\mathbb{Z}/_{n\mathbb{Z}}$, notées $\widehat{+}$ et $\widehat{\cdot}$, ou encore notées $+$ et $\cdot$, par :

$$\forall (x,y) \in \mathbb{Z}^2,\quad \begin{cases} \widehat{x}+\widehat{y} = \widehat{x+y} \\ \widehat{x}\cdot\widehat{y} = \widehat{xy} \end{cases}.$$

EXEMPLE :

Tables de l'addition et de la multiplication dans $\mathbb{Z}/_{4\mathbb{Z}}$:

$+$	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$
$\widehat{0}$	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$
$\widehat{1}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$	$\widehat{0}$
$\widehat{2}$	$\widehat{2}$	$\widehat{3}$	$\widehat{0}$	$\widehat{1}$
$\widehat{3}$	$\widehat{3}$	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$

$\cdot$	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$
$\widehat{0}$	$\widehat{0}$	$\widehat{0}$	$\widehat{0}$	$\widehat{0}$
$\widehat{1}$	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$
$\widehat{2}$	$\widehat{0}$	$\widehat{2}$	$\widehat{0}$	$\widehat{2}$
$\widehat{3}$	$\widehat{0}$	$\widehat{3}$	$\widehat{2}$	$\widehat{1}$

◆ **Proposition 3**

$\left(\mathbb{Z}/_{n\mathbb{Z}}, +, \cdot\right)$ est un anneau commutatif.

Preuve :

a) 1) $+$ est une loi interne dans $\mathbb{Z}/_{n\mathbb{Z}}$.

2) $\forall (a,b,c) \in \mathbb{Z}^3$, $(\widehat{a}+\widehat{b})+\widehat{c} = \widehat{a+b}+\widehat{c} = (a+\widehat{b})+c = a+\widehat{(b+c)} = \widehat{a}+\widehat{b+c} = \widehat{a}+(\widehat{b}+\widehat{c})$, donc $+$ est associative.

3) $\forall (a,b) \in \mathbb{Z}^2$, $\widehat{a}+\widehat{b} = \widehat{a+b} = \widehat{b+a} = \widehat{b}+\widehat{a}$, donc $+$ est commutative.

4) $\forall a \in \mathbb{Z}$, $\widehat{a}+\widehat{0} = \widehat{a+0} = \widehat{a}$, donc $\widehat{0}$ est neutre pour $+$.

5) $\forall a \in \mathbb{Z}$, $\widehat{a}+\widehat{(-a)} = \widehat{a+(-a)} = \widehat{0}$, donc tout élément de $\mathbb{Z}/_{n\mathbb{Z}}$ admet un opposé.

Ainsi, $(\mathbb{Z}/_{n\mathbb{Z}},+)$ est un groupe abélien.

b) 1) $\cdot$ est une loi interne dans $\mathbb{Z}/_{n\mathbb{Z}}$.

2) $\forall (a,b,c) \in \mathbb{Z}^3$, $(\widehat{ab})\widehat{c} = \widehat{(ab)c} = \widehat{a(bc)} = \widehat{a}(\widehat{bc}) = \widehat{a}(\widehat{bc})$, donc $\cdot$ est associative.

3) $\forall (a,b) \in \mathbb{Z}^2$, $\widehat{ab} = \widehat{ab} = \widehat{ba} = \widehat{ba}$, donc $\cdot$ est commutative.

4) $\forall a \in \mathbb{Z}$, $\widehat{a}\widehat{1} = \widehat{a1} = \widehat{a}$, donc $\widehat{1}$ est neutre pour $\cdot$

5) $\forall (a,b,c) \in \mathbb{Z}^3$, $\widehat{a}(\widehat{b}+\widehat{c}) = \widehat{a}(\widehat{b+c}) = \widehat{a(b+c)} = \widehat{ab+ac} = \widehat{ab}+\widehat{ac} = \widehat{a}\,\widehat{b}+\widehat{a}\,\widehat{c}$, donc $\cdot$ est distributive sur $+$.

Remarque :

Le groupe $(\mathbb{Z}/_{n\mathbb{Z}},+)$ est cyclique, engendré par $\widehat{1}$ puisque, pour tout a de $\mathbb{Z}$:

$$\widehat{a} = \begin{cases} \widehat{1}+\ldots+\widehat{1} \quad (a \text{ termes}) & \text{si } a \geqslant 1 \\ \widehat{0} & \text{si } a = 0 \\ -\widehat{1}-\ldots-\widehat{1} \quad (-a \text{ termes}) & \text{si } a \leqslant -1. \end{cases}$$

Exercices

◇ **4.1.1** Soit $n \in \mathbb{Z}$. Montrer :

$$\begin{cases} n^2 \equiv 0 \ [8] \quad \text{ou} \quad n^2 \equiv 4 \ [8], & \text{si } n \text{ est pair} \\ n^2 \equiv 1 \ [8] & \text{si } n \text{ est impair.} \end{cases}$$

◇ **4.1.2** Montrer : $\forall n \in \mathbb{N}-\{0,1\}$, $2^n \mid 5^{2^{n-2}}-1$ et $2^{n+1} \nmid 5^{2^{n-2}}-1$.

◇ **4.1.3** Montrer que, pout tout n de $\mathbb{N}^*$, $\displaystyle\sum_{k=1}^{2n} \frac{(2n)!}{k}$ est un entier divisible par $2n+1$.

◇ **4.1.4** Etablir : $\forall n \in \mathbb{N}^*$, $40^n \cdot n! \mid (5n)!$.

◇ **4.1.5** Montrer que le seul n de $\mathbb{N}-\{0,1\}$ tel que $2n-1$ divise $(3n^2-3n+1)(3n^2-3n+2)$ est 3.

◇ **4.1.6** Soit $n \in \mathbb{N}$ tel que $n \geqslant 4$; montrer qu'il existe $k \in \mathbb{N}$ tel que :

$$n! < k < (n+1)! \quad \text{et} \quad n^3 | k.$$

◇ **4.1.7** Soit $(a,b,c,d) \in \mathbb{Z}^4$ tel que $ad+bc \neq 0$. On suppose que $ad+bc$ divise $a.b,c,d$. Montrer:

$$ad + bc \in \{-1,1\}.$$

◇ **4.1.8** Montrer que, pour tout n de $\mathbb{N}$, $\left(3+\sqrt{5}\right)^n + \left(3-\sqrt{5}\right)^n$ est un entier divisible par 2^n.

◇ **4.1.9** Trouver les n de $\mathbb{Z}$ tels que :

a) $3n+4 \mid 11n+8$ *b)* $n^2+3n-2 \mid n^2-6$.

◇ **4.1.10** Etablir : $\forall (a,b,c) \in \mathbb{Z}^3, \quad a+b+c \mid a^3+b^3+c^3-3abc$.

◇ **4.1.11** On note d: $\mathbb{N}^* \longrightarrow \mathbb{N}^*$ l'application qui, à chaque n de $\mathbb{N}^*$, associe le nombre de diviseurs ($\geqslant 1$) de n. Montrer : $\forall a \in \mathbb{N}-\{0,1\}, \quad \forall n \in \mathbb{N}^*, \quad \mathrm{d}(a^n-1) \geqslant \mathrm{d}(n)$.

◇ **4.1.12** Soient $n \in \mathbb{N}^*$, $1 = d_1 < d_2 < \ldots < d_k = n$ les diviseurs $\geqslant 1$ de n; montrer :

$$\left(\prod_{i=1}^{k} d_i\right)^2 = n^k.$$

◇ **4.1.13** **Exemples d'équation diophantiennes.**

Résoudre les équations suivantes, dans l'ensemble indiqué :

a) $xy = 2x+3y, \quad \mathbb{Z}^2$

b) $x^2-y^2-x+3y = 30, \quad \mathbb{Z}^2$

c) $\dfrac{1}{x}+\dfrac{1}{y}=\dfrac{1}{5}, \quad (\mathbb{Z}^*)^2$

d) $x^2-3xy+2y^2+x-3y-6=0, \quad \mathbb{Z}^2$

e) $2x^3+xy-7=0, \quad \mathbb{Z}^2$

f) $x^3+xy+y^3=209, \quad \mathbb{N}^2$

g) $x(x+1)(x+7)(x+8)=y^2, \quad \mathbb{Z}^2$

h) $x^2=9y^2-39y+40, \quad \mathbb{Z}^2$

i) $\begin{cases} x^3-y^3-z^3=3xyz \\ x^2=2(y+z) \end{cases}, \quad \mathbb{N}^3$

j) $\begin{cases} z^2=x^2+y^2 \\ xy=2(x+y+z) \end{cases}, \quad (\mathbb{N}^*)^3$

k) $3^x = 8+y^2, \quad \mathbb{N}^2$.

◇ **4.1.14** Montrer, pour tout n de $\mathbb{N}$:

a) $5 \mid 2^{2n+1}+3^{2n+1}$

b) $9 \mid 4^n-1-3n$

c) $11 \mid 3^{n+3}-4^{4n+2}$

d) $16 \mid 5^n-1-4n$

e) $17 \mid 2^{6n+3}+3^{4n+2}$

f) $17 \mid 2^{7n+1}+3^{2n+1}+5^{10n+1}+7^{6n+1}$

g) $18 \mid 2^{2n+2}+24n+14$

h) $19 \mid 2^{3n+4}+3^{2n+1}$

i) $19 \mid 2^{2^{6n+2}}+3$

j) $21 \mid 2^{4^{n+1}}+5$

k) $25 \mid 2^{n+2}3^n+5n-4$

l) $29 \mid 2^{5n+1}+3^{n+3}$

m) $31 \mid 2^{4n+1}+3^{6n+9}$

n) $32 \mid 8n^2+4n-3(5^n-1)$

o) $33 \mid 5^{2n+1}+11^{2n+1}+17^{2n+1}$

p) $41 \mid 5 \cdot 7^{2n+2}+2^{3n}$

q) $73 \mid 9^{2n+1}+8^{n+2}$

r) $111 \mid 10^{6n}+10^{3n}-2$

s) $288 \mid 7^{2n+1}-48n-7$

t) $2304 \mid 7^{2n}-2352n-1$

u) $2^{12} \mid 3 \cdot 81^{n+1}+(16n-54)9^{n+1}-320n^2-144n+243$.

◇ **4.1.15** Soient $a \in \mathbb{Z}$ impair et $n \in \mathbb{N}$ tel que $n \geqslant 3$. Etablir : $a^{2^{n-2}} \equiv 1 \quad [2^n]$.

◇ **4.1.16** Montrer : $\forall (a,b,c) \in \mathbb{Z}^3, \quad \left(7 \mid a^3 + b^3 + c^3 \Longrightarrow 7 \mid abc\right)$.

◇ **4.1.17** Trouver tous les n de $\mathbb{Z}$ tels que : $10 \mid n^2 + (n+1)^2 + (n+3)^2$.

◇ **4.1.18** Pour quels n de $\mathbb{N}$ a-t-on : $8 \mid 3^n + 4n + 1$?

◇ **4.1.19** Trouver tous les n de $\mathbb{N}$ tels que :

a) $21 \mid 2^{2n} + 2^n + 1$ *b)* $7 \mid 2^{2^n} + 2^n + 1$.

◇ **4.1.20** Montrer : $\forall n \in \mathbb{N} - \{0,1\}, \quad 2^n \not\mid 3^n + 1$.

◇ **4.1.21** Montrer : $\forall (a,b) \in \mathbb{N}^2, \quad 23 \not\mid 2^a + 3^b$.

◇ **4.1.22** **Exemples d'équations diophantiennes.**

Montrer que les équations suivantes n'ont pas de solution dans l'ensemble indiqué :

a) $x^2 + 5y^2 = 3, \quad \mathbb{Z}^2$ *b)* $x^2 - 5y^2 = 3, \quad \mathbb{Z}^2$

c) $15x^2 - 7x^2 = 9, \quad \mathbb{Z}^2$ *d)* $x^2 + y^2 - 8z - 6 = 0, \quad \mathbb{Z}^3$

e) $x^3 - 3y^3 + 6y^2 - 16x + 8 = 0, \quad \mathbb{Z}^2$ *f)* $x^3 + 11^3 = y^3, \quad \mathbb{N}^{*2}$.

◇ **4.1.23** Trouver tous les (x,y,z) de $(\mathbb{N}^*)^3$ tels que :

$$\begin{cases} x + y \equiv 1 \quad [z] \\ y + z \equiv 1 \quad [x] \\ z + x \equiv 1 \quad [y]. \end{cases}$$

◇ **4.1.24** Montrer, pour tout n de $\mathbb{Z}$ impair : $n^4 \equiv 1[16]$. (Utiliser l'exercice 4.1.1. p. 103).

◇ **4.1.25** Quel est le dernier chiffre de $\sum_{k=1}^{10} k^{100}$ écrit en base 10?

◇ **4.1.26** Montrer, pour tout n de $\mathbb{N}^*$: $5 \mid 1^n + 2^n + 3^n + 4^n \Longleftrightarrow 4 \not\mid n$.

◇ **4.1.27** Soit $(a,b) \in \mathbb{N}^2$ tel que $a \geqslant 4b$. Montrer :

$$3^a + 1 \equiv 0 \quad [10] \quad \Longrightarrow \quad \begin{cases} 3^{a+4b} + 1 \equiv 0 \quad [10] \\ 3^{a-4b} + 1 \equiv 0 \quad [10]. \end{cases}$$

◇ **4.1.28** Soit $(\phi_n)_{n\in\mathbb{N}}$ la **suite de Fibonacci** :

$$\phi_0 = 0, \phi_1 = 1, \quad \forall n \in \mathbb{N} \quad \phi_{n+2} = \phi_{n+1} + \phi_n.$$

Montrer, pour tout n de $\mathbb{N}$:

a) $2|\phi_n \Longleftrightarrow 3|n$

b) $3|\phi_n \Longleftrightarrow 4|n$

c) $4|\phi_n \Longleftrightarrow 6|n$.

◇ **4.1.29** **Nombres de Fermat**

On note, pour $n \in \mathbb{N}^*$, $F_n = 2^{2^n} + 1$ (appelé $n^{\text{ème}}$ **nombre de Fermat**). Montrer :

$$\forall n \in \mathbb{N}^*, \quad F_n \mid 2^{F_n} - 2.$$

Les exercices 4.1.30 *à* 4.1.32 *utilisent l'arithmétique pour l'étude de groupes monogènes.*

◇ **4.1.30*** Montrer que les sous-groupes de $(\mathbb{Z}, +)$ sont les $k\mathbb{Z}$, $k \in \mathbb{N}$.

◇ **4.1.31** Déterminer les sous-groupes de $\left(\mathbb{Z}/_{n\mathbb{Z}}, +\right)$, $n \in \mathbb{N}^*$ (utiliser l'exercice 4.1.30).

◇ **4.1.32** Soit $(G, \cdot)$ un groupe monogène. Montrer :

$$\begin{cases} G \simeq \mathbb{Z} & \text{si } G \text{ est infini} \\ G \simeq \mathbb{Z}/_{n\mathbb{Z}} & \text{si } G \text{ est fini et } n = \text{Card}(G) \end{cases}$$

(utiliser l'exercice 4.1.30.)

◇ **4.1.33** Montrer, pour tout (x, y) de $\mathbb{Z}^2$: $17 \mid 2x + 3y \iff 17 \mid 9x + 5y$.

◇ **4.1.34** Résoudre :

a) $x^2 + x + \widehat{7} = \widehat{0}$ dans $\mathbb{Z}/_{13\mathbb{Z}}$

b) $x^2 - \widehat{4}x + \widehat{3} = \widehat{0}$ dans $\mathbb{Z}/_{12\mathbb{Z}}$.

◇ **4.1.35** Etant donné cinq entier relatifs, montrer qu'on peut en choisir trois dont la somme est divisible par 3.

◇ **4.1.36** Soit $n \in \mathbb{N}^*$. De combien de façons 2^n peut-il être décomposé en somme de quatre carrés d'entiers naturels?

◇ **4.1.37*** Soient $n \in \mathbb{N}^*$, et $a_0, \ldots, a_n \in \{1, \ldots, 2n\}$ deux à deux distincts. Montrer qu'il existe $(i, j) \in \{1, \ldots, n\}^2$ tel que : $i \neq j$ et $a_i | a_j$.

◇ **4.1.38*** Pour $n \in \mathbb{N}^*$, on note $\delta(n)$ le plus grand diviseur impair de n, $S(n) = \sum_{k=1}^{n} \frac{\delta(k)}{k}$, $F(n) = S(n) - \frac{2n}{3}$.

a) Vérifier : $\forall n \in \mathbb{N}^*$, $\begin{cases} \delta(2n+1) = 2n+1 \\ \delta(2n) = \delta(n) \end{cases}$

b) En déduire : $\forall n \in \mathbb{N}^*$, $\begin{cases} S(2n+1) = S(2n) + 1 \\ S(2n) = \frac{1}{2} S(n) + n. \end{cases}$

c) Etablir : $\forall n \in \mathbb{N}^*$, $0 < F(n) < \frac{2}{3}$.

4.2 pgcd, ppcm

4.2.1 Généralités

♦ **Proposition - Définition**

Soient $n \in \mathbb{N}^*$, $(x_1,\ldots,x_n) \in (\mathbb{Z}^*)^n$.

1) L'ensemble des diviseurs communs à $x_1,\ldots,x_n$ est fini et admet un plus grand élément (pour l'ordre $\leqslant$ usuel), appellé **plus grand commun diviseur** de $x_1,\ldots,x_n$ et noté pgcd $(x_1,\ldots,x_n)$, ou pgcd $\left((xi)_{1\leqslant i\leqslant n}\right)$.

2) L'ensemble des éléments de $\mathbb{N}^*$ multiples communs de $x_1,\ldots,x_n$ admet un plus petit élément (pour l'ordre $\leqslant$ usuel), appelé **plus petit commun multiple** de $x_1,\ldots,x_n$ et noté ppcm $(x_1,\ldots,x_n)$, ou ppcm $\left((x_i)_{1\leqslant i\leqslant n}\right)$.

Preuve :

1) L'ensemble $\mathrm{Div}(x_1,\ldots,x_n)$ des diviseurs communs à $x_1,\ldots,x_n$ est une partie finie de $\mathbb{Z}$ (car incluse dans $\{k \in \mathbb{Z};\quad |k| \leqslant |x_1|\}$, non vide (car elle contient 1), donc admet un plus grand élément.

2) L'ensemble des éléments de $\mathbb{N}^*$ multiples communs de $x_1,\ldots,x_n$ est une partie non vide de $\mathbb{N}^*$ (car elle contient $\left|\prod_{i=1}^{n} x_i\right|$), donc admet un plus petit élément. ■

En notant $\delta = \text{pgcd}\,(x_1,\ldots,x_n)$, $\mu = \text{ppcm}\,(x_1,\ldots,x_n)$, on a, par définition :

$$\begin{cases} \forall k \in \mathbb{Z}, & \left((\forall i \in \{1,\ldots,n\},\quad k \mid x_i) \Longrightarrow |k| \leqslant \delta\right) \\ \forall k \in \mathbb{N}^*, & \left((\forall i \in \{1,\ldots,n\},\quad x_i \mid k) \Longrightarrow \mu \leqslant k\right). \end{cases}$$

Remarque : Il est clair que :

$$\forall (x_1,\ldots,x_n) \in (\mathbb{Z}^*)^n,\quad \begin{cases} \text{pgcd}\,(x_1,\ldots,x_n) = \text{pgcd}\,(|x_1|,\ldots,|x_n|) \\ \text{ppcm}\,(x_1,\ldots,x_n) = \text{ppcm}\,(|x_1|,\ldots,|x_n|)\,. \end{cases}$$

4.2.2 Propriétés

♦ **Proposition 1** Soient $n \in \mathbb{N}^*$, $(x_1,\ldots,x_n) \in \left(\mathbb{Z}^*\right)^n$, $\delta = \text{pgcd}\,(x_1,\ldots,x_n)$, $\mu = \text{ppcm}\,(x_1,\ldots,x_n)$. On a :

$$\delta\mathbb{Z} = \sum_{i=1}^{n} x_i\mathbb{Z} \quad \text{et} \quad \mu\mathbb{Z} = \bigcap_{i=1}^{n} x_i\mathbb{Z}.$$

Preuve :

1) a) Soit $x \in \sum_{i=1}^{n} x_i\mathbb{Z}$; il existe $(u_1,\ldots,u_n) \in \mathbb{Z}^n$ tel que $x = \sum_{i=1}^{n} x_i u_i$. Comme $(\forall i \in \{1,\ldots,n\},\quad \delta | x_i)$, on déduit (cf. 4.1.1 Prop. 2 p. 100) $\delta | x$, c'est-à-dire $x \in \delta\mathbb{Z}$.

Ceci montre : $\sum_{i=1}^{n} x_i\mathbb{Z} \subset \delta\mathbb{Z}$.

b) $\left(\sum_{i=1}^{n} x_i\mathbb{Z}\right) \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}^*$ (elle contient $|x_1|$), donc admet un plus petit élément noté d. Comme $d \in \sum_{i=1}^{n} x_i\mathbb{Z}$, il est clair que $d\mathbb{Z} \subset \sum_{i=1}^{n} x_i\mathbb{Z}$.

Soit $x \in \sum_{i=1}^{n} x_i\mathbb{Z}$. Par division euclidienne de x par d, il existe $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$x = dq + r \quad \text{et} \quad 0 \leqslant r < d.$$

Comme x et d sont dans $\sum_{i=1}^{n} x_i\mathbb{Z}$, et que $\sum_{i=1}^{n} x_i\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$, on déduit $r = x - qd \in \sum_{i=1}^{n} x_i\mathbb{Z}$.

Mais $0 \leqslant r < d$, d'où, par définition de d, $r = 0$, $x = dq \in d\mathbb{Z}$ et donc $\sum_{i=1}^{n} x_i\mathbb{Z} \subset d\mathbb{Z}$.

c) On a montré ainsi : $d\mathbb{Z} = \sum_{i=1}^{n} x_i\mathbb{Z} \subset \delta\mathbb{Z}$. Il existe donc $e \in \mathbb{Z}$ tel que $d = \delta e$, et clairement $e \in \mathbb{N}^*$. Comme d et δ divisent $x_1,\ldots,x_n$ et sont dans $\mathbb{N}^*$, par définition de δ, on a : $d \leqslant \delta$, et donc $e = 1$, $d = \delta$.

Finalement : $\sum_{i=1}^{n} x_i\mathbb{Z} = d\mathbb{Z} = \delta\mathbb{Z}$.

2) a) $(\forall i \in \{1,\ldots,n\},\ x_i|\mu) \Longrightarrow (\forall i \in \{1,\ldots,n\}, x_i\mathbb{Z} \supset \mu\mathbb{Z}) \Longrightarrow \bigcap_{i=1}^{n} x_i\mathbb{Z} \supset \mu\mathbb{Z}$.

b) En raisonnant comme *1) b)* ci-dessus (ou encore : cf. exercice 4.1.30 p. 106), on montre qu'il existe $m \in \mathbb{N}^*$ tel que : $\bigcap_{i=1}^{n} x_i\mathbb{Z} = m\mathbb{Z}$. Alors $\mu\mathbb{Z} \subset m\mathbb{Z}$; il existe donc $f \in \mathbb{N}^*$ tel que $\mu = mf$. Comme m et μ sont des multiples communs à $x_1,\ldots,x_n$ et sont dans $\mathbb{N}^*$, par définition de μ, on a $\mu \leqslant m$, et ainsi $f = 1$, $m = \mu$.

Finalement : $\bigcap_{i=1}^{n} x_i\mathbb{Z} = m\mathbb{Z} = \mu\mathbb{Z}$.

◆ **Proposition 2**

$$\forall n \in \mathbb{N}^*,\ \forall \lambda \in \mathbb{Z}^*,\ \forall (x_1,\ldots,x_n) \in (\mathbb{Z}^*)^n,$$

$$\begin{cases} \text{pgcd}\,(\lambda x_1,\ldots,\lambda x_n) = |\lambda|\text{pgcd}\,(x_1,\ldots,x_n) \\ \text{ppcm}\,(\lambda x_1,\ldots,\lambda x_n) = |\lambda|\text{ppcm}\,(x_1,\ldots,x_n). \end{cases}$$

Preuve :

En notant $\delta = \text{pgcd}\,(x_1,\ldots,x_n)$, $\mu = \text{ppcm}\,(x_1,\ldots,x_n)$, on a :

$$\begin{cases} \sum_{i=1}^{n}(\lambda x_i)\mathbb{Z} = \lambda \sum_{i=1}^{n} x_i\mathbb{Z} = \lambda(\delta\mathbb{Z}) = (\lambda\delta)\mathbb{Z} \\ \bigcap_{i=1}^{n}(\lambda x_i)\mathbb{Z} = \lambda \bigcap_{i=1}^{n} x_i\mathbb{Z} = \lambda(\mu\mathbb{Z}) = (\lambda\mu)\mathbb{Z}, \end{cases}$$

d'où :

$$\begin{cases} \text{pgcd}\,(\lambda x_1,\ldots,\lambda x_n) = |\lambda\delta| = |\lambda|\delta \\ \text{ppcm}\,(\lambda x_1,\ldots,\lambda x_n) = |\lambda\mu| = |\lambda|\mu. \end{cases}$$

♦ **Proposition 3** Soient $n \in \mathbb{N}^*$, $(x_1,\ldots,x_n) \in (\mathbb{Z}^*)^n$, $\delta = \text{pgcd}\,(x_1,\ldots,x_n)$, $\mu = \text{ppcm}(x_1,\ldots,x_n)$, $(a,b) \in (\mathbb{Z}^*)^2$. On a :

1) $(\forall i \in \{1,\ldots,n\},\quad a|x_i) \iff a|\delta$

2) $(\forall i \in \{1,\ldots,n\},\quad x_i|b) \iff \mu|b.$

Preuve :

1) $(\forall i \in \{1,\ldots,n\},\ a|x_i) \iff (\forall i \in \{1,\ldots,n\},\ a\mathbb{Z} \supset x_i\mathbb{Z}) \iff \left(a\mathbb{Z} \supset \sum_{i=1}^{n} x_i\mathbb{Z}\right)$

$$\iff a\mathbb{Z} \supset \delta\mathbb{Z} \iff a|\delta.$$

2) $(\forall i \in \{1,\ldots,n\}, x_i|b) \iff (\forall i \in \{1,\ldots,n\},\ x_i\mathbb{Z} \supset b\mathbb{Z}) \iff \left(\bigcap_{i=1}^{n} x_i\mathbb{Z} \supset b\mathbb{Z}\right)$

$$\iff \mu\mathbb{Z} \supset b\mathbb{Z} \iff \mu|b.$$

♦ **Proposition 4** **(Associativité du pgcd et du ppcm)**

Soient $n \in \mathbb{N}^*$, P une partition de $\{1,\ldots,n\}$, $(x_1,\ldots,x_n) \in (\mathbb{Z}^*)^n$. On a :

$$\begin{cases} \text{pgcd}\,(x_1,\ldots,x_n) = \text{pgcd}\,\left((\text{pgcd}\,((x_i)_{i\in I}))_{I\in P}\right) \\ \text{ppcm}\,(x_1,\ldots,x_n) = \text{ppcm}\,\left((\text{ppcm}\,((x_i)_{i\in I}))_{I\in P}\right). \end{cases}$$

Preuve :

1) Par associativité et commutativité de l'addition dans $\mathbb{Z}$, on voit que :

$$\sum_{i=1}^{n} x_i\mathbb{Z} = \sum_{I\in P}\left(\sum_{i\in I} x_i\mathbb{Z}\right) = \sum_{I\in P} (\text{pgcd}\,(x_i)_{i\in I})\,\mathbb{Z}.$$

2) De même, par associativité et commutativité de l'intersection dans $\mathfrak{P}(\mathbb{Z})$:

$$\bigcap_{i=1}^{n} x_i\mathbb{Z} = \bigcap_{I\in P}\left(\bigcap_{i\in I} x_i\mathbb{Z}\right) = \bigcap_{I\in P} (\text{ppcm}\,(x_i)_{i\in I})\,\mathbb{Z}. \qquad \blacksquare$$

La Prop. précédente montre qu'on peut exprimer le pgcd (resp. ppcm) de plusieurs nombres en ne faisant intervenir que des pgcd (resp. ppcm) de deux nombres. Par exemple :

$$\text{pgcd}\,(x_1,x_2,x_3) = \text{pgcd}\,\left(\text{pgcd}\,(x_1,x_2),x_3\right),$$
$$\text{ppcm}\,(x_1,x_2,x_3,x_4) = \text{ppcm}\,\left(\text{ppcm}\,(x_1,x_2),\ \text{ppcm}\,(x_3,x_4)\right).$$

◆ **Notation**

Pour $(a,b) \in (\mathbb{Z}^*)^2$, on note $\begin{cases} a \wedge b = \text{pgcd}\,(a,b) \\ a \vee b = \text{ppcm}\,(a,b) \end{cases}$.

Remarques :

1) Le lecteur pourra trouver dans d'autres ouvrages (Cours de J.-M. Arnaudiès et H. Fraysse, Tome 1, pp. 127 et 128) des notations renversées par rapport à celles proposées ici : $\vee$ pour le pgcd, $\wedge$ pour le ppcm.

2) $\wedge$ et $\vee$ sont des lois de composition interne dans $\mathbb{Z}^*$, associatives et commutatives (cf. Prop. 4 p. 109). De plus : $\forall a \in \mathbb{Z}^*$, $(a_\wedge a = a_\vee a = |a|,\quad a_\wedge 1 = 1,\quad a_\vee 1 = |a|)$.

Nous verrons plus loin :

- $\wedge$ et $\vee$ sont distributives l'une sur l'autre (4.4.3 Cor. p. 125)
- $\forall (a,b) \in (\mathbb{Z}^*)^2, \forall k \in \mathbb{N}^*,\ a^k \wedge b^k = (a \wedge b)^k$ (4.3.3 Cor. p. 116).

4.2.3 Algorithme d'Euclide

Soit $(a,b) \in \mathbb{N}^2$ tel que $a \geqslant b$. Nous allons construire un algorithme permettant de calculer $a_\wedge b$.

Si $b|a$, alors $a_\wedge b = b$.

Supposons $b \nmid a$. Par division euclidienne de a par b, il existe $(q_1,r_1) \in \mathbb{N}^2$ tel que :

$$\begin{cases} a = bq_1 + r_1 \\ 0 < r_1 < b \end{cases}.$$

Montrons : $a_\wedge b = b_\wedge r_1$.

Pour tout c de $\mathbb{Z}$:

- si ($c|a$ et $c|b$), alors ($c|b$ et $c|r_1$) car $r_1 = a - bq_1$
- si ($c|b$ et $c|r_1$), alors ($c|b$ et $c|a$) car $a = bq_1 + r_1$.

Ceci montre $\text{Div}(a,b) = \text{Div}(b,r_1)$, et donc $a_\wedge b = b_\wedge r_1$.

Si $r_1|b$, alors $a_\wedge b = b_\wedge r_1 = r_1$.

Si $r_1 \nmid b$, on réitére.

On construit ainsi les couples (q_1,r_1), (q_2,r_2),... tels que :

$$\begin{cases} a = bq_1 + r_1 \\ 0 < r_1 < b \end{cases}, \quad \begin{cases} b = r_1q_2 + r_2 \\ 0 < r_2 < r_1 \end{cases}, \ldots$$

Comme $b > r_1 > r_2 \ldots$ et que $b,r_1,r_2,\ldots$ sont dans $\mathbb{N}^*$, le procédé s'arrête au bout d'un nombre fini d'étapes. Il existe donc $N \in \mathbb{N}^*$, $(q_1,r_1),\ldots,(q_N,r_N)$ dans $\mathbb{N}^2$ tels que :

$$\begin{cases} a = bq_1 + r_1 \\ 0 < r_1 < b \end{cases}, \quad \begin{cases} b = r_1q_2 + r_2 \\ 0 < r_2 < r_1 \end{cases}, \ldots \quad \begin{cases} r_{N-2} = r_{N-1}q_N + r_N \\ 0 < r_N < r_{N-1} \end{cases}, \quad r_N | r_{N-1}.$$

On a alors : $a_\wedge b = b_\wedge r_1 = r_1 \wedge r_2 = \ldots = r_{N-1} \wedge r_N = r_N$.

En pratique, on effectue des divisions euclidiennes successives, et le pgcd de a et b est le dernier reste à être non nul. On peut adopter la disposition pratique suivante (pour des calculs «à la main») :

	q_1	q_2	q_3	...	q_N	(q_{N+1})
a	b	r_1	r_2		r_{N-1}	r_N
r_1	r_2	r_3	...		0	

EXEMPLE :

Calculer $9\,100 \wedge 1\,848$.

	4	1	12	5
9 100	1 848	1 708	140	28
1 708	140	28	0	

$9\,100 \wedge 1\,848 = 28$.

Exercices

◇ **4.2.1** Montrer, pour tout n de $\mathbb{N}^*$:

a) $(n^2+n) \wedge (2n+1) = 1$ *b)* $(n^3+2n) \wedge (n^4+3n^2+1) = 1$

c) $(n^2+1) \wedge ((n+1)^2+1) \in \{1,5\}$.

◇ **4.2.2** Calculer pgcd $\{16^n + 10^n - 1;\ n \in \mathbb{N}^*\}$, c'est-à-dire le plus grand entier $\delta \geqslant 1$ tel que :

$$\forall n \in \mathbb{N}^*, \quad \delta \mid 16^n + 10^n - 1.$$

◇ **4.2.3** Soit $(a,b) \in (\mathbb{N}^*)^2$. On effectue l'algorithme d'Euclide :

$$r_0 = a, \quad r_1 = b, \quad \begin{cases} r_0 = r_1 q_1 + r_2 \\ 0 < r_2 < r_1 \end{cases}, \ldots, \quad \begin{cases} r_{n-2} = r_{n-1} q_{n-1} + r_n \\ 0 < r_n < r_{n-1} \end{cases}, \quad r_{n-1} = r_n q_n,$$

tous entiers naturels.

Montrer : *a)* $\displaystyle\sum_{i=1}^{n} r_i q_i = a + b - (a \wedge b)$ *b)* $\displaystyle\sum_{i=1}^{n} r_i^2 q_i = ab$.

◇ **4.2.4 Eléments d'ordre fini d'un groupe.**

Soit $(G,\cdot)$ un groupe de neutre noté e. Un élément x de G est dit **d'ordre fini** si et seulement s'il existe $n \in \mathbb{N}^*$ tel que $x^n = e$.

a) Montrer que, si $x \in G$ est d'ordre fini, alors il existe un unique élément de $\mathbb{N}^*$, noté $\omega(x)$, tel que : $\begin{cases} x^{\omega(x)} = e \\ \forall k \in \mathbb{N}^*,\ (k < \omega(x) \Longrightarrow x^k \neq e). \end{cases}$

Ainsi, $\omega(x)$ est le plus petit entier $\geqslant 1$ tel que $x^{\omega(x)} = e$.

L'élément $\omega(x)$ de $\mathbb{N}^*$ est appelé l'**ordre** de x (dans G).

b) α) Montrer que, si G est fini, tout élément de G est d'ordre fini et : $\forall x \in G,\quad \omega(x) | \mathrm{Card}(G)$.

(Utiliser le théorème de Lagrange, C 2.1 p. 63).

β) Si tout élément de G est d'ordre fini, peut-on déduire que G soit fini?

c) Montrer que, si $x \in G$ est d'ordre fini, alors : $\{n \in \mathbb{N}^*,\ x^n = e\} = \omega(x)\mathbb{N}^*$.

d) α) Etablir que, si deux éléments x, y de G sont d'ordres finis et commutent, alors xy est d'ordre fini et : $\omega(xy) | \omega(x) \vee \omega(y)$.

A-t-on nécessairement $\omega(xy) = \omega(x) \vee \omega(y)$?

β) Donner un exemple d'un groupe $(G,\cdot)$ et de deux éléments (x,y) de G d'ordres finis tels que xy ne soit pas d'ordre fini.

◇ **4.2.5** Soient $n \in \mathbb{N}^*$, $N \in \mathbb{N}$ un entier impair, $\sigma \in \mathfrak{S}_n$ telle que $\sigma^N = e$. Démontrer que σ est paire. (Utiliser la décomposition de σ en produit de cycles à supports deux à deux disjoints, cf. 3.4.3 Th. p. 88, et l'ordre d'un élément d'un groupe fini, exercice 4.2.4 p. 111).

◇ **4.2.6** Soient $n \in \mathbb{N} - \{0,1\}$, $\sigma \in \mathfrak{S}_n$, $\sigma = c_1 \circ \ldots \circ c_v$ la décomposition de σ en un produit de cycles à supports deux à deux disjoints (cf. 3.4.3 Th. p. 88). Montrer que l'ordre de σ est le ppcm des ordres des cycles $c_1, \ldots, c_v$ (cf. exercice 4.2.4 p. 111).

Exemple : Quel est l'ordre de

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 7 & 8 & 1 & 6 & 5 & 12 & 3 & 10 & 9 & 11 & 2 & 4 \end{pmatrix} \quad \text{dans } \mathfrak{S}_{12} ?$$

4.3 Nombres premiers entre eux

4.3.1 Généralités

◆ **Définition** Soient $n \in \mathbb{N}^*$, $(x_1,\ldots,x_n) \in (\mathbb{Z}^*)^n$.

1) On dit que $x_1,\ldots,x_n$ sont **premiers entre eux dans leur ensemble** (ou : **étrangers**) si et seulement si : $\operatorname{pgcd}(x_1,\ldots,x_n) = 1$.

2) On dit que $x_1,\ldots,x_n$ sont **premiers entre eux deux à deux** si et seulement si : $\forall (i,j) \in \{1,\ldots,n\}^2, \quad (i \neq j \Longrightarrow x_i \wedge x_j = 1)$.

Remarque :

1) Si $x_1,\ldots,x_n$ sont premiers entre eux deux à deux, alors $x_1,\ldots,x_n$ sont premiers entre eux dans leur ensemble, car alors :

$$\operatorname{pgcd}(x_1,\ldots,x_n) = \operatorname{pgcd}(x_1 \wedge x_2, x_3,\ldots,x_n) = \operatorname{pgcd}(1,x_3,\ldots,x_n) = 1.$$

2) La réciproque est fausse : il se peut (si $n \geqslant 3$) que $x_1,\ldots,x_n$, soient premiers entre eux dans leur ensemble sans être premiers entre eux deux à deux.

Exemple : $n = 3$, $x_1 = 6$, $x_2 = 10$, $x_3 = 15$.

3) Pour tout $(x_1,\ldots,x_n)$ de $(\mathbb{Z}^*)^n$, en notant $\delta = \operatorname{pgcd}(x_1,\ldots,x_n)$, il existe $(x'_1,\ldots,x'_n) \in (\mathbb{Z}^*)^n$ tel que : $\forall i \in \{1,\ldots,n\}, \quad x_i = \delta x'_i$,
et $x'_1,\ldots,x'_n$ sont premiers entre eux dans leur ensemble car :

$$\delta \operatorname{pgcd}(x'_1,\ldots,x'_n) = \operatorname{pgcd}(\delta x'_1,\ldots,\delta x'_n) = \delta.$$

◆ **Proposition**

$$\forall (a,b,c) \in (\mathbb{Z}^*)^3, \quad \left(\begin{cases} a \wedge b = 1 \\ c \mid b \end{cases} \Longrightarrow a \wedge c = 1 \right).$$

Preuve : Supposons $a \wedge b = 1$ et $c \mid b$.
Pour tout d de $\mathbb{N}^*$ si ($d \mid a$ et $d \mid c$), alors ($d \mid a$ et $d \mid b$), donc $d = 1$. On conclut : $a \wedge c = 1$.

4.3.2 Théorème de Bezout

◆ **Théorème 1** **(Théorème de Bezout)**

Soient $n \in \mathbb{N}^*$, $(x_1,\ldots,x_n) \in (\mathbb{Z}^*)^n$. Pour que $x_1,\ldots,x_n$ soient premiers entre eux dans leur ensemble, il faut et il suffit qu'il existe $(u_1,\ldots,u_n) \in \mathbb{Z}^n$ tel que :

$$\sum_{i=1}^{n} x_i u_i = 1.$$

Preuve :

1) Si $x_1,\ldots,x_n$ sont premiers entre eux dans leur ensemble, alors

$$\sum_{i=1}^{n} x_i\mathbb{Z} = \text{pgcd}\,(x_1,\ldots,x_n)\mathbb{Z} = \mathbb{Z}.$$

Comme $1 \in \mathbb{Z}$, il existe donc $(u_1,\ldots,u_n) \in \mathbb{Z}^n$ tel que $\sum_{i=1}^{n} x_i u_i = 1$.

2) Réciproquement, s'il existe $(u_1,\ldots,u_n)$ dans $\mathbb{Z}^n$ tel que $\sum_{i=1}^{n} x_i u_i = 1$, alors

$$1 \in \sum_{i=1}^{n} x_i\mathbb{Z} = \text{pgcd}\,(x_1,\ldots,x_n)\,\mathbb{Z},$$

d'où $\text{pgcd}\,(x_1,\ldots,x_n) = 1$.

Remarque :

Le théorème de Bezout (ou la Prop. 4 de 4.2.2) permet de former un lien entre une propriété «arithmétique» (nombres premiers entre eux dans leur ensemble) et une propriété «algébrique» (l'égalité $\sum_{i=1}^{n} x_i u_i = 1$). Par exemple, nous utiliserons le théorème de Bezout pour déterminer les éléments inversibles de l'anneau $\left(\mathbb{Z}/_{n\mathbb{Z}},+,\cdot\right)$, cf. 4.3.4 *1)* p. 118.

◆ **Théorème 2** **(Théorème de Gauss)**

$$\forall\,(a,b,c) \in \left(\mathbb{Z}^*\right)^3,\quad \left(\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \Longrightarrow a|c\right).$$

Preuve :

Supposons $a|bc$ et $a \wedge b = 1$. D'après le théorème de Bezout, il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$; d'où $c = acu + bcv$. Comme $a|acu$ et $a|bcv$, on conclut : $a|c$.

◆ **Proposition** Soit $(a,b) \in \left(\mathbb{Z}^*\right)^2$ tel que $a \wedge b = 1$. Il existe $(u,v) \in \mathbb{Z}^2$ tel que :

$$au + bv = 1,\quad |u| < |b|,\quad |v| \leqslant |a|.$$

Preuve :

Il est clair, quitte à remplacer (a,b) par $(-a,-b)$, qu'on peut supposer $b > 0$.

D'après le théorème de Bezout, il existe $(u_1,v_1) \in \mathbb{Z}^2$ tel que $au_1 + bv_1 = 1$.

Par division euclidienne de u_1 par b, il existe $(q,u) \in \mathbb{Z}^2$ tel que :

$$\begin{cases} u_1 = qb + u \\ 0 \leqslant u < b \end{cases}.$$

En notant $v = qa + v_1$, on a alors :

$$au + bv = a(u_1 - qb) + b(v_1 + qa) = au_1 + bv_1 = 1,$$

et $|bv| = |1 - au| \leqslant 1 + |a|u < 1 + |a|b$, d'où $|bv| \leqslant |a|b$ et donc $|v| \leqslant |a|$. ■

Nous allons maintenant décrire un algorithme de calcul d'un couple (u,v) tel que $au+bv = 1$, (a,b) étant donné tel que $a \wedge b = 1$.

Soit $(a,b) \in \mathbb{Z}^* \times \mathbb{N}^*$ tel que $a \wedge b = 1$. D'après l'algorithme d'Euclide (4.2.3 p. 110), il existe $N \in \mathbb{N}$, $q_1, r_1, \ldots, q_N, r_N, q_{N+1}$ dans $\mathbb{Z}$ tels que :

$$\begin{cases} a = bq_1 + r_1 \\ 0 < r_1 < b \end{cases}, \quad \begin{cases} b = r_1q_2 + r_2 \\ 0 < r_2 < r_1 \end{cases}, \ldots \begin{cases} r_{N-2} = r_{N-1}q_N + r_N \\ 0 < r_N < r_{N-1} \end{cases}, \quad r_{N-1} = r_Nq_{N+1},$$

et $r_N = a \wedge b = 1$.

On dispose ainsi des égalités;

$$r_{N-2} = r_{N-1}q_N + 1, \ r_{N-3} = r_{N-2}q_{N-1} + r_{N-1},$$
$$\vdots$$
$$b = r_1q_2 + r_2, \ a = bq_1 + r_1,$$

ce qui permet de faire apparaître un couple (u,v) de $\mathbb{Z}^2$ tel que $1 = au + bv$.

EXEMPLE : $a = 693, b = 680$

	1	52	3
693	680	13	4
13	4	1	

$$\begin{aligned} 1 &= \boxed{13} - 3 \cdot \boxed{4} = \boxed{13} - 3\left(\boxed{680} - 52 \cdot \boxed{13}\right) \\ &= 157 \cdot \boxed{13} - 3 \cdot \boxed{680} = 157\left(\boxed{693} - 1 \cdot \boxed{680}\right) - 3 \cdot \boxed{680} \\ &= 157 \cdot \boxed{693} - 160 \cdot \boxed{680}. \end{aligned}$$

Remarque :

Le lecteur pourra montrer, par récurrence forte sur $|a| + b$, que l'algorithme précédent fournit (si $|a| \geqslant 2$) le couple (u,v) de $\mathbb{Z}^2$ tel que :

$$au + bv = 1, \quad |u| < b, \quad |v| < |a|.$$

4.3.3 Propriétés

◆ **Proposition 1** Soient $n \in \mathbb{N}^*, a, x_1, \ldots, x_n \in \mathbb{Z}^*$. On a :

$$(\forall i \in \{1,\ldots,n\},\quad a \wedge x_i = 1) \iff a \wedge \left(\prod_{i=1}^{n} x_i\right) = 1.$$

Preuve :

1) $\Longrightarrow$: Récurrence sur n.

- La propriété est évidente pour $n = 1$.
- Cas $n = 2$.

Supposons $a \wedge x_1 = a \wedge x_2 = 1$. D'après le théorème de Bezout, il existe $u_1, v_1, u_2, v_2 \in \mathbb{Z}$ tels que $au_1 + x_1v_1 = 1$ et $au_2 + x_2v_2 = 1$. Alors :

$$1 = (au_1 + x_1v_1)(au_2 + x_2v_2) = a(au_1u_2 + x_1v_1u_2 + u_1x_2v_2) + (x_1x_2)(v_1v_2),$$

et $au_1u_2 + x_1v_1u_2 + u_1x_2v_2 \in \mathbb{Z}$, $v_1v_2 \in \mathbb{Z}$, d'où $a \wedge (x_1x_2) = 1$.

- Supposons la propriété vraie pour un n de $\mathbb{N} - \{0,1\}$, et soient $x_1, \ldots, x_{n+1} \in \mathbb{Z}^*$ tels que : $\forall i \in \{1,\ldots,n+1\}$, $a \wedge x_i = 1$.

Alors $(\forall i \in \{1,\ldots,n\},\ a \wedge x_i = 1)$, donc $a \wedge \left(\prod_{i=1}^{n} x_i\right) = 1$, puis, d'après l'étude du cas $n = 2$:

$$a \wedge \left(\prod_{i=1}^{n+1} x_i\right) = a \wedge \left(\left(\prod_{i=1}^{n} x_i\right) x_{n+1}\right) = 1.$$

2) $\Longleftarrow$:

Si $a \wedge \left(\prod_{i=1}^{n} x_i\right) = 1$, alors, d'après 4.3.1 Prop. p. 113 : $\forall i \in \{1,\ldots,n\}$, $a \wedge x_i = 1$.

◆ **Proposition 2**

$$\forall (a,b) \in (\mathbb{Z}^*)^2,\ \forall (k,\ell) \in (\mathbb{N}^*)^2,\quad \left(a \wedge b = 1 \iff a^k \wedge b^\ell = 1\right).$$

Preuve :

1) Supposons $a \wedge b = 1$.

D'après Prop. 1, $a \wedge b^\ell = 1$, puis, toujours d'après Prop. 1, $a^k \wedge b^\ell = 1$.

2) Réciproquement, si $a^k \wedge b^\ell = 1$, alors, d'après Prop. 1, $a^k \wedge b = 1$, puis, toujours d'après Prop. 1, $a \wedge b = 1$.

◆ **Corollaire** $\forall (a,b) \in (\mathbb{Z}^*)^2,\ \forall k \in \mathbb{N}^*,\quad a^k \wedge b^k = (a \wedge b)^k$.

Preuve :

En notant $\delta = a \wedge b$, il existe $(a',b') \in (\mathbb{Z}^*)^2$ tel que : $a = \delta a'$, $b = \delta b'$, $a' \wedge b' = 1$ (cf. 4.3.1 Rem. *3)* p. 113). On a alors : $a^k \wedge b^k = (\delta^k a'^k) \wedge (\delta^k b'^k) = \delta^k (a'^k \wedge b'^k) = \delta^k$.

◆ **Proposition 3** Soient $n \in \mathbb{N}^*$, $a,x_1,\ldots,x_n \in \mathbb{Z}^*$. Si $(\forall i \in \{1,\ldots,n\},\ x_i|a)$ et si $x_1,\ldots,x_n$ sont premiers entre eux deux à deux, alors $\prod_{i=1}^{n} x_i \Big| a$.

Preuve :

Récurrence sur n.

- La propriété est triviale pour $n = 1$.
- Cas $n = 2$.

Supposons $x_1|a,\ x_2|a,\ x_1 \wedge x_2 = 1$.

Il existe $y_1 \in \mathbb{Z}^*$ tel que $a = x_1y_1$. Comme $x_2|x_1y_1$ et $x_2 \wedge x_1 = 1$, le théorème de Gauss (4.3.2 Th. 2 p. 114) montre $x_2|y_1$.

Il existe donc $y_2 \in \mathbb{Z}$ tel que $y_1 = x_2y_2$, d'où : $a = x_1y_1 = (x_1x_2)y_2$, et donc $x_1x_2|a$.

• Supposons la propriété vraie pour un n de $\mathbb{N}^*$, et soient $x_1,\ldots,x_{n+1} \in \mathbb{Z}^*$, premiers entre eux deux à deux, tels que : $\forall i \in \{1,\ldots,n+1\},\ x_i|a$.

Alors $x_1,\ldots,x_n$ sont premiers entre eux deux à deux, et $(\forall i \in \{1,\ldots,n\},\ x_i|a)$, d'où : $\prod_{i=1}^{n} x_i|a$.

Comme $(\forall i \in \{1,\ldots,n\},\quad x_{n+1} \wedge x_i = 1)$, d'après la Prop. 1, p. 116 on a :

$$x_{n+1} \wedge \left(\prod_{i=1}^{n} x_i\right) = 1.$$

Puis, comme $\prod_{i=1}^{n} x_i|a$ et $x_{n+1}|a$, on déduit (cas $n = 2$) : $\prod_{i=1}^{n+1} x_i|a$.

◆ **Corollaire** Soient $n \in \mathbb{N}^*$, $(x_1,\ldots,x_n) \in (\mathbb{Z}^*)^n$. Si $x_1,\ldots,x_n$ sont premiers entre eux deux à deux, alors :

$$\text{ppcm}\,(x_1,\ldots,x_n) = \left|\prod_{i=1}^{n} x_i\right|.$$

◆ **Proposition 4**

$$\forall\,(a,b) \in \left(\mathbb{Z}^*\right)^2,\quad (a \wedge b)(a \vee b) = |ab|.$$

Preuve :

Soit $(a,b) \in (\mathbb{Z}^*)^2$; notons $\delta = a \wedge b$, $\mu = a \vee b$. Il existe $(a',b') \in (\mathbb{Z}^*)^2$ tel que : $a = \delta a'$, $b = \delta b'$, $a' \wedge b' = 1$ (cf. 4.3.1 Rem. *3)* p. 113).

Alors : $\mu = (\delta a') \vee (\delta b') = \delta(a' \vee b') = \delta|a'b'|$, d'après le Corollaire précédent, d'où :

$$\delta\mu = \delta^2|a'b'| = |\delta a'|\,|\delta b'| = |ab|.$$

Remarque :

La proposition précédente permet de calculer des ppcm par l'intermédiaire de pgcd.

Par exemple (cf. 4.2.3 p. 111) : $9\,100 \vee 1\,848 = \dfrac{9\,100 \cdot 1\,848}{28} = \dfrac{9\,100}{28} \cdot 1\,848 = 600\,600.$

4.3.4 Applications

1) Eléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Soit $n \in \mathbb{N}^*$.

a) Soit ξ un élément inversible de $\mathbb{Z}/n\mathbb{Z}$. Il existe $\zeta \in \mathbb{Z}/n\mathbb{Z}$ tel que $\xi\zeta = \widehat{1}$, et $(x,y) \in \mathbb{Z}^2$ tel que $\xi = \widehat{x}$, $\zeta = \widehat{y}$.

On a : $\widehat{xy} = \widehat{1}$, donc $n|xy - 1$. Il existe donc $k \in \mathbb{Z}$ tel que $xy - 1 = kn$. D'après le théorème de Bezout, on déduit $x \wedge n = 1$.

b) Réciproquement, soient $x \in \mathbb{Z}^*$ tel que $x \wedge n = 1$, et $\xi = \widehat{x}$. D'après le théorème de Bezout, il existe $(u,v) \in \mathbb{Z}^2$ tel que $xu + nv = 1$. On a alors : $\widehat{1} = \widehat{xu + nv} = \widehat{xu} + \widehat{nv} = \xi\widehat{u}$, ce qui montre que ξ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ (et admet $\widehat{u}$ pour inverse).

On conclut :

◆ **Proposition** Pour $n \in \mathbb{N}^*$, les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont les $\widehat{x}$, où $x \in \mathbb{Z}$ et $x \wedge n = 1$.

EXEMPLE : Les éléments inversibles de $\mathbb{Z}/9\mathbb{Z}$ sont : $\widehat{1}, \widehat{2}, \widehat{4}, \widehat{5}, \widehat{7}, \widehat{8}$.

2) Forme irréductible d'un rationnel non nul

On appelle **représentant irréductible** d'un rationnel r non nul tout couple (α,β) de $(\mathbb{Z}^*)^2$ tel que : $r = \dfrac{\alpha}{\beta}$ et $\alpha \wedge \beta = 1$.

a) Soit $r \in \mathbb{Q}^*$; il existe $(a,b) \in (\mathbb{Z}^*)^2$ tel que $r = \dfrac{a}{b}$.

En notant $\delta = a \wedge b$, il existe $(\alpha,\beta) \in (\mathbb{Z}^*)^2$ tel que : $a = \delta\alpha$, $b = \delta\beta$, $\alpha \wedge \beta = 1$ (cf. 4.3.1 Rem. *3)* p.113). Alors $r = \dfrac{\alpha}{\beta}$ et $\alpha \wedge \beta = 1$, donc (α,β) est un représentant irréductible de r. Ainsi :

Tout rationnel non nul admet au moins un représentant irréductible.

b) Soient $r \in \mathbb{Q}^*$, (α,β) un représentant irréductible de r, (c,d) un représentant de r $\left(\text{c'est-à-dire : } (c,d) \in (\mathbb{Z}^*)^2 \text{ et } r = \dfrac{c}{d}\right)$.

Comme $c\beta = d\alpha$ et $\alpha \wedge \beta = 1$, le théorème de Gauss montre $\alpha|c$. Il existe donc $k \in \mathbb{Z}^*$ tel que $c = k\alpha$, puis $d = k\beta$. Ainsi :

Soient $r \in \mathbb{Q}^*$ et (α,β) un représentant irréductible de r ; tout représentant de r est de la forme $(k\alpha,k\beta)$, $k \in \mathbb{Z}^*$.

c) Soient $r \in \mathbb{Q}^*$, (α,β), (γ,δ) deux représentants irréductibles de r. D'après *b)* , on a : $\alpha|\gamma$, $\beta|\delta$, $\gamma|\alpha$, $\delta|\beta$. On en déduit qu'il existe $\varepsilon \in \{-1,1\}$ tel que $\gamma = \varepsilon\alpha$ et $\delta = \varepsilon\beta$.

Ainsi :

Tout rationnel non nul admet exactement deux représentants irréductibles (α,β), $(-\alpha,-\beta)$.

Il s'ensuit que tout rationnel non nul admet un représentant irréductible (α,β) et un seul tel que $\beta \in \mathbb{N}^*$.

Exercices

◇ **4.3.1** Soit $n \in \mathbb{Z}$ impair, tel que $3 \not| n$; montrer : $n^2 \equiv 1\ [24]$.

◇ **4.3.2** Résoudre dans $(\mathbb{N}^*)^2$:

a) $\begin{cases} x \wedge y = 18 \\ x \vee y = 540 \end{cases}$ *b)* $\begin{cases} x \vee y - x \wedge y = 534 \\ x \vee y - 5(x \wedge y) = 510 \end{cases}$

c) $x \vee y - 3(x \wedge y) = 135$

d) $\begin{cases} x + y = 1\,008 \\ x \wedge y = 24 \end{cases}$ *e)* $\begin{cases} x^2 + y^2 = 19\,476 \\ x \vee y = 1\,260 \end{cases}$

f) $x \wedge y + x \vee y = y + 9$.

◇ **4.3.3** *a)* Vérifier que 442 et 495 sont premiers entre eux.

b) Trouver tous les (u,v) de $\mathbb{Z}^2$ tels que : $442u + 495v = 1$.

c) Résoudre l'équation $\widehat{442}x = \widehat{314}$ d'inconnue $x \in \mathbb{Z}/_{495\mathbb{Z}}$.

◇ **4.3.4** Quel est le cardinal de $\{(x,y) \in \mathbb{N}^2;\ 2x + 3y = n\}$, pour $n \in \mathbb{N}$ donné?

◇ **4.3.5** Pour $(a,b,c) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}$, résoudre l'équation $ax + by = c$ d'inconnue $(x,y) \in \mathbb{Z}^2$.

Exemples : résoudre dans $\mathbb{Z}^2$: *a)* $9x + 15y = 11$ *b)* $9x + 15y = 18$.

◇ **4.3.6*** Soit $(a,b) \in (\mathbb{N}^*)^2$ tel que : $a \wedge b = 1, a \geqslant 3, b \geqslant 3$.

Montrer qu'il existe $(x,y) \in \mathbb{Z}^2$ unique tel que : $ax + by = 1, \quad |x| < \frac{1}{2}b, \quad |y| < \frac{1}{2}a$.

◇ **4.3.7*** Soit $(a,b) \in (\mathbb{Z}^*)^2$ tel que $a \wedge b = 1$. Démontrer que tout c de $\mathbb{Z}$ tel que $|c| < |ab|$ peut s'écrire d'au moins une façon et d'au plus deux façons sous la forme $c = ua + vb$, avec : $(u,v) \in \mathbb{Z}^2, \ |u| < |b|, \ |v| < |a|$.

◇ **4.3.8** Montrer, pour tout n de $\mathbb{Z}$:

$$n \wedge 2 = n \wedge 5 = 1 \Longrightarrow 23\,040 \Big| (n^2 - 1)(n^2 - 9)(n^2 - 49).$$

◇ **4.3.9** Montrer, pour tout (x,y,z,t) de $\mathbb{Z}^4$: $\begin{cases} x^2 + 10y^2 = z^2 \\ 10x^2 + y^2 = t^2 \end{cases} \Longrightarrow x = y = z = t = 0.$

◇ **4.3.10** Montrer : $\forall n \in \mathbb{N}^*, \quad (n+1) \Big| C_{2n}^n$.

◇ **4.3.11***

a) Etablir : $\forall (a,b) \in (\mathbb{Z}^*)^2, \quad \left(a^2 \,|b^2 \Longrightarrow a|b\right)$.

b) En déduire : $\forall \alpha \in \mathbb{Q}^*, \quad (\alpha^2 \in \mathbb{Z} \Longrightarrow \alpha \in \mathbb{Z})$.

*c)** Résoudre dans $\mathbb{Z}^2$: $(x^2 + y)(x + y^2) = (x - y)^3$.

◇ **4.3.12** Montrer, pour tout (a,b,c) de $(\mathbb{Z}^*)^3$: $c \mid ab \Longrightarrow c \mid (a \wedge c)(b \wedge c)$.

◇ **4.3.13** Soient $n \in \mathbb{N} - \{0,1\}$, $(a,b) \in (\mathbb{N}^*)^2$ tel que $a \neq b$.

Montrer : $\left(\dfrac{a^n - b^n}{a-b}\right) \wedge (a-b) = \left(n(a \wedge b)^{n-1}\right) \wedge (a-b)$.

◇ **4.3.14*** Montrer que l'équation $6x^2 + 5x + 1 = 0$ n'a pas de solution dans $\mathbb{Z}$ mais que, pour tout n de $\mathbb{N}^*$, la congruence $6x^2 + 5x + 1 \equiv 0\ [n]$ admet au moins une solution dans $\mathbb{Z}$.

◇ **4.3.15** Soient $n \in \mathbb{N} - \{0,1\}$, $a_1, \ldots, a_n \in \mathbb{Z}^*$ premiers entre eux deux à deux. Pour chaque i de $\{1,\ldots,n\}$, on note $A_i = \prod_{\substack{1 \leqslant k \leqslant n \\ k \neq i}} a_k$.

Montrer que $A_1, \ldots, A_n$ sont premiers entre eux dans leur ensemble.

◇ **4.3.16*** **Théorème chinois**

Soient $n \in \mathbb{N}^*$, $a_1, \ldots, a_n \in \mathbb{N}^*$ premiers entre eux deux à deux, $a = \prod_{i=1}^{n} a_i$.

a) Démontrer que, pour tout $(b_1, \ldots, b_n)$ de $\mathbb{Z}^n$, il existe $\beta \in \mathbb{Z}$ tel que :

$$\forall x \in \mathbb{Z}, \quad \big((\forall i \in \{1,\ldots,n\},\ x \equiv b_i\ [a_i]) \Longleftrightarrow (x \equiv \beta\ [a])\big).$$

Exemple : Résoudre dans $\mathbb{Z}$: $\begin{cases} x \equiv 4\ [5] \\ x \equiv 3\ [6] \\ x \equiv 2\ [7]. \end{cases}$

b) Pour tout m de $\mathbb{N}^*$ et tout x de $\mathbb{Z}$, on note $\mathrm{cl}_m(x)$ la classe de x modulo m :

$$\mathrm{cl}_m(x) = \{y \in \mathbb{Z};\ m \mid y - x\} = x + m\mathbb{Z}.$$

Déduire de *a)* qu'il existe un isomorphisme de groupes $\theta : \mathbb{Z}/a\mathbb{Z} \longrightarrow \mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_n\mathbb{Z}$ tel que : $\forall x \in \mathbb{Z}, \quad \theta(\mathrm{cl}_a(x)) = (\mathrm{cl}_{a_1}(x), \ldots, \mathrm{cl}_{a_n}(x))$.

◇ **4.3.17** Soit $(a,b,x,y) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Q} \times \mathbb{Q}$ tel que : $\begin{cases} y - 2x - a = 0 \\ y^2 - xy + x^2 - b = 0 \end{cases}$. Montrer : $(x,y) \in \mathbb{Z}^2$. (Utiliser l'exercice 4.3.11 *b)* p. 119).

◇ **4.3.18** Soient $n \in \mathbb{N}^*$, $(a,b,c,d) \in \mathbb{Z}^4$ tels que n divise ac, $bc + ad$, bd. Montrer : $n \mid bc$ et $n \mid ad$. (Utiliser l'exercice 4.3.11 *a)* p. 119).

◇ **4.3.19*** Trouver tous les $(x,y,z) \in \mathbb{N}^3$ tels que :

$$2 \leqslant x \leqslant y \leqslant z \quad \text{et} \quad xy \equiv 1\ [z] \quad \text{et} \quad xz \equiv 1\ [y] \quad \text{et} \quad yz \equiv 1\ [x].$$

◇ **4.3.20*** Démontrer, pour tout (x,y,z) de $\mathbb{Z}^3$:

$$x^3 + 3y^3 + 9z^3 - 9xyz = 0 \implies x = y = z = 0.$$

◇ **4.3.21** Déterminer les générateurs du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$, $n \in \mathbb{N}^*$.

◇ **4.3.22** Pour $n \in \mathbb{N} - \{0,1\}$, déterminer les diviseurs de zéro de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$.

4.4 Nombres premiers

4.4.1 Généralités

On a vu (3.1.3 Déf. 2 p. 70) :

◆ **Définition** Un élément p de $\mathbb{N}$ est dit **premier** si et seulement si $p \geqslant 2$ et :

$$\forall a \in \mathbb{N}^*, \qquad \big(a|p \Longrightarrow (a = 1 \text{ ou } a = p)\big).$$

Un entier $n \geqslant 2$ est dit **composé** si et seulement s'il n'est pas premier.
On peut dire qu'un entier relatif est **premier** si et seulement si $|n|$ est premier.

Remarque : Pour qu'un élément p de $\mathbb{N} - \{0,1\}$ soit premier, il faut et il suffit que :

$$\mathrm{Div}(p) = \{-p,-1,1,p\}.$$

◆ **Proposition 1** Soient p premier, et $a \in \mathbb{Z}^*$. On a :

$$p|a \quad \text{ou} \quad p \wedge a = 1.$$

Preuve :
Comme $p \wedge a \mid p$, on a : $p \wedge a = p$ ou $p \wedge a = 1$, donc $p \mid a$ ou $p \wedge a = 1$.

◆ **Corollaire**
Si p,q sont deux nombres premiers distincts (et positifs), alors $p \wedge q = 1$.

◆ **Proposition 2** Soient p premier, $n \in \mathbb{N}^*$, $x_1,\ldots,x_n \in \mathbb{Z}^*$. On a :

$$p \left| \prod_{i=1}^{n} x_i \Longleftrightarrow (\exists\, i \in \{1,\ldots,n\}, \quad p|x_i) \right. .$$

Preuve :
1) $\Longrightarrow$:
Supposons $p \left| \prod_{i=1}^{n} x_i \right.$.
Raisonnons par l'absurde, et supposons :

$$\forall i \in \{1,\ldots,n\}, \ p \not| \ x_i.$$

D'après la Proposition 1, on a alors :

$$\forall i \in \{1,\ldots,n\}, \quad p \wedge x_i = 1.$$

On déduit (cf. 4.3.3 Prop. 1 p. 116) : $p \wedge \left(\prod_{i=1}^{n} x_i\right) = 1$.

Mais, comme $p \mid \prod_{i=1}^{n} x_i$, on aurait alors $p = 1$, contradiction.

Ceci montre : $\exists i \in \{1,\ldots,n\}, \quad p \mid x_i$.

2) $\Longleftarrow$:

Résulte de 4.3.1 Prop. p. 113, le fait que p soit premier n'intervenant pas ici.

Remarque :

Si un entier composé divise un produit, on ne peut pas déduire qu'il divise un des facteurs du produit, comme le montre l'exemple : $6 \mid 3 \cdot 4$, $6 \nmid 3$, $6 \nmid 4$.

4.4.2 Corps $\mathbb{Z}/_{p\mathbb{Z}}$, p premier

◆ **Proposition** Soit $n \in \mathbb{N}^*$. Les trois propriétés suivantes sont équivalentes :

(i) n est premier

(ii) $\mathbb{Z}/_{n\mathbb{Z}}$ est un corps (commutatif)

(iii) $\mathbb{Z}/_{n\mathbb{Z}}$ est un anneau intègre.

Preuve :

(i) $\Longrightarrow$ (ii)

Supposons n premier.

Soit $\xi \in \mathbb{Z}/_{n\mathbb{Z}} - \{\widehat{0}\}$; il existe $x \in \mathbb{Z}$ tel que $\xi = \widehat{x}$. Comme $\widehat{x} \neq \widehat{0}$, on a : $n \nmid x$.

Puisque n est premier, on déduit (cf. 4.4.1 Prop. 1 p. 121) : $n \wedge x = 1$, et donc (cf. 4.3.4 *1)* p. 118), $\widehat{x}$ est inversible dans $\mathbb{Z}/_{n\mathbb{Z}}$.

Ceci montre que $\mathbb{Z}/_{n\mathbb{Z}}$ est un corps.

(ii) $\Longrightarrow$ (iii)

Plus généralement, tout corps commutatif est un anneau intègre. En effet, si K est un corps commutatif et si $(a,b) \in K^2$ est tel que $ab = 0$ et $a \neq 0$, alors $b = a^{-1}(ab) = 0$.

(iii) $\Longrightarrow$ (i)

Par contre-apposition, montrons que, si n est composé, alors l'anneau $\mathbb{Z}/_{n\mathbb{Z}}$ n'est pas intègre.

En effet, si n est composé, il existe $(a,b) \in (\mathbb{N}^*)^2$ tel que $n = ab$, $1 < a < n$, $1 < b < n$, d'où : $\widehat{a}\widehat{b} = \widehat{0}$, $\widehat{a} \neq \widehat{0}$, $\widehat{b} \neq \widehat{0}$.

4.4.3 Décomposition primaire

♦ **Théorème 1** Tout élément de $\mathbb{N} - \{0,1\}$ admet une décomposition en produit de nombres premiers, unique à l'ordre près des facteurs.

Preuve :

1) **Existence**

Récurrence forte sur n.

La propriété est vraie pour $n = 2$ (2 est premier).

Supposons que tout entier de $\{2,\ldots,n\}$ se décompose en un produit de nombres premiers.

• Si $n+1$ est composé, il existe $(a,b) \in (\mathbb{N}^*)^2$ tel que :

$$n+1 = ab, \quad 2 \leqslant a \leqslant n, \quad 2 \leqslant b \leqslant n.$$

D'après l'hypothèse de récurrence, a et b se décomposent en produits de nombres premiers, et $n+1 = ab$ se décompose donc en un produit de nombres premiers.

• Si $n+1$ est premier, $n+1$ se décompose en un produit d'un seul facteur, lui-même.

2) **Unicité**

Récurrence forte sur n.

La propriété est évidente pour $n = 2$.

Supposons qu'il y ait unicité, à l'ordre près des facteurs, dans la décomposition de tout entier de $\{2,\ldots,n\}$ en produit de nombres premiers.

Soient $N, N' \in \mathbb{N}^*$, $p_1,\ldots,p_N$, $q_1,\ldots,q_{N'}$ premiers tels que :

$$n+1 = p_1,\ldots,p_N = q_1,\ldots,q_{N'}.$$

Comme p_1 est premier et divise $q_1 \cdot \ldots \cdot q_{N'}$, il existe $i_1 \in \{1,\ldots,N'\}$ tel que $p_1 | q_{i_1}$ (cf. 4.4.1 Prop. 2 p. 121); mais de plus, q_{i_1} est premier, donc $p_1 = q_{i_1}$.

En réordonnant $q_1,\ldots,q_{N'}$, on a donc , par exemple : $p_1 = q_1$.

Alors $p_2 \cdot \ldots \cdot p_N = q_2 \cdot \ldots \cdot q_{N'} \leqslant n$, donc, par l'hypothèse de récurrence, $N = N'$, $p_2 = q_2,\ldots,p_N = q_N$, à l'ordre près. ■

Soit $n \in \mathbb{N} - \{0,1\}$. D'après le théorème précédent, il existe $N \in \mathbb{N}^*$, $p_1,\ldots,p_N$ premiers et deux à deux distincts, $r_1,\ldots,r_N \in \mathbb{N}^*$ tels que $n = \prod_{i=1}^{N} p_i^{r_i}$. Cette égalité s'appelle la **décomposition primaire** de n.

Pour tout nombre premier $p(\geqslant 2)$, on appelle p-**valuation de** n, et on note $v_p(n)$, l'entier naturel tel que : $p^{v_p(n)} | n$ et $p^{v_p(n)+1} \nmid n$.

Avec les notations précédentes, on a : $\forall i \in \{1,\ldots,N\}$, $v_{p_i}(n) = r_i$,

et, pour tout nombre premier p autre que $p_1,\ldots,p_N$: $v_p(n) = 0$.

Il est clair que, pour tout (m,n) de $(\mathbb{N} - \{0,1\})^2$:

$$m|n \iff (\forall\, p \in \mathcal{P}, \quad v_p(m) \leqslant v_p(n)).$$

Il peut être commode, dans l'écriture $n = \prod_{i=1}^{N} p_i^{r_i}$, d'autoriser certains r_i à être nuls (cf. plus loin pp. 124-125).

Exemple : $9\,100 = 2^2 \cdot 5^2 \cdot 7 \cdot 13 = 2^2 \cdot 3^0 \cdot 5^2 \cdot 7^1 \cdot 11^0 \cdot 13^1$
$1\,848 = 2^3 \cdot 3 \cdot 7 \cdot 11 = 2^3 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^1 \cdot 13^0$. ■

◆ **Corollaire**

Tout entier a de $\mathbb{Z} - \{-1,0,1\}$ admet au moins un diviseur premier.

◆ **Théorème 2**

L'ensemble $\mathcal{P}$ des nombres premiers est infini.

Preuve :

Raisonnons par l'absurde : supposons que $\mathcal{P}$ soit fini et notons $k = \text{Card}(\mathcal{P})$, $p_1,\ldots,p_k$ les éléments de $\mathcal{P}$.

L'entier $M = 1 + \prod_{i=1}^{k} p_i$ admet au moins un facteur premier p. Il existe alors $j \in \{1,\ldots,k\}$ tel que $p = p_j$, d'où $p \Big| \prod_{i=1}^{k} p_i$ et donc $p \Big| M - \prod_{i=1}^{k} p_i$, $p|1$, contradiction. ■

◆ **Proposition** Soient $(a,b) \in (\mathbb{N} - \{0,1\})^2$, $a = \prod_{i=1}^{N} p_i^{r_i}$, $b = \prod_{i=1}^{N} p_i^{s_i}$, où $N \in \mathbb{N}^*$, $p_1,\ldots,p_N$ sont premiers et deux à deux distincts, $r_1,\ldots,r_N$, $s_1,\ldots,s_N \in \mathbb{N}$. On a : $a \wedge b = \prod_{i=1}^{N} p_i^{\text{Min}(r_i,s_i)}$ et $a \vee b = \prod_{i=1}^{N} p_i^{\text{Max}(r_i,s_i)}$.

Preuve :

1) Notons $d = \prod_{i=1}^{N} p_i^{\text{Min}(r_i,s_i)}$ et $\delta = a \wedge b$.

• Comme $\left(\forall i \in \{1,\ldots,n\}, \quad \begin{cases} \text{Min}(r_i,s_i) \leqslant r_i \\ \text{Min}(r_i,s_i) \leqslant s_i \end{cases}\right)$, on a $(d|a$ et $d|b)$, donc $d|\delta$.

• D'autre part, comme $\delta|a$ et $\delta|b$, on a :

$$\forall i \in \{1,\ldots,n\}, \quad \begin{cases} v_{p_i}(\delta) \leqslant v_{p_i}(a) = r_i \\ v_{p_i}(\delta) \leqslant v_{p_i}(b) = s_i \end{cases},$$

d'où : $\forall i \in \{1,\ldots,n\}$, $v_{p_i}(\delta) \leqslant \text{Min}(r_i,s_i)$. Il s'ensuit $\delta|d$, et finalement $\delta = d$.

2) Comme $(a \wedge b)(a \vee b) = |ab|$ (cf. 4.3.3 Prop. 4 p. 117), on a :

$$a \vee b = \prod_{i=1}^{N} p_i^{r_i+s_i-\text{Min}(r_i,s_i)} = \prod_{i=1}^{N} p_i^{\text{Max}(r_i,s_i)}.$$

EXEMPLE :

$$9\,100 = 2^2 \cdot 3^0 \cdot 5^2 \cdot 7^1 \cdot 11^0 \cdot 13^1 \quad \text{et} \quad 1\,848 = 2^3 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^1 \cdot 13^0,$$

d'où :

$$\begin{cases} 9\,100 \wedge 1\,848 = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^0 \cdot 13^0 = 28 \\ 9\,100 \vee 1\,848 = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^1 \cdot 11^1 \cdot 13^1 = 600\,600. \end{cases}$$

◆ **Corollaire**

Les lois $\wedge$ et $\vee$ sont distributives l'une sur l'autre dans $\mathbb{Z}^*$.

Preuve :

Soit $(a,b,c) \in (\mathbb{Z}^*)^3$.

Considérons les décompositions primaires :

$$|a| = \prod_{i=1}^{N} p_i^{\alpha_i}, \quad |b| = \prod_{i=1}^{N} p_i^{\beta_i}, \quad |c| = \prod_{i=1}^{N} p_i^{\gamma_i},$$

où $N \in \mathbb{N}^*$, $p_1,\ldots,p_N$ sont premiers deux à deux distincts, $\alpha_1,\ldots,\alpha_N$, $\beta_1,\ldots,\beta_N$, $\gamma_1,\ldots,\gamma_N \in \mathbb{N}$.

On a :

$$a \wedge (b \vee c) = \prod_{i=1}^{N} p_i^{u_i} \quad \text{et} \quad (a \wedge b) \vee (a \wedge c) = \prod_{i=1}^{N} p_i^{v_i},$$

où, pour tout i de $\{1,\ldots,N\}$:

$$u_i = \text{Min}\left(\alpha_i,\ \text{Max}(\beta_i,\gamma_i)\right) \quad \text{et} \quad v_i = \text{Max}\left(\text{Min}(\alpha_i,\beta_i),\text{Min}\,(\alpha_i,\gamma_i)\right).$$

Soit $i \in \{1,\ldots,N\}$; comme β_i et γ_i ont ici des rôles symétriques, on peut supposer, par exemple, $\beta_i \leqslant \gamma_i$.

Puisque l'ordre $\leqslant$ usuel dans $\mathbb{N}$ est total, nous pouvons séparer en trois cas :

	$\alpha_i \leqslant \beta_i \leqslant \gamma_i$	$\beta_i \leqslant \alpha_i \leqslant \gamma_i$	$\beta_i \leqslant \gamma_i \leqslant \alpha_i$
valeur de u_i	α_i	α_i	γ_i
valeur de v_i	α_i	α_i	γ_i

On a donc : $(\forall i \in \{1,\ldots,n\},\ u_i = v_i)$, d'où $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Preuve analogue pour $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

Exercices

◇ **4.4.1** Montrer que les entiers suivants sont composés :

a) $n^4 - n^2 + 16$ pour $n \in \mathbb{Z}$

b) $4n^3 + 6n^2 + 4n + 1$ pour $n \in \mathbb{N}^*$

c) $2^{4n+2} + 1$ pour $n \in \mathbb{N}^*$,

◇ **4.4.2** Soit $n \in \mathbb{N} - \{0,1\}$; montrer que, si $5^n - 3^n$ est premier, alors n est premier.

◇ **4.4.3** Soit $(a,b,c,d) \in (\mathbb{N}^*)^4$ tel que $ab = cd$. Montrer que, pour tout n de $\mathbb{N}^*$, $a^n + b^n + c^n + d^n$ est composé.

◇ **4.4.4** Trouver tous les p de $\mathbb{N} - \{0,1\}$ tels que p et $p^3 + p^2 + 11p + 2$ soient premiers.

◇ **4.4.5** Soient $n \in \mathbb{N}^*$, $x_1, \ldots, x_n \in \mathbb{N}^*$ deux à deux distincts et n'admettant aucun diviseur premier $\geqslant 5$. Montrer : $\displaystyle\sum_{k=1}^{n} \frac{1}{x_k} < 3$.

◇ **4.4.6** Soient p premier et $\geqslant 3$, $n \in \mathbb{N}$. Montrer : $(1+p)^{p^n} \equiv 1 + p^{n+1} \left[p^{n+2}\right]$.

◇ **4.4.7** Montrer que la suite $(u_n)_{n \geqslant 0}$ définie par : $\forall n \in \mathbb{N}, \quad u_n = \mathrm{E}(n + \sqrt{n} + 5)$ contient tous les nombres premiers $\geqslant 5$.

◇ **4.4.8** Soit $(a,b) \in \mathbb{N}^2$ tel que $\frac{1}{2}(a^3 + b^3)$ soit un nombre premier. Montrer : $a = b = 1$.

◇ **4.4.9** Soit $n \in \mathbb{N}$ tel que $n \geqslant 11$. Montrer que, si $n - 10$, $n + 10$, $n + 60$ sont premiers, alors $n + 90$ est aussi premier.

◇ **4.4.10** Soit $n \in \mathbb{N}$. Montrer que, si n et $n^2 + 8$ sont premiers, alors $n^3 + 4$ l'est aussi (montrer $n = 3$).

◇ **4.4.11** Trouver tous les n de $\mathbb{Z}$ tels que $n^4 + 4n^3 + 6n^2 + 4n + 5$ soit premier.

◇ **4.4.12** Trouver tous les p de $\mathbb{N} - \{0,1\}$ tels que p et $2^p + p^2$ soient premiers.

◇ **4.4.13** Soit p premier $\geqslant 5$, $n \in \mathbb{N}$. Montrer que p divise $\displaystyle\sum_{k=0}^{p-1} (n+k)^2$.

◇ **4.4.14** Soit $(a,b,m,n) \in (\mathbb{N}^*)^2$ tel que $a^m + b^n$ soit premier et $m \geqslant 2$, $n \geqslant 2$. Montrer qu'il existe $\alpha \in \mathbb{N}$ tel que $m \wedge n = 2^\alpha$.

◇ **4.4.15** Soit $p \in \mathbb{N}$ tel que $p \geqslant 4$. Montrer que, si p et $p + 2$ sont premiers, alors $p \equiv -1$ [6].

◇ **4.4.16** Soit $(p,q,r) \in (\mathbb{N} - \{0,1\})^3$. Montrer que, si $p,q,r,p^2 + q^2 + r^2$ sont premiers, alors l'un des trois nombres p,q,r vaut 3.

◇ **4.4.17** Trouver tous les nombre premiers de la forme $2^{2^n} + 5$, $n \in \mathbb{N}$.

◇ **4.4.18** Soient $n \in \mathbb{N} - \{0,1\}$ et p le plus petit diviseur premier de n; on suppose $\sqrt[3]{n} < p < n$. Montrer que $\dfrac{n}{p}$ est premier.

◇ **4.4.19** Quels sont les nombres premiers qui sont somme(s) de deux nombres composés?

◇ **4.4.20** Montrer que, si p est premier $\geqslant 5$, alors $4p^2+1$ peut se décomposer en la somme de trois carrés d'entiers $\geqslant 1$.

◇ **4.4.21** *a)* Soit p un nombre premier; montrer : $\forall k \in \{1,\ldots,p-1\}, \quad p|C_p^k$.

b) Généralisation.* Soient p un nombre premier, $n \in \mathbb{N}-\{0,1\}$, $(i_1,\ldots,i_n) \in \{0,\ldots,p-1\}$ tel que $i_1+\ldots+i_n = p$. Montrer que $\dfrac{p!}{i_1!\ldots i_n!}$ est un entier divisible par p.

◇ **4.4.22*** Soit p premier. Montrer qu'il n'existe aucun couple (a,n) de $(\mathbb{N}-\{0,1\})^2$ tel que : $2^p+3^p = a^n$.

◇ **4.4.23** Etablir : $\forall n \in \mathbb{Z}, \quad 49 \not| \ n^3-n^2-2n+1$.

◇ **4.4.24** Déterminer les n de $\mathbb{N}$ tels que : $(2n^7+1) \wedge (3n^2+2) \neq 1$.

◇ **4.4.25** *a)* Soit $k \in \mathbb{N}^*$; montrer que, si 2^k+1 est premier, alors k est une puissance de 2. Les nombres $F_n = 2^{2^n}+1$ ($n \in \mathbb{N}$) sont appelés **nombres de Fermat**. Ils ne sont pas tous premiers; par exemple F_5 est composé, divisible par 641.

b) Montrer, pour tout (m,n) de $\mathbb{N}^2$: $m \neq n \Longrightarrow F_m \wedge F_n = 1$.

Dans les exercices 4.4.26 *et* 4.4.27 *on pourra utiliser la théorie des polynômes* (ch. 5 pp. 139-206)

◇ **4.4.26*** Soit $n \in \mathbb{N}^*$ tel qu'il existe p premier tel que : $p \geqslant 5$ et $p|n$. Montrer que 4^n-2^n+1 est composé.

◇ **4.4.27*** Montrer que, si $n \in \mathbb{N}^*$ est tel que 4^n+2^n+1 soit premier, alors n est une puissance de 3.

◇ **4.4.28** Soit $n \in \mathbb{N}-\{0,1\}$. Montrer que n est composé si et seulement si $\sigma(n) > n+\sqrt{n}$, où $\sigma(n)$ désigne la somme des diviseurs $\geqslant 1$ de n.

◇ **4.4.29** Montrer : $\forall (a,b) \in (\mathbb{N}-\{0,1\})^2, \quad \dfrac{\sigma(a)}{a} \leqslant \dfrac{\sigma(ab)}{ab} \leqslant \dfrac{\sigma(a)\sigma(b)}{ab}$,
où, pour tout n de $\mathbb{N}-\{0,1\}$, $\sigma(n)$ désigne la somme des diviseurs $\geqslant 1$ de n.

◇ **4.4.30** Etablir : $\forall (a,b) \in (\mathbb{N}^*)^2, \quad (a^2+ab+b^2) \wedge (ab) = (a \vee b)^2$.

◇ **4.4.31** A-t-on : $\forall (a,b) \in (\mathbb{N}^*)^2, \quad (a^a|b^b \Longrightarrow a|b)$?

◇ **4.4.32** Soit $(a,b) \in (\mathbb{N}^*)^2$; montrer qu'il existe $(x,y) \in (\mathbb{N}^*)^2$ tel que :

$$x|a, \quad y|b, \quad x \wedge y = 1, \quad xy = a \vee b.$$

◇ **4.4.33** Soient $a,b,c,k \in \mathbb{N}^*$ tels que : $ab = c^k$ et $a \wedge b = 1$. Montrer qu'il existe $(\alpha,\beta) \in (\mathbb{N}^*)^2$ tel que : $a = \alpha^k$ et $b = \beta^k$.

◇ **4.4.34** Soient $(a,b) \in (\mathbb{Z}^*)^2$, $(f,g) \in (\mathbb{N}^*)^2$ tels que $a^f | b^g$. Montrer $a | b^\alpha$, où α est le plus petit entier tel que $\frac{g}{f} \leqslant \alpha$.

◇ **4.4.35** Montrer : $\forall (a,b,c) \in (\mathbb{Z}^*)^3$, $(a \vee b)(a \vee c)(b \vee c)(a \wedge b \wedge c) = (a \vee b \vee c)|abc|$.

◇ **4.4.36** Soient $n \in \mathbb{N}^*$, $a_1, \ldots, a_n \in \mathbb{Z}^*$, $a = \prod_{i=1}^{n} a_i$.

Montrer : $$\left(\bigwedge_{i=1}^{n} a_i\right)\left(\bigvee_{i=1}^{n} \frac{a}{a_i}\right) = \left(\bigvee_{i=1}^{n} a_i\right)\left(\bigwedge_{i=1}^{n} \frac{a}{a_i}\right) = a.$$

◇ **4.4.37** Pour $n \in \mathbb{N} - \{0,1\}$, on note $d(n)$ le nombre de diviseurs $\geqslant 1$ de n, et $\sigma(n)$ la somme des diviseurs $\geqslant 1$ de n. Montrer que, si la décomposition primaire de n est $n = \prod_{i=1}^{N} p_i^{r_i}$, alors :

$$d(n) = \prod_{i=1}^{N} (r_i + 1) \quad \text{et} \quad \sigma(n) = \prod_{i=1}^{N} \frac{p_i^{r_i+1} - 1}{p_i - 1}.$$

◇ **4.4.38** Pour $n \in \mathbb{N} - \{0,1\}$, calculer le produit des diviseurs de n (en faisant intervenir la décomposition primaire de n).

◇ **4.4.39** Soit $n \in \mathbb{N} - \{0,1\}$. Montrer que, pour que n soit le produit de ses diviseurs autres que n (c'est-à- dire : $n = \prod_{\substack{1 \leqslant d < n \\ d|n}} d$), il faut et il suffit que n soit le cube d'un nombre premier ou le produit de deux nombres premiers distincts.

◇ **4.4.40** Soit $k \in \mathbb{N}^*$. Pour tout n de $\mathbb{N}^*$, on note $\sigma_k(n)$ la somme des puissances $k^{\text{èmes}}$ des diviseurs $\geqslant 1$ de n : $\sigma_k(n) = \sum_{\substack{1 \leqslant d \leqslant n \\ d|n}} d^k$.

a) Montrer que, si la décomposition primaire de n est $n = \prod_{i=1}^{N} p_i^{r_i}$, alors $\sigma_k(n) = \prod_{i=1}^{N} \frac{p_i^{k(r_i+1)} - 1}{p_i^k - 1}$ (cf. exercice 4.4.37).

b) En déduire que σ_k est une **fonction arithmétique multiplicative**, c'est-à-dire :

$$\forall (a,b) \in (\mathbb{N}^*)^2, \quad \Big(a \wedge b = 1 \Longrightarrow \sigma_k(ab) = \sigma_k(a)\sigma_k(b)\Big).$$

◇ **4.4.41** Déterminer tous les (n,p) de $(\mathbb{N}^*)^2$ tels que p soit premier $\geqslant 5$ et qu'en notant $N = 2^n 3p$, on ait $\sigma(N) = 3N$, où $\sigma(N)$ est la somme des diviseurs de N.

◇ **4.4.42** Résoudre :

a) $x^2 + \widehat{4}x + \widehat{1} = \widehat{0}$ dans $\mathbb{Z}/11\mathbb{Z}$ *b)* $\begin{cases} \widehat{5}x + \widehat{2}y = \widehat{3} \\ \widehat{2}x + \widehat{4}y = \widehat{6} \end{cases}$ dans $(\mathbb{Z}/12\mathbb{Z})^2$.

◇ **4.4.43** Soit p un nombre premier.

a) Montrer : $\forall k \in \{1, \ldots, p-1\}$, $p | C_p^k$.

*b)** En déduire : $\forall N \in \mathbb{N}^*$, $\forall f \in \mathbb{N}^*$, $\forall (x_1, \ldots, x_N) \in \mathbb{Z}^N$, $\left(\sum_{i=1}^{N} x_i\right)^{p^f} \equiv \sum_{i=1}^{N} x_i^{p^f}$ $[p]$.

◇ **4.4.44** Soit $(a,b,c,d) \in \mathbb{Z}^4$ tel que $5 \not| d$. Montrer :

$$(\exists x \in \mathbb{Z},\ 5 \mid ax^3 + bx^2 + cx + d) \Longrightarrow (\exists y \in \mathbb{Z},\ 5 \mid dy^3 + cy^2 + by + a).$$

◇ **4.4.45** Soit p premier. Etablir, pour tout n de $\mathbb{N}^*$: $C_{np-1}^{p-1} \equiv 1[p]$ et $C_{np}^{p} \equiv n[p]$.

◇ **4.4.46** Trouver tous les (x,y) de $(\mathbb{N}^*)^2$ tels que : $\dfrac{x+y}{x^2-xy+y^2} = \dfrac{2}{7}$.

◇ **4.4.47*** Montrer que l'équation $15x^2 - 4y^2 = 3^z$ n'a pas de solution dans $\mathbb{N}^3$.

◇ **4.4.48*** **Théorème de Wolstenhome**

Soient p premier $\geqslant 5$, $H_{p-1} = \sum_{k=1}^{p-1} \frac{1}{k}$. Montrer que le numérateur de H_{p-1} est divisible par p^2.

◇ **4.4.49** Soit p premier, $p \geqslant 5$.

a) Montrer : $p \left| \sum_{k=1}^{p-1} k \right.$ et $p \left| \sum_{k=1}^{p-1} k^2 \right.$.

b) En déduire que, en notant $a = \sum_{i=1}^{p-1} \frac{(p-1)!}{i}$ et $b = \sum_{1 \leqslant i < j \leqslant p-1} \frac{(p-1)!}{ij}$,

on a : $p^2 | a$ et $p | b$.

c) Démontrer : $p^3 \left| C_{2p-1}^{p-1} - 1 \right.$.

◇ **4.4.50** **Petit théorème de Fermat**

Soit p premier.

a) Montrer : $\forall n \in \mathbb{Z},\ n^p \equiv n\ [p]$.

b) En déduire : $\forall n \in \mathbb{Z},\ (p \not| n \Longrightarrow n^{p-1} \equiv 1\ [p])$.

La résolution des exercices 4.4.51 *à* 4.4.64 *peut utiliser le petit théorème de Fermat*

◇ **4.4.51** Montrer : $\forall n \in \mathbb{Z},\ \dfrac{n^7}{7} + \dfrac{n^5}{5} + \dfrac{23n}{35} \in \mathbb{Z}$.

◇ **4.4.52** Montrer, pour tout n de $\mathbb{Z}$:

a) $42 \mid n^7 - n$

b) $2\,730 \mid n^{13} - n$

c) $2^{15} - 2^3 \mid n^{15} - n^3$.

◇ **4.4.53** Montrer :

a) Pour tout entier n impair tel que $n \geqslant 15$: $21\,840 \mid n^{12} - 1$

b) Pour tout nombre premier $p \geqslant 19$: $16\,320 \mid p^{16} - 1$.

◇ **4.4.54** Montrer : $\forall (a,b,c,d) \in (\mathbb{N}^*)^4,\ 30 \left| a^{4b+d} - a^{4c+d} \right.$.

◇ **4.4.55** Montrer que le nombre 1 729 vérifie :

$$\forall n \in \mathbb{Z},\ (n \wedge 1\,729 = 1 \Longrightarrow n^{1\,728} \equiv 1\ [1\,729]),$$

et cependant 1 729 n'est pas premier.

Autrement dit, la réciproque du petit théorème de Fermat est fausse.

◇ **4.4.56** Soient p premier et $n \in \mathbb{N}^*$ tels que $n \wedge p = 1$. Montrer :

a) Si p est impair, alors $p \left| n^{\frac{p-1}{2}} - 1 \right.$ ou $p \left| n^{\frac{p-1}{2}} + 1 \right.$

b) $p^2 \left| n^{\frac{p(p-1)}{2}} - 1 \right.$ ou $p^2 \left| n^{\frac{p(p-1)}{2}} + 1 \right.$.

◇ **4.4.57** Soit p un nombre premier impair. Montrer : $\forall n \in \mathbb{Z},\ (n+1)^p - (n^p + 1) \equiv 0\ [2p]$.

◇ **4.4.58** Soit p premier. Montrer, pour tout k de $\mathbb{N}$ et tout n de $\mathbb{Z}^*$ tel que $n \wedge p = 1$:

$$(n^{p-1})^{p^k} \equiv 1\ [p^{k+1}].$$

◇ **4.4.59*** *a)* Soient p un nombre premier, $(a,\alpha) \in \mathbb{Z}^2$, $(b,\beta) \in \mathbb{N}^2$ tels que : $p \not| a$, $\alpha \equiv a\ [p]$, $\beta \equiv b\ [p-1]$. Montrer : $\alpha^\beta \equiv a^b\ [p]$.

b) Résoudre dans $(\mathbb{N}^*)^2$: $\begin{cases} x^y \equiv 2\ [5] \\ y^x \equiv 3\ [7] \end{cases}$.

◇ **4.4.60** Soient p premier, $(a,b) \in \mathbb{Z}^2$ tel que $a^p \equiv b^p\ [p]$. Montrer : $a^p \equiv b^p\ [p^2]$.

◇ **4.4.61** Soient p,q deux nombres premiers distincts.
Montrer : $p^{q-1} + q^{p-1} \equiv 1\ [pq]$.

◇ **4.4.62** Soit p premier. Pour tout a de $\mathbb{N}^*$ tel que $p \not| a$, on note $F_p(a) = \dfrac{a^{p-1} - 1}{p}$ (qui est un entier d'après le petit théorème de Fermat). Montrer que, pour tout (a,b) de $(\mathbb{N}^*)^2$ tel que $p \not| a$ et $p \not| b$, on a : $F_p(ab) \equiv F_p(a) + F_p(b)\ [p]$.

◇ **4.4.63** Montrer que l'équation $x^4 + 781 = 3y^4$ n'a pas de solution dans $\mathbb{Z}^2$.

◇ **4.4.64** Résoudre dans $(\mathbb{N}^*)^2$: $x^3 - y^3 = 999$.

◇ **4.4.65** *a)* Soit p premier. Montrer, dans l'anneau $\mathbb{Z}/p\mathbb{Z}[X]$: $X^{p-1} - \widehat{1} = \prod_{k=1}^{p-1} (X - \widehat{k})$.

(On pourra utiliser le petit théorème de Fermat, ex. 4.4.50 p. 129).

En déduire le **théorème de Wilson** : si p est premier, alors $(p-1)! \equiv -1\ [p]$.

b) Réciproquement, montrer pour tout n que, si $(n-1)! \equiv -1\ [n]$, alors n est premier.

La résolution des exercices 4.4.66 *à* 4.4.74 *peut utiliser le théorème de Wilson.*

◇ **4.4.66** Soit $n \in \mathbb{N}$, $n \geqslant 5$. Montrer que, si $n+2$ est premier, alors $n! - 1$ est composé.

◇ **4.4.67** Soit n un entier pair tel que $p = 2n+1$ soit premier. Montrer : $p \mid (n!)^2 + 1$.

◇ **4.4.68** Soit p un nombre premier impair. Montrer : $2((p-3)!) \equiv -1\ [p]$.

◇ **4.4.69** Soit p un nombre premier tel que $p \equiv 3\ [4]$. Montrer : $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv 1\ [p]$.

◇ **4.4.70** Soit p un nombre premier impair. Montrer : $\left(\prod_{k=1}^{\frac{p-1}{2}} (2k-1)\right)^2 \equiv (-1)^{\frac{p+1}{2}}\ [p]$.

◇ **4.4.71** Soit $n \in \mathbb{N} - \{0,1\}$ impair. Montrer que n et $n+2$ sont premiers si et seulement si :

$$4((n-1)!+1)+n \equiv 0\ [n(n+2)].$$

◇ **4.4.72** Soit p premier. Montrer : $\forall n \in \mathbb{N}^*\ \left(\left\{\begin{array}{l} n < p \\ (-1)^n n! \equiv 1[p] \end{array}\right. \Longrightarrow (p-n-1)! \equiv -1[p]\right)$.

Application : montrer $61! \equiv 63! \equiv -1\ [71]$.

◇ **4.4.73** Soient p premier et $n \in \mathbb{N}$ tel que $1 \leqslant n \leqslant p-1$. Montrer :

$$(p-n)!(n-1)! \equiv (-1)^n\ [p].$$

◇ **4.4.74** Soit p premier. Montrer : $\forall n \in \mathbb{Z},\quad p \mid n^p + (p-1)!\, n$.
(Utiliser les théorèmes de Fermat et Wilson).

Indicateur d'Euler, exercices 4.4.75 *à* 4.4.89

◇ **4.4.75*** **Indicateur d'Euler**

Pour tout n de $\mathbb{N}^*$, on note $\varphi(n)$ le nombre d'entiers compris entre 1 et n et qui sont premiers à n :

$$\varphi(n) = \text{Card}\{k \in \{1,\ldots,n\},\ k \wedge n = 1\}.$$

L'application $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ est appelée l'**indicateur d'Euler**.

a) Soit $(a,b) \in (\mathbb{N}^*)^2$ tel que $a \wedge b = 1$. Montrer que les anneaux $\mathbb{Z}/_{ab\mathbb{Z}}$ et $\mathbb{Z}/_{a\mathbb{Z}} \times \mathbb{Z}/_{b\mathbb{Z}}$ (anneau-produit, cf. 2.1 Déf. 14 p. 44) sont isomorphes (cf. aussi exercice 4.3.16 p. 120).

b) En déduire : $\forall (a,b) \in (\mathbb{N}^*)^2,\quad (a \wedge b = 1 \Longrightarrow \varphi(ab) = \varphi(a)\varphi(b))$.

On dit que φ est une **fonction arithmétique multiplicative.**

c) Soit p premier. Montrer : $\forall r \in \mathbb{N}^*,\quad \varphi(p^r) = p^r - p^{r-1}$.

d) En déduire que, si $n \in \mathbb{N}^*$ admet la décomposition primaire $n = \prod_{i=1}^{N} p_i^{r_i}$, alors

$$\varphi(n) = \prod_{i=1}^{N} \left(p_i^{r_1} - p_i^{r_i-1}\right) = n \prod_{i=1}^{N} \left(1 - \frac{1}{p_i}\right).$$

◇ **4.4.76*** **Théorème d'Euler.**

Etablir : $\forall n \in \mathbb{N}^*,\ \forall a \in \mathbb{Z}^*,\quad (a \wedge n = 1 \Longrightarrow a^{\varphi(n)} \equiv 1\ [n])$.

(Utiliser le théorème de Lagrange, C 2.1 p. 63).

Le théorème d'Euler est une généralisation du petit théorème de Fermat (ex. 4.4.50 p. 129).

◇ **4.4.77** Montrer : $\forall (n,k) \in (\mathbb{N}^*)^2,\ \varphi(n^k) = n^{k-1}\varphi(n)$.

◇ **4.4.78** Montrer : $\forall n \in \mathbb{Z}^*, \quad \left(\begin{cases} n \wedge 2 = 1 \\ n \wedge 5 = 1 \end{cases} \Longrightarrow 13\,200 \middle| n^{21} - n \right)$.

◇ **4.4.79*** *a)* Montrer : $\forall n \in \mathbb{N}^*, \quad \sum_{d|n} \varphi(d) = n$.

b) En déduire : $\forall n \in \mathbb{N}^*, \quad \sum_{k=1}^{n} \mathrm{E}\left(\frac{n}{k}\right) \varphi(k) = \frac{n(n+1)}{2}$.

◇ **4.4.80** Montrer : $\forall n \in \mathbb{N} - \{0,1\}, \quad \sum_{\substack{1 \leqslant k \leqslant n \\ k \wedge n = 1}} k = \frac{n\varphi(n)}{2}$.

◇ **4.4.81** Soit $n \in \mathbb{N}^*$ pair. Montrer :

$$\sum_{\substack{d_1 | n \\ d_1 \text{impair}}} \varphi\left(\frac{n}{d_1}\right) = \sum_{\substack{d_2 | n \\ d_2 \text{pair}}} \varphi\left(\frac{n}{d_2}\right) = \frac{n}{2}.$$

(Utiliser l'ex. 4.4.79 *a)*).

◇ **4.4.82** Soit $n \in \mathbb{N} - \{0,1\}$, composé; montrer : $\varphi(n) \leqslant n - \sqrt{n}$.

◇ **4.4.83** Montrer : $\forall (a,b) \in (\mathbb{N}^*)^2, \quad \left(a \wedge b = 1 \Longrightarrow a^{\varphi(b)} + b^{\varphi(a)} \equiv 1\ [ab]\right)$.
(Utiliser le théorème d'Euler, exercice 4.4.76 p. 131).

◇ **4.4.84** Soit $(a,n) \in \mathbb{Z} \times \mathbb{N}^*$ tel que : $a \wedge n = (a-1) \wedge n = 1$. Montrer :

$$\sum_{k=0}^{\varphi(n)-1} a^k \equiv 0\ [n].$$

(Utiliser le théorème d'Euler, ex. 4.4.76 p. 131).

◇ **4.4.85** Montrer : $\forall (a,b) \in (\mathbb{N}^*)^2, \quad \left(a | b \Longrightarrow a\varphi(b) = b\varphi(a)\right)$.

◇ **4.4.86** Montrer : $\forall (a,b) \in \left(\mathbb{N}^*\right)^2, \quad \varphi(ab) = \frac{(a \wedge b)\varphi(a)\varphi(b)}{\varphi(a \wedge b)}$.
(Utiliser l'exercice 4.4.85).

◇ **4.4.87** Soient $(a,b) \in (\mathbb{N}^*)^2$, c le produit des diviseurs premiers de $a \wedge b$. Montrer :

$$\varphi(ab) = \frac{c\varphi(a)\varphi(b)}{\varphi(c)}.$$

(Utiliser l'ex. 4.4.85).

◇ **4.4.88*** Montrer : $\forall a \in \mathbb{N} - \{0,1\}, \forall k \in \mathbb{N}^*, \quad k | \varphi(a^k - 1)$. (utiliser le théorème d'Euler, ex. 4.4.76 p. 131).

◇ **4.4.89** Soient $n \in \mathbb{N}^*$ et $(u_k)_{k \in \mathbb{N}}$ la suite définie par $u_0 = n$ et : $\forall k \in \mathbb{N}, \ u_{k+1} = \varphi(u_k)$.
Montrer : $\exists r \in \mathbb{N}, \ u_r = 1$.

Compléments

◇ C 4.1 Théorème des quatre carrés de Lagrange et sommes de bicarrés

I – Il s'agit de montrer que tout entier naturel peut être décomposé en somme de quatre carrés d'entiers naturels.

1) a) **Identité de Lagrange**

Vérifier, pour tous a,b,c,d,x,y,z,t de $\mathbb{N}$:

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

b) En déduire que, si deux entiers sont décomposables en sommes de quatre carrés d'entiers, alors leur produit l'est aussi.

2) a) Soit p un nombre premier impair. Démontrer qu'il existe $(x,y)\in\left\{0,\dots,\dfrac{p-1}{2}\right\}^2$ tel que : $x^2+y^2+1\equiv 0\ [p]$.

(On pourra considérer $f : \mathbb{Z}/p\mathbb{Z}\longrightarrow\mathbb{Z}/p\mathbb{Z}$, $X\longmapsto X^2$ et $g : \mathbb{Z}/p\mathbb{Z}\longrightarrow\mathbb{Z}/p\mathbb{Z}$, $Y\longmapsto -Y^2-1$.)

b) En déduire que, pour tout nombre premier p, il existe $(k,x,y,z,t)\in\mathbb{N}^5$ tel que :

$$x^2+y^2+z^2+t^2=kp \quad\text{et}\quad 1\leqslant k\leqslant p-1.$$

3) Soit p un nombre premier impair. On note m le plus petit entier $\geqslant 1$ tel qu'il existe $(x,y,z,t)\in\mathbb{N}^4$ tel que $x^2+y^2+z^2+t^2=mp$.

a) Montrer que, si m est pair, on peut permuter x,y,z,t de façon que $\dfrac{x-y}{2}$, $\dfrac{x+y}{2}$, $\dfrac{z-t}{2}$, $\dfrac{z+t}{2}$ soient entiers, et en déduire une contradiction.

b) On suppose m impair et $m>1$. On note a,b,c,d les éléments de $\left\{-\dfrac{m-1}{2},\dots,\dfrac{m-1}{2}\right\}$ congrus modulo m à x,y,z,t respectivement.

Montrer qu'il existe $q\in\mathbb{N}$ tel que $a^2+b^2+c^2+d^2=qm$ et $q<m$, puis établir une contradiction (on pourra séparer les cas $q=0$, $q>0$).

On a ainsi montré qu'il existe $(x,y,z,t)\in\mathbb{N}^4$ tel que $x^2+y^2+z^2+t^2=p$.

4) Conclure par le **théorème des quatre carrés de Lagrange** : Tout entier naturel est décomposable, d'au moins une façon, en somme de quatre carrés d'entiers naturels.

II – *1) a)* Vérifier, pour tout (x_1,x_2,x_3,x_4) de $\mathbb{N}^4$: $\displaystyle\sum_{1\leqslant i<j\leqslant 4}\left((x_i+x_j)^4+(x_i-x_j)^4\right)=6\left(\sum_{k=1}^{4}x_k^2\right)^2$.

b) En déduire que tout entier de la forme $6n^2$ ($n\in\mathbb{N}$) est décomposable en somme de 12 bicarrés, un *bicarré* étant par définition la puissance $4^{\text{ème}}$ d'un entier.

(Utiliser le théorème des quatre carrés).

2) Montrer que tout entier de la forme $6m$ ($m\in\mathbb{N}$) est décomposable en somme de 48 bicarrés.

(Utiliser le théorème des quatre carrés).

3) a) Vérifier que $0,1,2,81,16,17$ sont décomposables en sommes d'au plus deux bicarrés.

b) En déduire que tout entier $\geqslant 81$ peut être décomposé en somme d'au plus 50 bicarrés.

4) Conclure par le théorème :

Tout entier naturel est décomposable en somme d'au plus 50 bicarrés.

Remarque : le résultat peut être amélioré (19 au lieu de 50).

Référence : K.H. Rosen, *Elementary Number Theory*, pp. 407-413, Addison-Wesley, Reading, 1988.

◇ **C 4.2** **Résolution de $x^2+y^2+2=xyz$ dans $\mathbb{Z}^3$**

On note $E=\{(x,y,z)\in\mathbb{Z}^3;\ x^2+y^2+2=xyz\}$.

1) a) Vérifier que, pour tout (x,y,z) de E, les éléments suivants sont aussi dans E :

$$(-x,-y,z),\ (-x,y,-z),\ (x,-y,-z),\ (y,x,z).$$

b) En déduire qu'il suffit de déterminer l'ensemble

$$F=\{(x,y,z)\in(\mathbb{N}^*)^3;\ x^2+y^2+2=xyz \text{ et } x\leqslant y\}.$$

2) On note $G=\{(x,y,z)\in(\mathbb{N}^*)^3;\ x^2+y^2+2=xyz \text{ et } x<y\}$ et

$$f:\begin{array}{ccc}\mathbb{Z}^3&\longrightarrow&\mathbb{Z}^3\\(x,y,z)&\longmapsto&(zx-y,x,z)\end{array}.$$

a) Montrer : $\forall(x,y,z)\in G,\quad f(x,y,z)\in F$.

b) Etablir : $\complement_F(G)=\{(1,1,4)\}$.

3) En déduire $F=\{g^n(1,1,4);\ n\in\mathbb{N}\}$, où $g:\begin{array}{ccc}\mathbb{Z}^3&\longrightarrow&\mathbb{Z}^3\\(X,Y,Z)&\longmapsto&(Y,YZ-X,Z)\end{array}$, $g^0=\mathrm{Id}_{\mathbb{Z}^3}$, $g^1=g$, $g^2=g\circ g,\ldots$

◇ **C 4.3*** **Résidus quadratiques**

Soit p un nombre premier impair (donc $p\geqslant 3$).

Pour $a\in\mathbb{Z}$ tel que $p\not| a$, on dit que a est un **résidu quadratique modulo** p (en abrégé : RQ mod p) si et seulement s'il existe $x\in\mathbb{Z}$ tel que $x^2\equiv a[p]$. Dans le cas contraire, on dit que a est un **non-résidu quadratique modulo** p (en abrégé : NRQ mod p).

Pour $\alpha\in\mathbb{Z}/_{p\mathbb{Z}}-\{0\}$, on dit que α est un **résidu quadratique dans** $\mathbb{Z}/_{p\mathbb{Z}}$ si et seulement s'il existe $\xi\in\mathbb{Z}/_{p\mathbb{Z}}$ tel que $\xi^2=\alpha$.

Il est clair que, pour tout a de $\mathbb{Z}$ tel que $p\not| a$, a est RQ mod p si et seulement si $\widehat{a}$ (classe de a modulo p) est résidu quadratique dans $\mathbb{Z}/_{p\mathbb{Z}}$. Autrement dit, pour tout (a,b) de $\mathbb{Z}^2$ tel que $p\not| a$, $p\not| b$ et $\widehat{a}=\widehat{b}$, a est RQ mod p si et seulement si b l'est. On pourra ainsi souvent se ramener à supposer $a\in\{1,\ldots,p-1\}$.

Exemple : $p=11$

x	1	2	3	4	5
x^2	1	4	9	5	3

Les résidus quadratiques modulo 11 sont : 1,3,4,5,9.

I – 1) a) Soit $a\in\mathbb{Z}$ tel que $p\not| a$. Montrer que l'équation $\xi^2=\widehat{a}$, d'inconnue $\xi\in\mathbb{Z}_{p\mathbb{Z}}$, n'admet aucune solution ou bien en admet deux exactement.

b) En déduire qu'il n'y a, dans $\{1,\ldots,p-1\}$, exactement $\dfrac{p-1}{2}$ résidus quadratiques modulo p, et $\dfrac{p-1}{2}$ non-résidus quadratiques modulo p.

Exemple : Pour $p=11$, il y a cinq RQ mod 11, qui sont 1,3,4,5,9, et cind NRQ mod 11, qui sont 2,6,7,8,10.

Pour $a\in\mathbb{Z}$ tel que $p\not| a$, on définit le **symbole de Legendre** :

$$\left(\frac{a}{p}\right)=\begin{cases}1 & \text{si } a \text{ est RQ mod } p\\ -1 & \text{si } a \text{ est NRQ mod } p\end{cases}.$$

Exemple :

$$\left|\begin{array}{l}\left(\dfrac{3}{11}\right)=1 \quad \text{car 3 est RQ mod 11}\\ \left(\dfrac{6}{11}\right)=-1 \quad \text{car 6 n'est pas RQ mod 11.}\end{array}\right.$$

c) α) Etablir, pour tout a de $\mathbb{Z}$ tel que $p \nmid a$: $\displaystyle\sum_{k=1}^{p-1}\left(\frac{ka}{p}\right) = 0$.

β) *1)* Soient $k \in \{1,\ldots,p-2\}$, $k' \in \{1,\ldots,p-1\}$ tels que $kk' \equiv 1\ [p]$.

Montrer $k' \neq p-1$ et : $\left(\dfrac{k(k+1)}{p}\right) = \left(\dfrac{k'+1}{p}\right)$.

2) En déduire : $\displaystyle\sum_{k=1}^{p-2}\left(\frac{k(k+1)}{p}\right) = -1$.

2) a) **Théorème d'Euler**

Montrer, pour tout a de $\mathbb{Z}$ tel que $p \nmid a$: $\left(\dfrac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ [p]$.

(Utiliser le petit théorème de Fermat ex 4.4.50 p. 129 et le théorème de Wilson ex 4.4.65 *a)* p. 130).

Exemple : Calculer $\left(\dfrac{10}{31}\right)$.

b) En déduire : $\left(\dfrac{-1}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1\ [4] \\ -1 & \text{si } p \equiv 3\ [4] \end{cases}$.

c) α) Soit $n \in \mathbb{N}^*$ tel que $n \equiv 3\ [4]$. Démontrer qu'il existe au moins un diviseur premier q de n tel que $q \equiv 3\ [4]$.

β) En déduire que l'équation $x^2 + y^3 - 8(2z+1)^3 + 1 = 0$, d'inconnue $(x,y,z) \in \mathbb{Z}^3$ n'a pas de solution.

En particulier, l'**équation de Lebesgue** $x^2 + y^3 = 7$ n'a pas de solution dans $\mathbb{Z}^2$.

3) a) Soient $a,b \in \mathbb{Z}$ tels que $p \nmid a$ et $p \nmid b$. Montrer :

1) $\left(\dfrac{1}{p}\right) = 1$

2) $a \equiv b[p] \Longrightarrow \left(\dfrac{a}{p}\right) = \left(\dfrac{b}{p}\right)$

3) $\left(\dfrac{a^2}{p}\right) = 1$

4) $\left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right) = \left(\dfrac{ab}{p}\right)$.

La propriété 4) peut s'exprimer sous la forme d'une «règle des signes» pour le produit (en notant R pour RQ mod p, et N pour NRQ mod p) :

b \ a	R	N
R	R	N
N	N	R

b) Soit $a \in \mathbb{N}^*$ tel que $p \nmid a$; on note $a = \displaystyle\prod_{i=1}^{N} p_i^{r_i}$ la décomposition primaire de a, I l'ensemble des i de $\{1,\ldots,N\}$ tels que r_i soit impair, $a' = \displaystyle\prod_{i\in I} p_i$. Etablir :

$$\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right).$$

4) **Lemme de Gauss**

Soit $a \in \mathbb{Z}$ tel que $p \nmid a$.

Pour tout j de $\left\{1,\ldots,\dfrac{p-1}{2}\right\}$, on note r_j le reste de la division euclidienne de ja par p.

a) Montrer $r_1,\ldots,r_{\frac{p-1}{2}}$ sont deux à deux distincts.

On note $u_1,\ldots,u_s$ les éléments de $\left\{r_1,\ldots,r_{\frac{p-1}{2}}\right\}$ qui sont $\leqslant \dfrac{p-1}{2}$, et $v_1,\ldots,v_t$ les éléments de $\left\{r_1,\ldots,r_{\frac{p-1}{2}}\right\}$ qui sont $\geqslant \dfrac{p+1}{2}$.

b) Etablir : *1)* $u_1,\ldots u_s,\ v_1,\ldots,v_t$ sont deux à deux distincts et forment $\left\{r_1,\ldots,r_{\frac{p-1}{2}}\right\}$.

2) $u_1,\ldots u_s,\ p-v_1,\ldots,p-v_t$ sont deux à deux distinct et forment $\left\{1,\ldots,\dfrac{p-1}{2}\right\}$.

c) En déduire : $\left(\dfrac{a}{p}\right) = (-1)^t$.

On a ainsi montré le **lemme de Gauss** : $\left(\dfrac{a}{p}\right) = (-1)^t$, où t est le nombre de restes des divisions euclidiennes de $a, 2a, \ldots, \dfrac{p-1}{2}a$ par p qui soient supérieurs à $\dfrac{p}{2}$.

Exemple : Calculer $\left(\dfrac{8}{29}\right)$ en utilisant le lemme de Gauss.

d) Etablir : $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

(On pourra montrer : $\dfrac{p-1}{2} - \mathrm{E}\left(\dfrac{p}{4}\right) \equiv \dfrac{p^2-1}{8}$ [2]).

Par exemple : $\begin{cases} \left(\dfrac{2}{3}\right), \left(\dfrac{2}{5}\right), \left(\dfrac{2}{11}\right), \left(\dfrac{2}{13}\right), \left(\dfrac{2}{19}\right) & \text{sont égaux à } -1 \\ \left(\dfrac{2}{7}\right), \left(\dfrac{2}{17}\right), \left(\dfrac{2}{23}\right) & \text{sont égaux à } 1. \end{cases}$

Exemple : Calculer $\left(\dfrac{8}{31}\right)$.

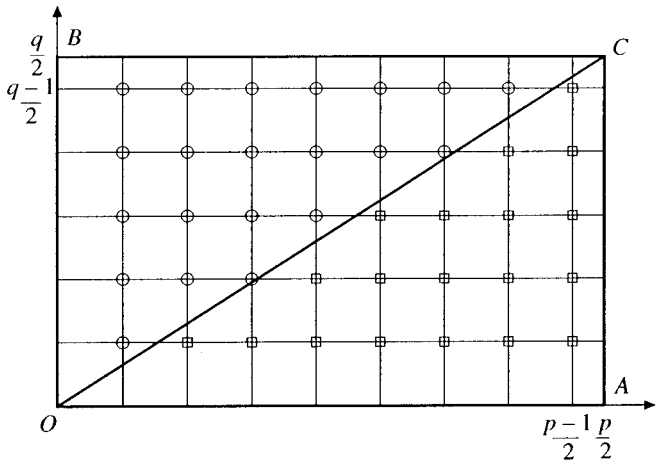
e) Soit $n \in \mathbb{N}$. Montrer que, si $8n+7$ est premier, alors $8n+7 \mid 2^{4n+3}-1$ et (si $n \geqslant 1$) $2^{4n+3}-1$ est composé.

Exemples : $23|2^{11}-1$, $31|2^{15}-1$, $47|2^{23}-1$, $71|2^{35}-1$, $79|2^{39}-1$.

II – Loi de réciprocité quadratique de Gauss

1) Soient p,q deux nombres premiers impairs distincts.

Dans le plan usuel, on note $A\left(\frac{p}{2},0\right)$, $B\left(0,\frac{q}{2}\right)$, $C\left(\frac{p}{2},\frac{q}{2}\right)$.



Exemple : $p = 17, q = 11$

a) Montrer que le nombre de points de $(\mathbb{N}^*)^2$ situés (strictement) dans le rectangle $OACB$ est $\frac{p-1}{2}\,\frac{q-1}{2}$.

b) Etablir qu'il n'y a aucun point de $(\mathbb{N}^*)^2$ sur le segment OC.

c) Démontrer que le nombre de points de $(\mathbb{N}^*)^2$ situées dans le triangle OAC est $\sum_{j=1}^{\frac{p-1}{2}} \mathrm{E}\left(\frac{jq}{p}\right)$, et que le nombre de points de $(\mathbb{N}^*)^2$ situés dans le triangle OBC est $\sum_{k=1}^{\frac{q-1}{2}} \mathrm{E}\left(\frac{kp}{q}\right)$.

d) Montrer, en utilisant les notations du lemme de Gauss (*I 4*), avec q à la place de a) :

$$t \equiv \sum_{j=1}^{\frac{p-1}{2}} \mathrm{E}\left(\frac{jq}{p}\right) \quad [2].$$

e) Déduire : $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

On a ainsi montré la **loi de réciprocité quadratique de Gauss** :

Pour tous nombres premiers impairs distincts p et q : $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

2) a) Déduire de la loi de réciprocité quadratique que, pour tous nombres premiers impairs distincts p et q :

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{si} \quad (p \equiv 1\ [4] \text{ ou } q \equiv 1\ [4]) \\ -\left(\frac{p}{q}\right) & \text{si} \quad (p \equiv 3\ [4] \text{ et } q \equiv 3\ [4]) \end{cases}.$$

b) *Exemple* : Calculer $\left(\frac{6417}{6607}\right)$ (6 607 est premier).

*3)** **Test de Pépin**

Pour tout n de $\mathbb{N}^*$, on note $F_n = 2^{2^n} + 1$ (**nombres de Fermat**).

Démontrer que F_n est premier si et seulement si $3^{\frac{F_n-1}{2}} \equiv -1 \quad [F_n]$.

(pour la réciproque, on fera intervenir un diviseur premier quelconque p de F_n et le plus petit entier $\alpha \geqslant 1$ tel que $3^\alpha \equiv 1[p]$, et on montrera $\alpha | F_n - 1$ et $\alpha \not| \frac{F_n - 1}{2}$).

Exemple : Montrer que $F_5 = 2^{2^5} + 1$ est composé.

4) On suppose dans cette question $p \geqslant 5$. Montrer :

a) $\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{si } p \equiv \pm 1\ [12] \\ -1 & \text{si } p \equiv \pm 5\ [12] \end{cases}$

b) $\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1\ [6] \\ -1 & \text{si } p \equiv -1\ [6] \end{cases}$.

Chapitre 5

Polynômes fractions rationnelles

Les fonctions polynômes $f : \mathbb{R} \longrightarrow \mathbb{R}$, $x \longmapsto a_0 + a_1 x + \ldots + a_n x^n$ sont connues du lecteur en classe de Terminale. Les propriétés de f se déduisent des coefficients $a_0, \ldots, a_n$; c'est pourquoi nous allons introduire et étudier les polynômes «formels».

Même lorsque $a_0, \ldots, a_n$ sont réels, les propriétés de f peuvent faire intervenir les corps des complexes, ce qui motive l'introduction et l'étude des polynômes à coefficients complexes et, plus généralement, à coefficient dans un corps commutatif.

Dans tout ce chapitre 5, K désigne un corps commutatif.

En pratique, le plus souvent, $K = \mathbb{R}$ ou $\mathbb{C}$.

5.1 Algèbre $K[X]$

5.1.1 Définition

◆ **Définition 1**

1) Pour toute suite $(a_n)_{n\in\mathbb{N}}$ de $K^{\mathbb{N}}$, on appelle **support** de $(a_n)_{n\in\mathbb{N}}$ l'ensemble des n de $\mathbb{N}$ tels que $a_n \neq 0$.

2) On appelle **polynôme (à une indéterminée et à coefficients dans K)** toute suite $(a_n)_{n\in\mathbb{N}}$ de $K^{\mathbb{N}}$ à support fini.

L'ensemble des polynômes à une indéterminée et à coefficients dans K est noté $K[X]$ (ou $K^{(\mathbb{N})}$).

Ainsi, $K[X] \subset K^{\mathbb{N}}$ et, pour toute suite $(a_n)_{n\in\mathbb{N}}$ de $K^{\mathbb{N}}$:

$$(a_n)_{n\in\mathbb{N}} \in K[X] \Longleftrightarrow \Big(\exists N \in \mathbb{N},\ \forall n \in \mathbb{N},\quad (n > N \Longrightarrow a_n = 0)\Big).$$

La notation $K[X]$ sera justifiée plus loin (5.1.4 p. 145).

Les éléments de $K[X]$ sont aussi appelés **polynômes formels**.

On note 0 la suite constante nulle de $K^{\mathbb{N}}$ (définie par : $\forall n \in \mathbb{N}, a_n = 0$), appelée **polynôme nul**.

On appelle **polynômes constants** les polynômes $(a_n)_{n\in\mathbb{N}}$ de $K[X]$ tels que :

$$\forall n \geqslant 1, \ a_n = 0.$$

On appelle **monôme** tout polynôme $(a_n)_{n\in\mathbb{N}}$ de $K[X]$ tel qu'il existe $n_0 \in \mathbb{N}$ tel que :

$$\forall n \in \mathbb{N}, \quad (n \neq n_0 \Longrightarrow a_n = 0).$$

Remarques :

1) D'après la Définition, deux polynômes $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$ sont égaux si et seulement si :

$$\forall n \in \mathbb{N}, \quad a_n = b_n.$$

2) $K[X] \neq K^{\mathbb{N}}$ puisque la suite constante (1) (définie par : $\forall n \in \mathbb{N}, \ a_n = 1$) de $K^{\mathbb{N}}$ n'est pas dans $K[X]$.

◆ **Définition 2** Soit $P = (a_n)_{n\in\mathbb{N}} \in K[X]$.

1) • Si $P \neq 0$, on appelle **degré de** P, et on note $\deg(P)$ le plus grand entier naturel n tel que $a_n \neq 0$. L'élément $a_{\deg(P)}$ est appelé le **coefficient du terme de plus haut degré** (ou : **coefficient dominant**) **de** P. On dit que P est **unitaire** (ou : **normalisé**) si et seulement si : $P \neq 0$ et $a_{\deg(P)} = 1$.

• On note $\deg(0) = -\infty$.

2) • Si $P \neq 0$, on appelle **valuation de** P, et on note $\mathrm{val}(P)$ le plus petit entier naturel n tel que $a_n \neq 0$.

• On note $\mathrm{val}(0) = +\infty$.

Remarque :

$$\forall P \in K[X] - \{0\}, \quad \mathrm{val}(P) \leqslant \deg(P).$$

◆ **Définition 3** Soit $P = (a_n)_{n\in\mathbb{N}} \in K[X]$.

1) On dit que P est **pair** si et seulement si :

$$\forall p \in \mathbb{N}, \quad a_{2p+1} = 0.$$

2) On dit que P est **impair** si et seulement si :

$$\forall p \in \mathbb{N}, \quad a_{2p} = 0.$$

5.1.2 Addition

♦ **Proposition 1**

Soient $P = (a_n)_{n\in\mathbb{N}}$, $Q = (b_n)_{n\in\mathbb{N}} \in K[X]$.
Alors $P + Q = (a_n + b_n)_{n\in\mathbb{N}} \in K[X]$.

Preuve :

Puisque P, Q sont des polynômes, il existe $N_1, N_2 \in \mathbb{N}$ tels que :

$$\begin{cases} \forall n \in \mathbb{N}, & (n > N_1 \Longrightarrow a_n = 0) \\ \forall n \in \mathbb{N}, & (n > N_2 \Longrightarrow b_n = 0). \end{cases}$$

En notant $N = \text{Max}(N_1, N_2) \in \mathbb{N}$, on a :

$$\forall n \in \mathbb{N}, \quad (n > N \Longrightarrow a_n = b_n = 0 \Longrightarrow a_n + b_n = 0),$$

et donc : $P + Q \in K[X]$. ■

Ceci montre que $K[X]$ est une partie de $K^{\mathbb{N}}$ stable pour $+$.

♦ **Proposition 2** On a, pour tous P, Q de $K[X]$:

1) • $\deg(P + Q) \leqslant \text{Max}\,(\deg(P), \deg(Q))$
• $\deg(P) \neq \deg(Q) \Longrightarrow \deg(P + Q) = \text{Max}\,(\deg(P), \deg(Q))$

2) • $\text{val}(P + Q) \geqslant \text{Min}\,(\text{val}(P), \text{val}(Q))$
• $\text{val}(P) \neq \text{val}(Q) \Longrightarrow \text{val}(P + Q) = \text{Min}\,(\text{val}(P), \text{val}(Q))$.

Preuve :

Les propriétés sont évidentes si $P = 0$ ou $Q = 0$.

• Supposons $P \neq 0$ et $Q \neq 0$, et notons

$$P = (a_n)_{n\in\mathbb{N}}, \quad Q = (b_n)_{n\in\mathbb{N}}, \quad \nu_1 = \text{val}(P), \quad \nu_2 = \text{val}(Q),$$
$$N_1 = \deg(P), \quad N_2 = \deg(Q), \quad \nu = \text{Min}(\nu_1, \nu_2), \quad N = \text{Max}\,(N_1, N_2).$$

Alors $P + Q = (a_n + b_n)_{n\in\mathbb{N}}$ et, pour tout n de $\mathbb{N}$:

$$n < \nu \Longrightarrow \begin{cases} n < \nu_1 \\ n < \nu_2 \end{cases} \Longrightarrow \begin{cases} a_n = 0 \\ b_n = 0 \end{cases} \Longrightarrow a_n + b_n = 0$$

$$n > N \Longrightarrow \begin{cases} n > N_1 \\ n > N_2 \end{cases} \Longrightarrow \begin{cases} a_n = 0 \\ b_n = 0 \end{cases} \Longrightarrow a_n + b_n = 0.$$

Ceci prouve : $\text{val}(P + Q) \geqslant \nu$ et $\deg(P + Q) \leqslant N$.

• Supposons $\deg(P) \neq \deg(Q)$; par exemple : $N_1 = \deg(P) < \deg(Q) = N_2$.

Alors $a_N + b_N = a_{N_2} + b_{N_2} = b_{N_2} \neq 0$, donc $\deg(P + Q) = N_2 = N$.

De même, si, par exemple, $\nu_1 = \text{val}(P) > \text{val}(Q) = \nu_2$, alors $a_\nu + b_\nu = a_{\nu_2} + b_{\nu_2} = b_{\nu_2} \neq 0$, donc $\text{val}(P + Q) = \nu_2 = \nu$.

Remarque :

D'après la Proposition précédente, si $\deg(P) < \deg(Q)$, le terme de plus haut degré de $P + Q$ est le même que celui de Q.

◆ **Proposition 3**

$(K[X],+)$ est un groupe abélien.

Preuve :

1) La loi $+$ est interne dans $K[X]$ (cf. Prop.1 p. 141).

2) La loi $+$ étant associative et commutative dans $K^{\mathbb{N}}$ (cf. exercice 2.1.13 p. 45) l'est a fortiori dans $K[X]$.

3) 0 est neutre pour $+$ dans $K[X]$.

4) Tout $P = (a_n)_{n\in\mathbb{N}}$ de $K[X]$ admet un symétrique pour $+$ dans $K[X]$, qui est $(-a_n)_{n\in\mathbb{N}}$ et est noté $-P$.

5.1.3 Multiplication

◆ **Proposition - Définition 1** Soient $P = (a_n)_{n\in\mathbb{N}}$, $Q = (b_n)_{n\in\mathbb{N}} \in K[X]$.

On appelle **produit** de P par Q, et on note PQ, la suite $(c_n)_{n\in\mathbb{N}}$ de $K^{\mathbb{N}}$ définie par :

$$\forall n \in \mathbb{N}, \quad c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{i+j=n} a_i b_j.$$

On a alors : $PQ \in K[X]$.

Preuve :

Si $P = 0$ ou $Q = 0$, alors $PQ = 0$.

Supposons $P \neq 0$ et $Q \neq 0$. Notons $N_1 = \deg(P)$, $N_2 = \deg(Q)$.

Soit $n \in \mathbb{N}$ tel que $n > N_1 + N_2$. Alors : $\forall k \in \{0,\dots,n\}$, $(k > N_1$ ou $n - k > N_2)$,

donc : $\forall k \in \{0,\dots,n\}$, $a_k b_{n-k} = 0$, et donc $c_n = 0$.

Ceci prouve : $PQ \in K[X]$.

◆ **Proposition 2**

$$\forall (P,Q) \in (K[X])^2, \quad \begin{cases} \deg(PQ) = \deg(P) + \deg(Q) \\ \mathrm{val}(PQ) = \mathrm{val}(P) + \mathrm{val}(Q). \end{cases}$$

On convient ici que :

- $\forall N \in \mathbb{N}$, $\big((-\infty) + N = -\infty, \quad (+\infty) + N = +\infty\big)$
- $(-\infty) + (-\infty) = -\infty, \quad (+\infty) + (+\infty) = +\infty.$

Preuve :

La propriété est immédiate lorsque $P = 0$ ou $Q = 0$. Supposons $P \neq 0$ et $Q \neq 0$, et notons

$$P = (a_n)_{n\in\mathbb{N}}, \quad Q = (b_n)_{n\in\mathbb{N}}, \quad N_1 = \deg(P) \quad N_2 = \deg(Q), \quad PQ = (c_n)_{n\in\mathbb{N}}.$$

D'après la preuve de la Prop.-Déf. précédente : $\forall n \in \mathbb{N}$, $(n > N_1 + N_2 \Longrightarrow c_n = 0)$.

De plus :

$$c_{N_1+N_2} = \sum_{k=0}^{N_1+N_2} a_k b_{N_1+N_2-k} = a_{N_1} b_{N_2},$$

car, pour tout k de $\mathbb{N}$:

$$\begin{cases} k < N_1 \Longrightarrow N_1 + N_2 - k > N_2 \Longrightarrow b_{N_1+N_2-k} = 0 \\ k > N_1 \Longrightarrow a_k = 0. \end{cases}$$

Ceci prouve : $\deg(PQ) = \deg(P) + \deg(Q)$.
La formule sur les valuations se montre de façon analogue.

◆ **Proposition 3**

$(K[X],+,\cdot)$ est un anneau intègre.

Preuve : (pouvant être omise en première lecture) :

1) D'après 5.1.2 Prop. 3 p. 142 $(K[X],+)$ est un groupe abélien.

2) La multiplication est interne dans $K[X]$ (cf. Prop.- Déf. 1 p. 142).

3) Montrons que $\cdot$ est associative dans $K[X]$.

Soient $P = (a_n)_{n\in\mathbb{N}}$, $Q = (b_n)_{n\in\mathbb{N}}$, $R = (c_n)_{n\in\mathbb{N}} \in K[X]$.

Alors : $PQ = (d_n)_{n\in N}$ où : $\forall n \in \mathbb{N}$, $d_n = \sum_{k=0}^{n} a_k b_{n-k}$,

puis $(PQ)R = (e_n)_{n\in\mathbb{N}}$ où : $\forall n \in \mathbb{N}$, $e_n = \sum_{k=0}^{n} d_k c_{n-k}$.

Et $QR = (f_n)_{n\in\mathbb{N}}$ où : $\forall n \in \mathbb{N}$, $f_n = \sum_{k=0}^{n} b_k c_{n-k}$,

puis $P(QR) = (g_n)_{n\in\mathbb{N}}$ où : $\forall n \in \mathbb{N}$, $g_n = \sum_{k=0}^{n} a_k f_{n-k}$.

On a, pour tout n de $\mathbb{N}$:

$$\begin{aligned} g_n &= \sum_{i+p=n} a_i f_p = \sum_{i+p=n} a_i \left(\sum_{j+k=p} b_j c_k \right) \\ &= \sum_{i+(j+k)=n} a_i (b_j c_k) = \sum_{(i+j)+k=n} (a_i b_j) c_k \\ &= \sum_{q+k=n} \left(\sum_{i+j=q} a_i b_j \right) c_k \\ &= \sum_{q+k=n} d_q c_k = e_n. \end{aligned}$$

Ceci prouve : $(PQ)R = P(QR)$.

4) De manière analogue, on montre que $\cdot$ est commutative, et distributive sur $+$.

5) Il est clair que le polynôme $(1,0,\ldots,0,\ldots)$ est neutre pour la multiplication. On note 1 au lieu de $(1,0,\ldots,0,\ldots)$.

6) D'après la Prop. p. 000, si $P \neq 0$ et $Q \neq 0$, alors $\deg(PQ) = \deg(P)+\deg(Q) \neq -\infty$, donc $PQ \neq 0$.

◆ **Proposition 3** Les éléments inversibles de l'anneau $K[X]$ sont les suites $(\alpha,0,\ldots,0\ldots)$ pour $\alpha \in K - \{0\}$.

Preuve :

1) Soit P un élément inversible de $K[X]$; il existe donc $Q \in K[X]$ tel que $PQ = 1$. Alors $P \neq 0$, $Q \neq 0$ et $\deg(P) + \deg(Q) = \deg(PQ) = 0$, d'où $\deg(P) = \deg(Q) = 0$. Il existe donc $\alpha \in K - \{0\}$ tel que $P = (\alpha,0,\ldots,0,\ldots) = \alpha 1$.

2) Réciproquement, il est clair que, pour tout α de $K - \{0\}$, le polynôme $(\alpha,0,\ldots,0,\ldots)$ est inversible et a pour inverse $(\alpha^{-1},0,\ldots,0,\ldots)$.

5.1.4 Loi externe

Les propositions suivantes sont immédiates.

◆ **Proposition - Définition 1**

Soient $\lambda \in K$, $P = (a_n)_{n\in\mathbb{N}} \in K[X]$.

On note $\lambda P = (\lambda a_n)_{n\in\mathbb{N}}$, et on a : $\lambda P \in K[X]$.

◆ **Proposition 2**

$$\forall \lambda \in K - \{0\},\ \forall P \in K[X],\quad \begin{cases} \deg(\lambda P) = \deg(P) \\ \mathrm{val}(\lambda P) = \mathrm{val}(P) \end{cases}.$$

◆ **Proposition 3** $K[X]$, muni des lois $+$, $\cdot$ (externe), $\cdot$ (interne) est une K-algèbre associative, commutative , unitaire.

Pour la définition d'une K-algèbre, voir 6.1, Déf.2 p. 209.

Preuve :

1) $(K[X],+)$ est un groupe abélien (cf. 5.1.2 Prop. 3 p. 142).

2) Les propriétés suivantes, pour tous λ,μ de K et P,Q de $K[X]$ sont immédiates :

$$(\lambda+\mu)P = \lambda P + \mu P,\ \lambda(P+Q) = \lambda P + \lambda Q,\ 1P = P,\ \lambda(\mu P) = (\lambda\mu)P.$$

Ainsi, $(K[X],+,\cdot$ (externe)) est un K-ev .

3) On a vu (5.1.3 Prop. p. 143) que la multiplication dans $K[X]$ est associative, commutative, distributive sur $+$, et admet un neutre (qui est 1).

4) Enfin, la propriété $\forall \lambda \in K,\ \forall P,Q \in K[X],\ \lambda(PQ) = (\lambda P)Q$ est immédiate.

◆ **Proposition 4**

L'application $\theta : \begin{array}{ccc} K & \longrightarrow & K[X] \\ \lambda & \longmapsto & \lambda 1 \end{array}$ est un morphisme injectif de K-algèbres.

Pour la définition de morphisme de K-algèbres, voir 7.1.1, Déf. 4 p. 241.

Preuve :

Les propriétés suivantes sont immédiates :

1) $\forall (\lambda,\mu) \in K^2, \quad \theta(\lambda+\mu) = \theta(\lambda) + \theta(\mu)$

2) $\forall (\lambda,\mu) \in K^2, \quad \theta(\lambda\mu) = \theta(\lambda)\theta(\mu)$

3) $\theta(1) = 1$

4) $\forall \lambda \in K, (\theta(\lambda) = 0 \Longrightarrow \lambda = 0)$. ■

La Proposition précédente permet d'«identifier» un élément λ de K et le polynôme $\lambda 1$ de $K[X]$, donc de «plonger» K dans $K[X]$.

◆ **Notation**

On note $X = (0,1,0\ldots,0,\ldots)$, appelée **l'indéterminée**.

Conformément à 2.1 Not. p. 41, on note $X^0 = 1$ et, pour tout n de $\mathbb{N}$, $X^{n+1} = X^n X$; en particulier : $X^1 = X$.

Une récurrence immédiate montre :

$$\forall n \in \mathbb{N}^*, \ X^n = (0,\ldots,0,1,0,\ldots,0,\ldots)$$

où 1 est à la place n° n (le premier 0 étant situé à la place n° 0).

Soit $P = (a_n)_{n\in\mathbb{N}} \in K[X]$, $N \in \mathbb{N}$ tel que $N \geqslant \deg(P)$; on a :

$$\begin{aligned} P &= (a_0,a_1,\ldots,a_N,0,\ldots,0,\ldots) \\ &= a_0(1,0,\ldots,0,\ldots) + a_1(0,1,0,\ldots,0,\ldots) + \ldots + a_N(0,\ldots,0,1,0,\ldots,0,\ldots) \\ &= a_0 + a_1 X + \ldots, + a_N X^N = \sum_{n=0}^{N} a_n X^n. \end{aligned}$$

Nous abandonnons maintenant la notation $(a_n)_{n\in\mathbb{N}}$ pour un polynôme, et nous adoptons à sa place la notation $\sum_{n=0}^{N} a_n X^n$ (où $N \geqslant \deg(P)$), ou encore $\sum_{n\in\mathbb{N}} a_n X^n$ ou $\sum_{n=0}^{+\infty} a_n X^n$ (qui évite d'indiquer le degré du polynôme).

Pour $P = \sum_{n\in\mathbb{N}} a_n X^n \in K[X]$ et $n \in \mathbb{N}$, l'élément a_n de K est appellé **le coefficient de X^n dans P**, et le monôme $a_n X^n$ est le **terme de degré n de P**.

La Proposition suivante est immédiate.

◆ **Proposition - Définition 5**

La famille infinie $(X^n)_{n\in\mathbb{N}}$, c'est-à-dire $(1,X,X^2,\ldots,X^n,\ldots)$, est une base du K-ev $K[X]$, appelée **base canonique** de $K[X]$.

Pour $n \in \mathbb{N}$ fixé, l'ensemble $\{P \in K[X];\ \deg(P) \leqslant n\}$ est clairement un K-sev de $K[X]$, souvent noté $K_n[X]$. La famille finie $(1,X,\ldots,X^n)$ est une base de $K_n[X]$, appelée **base canonique** de $K_n[X]$. On a donc : $\dim(K_n[X]) = n+1$.

◆ **Proposition 6** Soient I une partie de $\mathbb{N}$, $(P_i)_{i\in I}$ une famille de polynômes de $K[X] - \{0\}$ telle que :

$$\forall (i,j) \in I^2, \quad \big(i \neq j \Longrightarrow \deg(P_i) \neq \deg(P_j)\big).$$

Alors $(P_i)_{i\in I}$ est libre dans le K-ev $K[X]$.

Preuve :

Soient J une partie finie non vide de I, $i_1,\ldots,i_k$ les éléments de J, qu'on peut supposer rangés de façon que :

$$\deg\left(P_{i_1}\right) < \ldots < \deg\left(P_{i_k}\right).$$

Soient $\lambda_1,\ldots,\lambda_k \in K$ tels que $\sum_{j=1}^{k} \lambda_j P_{i_j} = 0$.

Le coefficient de $X^{\deg\left(P_{i_k}\right)}$ dans $\sum_{j=1}^{k} \lambda_j P_{i_j}$ est $\lambda_k \alpha_{i_k}$ (où α_{i_k} est le coefficient dominant de P_{i_k}), d'où $\lambda_k = 0$.

En réitérant, on déduit : $\lambda_k = 0$, $\lambda_{k-1} = 0,\ldots,\lambda_1 = 0$, et donc $(P_i)_{i\in J}$ est libre.

Comme toute sous-famille finie de $(P_i)_{i\in I}$ est libre, $(P_i)_{i\in I}$ est libre (cf. 6.3.1 *2)* p. 217).

Remarque :

Un cas particulier fréquent est celui où $I = \mathbb{N}$ et $(\forall i \in \mathbb{N}\ \deg(P_i) = i)$.

On dit alors que $(P_i)_{i\in\mathbb{N}}$ est une famille de polynômes **à degrés successifs.**

Dans ce cas, $(P_i)_{i\in\mathbb{N}}$ est une base de $K[X]$ et, pour chaque n de $\mathbb{N}$, $(P_i)_{0\leqslant i\leqslant n}$ est une base de $K_n[X]$.

Pour chaque n de $\mathbb{N}$, la matrice de passage de la base canonique $(1,X,\ldots,X^n)$ de $K_n[X]$ à la base $(P_i)_{0\leqslant i\leqslant n}$ (cf. 8.2.1 Déf. p. 286) est triangulaire supérieure à termes diagonaux tous non nuls. Son inverse pourra donc être calculé «en cascade».

5.1.5 Composition

◆ **Définition** Soient $P = \sum_{n=0}^{N} a_n X^n \in K[X]$ et $Q \in K[X]$. On définit le polynôme **composé** $P \circ Q$ (ou : $P(Q)$) par : $P \circ Q = P(Q) = \sum_{n=0}^{N} a_n Q^n$.

Ainsi, $P(Q)$ s'obtient en substituant Q à X dans P. Le lecteur pourra montrer les propositions suivantes :

◆ **Proposition 1**

$$\forall (P,Q) \in (K[X] - \{0\})^2, \quad \deg(P \circ Q) = \deg(P) \cdot \deg(Q).$$

◆ **Proposition 2** Pour tous α de K et P, Q, R de $K[X]$:

1) $(P + \alpha Q) \circ R = P \circ R + \alpha Q \circ R$

2) $(PQ) \circ R = (P \circ R) \cdot (Q \circ R)$

3) $(P \circ Q) \circ R = P \circ (Q \circ R)$

4) $X \circ P = P \circ X = P$.

D'après *4)*, on notera P ou $P(X)$ un polynôme.

Remarques :

1) La loi $\circ$ n'est pas commutative dans $K[X]$.

Exemple : $K = \mathbb{R}$, $\begin{cases} X^2 \circ (X+1) = (X+1)^2 = X^2 + 2X + 1 \\ (X+1) \circ X^2 = X^2 + 1. \end{cases}$

2) La loi $\circ$ n'est pas distributive à gauche sur $+$ dans $K[X]$.

Exemple : $K = \mathbb{R}$, $P = X^2$, $Q = 1$, $R = 1$; on a : $P \circ (Q + R) = X^2 \circ 2 = 4$ et $(P \circ Q) + (P \circ R) = (X^2 \circ 1) + (X^2 \circ 1) = 1 + 1 = 2$.

5.1.6 Dérivation

◆ **Définition** Pour tout $P = \sum_{n=0}^{N} a_n X^n$ de $K[X]$, on appelle **polynôme dérivé de** P, et on note P', le polynôme défini par :

$$P' = \sum_{n=1}^{N} n a_n X^{n-1} = \sum_{n=0}^{N-1} (n+1) a_{n+1} X^n.$$

On note $P^{(0)} = P$, $P^{(1)} = P'$, $P^{(2)} = P'' = (P')'$, et, pour tout k de $\mathbb{N}^*$, $P^{(k)} = \left(P^{(k-1)}\right)'$.

Avec les notations précédentes, si $N = 0$, alors $P' = 0$.

Les trois Propositions suivantes sont immédiates.

◆ **Proposition 1**

$$\forall P \in K[X], \quad \deg(P') = \begin{cases} \deg(P) - 1 & \text{si } \deg(P) \geqslant 1 \\ -\infty & \text{si } \deg(P) \leqslant 0. \end{cases}$$

◆ **Proposition 2**

$$\forall P \in K[X], \ \forall n \in \mathbb{N}, \quad \Big(\deg(P) \leqslant n \iff P^{(n+1)} = 0\Big).$$

◆ **Proposition 3** Pour tous α de K et P, Q de $K[X]$:

1) $(P + \alpha Q)' = P' + \alpha Q'$

2) $(PQ)' = P'Q + PQ'$.

Ainsi, d'après Prop. 3 *1)*, la dérivation des polynômes $\begin{array}{ccc} K[X] & \longrightarrow & K[X] \\ P & \longmapsto & P' \end{array}$ est K-linéaire.

◆ **Proposition 4** **(Formule de Leibniz)**

$$\forall (P, Q) \in (K[X])^2, \ \forall k \in \mathbb{N}, \ (PQ)^{(k)} = \sum_{i=0}^{k} C_k^i P^{(i)} Q^{(k-i)}.$$

Preuve :

Récurrence sur k, comme pour la preuve de la formule du binôme de Newton (2.3.2 Th. p. 56), ou pour la formule de Leibniz de dérivation des fonctions d'une variable réelle (Tome 1, 5.1.4).

5.1.7 Fonctions polynomiales

◆ **Définition** Pour tout $P = \sum_{n=0}^{N} a_n X^n$ de $K[X]$, on note $\widetilde{P} : \begin{array}{ccc} K & \longrightarrow & K \\ x & \longmapsto & \sum_{n=0}^{N} a_n x^n \end{array}$,

appelée **fonction polynomiale associée à P.**

Schéma de Hörner

Remarquons, par exemple : $a_3x^3 + a_2x^2 + a_1x + a_0 = a_0 + (a_1 + (a_2 + a_3x)x)\,x$.

Pour le calcul pratique de $\widetilde{P}(x)$ connaissant P et x, on peut utiliser l'algorithme suivant, appelé **schéma de Hörner**.

Notons $b_N = a_N$, et pour n allant de $N - 1$ à 0 : $b_n = a_n + a_{n+1}x$.

On a alors : $P(x) = b_0$.

Exemple : $K = \mathbb{R}$, $P = X^3 - 2X^2 + 4X + 5$, $x = 4$:

$$b_3 = a_3 = 1 \quad b_2 = a_2 + b_3x = 2 \quad b_1 = a_1 + b_2x = 12 \quad b_0 = a_0 + b_1x = 53,$$

d'où $\widetilde{P}(4) = 53$. ■

Remarque :

On peut généraliser la Définition précédente. Soient A une K-algèbre associative et commutative, $P = \sum_{n=0}^{N} a_n X^n \in K[X]$; on note $\widetilde{P} : A \longrightarrow A$, $x \longmapsto \sum_{n=0}^{N} a_n x^n$ (où $x^0 = 1_A$, $x^n = x(x^{n-1})$, pour $n \in \mathbb{N}^*$, cf. 2.1 Not. p. 39 et p. 41).

• Par exemple, si E est un K-ev, pour tout $P = \sum_{n=0}^{N} a_n X^n$ de $K[X]$ et tout f de $\mathcal{L}_K(E)$, on note $\widetilde{P}(f) = \sum_{n=0}^{N} a_n f^n$ (aussi noté $P(f)$), appelé **polynôme d'endomorphisme.**

• De même, pour tout $P = \sum_{n=0}^{N} a_n X^n$ de $K[X]$ et toute A de $\mathbf{M}_p(K)$ $(p \in \mathbb{N}^*)$, on note $\widetilde{P}(A) = \sum_{n=0}^{N} a_n A^n$ (aussi noté $P(A)$), appelé **polynôme de matrice**.

Nous utiliserons ces notations dans le Tome 6 (2.4 p. 59).

• La composition des polynômes (cf. 5.1.5 p. 147) en relève aussi :

$$\forall P, Q \in K[X], \quad P \circ Q = \widetilde{P}(Q).$$

◆ **Proposition 1** Pour tous α de K et P, Q de $K[X]$:

1) $\widetilde{P + \alpha Q} = \widetilde{P} + \alpha \widetilde{Q}$ *2)* $\widetilde{PQ} = \widetilde{P}\widetilde{Q}$ *3)* $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$.

Preuve :

Notons $P = \sum_{n=0}^{N} a_n X^n$, $Q = \sum_{n=0}^{N} b_n X^n$, où $N \geqslant \operatorname{Max}\big(\deg(P), \deg(Q)\big)$.

1) $\forall x \in K$,

$$\widetilde{P + \alpha Q}(x) = \sum_{n=0}^{N} (a_n + \alpha b_n) x^n = \sum_{n=0}^{N} a_n x^n + \alpha \sum_{n=0}^{N} b_n x^n = \widetilde{P}(x) + \alpha \widetilde{Q}(x),$$

d'où $\widetilde{P + \alpha Q} = \widetilde{P} + \alpha \widetilde{Q}$.

2) $\forall x \in K$, $\widetilde{PQ}(x) = \sum_{n \in \mathbb{N}} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n = \sum_{n \in \mathbb{N}} \sum_{k=0}^{n} a_k x^k b_{n-k} x^{n-k}$

$$= \left(\sum_{k=0}^{N} a_k x^k \right) \left(\sum_{\ell=0}^{N} b_\ell x^\ell \right) = \widetilde{P}(x) \widetilde{Q}(x),$$

d'où $\widetilde{PQ} = \widetilde{P}\widetilde{Q}$.

3) $\forall x \in K$, $\widetilde{P \circ Q}\,(x) = \widetilde{\left(\sum_{n=0}^{N} a_n Q^n \right)}\,(x) = \sum_{n=0}^{N} a_n (\widetilde{Q}(x))^n$ (cf. *1)* et *2)*)

$$= \widetilde{P}(\widetilde{Q}(x)) = \big(\widetilde{P} \circ \widetilde{Q}\big)(x),$$

d'où $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$.

Remarque : On a, pour tout P de $\mathbb{R}[X]$, $\widetilde{P'} = \widetilde{P}'$, où :

- $\widetilde{P'}$ est la fonction polynomiale associée à P'
- $\widetilde{P}'$ est la dérivée (au sens du Tome 1, 5.1.3) de la fonction polynomiale associée à P. ■

Considérons l'application $\phi : K[X] \longrightarrow K^K$, $P \longmapsto \widetilde{P}$.

D'après *1)* et *2)* de la Prop. précédente (et $\phi(1) = 1$), ϕ est un morphisme de K-algèbres unitaires. Nous allons étudier l'injectivité de ϕ.

1) Supposons K fini; notons $\{x_1,\dots,x_N\} = K$ et considérons $P = \prod_{k=1}^{N}(X - x_k)$. On a :

- $P \neq 0$, car $\deg(P) = N \geqslant 1$
- $\widetilde{P} = 0$, car : $\forall k \in \{1,\dots,N\}$, $\widetilde{P}(x_k) = 0$.

Ceci montre que ϕ n'est pas injective.

2) Supposons K infini et soit $P \in K[X]$ tel que $\widetilde{P} = 0$. Supposons $P \neq 0$, et notons $N = \deg(P)$. Comme K est infini, il existe $x_1,\dots,x_{N+1} \in K$ deux à deux distincts. On a alors : $\forall k \in \{1,\dots,N+1\}$, $\widetilde{P}(x_k) = 0$.

D'après 5.3.1 Cor. 1 p. 169 qu'on verra plus loin, on déduit $P = 0$, contradiction.

Ceci montre que, si K est infini, alors ϕ est injective.

Finalement :

◆ **Proposition 2** L'application $K[X] \longrightarrow K^K$, $P \longmapsto \widetilde{P}$ est injective si et seulement si K est infini.

Remarque : Lorsque K est infini, on pourra donc confondre P et $\widetilde{P}$, c'est-à-dire noter P au lieu de $\widetilde{P}$. En pratique, souvent $K = \mathbb{R}$ ou $\mathbb{C}$, ce qui permet de confondre P et $\widetilde{P}$; dans ce cas, nous noterons $\widetilde{P}$ ou P, suivant la commodité.

◆ **Théorème** **(Théorème de Taylor pour les polynômes)**

Soient $P \in \mathbb{C}[X]$, $N \in \mathbb{N}$ tel que $\deg(P) \leqslant N$, $a \in \mathbb{C}$. On a :

$$P(a + X) = \sum_{n=0}^{N} \frac{\widetilde{P^{(n)}}(a)}{n!} X^n.$$

Preuve :

1) Pour tout i de $\mathbb{N}$, notons $e_i = X^i$, et montrons la formule pour e_i.

Une récurrence immédiate montre :

$$\forall n \in \mathbb{N},\quad e_i^{(n)} = \begin{cases} i(i-1)\dots(i-n+1)e_{i-n} & \text{si } n \leqslant i \\ 0 & \text{si } n > i \end{cases},$$

d'où : $$\forall n \in \mathbb{N},\quad e_i^{(n)}(a) = \begin{cases} \dfrac{i!}{(i-n)!}a^{i-n} & \text{si } n \leqslant i \\ 0 & \text{si } n > i \end{cases}.$$

On obtient, d'après la formule du binôme de Newton :

$$e_i(a + X) = (a + X)^i = \sum_{n=0}^{i} C_i^n a^{i-n} X^n = \sum_{n=0}^{i} \frac{i!}{(i-n)!n!} a^{i-n} X^n = \sum_{n=0}^{i} \frac{e_i^{(n)}(a)}{n!} X^n.$$

2) Pour tout polynôme $P = \sum_{i=0}^{N} \alpha_i X^i$:

$$P(a+X) = \sum_{i=0}^{N} \alpha_i e_i(a+X) = \sum_{i=0}^{N} \alpha_i \left(\sum_{n=0}^{i} \frac{e_i^{(n)}(a)}{n!} X^n \right)$$
$$= \sum_{i=0}^{N} \alpha_i \left(\sum_{n=0}^{N} \frac{e_i^{(n)}(a)}{n!} X^n \right) \quad (\text{car } e_i^{(n)}(a) = 0 \text{ si } n > i)$$
$$= \sum_{n=0}^{N} \frac{1}{n!} \left(\sum_{i=0}^{N} \alpha_i e_i^{(n)}(a) \right) X^n = \sum_{n=0}^{N} \frac{1}{n!} \widetilde{P^{(n)}}(a) X^n.$$

Remarques :

1) Dans le théorème précédent, le corps utilisé est $\mathbb{C}$, car nous avons besoin de diviser (dans K) par des entiers (les $n!$). Plus généralement, le théorème de Taylor pour les polynômes s'applique lorsque K est un corps de caractéristique 0 (cf. exercice 2.3.4 p. 58), c'est-à-dire un corps tel que : $\forall n \in \mathbb{N}^*,\ n1_K \neq 0_K$.

2) Le théorème de Taylor pour les polynômes fournit la décomposition de $P(a+X)$ sur la base canonique $(1, X, \ldots, X^n, \ldots)$ de $K[X]$.

3) Dans l'algèbre $\mathbb{C}[X,Y]$ des polynômes à deux indéterminées sur $\mathbb{C}$ (cf. plus loin, 5.1.8 p. 152), on montre plus généralement, pour tout P de $\mathbb{C}[X]$ et N de $\mathbb{N}$ tel que $\deg(P) \leqslant N$:

$$P(X+Y) = \sum_{n=0}^{N} \frac{P^{(n)}(X)}{n!} Y^n.$$

En remplaçant Y par a, on déduit :

$$P(X+a) = \sum_{n=0}^{N} \frac{a^n}{n!} P^{(n)}(X),$$

ce qui fournit la décomposition de $P(X+a)$ sur la base $\left(P^{(n)}(X)\right)_{0 \leqslant n \leqslant N}$ de $\mathbb{C}_N[X]$ (si $N = \deg(P)$).

4) En remplaçant X par $X - a$, on obtient (en supposant $\deg(P) \leqslant N$) :

$$P(X) = \sum_{n=0}^{N} \frac{\widetilde{P^{(n)}}(a)}{n!} (X-a)^n.$$

5) Pour le calcul pratique des coefficients de la décomposition de $P(X+a)$ sur la base canonique de $K[X]$, on peut utiliser un algorithme issu du schéma de Hörner (cf. p. 148).

Soient $n \in \mathbb{N}^*$, $P = \alpha_0 + \alpha_1 X + \ldots + \alpha_n X^n \in K[X]$, $a \in K$.

Notons $\beta_{n-1} = \alpha_n$, puis, pour k allant de $n-1$ à 0 : $\beta_{k-1} = \beta_k a + \alpha_k$, et enfin $\gamma_0 = \beta_{-1}$.

On vérifie aisément qu'en notant $P_1 = \beta_0 + \beta_1 X + \ldots + \beta_{n-1} X^{n-1}$, on a :

$$\begin{cases} P = (X-a)P_1 + \gamma_0 \\ \gamma_0 = \widetilde{P}(a) \end{cases}.$$

En réitérant la même construction sur $P_1, \ldots$, on en déduit la décomposition de P sur la famille $(1, X-a, (X-a)^2, \ldots, (X-a)^n)$.

Exemple : $K = \mathbb{R}$, $P = X^3 + 4X^2 - 6X + 2$, $a = 3$:

coefficients de P :	1	4	-6	2		
coefficients de P_1 :		1	7	15	47	$(= \gamma_0)$
			1	10	45	
				1	13	
					1	

Chaque terme (sauf ceux de la 1ère ligne) vaut le produit de a par le terme situé à sa gauche, augmenté du terme situé au-dessus de ce dernier.

On déduit : $P = 47 + 45(X - 3) + 13(X - 3)^2 + (X - 3)^3$.

5.1.8 Notion de polynôme à plusieurs indéterminées

La théorie précédente (§§ 5.1.1 à 5.1.7) peut être reprise plus généralement, avec quelques modifications, en remplaçant le corps K par un anneau commutatif A. On construit ainsi **l'anneau $A[X]$ des polynômes à une indéterminée et à coefficients dans A.**

En particulier, en prenant $A = K[Y]$ on construit l'**algèbre** $K[X,Y] = (K[Y])[X]$ **des polynômes à deux indéterminées et à coefficients dans** K. En réitérant, pour $n \in \mathbb{N}^*$, on construit l'**algèbre** $K[X_1,\dots,X_n] = (K[X_2,\dots,X_n])[X_1]$ **des polynômes à n indéterminées et à coefficients dans** K.

Le lecteur pourra montrer que le K-ev $K[X_1,\dots,X_n]$ admet $\left(X_1^{i_1}\dots X_n^{i_n}\right)_{(i_1,\dots,i_n)\in\mathbb{N}^n}$ pour base.

Exercices

◇ **5.1.1** CNS sur $(\lambda,\mu) \in \mathbb{R}^2$ pour que $X^4 + \lambda X^3 + \mu X^2 + 12X + 4$ soit le carré d'un polynôme de $\mathbb{R}[X]$.

◇ **5.1.2** Soit $n \in \mathbb{N}$. En utilisant $(1 + X)^{2n}(1 - X)^{2n} = (1 - X^2)^{2n}$, montrer :

$$\sum_{k=0}^{2n}(-1)^k \left(C_{2n}^k\right)^2 = (-1)^n C_{2n}^n.$$

◇ **5.1.3** Soient $n \in \mathbb{N}$, $(a_0,\dots,a_n) \in \mathbb{R}^{n+1}$ tel que $(\forall k \in \{1,\dots,n\},\ 0 \leqslant a_k \leqslant a_0)$, $P = \sum_{k=0}^{n} a_k X^k$.

Soit $(b_0,\dots,b_{2n}) \in \mathbb{R}^{2n+1}$ tel que : $P^2 = \sum_{l=0}^{2n} b_l X^l$. Montrer :

$$b_{n+1} \leqslant \frac{1}{2}(P(1))^2.$$

◇ **5.1.4** Soit $n \in \mathbb{N}$; pour $k \in \{0,\dots,n\}$, on note $P_k = (X + k)^k$.

Montrer que $(P_k)_{0\leqslant k\leqslant n}$ est une base de $\mathbb{R}_n[X]$.

◇ **5.1.5** Soit $n \in \mathbb{N}^*$.

a) Montrer : $\forall P \in \mathbb{R}_n[X],\ \exists ! \widehat{P} \in \mathbb{R}_n[X],\ \widehat{P}(X^2) = P(X)P(-X)$.

b) Etablir que l'application $\varphi : \mathbb{R}_n[X] \longrightarrow \mathbb{R}_n[X]$ (définie en *a)*) vérifie :
$P \longmapsto \widehat{P}$

$$\forall P, Q \in \mathbb{R}_n[X],\quad \varphi(PQ) = \varphi(P)\varphi(Q).$$

c) φ est-elle linéaire ?

◇ **5.1.6** Soient $n \in \mathbb{N}^*$, $P \in \mathbb{C}[X]$ tel que $\deg(P) < n$.

Montrer : $\displaystyle\sum_{k=0}^{n} P(k)(-1)^k C_n^k = 0$. $\Big($On pourra considérer $\Delta : \mathbb{C}[X] \longrightarrow \mathbb{C}[X]$, $A \longmapsto A(X+1) - A(X)\Big)$.

◇ **5.1.7** Soient $(\alpha, \beta) \in \mathbb{C}^2$ tel que $\alpha \neq \beta$, $A \in \mathbb{C}[X]$.

Montrer : $\exists ! P \in \mathbb{C}[X],\quad P(X - \alpha) + P(X - \beta) = A$.

◇ **5.1.8*** Trouver tous les automorphismes de la K-algèbre $K[X]$.

◇ **5.1.9** Résoudre les équations suivantes :

a) $X(X+1)P'' + (X+2)P' - P = 0$, d'inconnue $P \in \mathbb{R}[X]$

b) $P(2X) = P'(X)P''(X)$, d'inconnue $P \in \mathbb{C}[X]$.

◇ **5.1.10** Montrer que, pour tout n de $\mathbb{N}$, il existe $P_n \in \mathbb{Q}[X]$ unique tel que $P_n - P_n' = X^n$, et calculer P_n.

◇ **5.1.11*** Soit $(P_n)_{n \geqslant 0}$ la suite dans $\mathbb{R}[X]$ définie par $P_0 = 1$ et :

$$\forall n \in \mathbb{N}^*,\quad P_n = \frac{1}{n!} X(X+n)^{n-1}.$$

a) Montrer : $\forall n \in \mathbb{N}^*,\ P_n' = P_{n-1}(X+1)$

(où $P_{n-1}(X+1)$ désigne le polynôme composé de P_{n-1} et de $X+1$).

b) En déduire : $\forall n \in \mathbb{N},\ \forall (x,y) \in \mathbb{R}^2,\quad P_n(x+y) = \displaystyle\sum_{i+j=n} P_i(x)P_j(y)$.

c) En déduire : $\forall n \in \mathbb{N},\ \displaystyle\sum_{i+j=n} C_n^i (i+1)^{i-1}(j+1)^{j-1} = 2(n+2)^{n-1}$.

◇ **5.1.12** Factoriser :

a) $-X^4 - Y^4 - Z^4 + 2X^2Y^2 + 2X^2Z^2 + 2Y^2Z^2$ dans $\mathbb{C}[X,Y,Z]$

b) $(X+Y+Z)^5 - (X^5 + Y^5 + Z^5)$ dans $\mathbb{R}[X,Y,Z]$.

◇ **5.1.13*** Soient $A = K[X_1, X_2, X_3, X_4]$, $I = \{P_1X_1 + P_2X_2;\ (P_1, P_2) \in A^2\}$,

$J = \{P_3X_3 + P_4X_4;\ (P_3, P_4) \in A^2\}$, $E = \{PQ;\ (P,Q) \in I \times J\}$.

Vérifier que I, J sont des idéaux de A (cf. plus loin, 5.2.3 *1)* Déf. p. 158), mais que E n'est pas un idéal de A.

5.2 Arithmétique dans $K[X]$

Le lecteur pourra utilement comparer ce § 5.2 au ch. 4 sur l'arithmétique dans $\mathbb{Z}$.

5.2.1 Divisibilité

◆ **Définition** Soit $(A,P) \in (K[X])^2$. On dit que A **divise** P (dans $K[X]$) et on note $A|P$ si et seulement s'il existe $Q \in K[X]$ tel que $P = AQ$.

Au lieu de A divise P, on dit aussi : A est un **diviseur** de P, ou : P est un **multiple** de A.

Remarques :

1) $\forall A \in K[X], \quad A|0.$

2) $\forall P \in K[X], \quad (0|P \iff P = 0).$

3) En notant, pour tout A de $K[X]$, $AK[X] = \{P \in K[X];\ \exists Q \in K[X],\ P = AQ\}$, on a, pour tout (A,P) de $(K[X])^2$: $A|P \iff AK[X] \supset PK[X]$.

◆ **Propositon 1**

1) $\forall A \in K[X], \quad A|A$

2) $\forall (A,P) \in (K[X])^2, \quad \left(\begin{cases} A|P \\ P|A \end{cases} \iff (\exists \alpha \in K - \{0\},\ P = \alpha A) \right)$

3) $\forall (A,B,C) \in (K[X])^3, \quad \left(\begin{cases} A|B \\ B|C \end{cases} \implies A|C \right).$

Preuve :

1) Evident.

2) • Supposons $A|P$ et $P|A$. Il existe $B,Q \in K[X]$ tels que $P = AQ$ et $A = PB$, d'où $P = P(BQ)$.

Si $P = 0$, alors $A = P = 0$.

Si $P \neq 0$, comme l'anneau $K[X]$ est intègre, on déduit $BQ = 1$, puis (cf. 5.1.3 Prop. 2 p. 142) $\deg(B) = \deg(Q) = 0$. Il existe donc $\alpha \in K - \{0\}$ tel que $Q = \alpha$, d'où $P = \alpha A$.

• Réciproquement, s'il existe $\alpha \in K - \{0\}$ tel que $P = \alpha A$, il est clair que $A|P$ et $P|A$ (car $\alpha^{-1} \in K$ et $A = \alpha^{-1}P$).

3) Supposons $A|B$ et $B|C$. Il existe $(D,E) \in (K[X])^2$ tel que $B = AD$ et $C = BE$, d'où $C = A(DE)$ et $DE \in K[X]$, donc $A|C$.

Remarque :

Les *1)* et *3)* ci-dessus montrent que la divisibilité est un **préordre** dans $K[X]$, c'est-à-dire est réflexive et transitive. ■

On montre comme dans 4.1.1 p. 100 la Proposition suivante :

◆ **Propositon 2**

1) $\forall (A,B,C) \in (K[X])^3, \quad (A|B \Longrightarrow A|BC).$

2) $\forall (A,B,C) \in (K[X])^3, \quad \left(\begin{cases} A|B \\ A|C \end{cases} \Longrightarrow A \mid B+C\right).$

3) $\forall (A,B,P,Q) \in (K[X])^4, \quad \left(\begin{cases} A|B \\ P|Q \end{cases} \Longrightarrow AP|BQ\right).$

4) $\forall (A,B,n) \in (K[X])^2 \times \mathbb{N}^*, \quad (A|B \Longrightarrow A^n|B^n).$

Exercices

◇ **5.2.1** Montrer : $\forall n \in \mathbb{N}, \quad X^2 \mid (X+1)^n - nX - 1$ dans $K[X]$.

◇ **5.2.2** Montrer : $\forall (n,p) \in (\mathbb{N}^*)^2, \quad \sum_{i=0}^{n-1} X^i \left| \left(\sum_{i=0}^{n} X^i\right)^p - X^n \right.$ dans $K[X]$.

◇ **5.2.3** Soient $\theta \in \mathbb{R}$, $n \in \mathbb{N}^*$, $A = X^2 - 2X\cos\theta + 1$, $B_n = X^n \sin\theta - X \sin n\theta + \sin(n-1)\theta$. Montrer $A|B_n$ et former le polynôme C_n tel que $B_n = AC_n$.
(On pourra remarquer : $B_n = XB_{n-1} + A \sin(n-1)\theta$).

5.2.2 Division euclidienne

◆ **Théorème - Définition** Soit $(A,B) \in K[X] \times (K[X] - \{0\})$. Il existe un couple unique (Q,R) de $(K[X])^2$ tel que :

$$\begin{cases} A = BQ + R \\ \deg(R) < \deg(B). \end{cases}$$

Le polynôme Q (resp. R) s'appelle le **quotient** (resp. **reste**) **de la division euclidienne de** A **par** B.

Preuve :

1) **Existence**

Notons $p = \deg(B) \geqslant 0, \quad B = \sum_{j=0}^{p} b_j X^j$ (donc $b_p \neq 0$). Nous allons procéder à une récurrence sur le degré de A. Considérons la propriété $\mathcal{P}_n$ suivante :

Pour tout A de $K[X]$ tel que $\deg(A) \leqslant n$, il existe $(Q,R) \in (K[X])^2$ tel que :

$$A = BQ + R \text{ et } \deg(R) < \deg(B).$$

• $\mathcal{P}_0$ est vraie. En effet, si A est une constante, il suffit de prendre :

$$\begin{cases} Q = 0 \text{ et } R = A, & \text{si } \deg(B) \geqslant 1 \\ Q = Ab_p^{-1} \text{ et } R = 0, & \text{si } \deg(B) = 0. \end{cases}$$

• Supposons $\mathcal{P}_n$ vraie pour un n de $\mathbb{N}$, et soit $A \in K[X]$ tel que $\deg(A) = n+1$. Notons $A = \sum_{i=0}^{n+1} a_i X^i$, et considérons :

$$Q_{n+1} = a_{n+1}b_p^{-1}X^{n+1-p} \text{ et } R_{n+1} = A - BQ_{n+1}.$$

Par le choix de Q_{n+1}, les termes de degré $n+1$ de A et de BQ_{n+1} sont les mêmes, donc $\deg(R_{n+1}) \leqslant n$.

D'après $\mathcal{P}_n$, il existe $(Q_n, R_n) \in (K[X])^2$ tel que : $R_{n+1} = BQ_n + R_n$ et $\deg(R_n) < \deg(B)$.

En notant $Q = Q_{n+1} + Q_n$ et $R = R_n$, on a :

$$A = BQ_{n+1} + (BQ_n + R_n) = BQ + R \text{ et } \deg(R) < \deg(B).$$

2) **Unicité**

Supposons qu'il existe (Q_1,R_1), (Q_2,R_2) convenant. On a alors $R_1 - R_2 = B(Q_2 - Q_1)$.

Si $Q_1 \neq Q_2$, alors $Q_2 - Q_1 \neq 0$ et $\deg(R_1 - R_2) = \deg(B) + \deg(Q_2 - Q_1) \geqslant \deg(B)$, ce qui contredit :

$$\deg(R_1 - R_2) \leqslant \text{Max}\left(\deg(R_1),\deg(R_2)\right) < \deg(B).$$

D'où $Q_1 = Q_2$ et $R_1 = R_2$.

EXEMPLES :

1) Effectuer la division euclidienne de $A = X^4 + 2X^3 - X + 6$ par $B = X^3 - 6X^2 + X + 4$ dans $\mathbb{R}[X]$.

$$\begin{array}{l|l} X^4+2X^3 \quad -X+6 & X^3 - 6X^2 + X + 4 \\ \hline 8X^3 - X^2 \ -5X+6 & X+8 \\ \quad 47X^2-13X-26 & \end{array}$$

$$Q = X + 8, \quad R = 47X^2 - 13X - 26.$$

2) Effectuer la division euclidienne de $A = iX^3 - X^2 + (1-i)$ par $B = (1+i)X^2 - iX + 3$ dans $\mathbb{C}[X]$.

$$\begin{array}{l|l} iX^3 - X^2 \qquad +(1-i) & (1+i)X^2 - iX + 3 \\ \hline \dfrac{-3+i}{2}X^2 - \dfrac{3+3i}{2}X + (1-i) & \dfrac{1+i}{2}X + \dfrac{-1+2i}{2} \\ \qquad \dfrac{-5-4i}{2}X + \dfrac{5-8i}{2} & \end{array}$$

$$Q = \frac{1+i}{2}X + \frac{-1+2i}{2}, \quad R = \frac{-5-4i}{2}X + \frac{5-8i}{2}.$$

Remarque :

Il est clair que, pour tout (A,B) de $K[X] \times (K[X] - \{0\})$, B divise A si et seulement si le reste de la divison euclidienne de A par B est le polynôme nul. ■

Soient $P \in K[X]$, $a \in K$.

Par division euclidienne de P par $X - a$, il existe $(Q,R) \in (K[X])^2$ tel que :

$$P = (X-a)Q + R \text{ et } \deg(R) < 1.$$

Ainsi, R est une constante.

De plus : $\widetilde{P}(a) = \tilde{R}(a)$, d'où $R = \tilde{R}(a) = \widetilde{P}(a)$. Ceci montre que le reste de la division euclidienne de P par $X - a$ est $\widetilde{P}(a)$. En particulier :

◆ **Proposition**

$$\forall P \in K[X], \quad \forall a \in K, \quad \big(X - a \mid P \iff \widetilde{P}(a) = 0\big). \qquad \blacksquare$$

Remarque : **Changement de corps**

Soient L un corps, K un sous-corps de L (en pratique : $K = \mathbb{R}$, $L = \mathbb{C}$), $(A,B) \in (K[X])^2$, Q,R les quotient et reste de la division euclidienne de A par B dans $K[X]$. Comme Q,R sont aussi dans $L[X]$, il est clair que Q,R sont aussi le quotient et reste de la division euclidienne de A par B dans $L[X]$. En particulier, B divise A dans $K[X]$ si et seulement si B divise A dans $L[X]$.

Exercices

◇ **5.2.4** Trouver les $a \in \mathbb{R}$ tels que $X^2 - aX + 1 | X^4 - X + a$ dans $\mathbb{R}[X]$.

◇ **5.2.5** Quel est, pour $(n,\theta) \in \mathbb{N}^* \times \mathbb{R}$ fixé, le reste de la division euclidienne de $(X\sin\theta + \cos\theta)^n$ par $X^2 + 1$, dans $\mathbb{C}[X]$?

◇ **5.2.6** Soient $(k,n) \in (\mathbb{N}^*)^2$, r le reste de la division euclidienne de k par n. Montrer que le reste de la division euclidienne de X^k par $X^n - 1$ est X^r.

◇ **5.2.7** Soient $P \in \mathbb{C}[X]$, $a \in \mathbb{C}$. Former le quotient de la division euclidienne de P par $X - a$. On exprimera le résultat sur la base $\big((X-a)^k\big)_{0 \leqslant k \leqslant n-1}$.

◇ **5.2.8** Soit $P \in K[X]$ tel que $\deg(P) \geqslant 1$.

a) Soient Q et R les quotient et reste de la division euclidienne de A par B. Montrer que les quotient et reste de la division euclidienne de $A \circ P$ par $B \circ P$ sont $Q \circ P$ et $R \circ P$.

b) En déduire : $\forall (A,B) \in (K[X])^2$, $(B|A \iff B \circ P | A \circ P)$.

5.2.3 Pgcd, ppcm

1) Idéaux de $K[X]$

◆ **Définition** On appelle **idéal** de $K[X]$ toute partie $\mathcal{I}$ de $K[X]$ telle que :

- $\mathcal{I} \neq \varnothing$
- $\forall (P,Q) \in \mathcal{I}^2, \quad P+Q \in \mathcal{I}$
- $\forall A \in K[X], \ \forall P \in \mathcal{I}, \ AP \in \mathcal{I}.$

On définit plus généralement la notion **d'idéal d'un anneau commutatif** ou même d'**idéal à gauche**, d'**idéal à droite d'un anneau**.

Remarques :

1) Si $\mathcal{I}$ est un idéal de $K[X]$, alors en particulier :

$$\begin{cases} \mathcal{I} \neq \varnothing \\ \forall (P,Q) \in \mathcal{I}^2, \quad P+Q \in \mathcal{I}, \\ \forall P \in \mathcal{I}, \ -P \in \mathcal{I} \end{cases}$$

et donc $\mathcal{I}$ est un sous-groupe de $(K[X],+)$.

2) Soient $P_0 \in K[X]$ et $P_0K[X]$ l'ensemble des multiples de P_0 dans $K[X]$, c'est-à-dire :

$$P_0K[X] = \{P_0A; \ A \in K[X]\}.$$

Il est clair que $P_0K[X]$ est un idéal de $K[X]$.

◆ **Théorème** Pour tout idéal $\mathcal{I}$ de $K[X]$, il existe $P_0 \in K[X]$ tel que :

$$\mathcal{I} = P_0K[X] = \{P \in K[X]; \ \exists A \in K[X], \ P = P_0A\}.$$

On exprime ce résultat par : tout idéal de $K[X]$ est **principal**, ou encore : $K[X]$ est un **anneau principal**.

Preuve :

Soit $\mathcal{I}$ un idéal de $K[X]$.

Si $\mathcal{I} = \{0\}$, alors $\mathcal{I} = 0K[X]$.

Supposons $\mathcal{I} \neq \{0\}$. L'ensemble $\{\deg(P); \ P \in K[X] - \{0\}\}$ est une partie non vide de $\mathbb{N}$, donc admet un plus petit élément, noté n_0, et il existe $P_0 \in \mathcal{I} - \{0\}$ tel que $\deg(P_0) = n_0$.

Nous allons montrer : $\mathcal{I} = P_0K[X]$.

1) Puisque $P_0 \in \mathcal{I}$ et que $\mathcal{I}$ est un idéal de $K[X]$, on a : $\forall A \in K[X], \ P_0A \in \mathcal{I}$,

c'est-à-dire : $P_0K[X] \subset \mathcal{I}$.

2) Réciproquement, soit $P \in \mathcal{I}$. Par division euclidienne de P par P_0, il existe $(Q,R) \in (K[X])^2$ tel que : $P = P_0Q + R$ et $\deg(R) < \deg(P_0)$.

Comme $R = P - P_0Q$, que P, P_0 sont dans $\mathcal{I}$, et que $\mathcal{I}$ est un idéal de $K[X]$, on déduit : $R \in \mathcal{I}$. Puis, par définition de P_0, comme $\deg(R) < \deg(P_0)$, on obtient $R = 0$, d'où : $P = P_0Q \in P_0K[X]$. ■

Remarque :

La preuve précédente établit, plus généralement, que tout anneau dit euclidien est principal.

2) Pgcd, ppcm

Soient $n \in \mathbb{N}^*$, $(P_1,\dots,P_n) \in (K[X]-\{0\})^n$.

L'ensemble des degrés des polynômes P de $K[X]-\{0\}$ tels que $(\forall i \in \{1,\dots,n\},\ P|P_i)$ est une partie non vide de $\mathbb{N}$ (car : $\forall i \in \{1,\dots,n\}$, $1|P_i$), majorée par $\deg(P_1)$.

Il existe donc un polynôme unitaire Δ, non nul, diviseur commun de $P_1,\dots,P_n$ et de plus grand degré parmi les diviseurs communs de $P_1,\dots,P_n$. De même, il existe un polynôme unitaire M, non nul, multiple commun de $P_1,\dots,P_n$, et de plus petit degré parmi les multiples communs de $P_1,\dots,P_n$.

Nous allons montrer :

$$\sum_{i=1}^{n} P_i K[X] = \Delta K[X], \quad \bigcap_{i=1}^{n} P_i K[X] = M K[X],$$

ce qui, d'après 5.2.1 Prop. 1 *2)* p. 154, établira l'unicité de Δ et de M.

1) • Puisque chaque $P_i K[X]$ $(1 \leqslant i \leqslant n)$ est un idéal de $K[X]$, il est clair que $\sum_{i=1}^{n} P_i K[X]$ est un idéal de $K[X]$.

Comme $K[X]$ est un anneau principal, il existe $D \in K[X]$ tel que :

$$\sum_{i=1}^{n} P_i K[X] = DK[X].$$

• Par définition de Δ : $\forall i \in \{1,\dots,n\}$, $\Delta|P_i$, d'où : $\forall i \in \{1,\dots,n\}$, $P_i K[X] \subset \Delta K[X]$, puis : $\sum_{i=1}^{n} P_i K[X] \subset \Delta K[X]$.

Il existe donc $D_1 \in K[X]$ tel que $D = \Delta D_1$.

• D'autre part : $\forall i \in \{1,\dots,n\}$, $P_i K[X] \subset \sum_{i=1}^{n} P_i K[X] = DK[X]$,

d'où : $\forall i \in \{1,\dots,n\}$, $D|P_i$.

De plus, il est clair que $D \neq 0$ (car $P_1 \in DK[X]$).

Par définition de Δ, on a alors : $\deg(D) \leqslant \deg(\Delta)$.

• Comme $D = \Delta D_1$ et $\deg(D) \leqslant \deg(\Delta)$, on déduit $D_1 \in K - \{0\}$, d'où :

$$\sum_{i=1}^{n} P_i K[X] = DK[X] = \Delta K[X].$$

• Enfin, si Δ_1, Δ_2 sont deux polynômes unitaires, non nuls, diviseurs communs de $P_1,\dots,P_n$ et de plus haut degré, comme

$$\Delta_1 K[X] = \sum_{i=1}^{n} P_i K[X] = \Delta_2 K[X],$$

on déduit $\Delta_1 = \Delta_2$, ce qui prouve l'unicité de Δ défini plus haut.

2) • Puisque chaque $P_i K[X]$ $(1 \leqslant i \leqslant n)$ est un idéal de $K[X]$, il est clair que $\bigcap_{i=1}^{n} P_i K[X]$ est aussi un idéal de $K[X]$. Comme $K[X]$ est un anneau principal, il existe $P \in K[X]$ tel que :

$$\bigcap_{i=1}^{n} P_i K[X] = PK[X].$$

• Par définition de M : $\forall i \in \{1,\ldots,n\}$, $P_i | M$, d'où :

$\forall i \in \{1,\ldots,n\}$, $MK[X] \subset P_i K[X]$, puis : $MK[X] \subset \bigcap_{i=1}^{n} P_i K[X]$.

Il existe donc $Q_1 \in K[X]$ tel que $M = Q_1 P$.

• D'autre part :

$$\forall i \in \{1,\ldots,n\}, \quad P_i K[X] \supset \bigcap_{i=1}^{n} P_i K[X] = PK[X],$$

d'où : $\forall i \in \{1,\ldots,n\}$, $P_i | P$.

De plus, il est clair que $P \neq 0$ (car $\prod_{i=1}^{n} P_i \in PK[X]$).

Par définition de M, on a alors : $\deg(M) \leqslant \deg(P)$.

• Comme $M = Q_1 P$ et $\deg(M) \leqslant \deg(P)$, on déduit $Q_1 \in K - \{0\}$, d'où :

$$\bigcap_{i=1}^{n} P_i K[X] = PK[X] = MK[X].$$

• Enfin, si M_1, M_2 sont deux polynômes unitaires, non nuls, multiples communs de $P_1,\ldots,P_n$ et de plus bas degré, comme

$$M_1 K[X] = \bigcap_{i=1}^{n} P_i K[X] = M_2 K[X],$$

on déduit $M_1 = M_2$, ce qui prouve l'unicité de M défini plus haut.

Résumons l'étude :

◆ **Proposition - Définition 1**

Soient $n \in \mathbb{N}^*$, $(P_1,\ldots,P_n) \in (K[X] - \{0\})^n$.

1) Il existe un polynôme et un seul Δ, unitaire, non nul, diviseur commun de $P_1,\ldots,P_n$ et de plus haut degré parmi les diviseurs communs de $P_1,\ldots,P_n$; Δ est appelé **le plus grand commun diviseur** (en abrégé : **pgcd**) de $P_1,\ldots,P_n$, et noté pgcd $(P_1,\ldots,P_n)$ (ou : pgcd $\big((P_i)_{1\leqslant i\leqslant n}\big)$).

2) Il existe un polynôme et un seul M, unitaire, non nul, multiple commun de $P_1,\ldots,P_n$ et de plus bas degré parmi les multiples communs de $P_1,\ldots,P_n$; M est appelé **le plus petit commun multiple** (en abrégé : **ppcm**) de $P_1,\ldots,P_n$, et noté ppcm $(P_1,\ldots,P_n)$ (ou : ppcm $\big((P_i)_{1\leqslant i\leqslant n}\big)$).

◆ **Proposition 2** Soient $n \in \mathbb{N}^*$, $(P_1,\dots,P_n) \in (K[X]-\{0\})^n$, $\Delta = \text{pgcd}(P_1,\dots,P_n)$, $M = \text{ppcm}(P_1,\dots,P_n)$. On a :

$$\sum_{i=1}^{n} P_i K[X] = \Delta K[X] \text{ et } \bigcap_{i=1}^{n} P_i K[X] = M K[X]. \quad \blacksquare$$

Le lecteur pourra, en s'inspirant de l'étude de l'arithmétique dans $\mathbb{Z}$ (4.2 pp. 107-110), montrer les Propositions suivantes :

◆ **Proposition 3** Soient $n \in \mathbb{N}^*$, $(P_1,\dots,P_n) \in (K[X]-\{0\})^n$, $(\alpha_1,\dots,\alpha_n) \in (K-\{0\})^n$. On a :

$$\begin{cases} \text{pgcd}\left((\alpha_i P_i)_{1\leqslant i\leqslant n}\right) = \text{pgcd}\left((P_i)_{1\leqslant i\leqslant n}\right) \\ \text{ppcm}\left((\alpha_i P_i)_{1\leqslant i\leqslant n}\right) = \text{ppcm}\left((P_i)_{1\leqslant i\leqslant n}\right). \end{cases}$$

◆ **Proposition 4** Soient $n \in \mathbb{N}^*$, $(P_1,\dots,P_n) \in (K[X]-\{0\})^n$, $A \in K[X]-\{0\}$ unitaire. On a :

$$\begin{cases} \text{pgcd}\left((AP_i)_{1\leqslant i\leqslant n}\right) = A\ \text{pgcd}\left((P_i)_{1\leqslant i\leqslant n}\right) \\ \text{ppcm}\left((AP_i)_{1\leqslant i\leqslant n}\right) = A\ \text{ppcm}\left((P_i)_{1\leqslant i\leqslant n}\right). \end{cases}$$

◆ **Proposition 5** Soient $n \in \mathbb{N}^*$, $(P_1,\dots,P_n) \in (K[X]-\{0\})^n$, $\Delta = \text{pgcd}(P_1,\dots,P_n)$, $M = \text{ppcm}(P_1,\dots,P_n)$, $(A,B) \in (K[X]-\{0\})^2$.
On a :
1) $(\forall i \in \{1,\dots,n\},\ A|P_i) \iff A|\Delta$
2) $(\forall i \in \{1,\dots,n\},\ P_i|B) \iff M|B$.

◆ **Proposition 6** **(Associativité du pgcd et du ppcm)**
Soient $n \in \mathbb{N}^*$, Π une partition de $\{1,\dots,n\}$, $(P_1,\dots,P_n) \in (K[X]-\{0\})^n$.
On a :

$$\begin{cases} \text{pgcd}\left((P_i)_{1\leqslant i\leqslant n}\right) = \text{pgcd}\left(\left(\text{pgcd}\left((P_i)_{i\in I}\right)\right)_{I\in\Pi}\right) \\ \text{ppcm}\left((P_i)_{1\leqslant i\leqslant n}\right) = \text{ppcm}\left(\left(\text{ppcm}\left((P_i)_{i\in I}\right)\right)_{I\in\Pi}\right). \end{cases}$$

La Prop. précédente montre qu'on peut exprimer le pgcd (resp. ppcm) de plusieurs polynômes en ne faisant intervenir que des pgcd (resp. ppcm) de deux polynômes.

◆ **Notation**
Pour $(P,Q) \in (K[X]-\{0\})^2$, on note $\begin{cases} P \wedge Q = \text{pgcd}(P,Q) \\ P \vee Q = \text{ppcm}(P,Q) \end{cases}$.

Remarque :
$\wedge$ et $\vee$ sont des lois de composition interne dans $K[X]-\{0\}$, associatives et commutatives. De plus, pour tout polynôme unitaire et non nul P :

$$P \wedge P = P, \quad P \vee P = P, \quad P \wedge 1 = 1, \quad P \vee 1 = P.$$

Nous verrrons plus loin :

- $\wedge$ et $\vee$ sont distributives l'une sur l'autre (5.2.5 Cor. p. 166)
- $\forall (P,Q) \in (K[X]-\{0\})^2, \forall k \in \mathbb{N}^*,\ P^k \wedge Q^k = (P \wedge Q)^k$ (5.2.4 *3)* Cor. p. 165).

3) Algorithme d'Euclide

En raisonnant comme dans l'étude de l'algorithme d'Euclide dans $\mathbb{Z}$ (4.2.3 p. 110), on voit que, pour tout (P,Q) de $(K[X]-\{0\})^2$, le pgcd de P et Q est le dernier reste non nul normalisé dans la suite des divisions euclidiennes successives.

EXEMPLE :

Calculer le pgcd de $P = X^5 + X + 1$ et $Q = X^4 - 2X^3 - X + 2$ dans $\mathbb{R}[X]$.

	$X+2$	$\frac{1}{4}X - \frac{9}{16}$	$4X-3$
$P = X^5 \quad +X+1$	$Q = X^4 - 2X^3 - X + 2$	$R_1 = 4X^3 + X^2 + X - 3$	$R_2 = X^2 + X + 1$
$2X^4 + X^2 - X + 1$	$-\frac{9}{4}X^3 - \frac{1}{4}X^2 - \frac{1}{4}X + 2$	$-3X^2 - 3X - 3$	
$R_1 = 4X^3 + X^2 + X - 3$	$R_2 = \frac{5}{16}X^2 + \frac{5}{16}X + \frac{5}{16}$	0	

On obtient : $P \wedge Q = X^2 + X + 1$.

Dans cet exemple, on a remplacé, dans une phase de calcul, $\frac{5}{16}(X^2 + X + 1)$ par $X^2 + X + 1$ (cf. *2)* Prop. 3 p. 161).

Exercice

◇ **5.2.9** Soient L un corps, K un sous-corps de L, $P, Q \in K[X]$. Montrer que le pgcd de P, Q dans $K[X]$ est le même que le pgcd de P, Q dans $L[X]$.

5.2.4 Polynômes premiers entre eux

1) Généralités

◆ **Définition** Soient $n \in \mathbb{N}^*$, $(P_1, \ldots, P_n) \in (K[X]-\{0\})^n$.

1) On dit que $P_1, \ldots, P_n$ sont **premiers entre eux dans leur ensemble** (ou : **étrangers**) si et seulement si : pgcd $(P_1, \ldots, P_n) = 1$.

2) On dit que $P_1, \ldots, P_n$ sont **premiers entre eux deux à deux** si et seulement si :

$$\forall (i,j) \in \{1, \ldots, n\}^2, \quad (i \neq j \Longrightarrow P_i \wedge P_j = 1).$$

Remarques :

1) Si $P_1,\dots,P_n$ sont premiers entre eux deux à deux, alors $P_1,\dots,P_n$ sont premiers entre eux dans leur ensemble.

2) La réciproque est fausse : il se peut (si $n \geqslant 3$) que $P_1,\dots,P_n$ soient premiers entre eux dans leur ensemble sans être premiers entre eux deux à deux.

Exemple : $n = 3$, $K = \mathbb{R}$, $P_1 = (X-1)X$, $P_2 = (X-1)(X+1)$, $P_3 = X(X+1)$.

3) Pour tout n de $\mathbb{N}^*$ et tout $(P_1,\dots P_n)$ de $(K[X]-\{0\})^n$, en notant $\Delta = \text{pgcd}(P_1,\dots,P_n)$, il existe $(Q_1,\dots,Q_n) \in (K[X]-\{0\})^n$ tel que $(\forall i \in \{1,\dots,n\},\ P_i = \Delta Q_i)$, et $Q_1,\dots,Q_n$ sont premiers entre eux dans leur ensemble. ■

Comme dans 4.3.1 p. 113, le lecteur pourra montrer la Proposition suivante :

◆ **Proposition**

$$\forall (A,B,C) \in (K[X]-\{0\})^3,\quad \left(\begin{cases} A \wedge B = 1 \\ C \mid B \end{cases} \Longrightarrow A \wedge C = 1\right).$$

2) Théorème de Bezout

◆ **Théorème 1** **(Théorème de Bezout)**

Soient $n \in \mathbb{N}^*, (P_1,\dots,P_n) \in (K[X]-\{0\})^n$. Pour que $P_1,\dots,P_n$ soient premiers entre eux dans leur ensemble, il faut et il suffit qu'il existe $(U_1,\dots,U_n) \in (K[X])^n$ tel que :

$$\sum_{i=1}^{n} P_i U_i = 1.$$

Preuve : Comme pour le théorème de Bezout dans $\mathbb{Z}$, 4.3.2 Th. 1 p. 113.

◆ **Théorème 2** **(Théorème de Gauss)**

$$\forall (A,B,C) \in (K[X]-\{0\})^3,\quad \left(\begin{cases} A \mid BC \\ A \wedge B = 1 \end{cases} \Longrightarrow A \mid C\right).$$

Preuve : Comme pour le théorème de Gauss dans $\mathbb{Z}$, 4.3.2 Th. 2 p. 114.

◆ **Proposition**

Soient $A,B \in K[X]-\{0\}$, premiers entre eux et non tous deux constants. Il existe $(U,V) \in (K[X])^2$ unique tel que :

$$AU + BV = 1,\quad \deg(U) < \deg(B),\quad \deg(V) < \deg(A).$$

Preuve :

1) **Existence**

Si, par exemple, A est constant, il suffit de prendre $U = A^{-1}$, $V = 0$.

Supposons donc : $\deg(A) \geqslant 1$ et $\deg(B) \geqslant 1$.

D'après le théorème de Bezout, il existe $(U_1, V_1) \in (K[X])^2$ tel que $AU_1 + BV_1 = 1$. Par division euclidienne de U_1 par B, il existe $(Q,U) \in (K[X])^2$ tel que :

$$U_1 = BQ + U \quad \text{et} \quad \deg(U) < \deg(B).$$

Notons $V = AQ + V_1$.

On a : $AU + BV = A(U_1 - BQ) + B(AQ + V_1) = AU_1 + BV_1 = 1$.

Puisque A et B sont non constants, il est clair que U, V sont non nuls et que : $\deg(AU) = \deg(BV) \geqslant 1$. Alors :

$\deg(V) + \deg(B) = \deg(BV) = \deg(AU) = \deg(A) + \deg(U) < \deg(A) + \deg(B)$,

d'où $\deg(V) < \deg(A)$.

2) **Unicité**

Soient $(U_1, V_1), (U_2, V_2)$ convenant. On a alors $A(U_1 - U_2) = B(V_2 - V_1)$. Comme $A \wedge B = 1$, le théorème de Gauss montre : $A \mid V_2 - V_1$.

Mais $\deg(V_2 - V_1) \leqslant \text{Max}\big(\deg(V_1), \deg(V_2)\big) < \deg(A)$.

D'où $V_2 - V_1 = 0$, $V_2 = V_1$, $U_2 = U_1$. ∎

Comme dans 4.3.2 p. 115, on dispose d'un algorithme pour le calcul d'un couple (U,V) de $(K[X])^2$ tel que $AU + BV = 1$ (si $A \wedge B = 1$), et le couple (U,V) ainsi obtenu vérifie : $\deg(U) < \deg(B)$ et $\deg(V) < \deg(A)$ (si $\deg(A) \geqslant 1$ et $\deg(B) \geqslant 1$).

EXEMPLE :

Montrer que (dans $\mathbb{R}[X]$) les polynômes $A = X^4 + 1$ et $B = X^3 - 1$ sont premiers entre eux et calculer un couple (U,V) de $(K[X])^2$ tel que $AU + BV = 1$.

On effectue les divisions euclidiennes successives :

			X	$X^2 - X + 1$
X^4	$+1$	X^3	-1	$X + 1$
	$X + 1$	$-X^2$	-1	
			$X - 1$	
			-2	

On obtient : $-2 = (X^3 - 1) - (X + 1)(X^2 - X + 1)$

$= (X^3 - 1) - \big((X^4 + 1) - X(X^3 - 1)\big)(X^2 - X + 1)$

$= (X^3 - X^2 + X + 1)(X^3 - 1) - (X^2 - X + 1)(X^4 + 1)$.

Un couple (U,V) convenant est :

$$U = \frac{1}{2}(X^2 - X + 1), \quad V = -\frac{1}{2}(X^3 - X^2 + X + 1).$$

3) Propriétés

◆ **Proposition 1** Soient $n \in \mathbb{N}^*$, $A, P_1, \ldots, P_n \in K[X] - \{0\}$. On a :

$$(\forall i \in \{1,\ldots,n\}, \quad A \wedge P_i = 1) \implies A \wedge \left(\prod_{i=1}^{n} P_i\right) = 1.$$

◆ **Proposition 2** $\forall (A,B) \in (K[X] - \{0\})^2$, $\forall (k,l) \in (\mathbb{N}^*)^2$,

$$(A \wedge B = 1 \iff A^k \wedge B^l = 1).$$

◆ **Corollaire**

$$\forall (A,B) \in (K[X] - \{0\})^2, \ \forall k \in \mathbb{N}^*, \quad A^k \wedge B^k = (A \wedge B)^k.$$

◆ **Proposition 3** Soient $n \in \mathbb{N}^*$, $A, P_1, \ldots, P_n \in K[X] - \{0\}$.
Si $(\forall i \in \{1,\ldots,n\}, \ P_i | A)$ et si $P_1, \ldots, P_n$ sont premiers entre eux deux à deux, alors $\prod_{i=1}^{n} P_i \,|A$.

◆ **Corollaire** Soient $n \in \mathbb{N}^*, (P_1, \ldots, P_n) \in (K[X] - \{0\})^n$. Si $P_1, \ldots, P_n$ sont premiers entre eux deux à deux, alors le ppcm de $P_1, \ldots, P_n$ est le polynôme normalisé de $\prod_{i=1}^{n} P_i$ (c'est-à-dire $\frac{1}{\alpha} \prod_{i=1}^{n} P_i$ où α est le coefficient dominant de $\prod_{i=1}^{n} P_i$).

◆ **Proposition 4** Pour tout (A,B) de $(K[X] - \{0\})^2$, $(A \wedge B)(A \vee B)$ est le polynôme normalisé de AB.

5.2.5 Polynômes irréductibles

◆ **Définition** Un polynôme P de $K[X]$ est dit **irréductible** (ou : **premier**) si et seulement si $\deg(P) \geqslant 1$ et P n'admet comme diviseur (dans $K[X]$) que les $\alpha (\alpha \in K - \{0\})$ et les βP $(\beta \in K - \{0\})$.

Remarque : **Changement de corps**

Soient L un corps, K un sous-corps de L (en pratique : $K = \mathbb{R}$ et $L = \mathbb{C}$), $P \in K[X]$.

- Si P est irréductible dans $L[X]$, alors P est irréductible dans $K[X]$.
- La réciproque est fausse : P peut être irréductible dans $K[X]$ et non irréductible dans $L[X]$.

Exemple : $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$, mais n'est pas irréductible dans $\mathbb{C}[X]$:

$$X^2 + 1 = (X + i)(X - i).$$

◆ **Proposition 1** Soient $P \in K[X]$ irréductible, $A \in K[X] - \{0\}$. On a :
$$P|A \quad \text{ou} \quad P \wedge A = 1.$$

◆ **Proposition 2** Soient $P \in K[X]$ irréductible, $n \in \mathbb{N}^*$, $A_1, \ldots, A_n \in K[X] - \{0\}$.
On a : $P \Big| \prod_{i=1}^{n} A_i \iff (\exists\, i \in \{1, \ldots, n\},\ P|A_i)$.

◆ **Théorème** Tout polynôme de $K[X]$ de degré $\geqslant 1$ admet une décomposition en produit de polynômes irréductibles, unique à l'ordre près des facteurs et à des constantes de $K - \{0\}$ multiplicatives près.

Preuve : Comme dans 4.4.3 Th. 1 p. 123. ■

Soit $A \in K[X]$ tel que $\deg(A) \geqslant 1$. D'après le théorème précédent, il existe $N \in \mathbb{N}^*$, $P_1, \ldots, P_N$ irréductibles et premiers entre eux deux à deux, $r_1, \ldots, r_N \in \mathbb{N}^*$ tels que $A = \prod_{i=1}^{N} P_i^{r_i}$. Cette égalité s'appelle **la décomposition primaire** (en abrégé : DP) **de A dans $K[X]$.**

EXEMPLE :

- La DP de $X^4 + X^3 + X + 1$ dans $\mathbb{R}[X]$ est :
$$X^4 + X^3 + X + 1 = (X + 1)^2(X^2 - X + 1).$$
- La DP de $X^4 + X^3 + X + 1$ dans $\mathbb{C}[X]$ est :
$$X^4 + X^3 + X + 1 = (X + 1)^2(X + j)(X + j^2).$$

Remarque :

Il peut être commode, dans la DP de A, $A = \prod_{i=1}^{N} P_i^{r_i}$, d'autoriser certains r_i à être nuls.

◆ **Corollaire** Tout polynôme de $K[X]$ de degré $\geqslant 1$ admet au moins un diviseur irréductible.

◆ **Proposition 3** Soient $A, B \in K[X]$, de degrés $\geqslant 1$, unitaires, $A = \prod_{i=1}^{N} P_i^{r_i}$, $B = \prod_{i=1}^{N} P_i^{s_i}$ les DP de A et B (où $N \in \mathbb{N}^*$, $P_1, \ldots, P_N$ sont irréductibles, unitaires, et premiers entre eux deux à deux, $r_1, \ldots, r_N$, $s_1, \ldots, s_N \in \mathbb{N}$).

On a : $\begin{cases} A \wedge B = \prod_{i=1}^{N} P_i^{\mathrm{Min}(r_i, s_i)} \\ A \vee B = \prod_{i=1}^{N} P_i^{\mathrm{Max}(r_i, s_i)}. \end{cases}$

◆ **Corollaire** Les lois $\wedge$ et $\vee$ sont distributives l'une sur l'autre dans $K[X] - \{0\}$.

Exercices

◇ **5.2.10** Soit $(P_n)_{n\in\mathbb{N}}$ la suite dans $K[X]$ définie par : $\begin{cases} P_0 = 1, P_1 = X \\ \forall n \in \mathbb{N},\ P_{n+2} = XP_{n+1} - P_n \end{cases}$.

a) Montrer : $\forall n \in \mathbb{N},\quad P_{n+1}^2 - P_n P_{n+2} = 1$.

b) En déduire : $\forall n \in \mathbb{N},\quad P_n \wedge P_{n+1} = 1$.

◇ **5.2.11** Soient $A, B, C \in K[X]$. Montrer que, si A, B, C sont premiers entre eux deux à deux, alors $AB + BC + CA$ et ABC sont premiers entre eux.

◇ **5.2.12** Soit $(A, B) \in (K[X]-\{0\})^2$. Montrer que les deux propriétés suivantes sont équivalentes :

(i) A et B ne sont pas premiers entre eux

(ii) $\exists (U,V) \in (K[X]-\{0\})^2,\ \begin{cases} \deg(U) < \deg(B) \\ \deg(V) < \deg(A) \\ AU + BV = 0 \end{cases}$.

◇ **5.2.13** Soient $n \in \mathbb{N}^*$, $(a,b) \in \mathbb{R}^2$ tel que $a \neq b$. Trouver un couple (U,V) de $(\mathbb{R}[X])^2$ tel que :

$$\begin{cases} (X-a)^n U + (X-b)^n V = 1 \\ \deg(U) \leqslant n-1,\ \deg(V) \leqslant n-1. \end{cases}$$

(On pourra développer $\big((X-a)-(X-b)\big)^{2n-1}$ en utilisant la formule du binôme de Newton).

5.2.6 Division suivant les puissances croissantes

◆ **Proposition - Définition** Soient $n \in \mathbb{N}$, $A \in K[X]$, $B \in K[X]$ tel que $\mathrm{val}(B) = 0$ (c'est-à-dire : $\widetilde{B}(0) \neq 0$). Il existe un couple unique (Q,R) de $(K[X])^2$ tel que :

$$A = BQ + X^{n+1}R \quad \text{et} \quad \deg(Q) \leqslant n.$$

Le polynôme Q (resp. R) s'appelle le **quotient** (resp. **reste**) **de la division de** A **par** B **suivant les puissances croissantes jusqu'à l'ordre** n**.**

Preuve : *1)* **Existence**

Récurrence sur n

- Cas $n = 0$

Notons a_0, b_0 les termes constants de A, B respectivement (c'est-à-dire : $a_0 = \tilde{A}(0)$, $b_0 = \tilde{B}(0) \neq 0$), $Q = a_0 b_0^{-1}$. Le terme constant de $A - BQ$ est nul, donc il existe $R \in K[X]$ tel que $A - BQ = XR$. Ainsi : $A = BQ + XR$ et $\deg(Q) \leqslant 0$.

• Soit $n \in \mathbb{N}$ et supposons qu'il existe $(Q,R) \in (K[X])^2$ tel que : $A = BQ + X^{n+1}R$ et $\deg(Q) \leqslant n$. D'après l'étude du cas $n = 0$, appliqué à R au lieu de A, il existe $(q,R_1) \in (K[X])^2$ tel que : $R = Bq + XR_1$ et $\deg(q) \leqslant 0$.

On a alors, en notant $Q_1 = Q + X^{n+1}q$:

$$\begin{cases} A = BQ + X^{n+1}(Bq + XR_1) = BQ_1 + X^{n+2}R_1 \\ \deg(Q_1) \leqslant n+1. \end{cases}$$

2) **Unicité**

Soient (Q_1,R_1), (Q_2,R_2) convenant. On a alors $B(Q_1 - Q_2) = X^{n+1}(R_2 - R_1)$, d'où, en passant aux valuations :

$$\text{val}(Q_1 - Q_2) = n + 1 + \text{val}(R_2 - R_1) \geqslant n + 1.$$

Si $Q_1 - Q_2 \neq 0$, alors : $n \geqslant \deg(Q_1 - Q_2) \geqslant \text{val}(Q_1 - Q_2) \geqslant n + 1$, contradiction.

Donc $Q_1 = Q_2$, puis $R_1 = R_2$.

EXEMPLE :

Effectuer la division de $A = 2 + X - 3X^2 + X^3$ par $B = 1 + 4X - X^2 + X^3$ (dans $\mathbb{R}[X]$) suivant les puissances croissantes jusqu'à l'ordre 2

$$\begin{array}{l|l} 2 + X - 3X^2 + X^3 & 1 + 4X - X^2 + X^3 \\ \cline{2-2} -7X - X^2 - X^3 & 2 - 7X + 27X^2 \\ \quad 27X^2 - 8X^3 + 7X^4 & \\ \quad\quad -116X^3 + 34X^4 - 27X^5 & \end{array}$$

D'où le quotient $Q = 2 - 7X + 27X^2$ et le reste $R = -116 + 34X - 27X^2$. ■

La division suivant les puissances croissantes est surtout utilisée pour :

• l'obtention de la décomposition en éléments simples d'une fraction rationnelle (cf. 5.4.2 *2) b) 1)* p. 198)

• le calcul du développement limité d'un quotient (cf. Tome 2, 8.3.4 Remarque).

Exercices

◇ **5.2.14** Soient $n \in \mathbb{N}^*$, $(a,b) \in K^2$, $A = 1 - abX^2$, $B = 1 - (a+b)X + abX^2$. Former le quotient et le reste de la division suivant les puissances croissantes de A par B jusqu' à l'ordre n.

◇ **5.2.15*** Soient $n \in \mathbb{N}^*$, $A = \sum_{k=0}^{n} X^k$, $B = \sum_{k=0}^{n} (-1)^k X^k$. Former le quotient et le reste de la division suivant les puissances croissantes de A par B jusqu'à l'ordre n.

5.3 Zéros des polynômes

5.3.1 Généralités

♦ **Définition 1** Soient $P \in K[X]$, $a \in K$. On dit que a est un **zéro** (ou : une **racine**) de P si et seulement si : $\widetilde{P}(a) = 0$.

Rappelons que $\widetilde{P}$ est l'application polynomiale associée à P, et que, si K est infini (cas le plus fréquent en pratique), on peut confondre P et $\widetilde{P}$ (cf. 5.1.7 Prop. 2 p. 150).

On appelle **équation algébrique** toute équation $\widetilde{P}(x) = 0$, d'inconnue $x \in K$, où $P \in K[X]$ est fixé.

On a vu (5.2.2 Prop. p. 157) que a est un zéro de P si et seulement si $X - a$ divise P.

♦ **Proposition 1** Soient $P \in K[X]$, $n \in \mathbb{N}^*, x_1, \ldots, x_n \in K$ deux à deux distincts.
Si $x_1, \ldots, x_n$ sont zéros de P, alors : $\prod_{i=1}^{n}(X - x_i) | P$.

Preuve :

D'après 5.2.2 Prop. p. 157 : $\forall i \in \{1, \ldots, n\}$, $X - x_i | P$. Comme $x_1, \ldots, x_n$ sont deux à deux distincts, les polynômes $X - x_1, \ldots, X - x_n$ sont premiers entre eux deux à deux, et donc (cf. 5.2.4 *3)* Prop. 3 p. 165) : $\prod_{i=1}^{n}(X - x_i) \mid P$.

♦ **Corollaire 1** Soient $P \in K[X]$, $n \in \mathbb{N}^*$. Si $\deg(P) < n$ et si P admet au moins n zéros deux à deux distincts, alors $P = 0$. ■

♦ **Corollaire 2** Si un polynôme P de $K[X]$ s'annule en une infinité d'éléments de K, alors $P = 0$. ■

EXEMPLE

Polynômes d'interpolation de Lagrange

Soient $n \in \mathbb{N}$, $x_0, \ldots, x_n \in K$ deux à deux distincts.

• Pour chaque i de $\{0, \ldots, n\}$, il existe un polynôme L_i de $K[X]$ et un seul tel que :

$$\begin{cases} \deg(L_i) \leqslant n \\ \forall j \in \{0, \ldots, n\}, \quad (j \neq i \Longrightarrow \widetilde{L_i}(x_j) = 0) \\ \widetilde{L_i}(x_i) = 1 \end{cases}$$

et on a : $L_i = \dfrac{1}{\prod\limits_{\substack{0 \leqslant j \leqslant n \\ j \neq i}} (x_i - x_j)} \prod\limits_{\substack{0 \leqslant j \leqslant n \\ j \neq i}} (X - x_j)$.

Les polynômes $L_i \quad (0 \leqslant i \leqslant n)$ sont appelés les **polynômes d'interpolation de Lagrange** sur les points $x_0,\ldots,x_n$.

• Pour tout $(b_0,\ldots,b_n)$ de K^{n+1}, il existe un polynôme P de $K[X]$ et un seul tel que :

$$\begin{cases} \deg(P) \leqslant n \\ \forall i \in \{0,\ldots,n\}, \quad \widetilde{P}(x_i) = b_i \end{cases},$$

et on a : $P = \sum_{i=0}^{n} b_i L_i$. ■

◆ **Définition 2** Soient $P \in K[X]$, $a \in K$, $\alpha \in \mathbb{N}^*$.

1) On dit que a est un **zéro d'ordre au moins** α **de** P si et seulement si :

$$(X-a)^\alpha \mid P.$$

2) On dit que a est un **zéro d'ordre exactement** α **de** P si et seulement si :

$$(X-a)^\alpha \mid P \quad \text{et} \quad (X-a)^{\alpha+1} \nmid P.$$

Si $\alpha = 1$ (resp. 2, resp. 3), on parle de **zéro simple** (resp. **double**, resp. **triple**).

La Proposition suivante est immédiate.

◆ **Proposition - Définition 2**

Soient $P \in K[X] - \{0\}$, $a \in K$. Si a est zéro de P, alors il existe $\alpha \in \mathbb{N}^*$ unique tel que a soit zéro d'ordre α exactement de P, et on dit que α est l'**ordre de multiplicité du zéro** a **dans** (ou : **de**) P.

◆ **Proposition 3** Soient $n \in \mathbb{N}^*, x_1,\ldots,x_n \in K$ deux à deux distincts, $A = \prod_{k=1}^{n}(X-x_k)$, $B \in K[X]$. On a alors :

$$A \mid B \iff (\forall k \in \{1,\ldots,n\}, \quad \widetilde{B}(x_k) = 0).$$

Preuve :

1) Si $A \mid B$, il existe $Q \in K[X]$ tel que $B = AQ$, d'où :

$$\forall k \in \{1,\ldots,n\}, \quad \widetilde{B}(x_k) = \widetilde{A}(x_k)\widetilde{Q}(x_k) = 0.$$

2) Réciproquement, si $(\forall k \in \{1,\ldots,n\}, \widetilde{B}(x_k) = 0)$, alors : $\forall k \in \{1,\ldots,n\}$, $X - x_k \mid B$, donc, comme $X - x_1,\ldots,X - x_n$ sont premiers entre eux deux à deux, on conclut, d'après 5.2.4 *3)* Prop. 3 p. 165 : $A \mid B$.

Exercices

◇ **5.3.1** Soient $n \in \mathbb{N}$, $x_0,\ldots,x_n \in K$ deux à deux distincts, $P = \prod_{i=0}^{n}(X - x_i)$. Pour tout i de $\{0,\ldots,n\}$, on note $L_i = \dfrac{1}{\prod\limits_{\substack{0\leqslant j\leqslant n\\ j\neq i}}(x_i - x_j)} \prod\limits_{\substack{0\leqslant j\leqslant n\\ j\neq i}} (X - x_j)$ (polynômes d'interpolation de Lagrange sur les points $x_0,\ldots,x_n$ cf. 5.3.1 Exemple p. 169). Montrer que, pour tout A de $K[X]$, le reste de la division euclidienne de A par P est : $\sum_{i=0}^{n} \tilde{A}(x_i)L_i$.

◇ **5.3.2** Soient $n \in \mathbb{N}^*, a_1,\ldots,a_n \in \mathbb{R}$, $P_n = \prod_{k=1}^{n}(X \sin a_k + \cos a_k)$. Quel est le reste de la division euclidienne de P_n par $X^2 + 1$?

◇ **5.3.3** Soient $P \in K[X]$, $n \in \mathbb{N}^*$. Montrer :

a) $X - 1 | P(X^n) \Longrightarrow \sum_{k=0}^{2n-1} X^k \Big| P(X^{2n})$

b) $X - 1 | P(X^n) \Longrightarrow \left(\forall k \in \mathbb{N}^*,\ X^k - 1 \Big| P(X^k)\right)$.

◇ **5.3.4** Pour $n \in \mathbb{N}$, calculer le reste de la division euclidienne de $X^{2n+1} + (X+1)^{n+2}$ par $X^2 + X + 1$ dans $\mathbb{C}[X]$.

◇ **5.3.5** Soient $n \in \mathbb{N}^*$, $A = X^5 + 1$,

$$P_n = (X^4 - 1)(X^3 - X^2 + X - 1)^n + (X + 1)X^{4n-1} \in \mathbb{C}[X].$$

Montrer : $A | P_n$.

5.3.2 Polynômes scindés

◆ **Définition 1** Un polynôme P de $K[X]$ est dit **scindé** (ou : **scindable**) sur K si et seulement s'il existe $\lambda \in K - \{0\}$, $n \in \mathbb{N}^*$, $x_1,\ldots,x_n \in K$ tels que :

$$P = \lambda \prod_{i=1}^{n}(X - x_i).$$

Ici, $x_1,\ldots,x_n$ ne sont pas nécessairement deux à deux distincts.

Nous verrons plus loin (théorème de d'Alembert, 5.3.4 p. 177) que tout polynôme non constant de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$.

Remarque :

Changement de corps

Soient L un corps, K un sous-corps de L, $P \in K[X]$. Il se peut que P soit scindé sur L sans être scindé sur K. Exemple : $K = \mathbb{R}$, $L = \mathbb{C}$, $P = X^2 + 1$. ■

Pour $x_1, x_2, x_3 \in K$, développons :

- $\prod_{i=1}^{2}(X - x_i) = (X - x_1)(X - x_2) = X^2 - (x_1 + x_2)X + x_1x_2$
- $\prod_{i=1}^{3}(X - x_i) = (X - x_1)(X - x_2)(X - x_3)$
$$= X^3 - (x_1 + x_2 + x_3)X^2 + (x_1x_2 + x_1x_3 + x_2x_3)X - x_1x_2x_3.$$

Ceci nous amène à la Définition suivante.

◆ **Définition 2**

Soient $n \in \mathbb{N}^*$, $x_1, \ldots, x_n \in K$. On apelle **fonctions symétriques élémentaires** (en abrégé : fse) de $x_1, \ldots x_n$ les «expressions» :

$$\sigma_1 = \sum_{i=1}^{n} x_i = x_1 + x_2 + \ldots + x_n$$

$$\sigma_2 = \sum_{1 \leqslant i_1 < i_2 \leqslant n} x_{i_1}x_{i_2} = (x_1x_2 + x_1x_3 + \ldots + x_1x_n) + (x_2x_3 + \ldots + x_2x_n) + \ldots$$
$$\ldots + (x_{n-2}x_{n-1} + x_{n-2}x_n) + x_{n-1}x_n$$

$$\vdots$$

$$\sigma_k = \sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} x_{i_1}x_{i_2} \ldots x_{i_k} \quad (1 \leqslant k \leqslant n)$$

$$\vdots$$

$$\sigma_n = x_1x_2 \ldots x_n.$$

Par exemple, les fse de x_1, x_2, x_3, x_4 sont :

$$\begin{cases} \sigma_1 = x_1 + x_2 + x_3 + x_4 \\ \sigma_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\ \sigma_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\ \sigma_4 = x_1x_2x_3x_4. \end{cases}$$

Remarques :

1) Plus généralement, en considérant des indéterminées $X_1, \ldots, X_n$ au lieu des éléments $x_1, \ldots, x_n$ de K, on peut définir les **polynômes symétriques élémentaires** $\sigma_1, \ldots, \sigma_n$ de $K[X_1, \ldots, X_n]$ par :

$$\forall k \in \{1, \ldots, n\}, \quad \sigma_k = \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} X_{i_1}X_{i_2} \ldots X_{i_k}.$$

2) La fse σ_k de $x_1, \ldots, x_n$ comporte C_n^k «termes ».

♦ **Proposition (Relations entre coefficients et zéros)**

Soient $n \in \mathbb{N}^*$, $(a_0,\ldots,a_n) \in K^{n+1}$ tel que $a_n \neq 0$, et $P = \sum_{i=0}^{n} a_i X^i$.

Supposons P scindé sur K, et notons $x_1,\ldots,x_n$ les zéros de P (non nécessairement deux à deux distincts), de sorte que :

$$P = a_n \prod_{i=1}^{n} (X - x_i).$$

On a alors, en notant $\sigma_1,\ldots,\sigma_n$ les fse de $x_1,\ldots,x_n$:

$$\sigma_1 = -\frac{a_{n-1}}{a_n},\ldots,\sigma_k = (-1)^k \frac{a_{n-k}}{a_n},\ldots,\sigma_n = (-1)^n \frac{a_0}{a_n}.$$

Preuve :

Il suffit de développer et d'identifier dans :

$$a_n \prod_{i=1}^{n} (X - x_i) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0.$$

EXEMPLE :

Calculer $\sum_{i=1}^{4} x_i^2$ où $x_1,\ldots,x_4$ sont les zéros de $X^4 + X^3 + X^2 + 1$ dans $\mathbb{C}$.

On a : $\sum_{i=1}^{4} x_i^2 = \sigma_1^2 - 2\sigma_2$, $\sigma_1 = -1$, $\sigma_2 = 1$, d'où $\sum_{i=1}^{4} x_i^2 = -1$. En particulier, $x_1,\ldots,x_4$ ne sont pas tous réels.

Exercices

◇ **5.3.6** Soient a,b deux zéros distincts de $z^3 + 3z^2 + z + 1 = 0$ (inconnue $z \in \mathbb{C}$). Quelle est la valeur de $a^2b + ab^2 + 3ab$?

◇ **5.3.7** *Exemples de calcul de fonctions symétriques des zéros d'une équation algébrique*

En notant $x_1,x_2,x_3,\ldots$ les zéros de l'équation indiquée (dans $\mathbb{C}$), calculer l'expression E proposée où le symbole $\sum$ indique la somme de tous les termes obtenus par permutation d'indice(s) :

a) $x^3 + px + q = 0$, $(p,q) \in \mathbb{C} \times \mathbb{C}^*$, $E = \sum \frac{1}{x_1^2}$ (trois termes)

b) $x^3 - 3x^2 + x - 1 = 0$, $E = \sum x_1^3 x_2^2$ (six termes)

c) $x^3 + px^2 + qx + r = 0$, $(p,q,r) \in \mathbb{C}^3$, $E = \sum (x_1 + x_2)^3$ (trois termes)

d) $x^3 + px + q = 0$, $(p,q) \in \mathbb{C}^2$, $E = \sum x_1^5 x_2^2$ (six termes)

e) $x^5 + 4x^4 + 3x^3 + x + 1 = 0$, $E = \sum x_1^4 x_2$ (vingt termes).

◇ **5.3.8** Soient $z_1,\ldots,z_4 \in \mathbb{C}$, $u_1 = z_1z_2 + z_3z_4$, $u_2 = z_1z_3 + z_2z_4$, $u_3 = z_1z_4 + z_2z_3$.

Calculer les fse $\sigma_1,\sigma_2,\sigma_3$ de u_1,u_2,u_3 en fonction des fse $\tau_1,\ldots,\tau_4$ de $z_1,\ldots,z_4$.

◇ **5.3.9** Déterminer l'ensemble des réels p tels que le système d'équations $\begin{cases} x+y+z=2 \\ xy+xz+yz=1 \\ xyz=p \end{cases}$ admette au moins une solution (x,y,z) dans $\mathbb{R}^3$.

◇ **5.3.10** Résoudre les systèmes d'équations suivants, d'inconnue $(x,y,z) \in \mathbb{C}^3$:

a) $\begin{cases} x+y+z=3 \\ xy+yz+zx=2 \\ x^3+y^3+z^3=9 \end{cases}$ *b)* $\begin{cases} x+y+z=0 \\ x^3+y^3+z^3=6 \\ x^5+y^5+z^5=30 \end{cases}$

c) $\begin{cases} x+y+z=1 \\ \frac{1}{x}+\frac{1}{y}+\frac{1}{z}=1 \\ x^2+y^2+z^2=-1 \end{cases}$ *d)* $\begin{cases} x+y+z=-2 \\ \frac{1}{x}+\frac{1}{y}+\frac{1}{z}=-2 \\ \frac{xy}{z}+\frac{yz}{x}+\frac{zx}{y}=0. \end{cases}$

◇ **5.3.11** *Exemples de CNS portant sur les coefficients d'une équation algébrique pour que les zéros vérifient une relation donnée (dans* $\mathbb{C}$*)*

a) CNS sur $\lambda \in \mathbb{C}$ pour que deux des zéros z_1,z_2,z_3 de $z^3+5z^2-8z+\lambda=0$ vérifient $z_1+z_2=-1$. Dans ce cas, résoudre l'équation.

b) CNS sur $(p,q) \in \mathbb{C}^2$ pour que $z^3+pz+q=0$ admette deux zéros de différence 1.

c) CNS sur $(p,q,r) \in \mathbb{C}^3$ pour que les zéros de $z^3+pz^2+qz+r=0$ soient les affixes des sommets d'un triangle équilatéral dans le plan complexe. (Utiliser l'exercice 2.3.3 du Tome 1).

d) CNS sur $\lambda \in \mathbb{C}$ pour que deux des zéros z_1,z_2,z_3 de $z^3-7z+\lambda=0$ vérifient $z_2=2z_1$.

e) CNS sur $(a,b,c,d) \in \mathbb{C}^4$ pour que le polynôme $X^4+aX^3+bX^2+cX+d$ ait deux zéros doubles.

f) CNS sur $(a,b) \in \mathbb{C}^2$ pour que $z^4+az+b=0$ admette deux solutions z_1,z_2 telles que $z_1z_2=1$. *Application* : résoudre $z^4-21z+8=0$ dans $\mathbb{C}$.

g) CNS sur $(\lambda,\mu) \in \mathbb{C}^2$ pour que les zéros z_1,z_2,z_3,z_4 de $z^4-4z^3+\lambda z^2+\mu z+5=0$, vérifient $z_1+z_2=z_3+z_4$.

h) CNS sur $\lambda \in \mathbb{C}$ pour que les zéros z_1, z_2, z_3, z_4 de $z^4-z^3+\lambda z^2+23z-20=0$ vérifient $z_1z_2=-5$. Dans ce cas, résoudre l'équation.

i) CNS sur $\lambda \in \mathbb{R}$ pour que le polynôme $X^5-209X+\lambda$ admette deux zéros réels et de produit 1.

◇ **5.3.12** *Exemples d'équations réciproques*

Résoudre dans $\mathbb{C}$ les équations (d'inconnue x) :

a) $x^5+3x^4+x^3+x^2+3x+1=0$

b) $x^6-4x^5+7x^4-9x^3+7x^2-4x+1=0.$

(Après avoir éliminé les éventuelles solutions 1, -1, diviser par une puissance convenable de x et poser $y=x+\frac{1}{x}$).

◇ **5.3.13** Résoudre $z^6-z^5-4z^4+5z^3-41z^2+36z-36=0$ (inconnue $z \in \mathbb{C}$) sachant qu'il y a deux solutions opposées.

◇ **5.3.14** *Une méthode de résolution de l'équation du 3ème degré (dans $\mathbb{C}$)*

a) Montrer que, par le changement d'inconnue $z = x + \frac{a}{3}$, l'équation $x^3 + ax^2 + bx + c = 0$ (inconnue $x \in \mathbb{C}$; $(a,b,c) \in \mathbb{C}^3$ fixé) est ramenée à une équation $z^3 + pz + q = 0$ (inconnue $z \in \mathbb{C}$; $(p,q) \in \mathbb{C}^2$ fixé).

b) Montrer que, par le changement d'inconnue $y = \frac{\alpha - z}{\beta - z}$ ($(\alpha,\beta) \in \mathbb{C}^2$ à trouver), l'équation $z^3 + pz + q = 0$ est ramenée à une équation $y^3 + A = 0$, $A \in \mathbb{C}$.

◇ **5.3.15** Pour $P \in K[X]$ et $a \in K$, on note $\omega_P(a)$ l'ordre de la multiplicité de a dans P, avec les conventions :

$$\begin{cases} \omega_P(a) = 0 & \text{si } a \text{ n'est pas zéro de } P \\ \omega_0(a) = +\infty. \end{cases}$$

Montrer, pour tous P, Q de $K[X]$:

a) $\omega_{P+Q}(a) \geqslant \text{Min}\left(\omega_P(a), \omega_Q(a)\right)$

b) $\omega_{PQ}(a) = \omega_P(a) + \omega_Q(a)$

c) $\sum_{a \in Z(P)} \omega_P(a) \leqslant \deg(P)$ si $P \neq 0$, où $Z(P)$ est l'ensemble des zéros de P dans K

d) $\sum_{a \in Z(P)} \omega_P(a) = \deg(P)$ si et seulement si $P (\neq 0)$ est scindé.

◇ **5.3.16** Soit $P \in \mathbb{C}[X] - \{0\}, n = \deg(P)$; montrer que les sommes des zéros de $P, P', \ldots, P^{(n-1)}$ forment une progression arithmétique.

◇ **5.3.17** Soient $(a,b) \in \mathbb{R}^2$, $A = X^4 + (2a+1)X^3 + (a-1)^2X^2 + bX + 4$.
Trouver tous les (a,b) tels qu'ils existe $P, Q \in \mathbb{R}[X]$ tels que :

$$\begin{cases} A = PQ \\ \deg(P) = \deg(Q) = 2 \\ P \text{ et } Q \text{ sont normalisés} \\ Q \text{ admet deux zéros distincts } \alpha, \beta \text{ dans } \mathbb{R} \\ P(\alpha) = \beta \quad \text{et} \quad P(\beta) = \alpha. \end{cases}$$

◇ **5.3.18** Soient $(p,q,r) \in \mathbb{C}^3$, a,b,c les solutions de $x^3 + px^2 + qx + r = 0$ dans $\mathbb{C}$; former l'équation du 3ème degré dont les solutions sont $a^2 - bc$, $b^2 - ca$, $c^2 - ab$.

◇ **5.3.19** CNS sur $(p,q) \in \mathbb{C}^2$ pour que les deux équations $z^4 + 2z^2 + p = 0$, $z^3 + z + q = 0$ (inconnue $z \in \mathbb{C}$) aient deux solutions communes distinctes.

◇ **5.3.20** Soient $n \in \mathbb{N}^*$, $x_1, \ldots, x_n \in \mathbb{R}$, $\sigma_1, \ldots, \sigma_n$ les fse de $x_1, \ldots, x_n$. Etablir :

$$\left(\forall i \in \{1,\ldots,n\}, \quad x_i \in \mathbb{R}_+\right) \Longleftrightarrow \left(\forall i \in \{1,\ldots,n\}, \quad \sigma_i \in \mathbb{R}_+\right).$$

◇ **5.3.21** Soient $P, Q \in K[X]$ tels que $P | Q$. Montrer que, si Q est scindé, alors P l'est aussi.

◇ **5.3.22** Soient $A, B \in K[X]$ tels que B soit scindé et à zéros tous simples. Montrer qu'il existe $P \in K[X]$ tel que : $B | P^2 - A$.

5.3.3 Utilisation de la dérivation

On suppose, dans ce § 5.3.3, que K est un sous-corps de $\mathbb{C}$; en pratique, le plus souvent : $K = \mathbb{R}$ ou $\mathbb{C}$. On peut donc confondre polynôme P et fonction polynomiale associée $\widetilde{P}$ (cf. 5.1.7 Rem. p. 150).

◆ **Théorème** Soient $P \in K[X]$, $a \in K$, $\alpha \in \mathbb{N}^*$.

1) Pour que a soit zéro d'ordre α au moins de P, il faut et il suffit que :

$$\forall k \in \{0,\ldots,\alpha-1\}, \quad P^{(k)}(a) = 0.$$

2) Pour que a soit zéro d'ordre α exactement de P, il faut et il suffit que :

$$\begin{cases} \forall k \in \{0,\ldots,\alpha-1\}, & P^{(k)}(a) = 0 \\ P^{(\alpha)}(a) \neq 0 \end{cases}.$$

Preuve :

D'après la formule de Taylor pour les polynômes, on a, en notant $N = \text{Max}(\alpha, \deg(P))$:

$$P(X) = \sum_{k=0}^{N} \frac{P^{(k)}(a)}{k!}(X-a)^k.$$

Il en résulte :

- $(X-a)^\alpha | P \iff P(a) = P'(a) = \ldots = P^{(\alpha-1)}(a) = 0$
- $\begin{cases} (X-a)^\alpha | P \\ (X-a)^{\alpha+1} \nmid P \end{cases} \iff \begin{cases} P(a) = P'(a) = \ldots = P^{(\alpha-1)}(a) = 0 \\ P^{(\alpha)}(a) \neq 0. \end{cases}$

Exercices

◇ **5.3.23** Trouver tous les P de $\mathbb{R}[X]$ tels que :

$$P(0) = 1, \ P(1) = 0, \ P'(0) = 0, \ P'(1) = 1.$$

◇ **5.3.24** Montrer : *a)* $\forall n \in \mathbb{N}^*$, $(X-1)^2 \left| \left(\sum_{k=0}^{n-1} X^k\right)^2 - n^2 X^{n-1} \right.$

b) $\forall n \in \mathbb{N}$, $(X-1)^3 \left| nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n. \right.$

◇ **5.3.25** Soient $n \in \mathbb{N}^*$, $(a,b) \in \mathbb{C}^2$ tel que $a \neq b$, $A = (X-a)^{2n} + (X-b)^{2n}$, $B = (X-a)^2(X-b)^2$.

Déterminer le reste de la division euclidienne de A par B.

◇ **5.3.26** CNS sur $(a,b) \in \mathbb{C}^2$ pour que $X^4 + aX^3 + bX + 1$ (de $\mathbb{C}[X]$) ait au moins un zéro au moins triple.

◇ **5.3.27** Soient $n \in \mathbb{N} - \{0,1\}$, $P_n = X^{2n} - n^2X^{n+1} + 2(n^2-1)X^n - n^2X^{n-1} + 1 \in \mathbb{C}[X]$. Montrer que 1 est zéro de P_n et déterminer son ordre de multiplicité.

◇ **5.3.28** Soient $(p,q) \in (\mathbb{N}^*)^2$, $A = X^{p+q} - X^p - X^q + 1$. Déterminer $A \wedge A'$.

◇ **5.3.29** Soient $\lambda \in \mathbb{R}^*$, $P, Q \in \mathbb{R}[X]$, $a \in \mathbb{R}$. On suppose que a est un zéro double de $P^2 + \lambda Q^2$; montrer que $PQ' - P'Q$ s'annule en a.

◇ **5.3.30** Soient $A, B \in \mathbb{C}[X]$ tels que : $A \wedge B = 1$, $\deg(A) \geqslant 1$, $\deg(B) \geqslant 1$. On suppose que les zéros de B sont tous simples; démontrer : $(A'B - AB') \wedge B^2 = 1$.

5.3.4 Cas de $\mathbb{C}[X]$

Le corps $\mathbb{C}$ étant infini, nous confondons ici polynôme P de $\mathbb{C}[X]$ et fonction polynomiale $\widetilde{P}$.

◆ **Théorème (Théorème de d'Alembert)**

Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins un zéro dans $\mathbb{C}$. On dit que le corps $\mathbb{C}$ est algébriquement clos.

Preuve : (pouvant être omise en première lecture) :

Il existe de nombreuses démonstrations du théorème de d'Alembert (appelé aussi : théorème fondamental de l'Algèbre), et elles font toutes appel à l'Analyse. En voici une.

Raisonnons par l'absurde : supposons qu'il existe $P \in \mathbb{C}[X]$, non constant et n'admettant aucun zéro dans $\mathbb{C}$. Notons $n = \deg(P) \geqslant 1$, $P = \sum_{i=0}^{n} a_i X^i$, et $\varphi : \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & |P(z)| \end{array}$.

1) Puisque $\varphi(z) \xrightarrow[|z| \to +\infty]{} +\infty$, on a :

$$\forall A > 0,\ \exists B > 0,\ \forall z \in \mathbb{C},\quad (|z| > B \Longrightarrow \varphi(z) > A).$$

En particulier, il existe $B \in \mathbb{R}_+^*$ tel que :

$$\forall z \in \mathbb{C},\quad \big(|z| > B \Longrightarrow \varphi(z) > \varphi(0)\big).$$

D'autre part, φ étant continue sur le compact $\{z \in \mathbb{C};\ |z| \leqslant B\}$, φ y est bornée et y atteint ses bornes; il existe donc $z_0 \in \mathbb{C}$ tel que :

$$\varphi(z_0) = \inf_{|z| \leqslant B} \varphi(z).$$

Comme de plus :

$$\forall\, z \in \mathbb{C},\quad \big(|z| > B \Longrightarrow \varphi(z) > \varphi(0) \geqslant \varphi(z_0)\big),$$

on conclut :

$$\varphi(z_0) = \inf_{z \in \mathbb{C}} \varphi(z).$$

On pourra comparer ce résultat avec l'exercice 4.3.16 du Tome 1 concernant le cas d'une application de $\mathbb{R}$ dans $\mathbb{R}$.

2) D'après la formule de Taylor pour les polynômes (5.1.7 Th. p. 150), on a :

$$\forall h \in \mathbb{C}, \quad P(z_0 + h) = P(z_0) + hP'(z_0) + \ldots + \frac{h^n}{n!} P^{(n)}(z_0).$$

Nous allons montrer qu'on peut choisir h de façon que $|P(z_0 + h)| < |P(z_0)|$, c'est-à-dire $\varphi(z_0 + h) < \varphi(z_0)$, ce qui fournira une contradiction.

Comme $P^{(n)}(z_0) = n!\, a_n \neq 0$, il existe $k \in \mathbb{N}^*$ tel que :

$$\begin{cases} P^{(k)}(z_0) \neq 0 \\ \forall l \in \{1, \ldots, k\}, \quad \big(l < k \Longrightarrow P^{(l)}(z_0) = 0\big). \end{cases}$$

Autrement dit, k est le plus petit entier $\geqslant 1$ tel que $P^{(k)}(z_0) \neq 0$.

On a donc : $\forall h \in \mathbb{C}, \quad \dfrac{P(z_0 + h)}{P(z_0)} = 1 + h^k \dfrac{P^{(k)}(z_0)}{k!P(z_0)} + \ldots + h^n \dfrac{P^{(n)}(z_0)}{n!P(z_0)}.$

D'après l'étude des racines $k^{\text{èmes}}$ dans $\mathbb{C}$, Tome 1, 2.4.3 (qui n'utilise pas le théorème de d'Alembert), il existe $\omega \in \mathbb{C}^*$ tel que : $\omega^k = -\dfrac{P^{(k)}(z_0)}{k!P(z_0)}$.

On a alors (pour $t \in \mathbb{R}$) le $DL_1(0)$ suivant :

$$\frac{P\left(z_0 + \dfrac{t}{\omega}\right)}{P(z_0)} = 1 - t^k + \underset{t \to 0}{o}(t^k)$$

Il existe donc $\eta > 0$ tel que : $\forall t \in]0; \eta[, \quad \left|\dfrac{P\left(z_0 + \dfrac{t}{\omega}\right)}{P(z_0)}\right| < 1,$

ce qui contredit la définition de z_0.

◆ **Corollaire 1**

Tout polynôme non constant de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$.

◆ **Corollaire 2**

Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Ainsi, la DP d'un polynôme quelconque P de $\mathbb{C}[X]$ (de degré $\geqslant 1$) est de la forme : $P = \lambda \prod_{i=1}^{N} (X - x_i)^{r_i}$, où $\lambda \in \mathbb{C}^*$, $N \in \mathbb{N}^*$, $x_1, \ldots, x_N \in \mathbb{C}$ deux à deux distincts, $r_1, \ldots, r_N \in \mathbb{N}^*$.

Exercices

◇ **5.3.31** Factoriser $2X^3 - X^2 - X - 3$ dans $\mathbb{C}[X]$.

◇ **5.3.32** Soient $a \in \mathbb{C}^*$, $n \in \mathbb{N}^*$. Montrer que, pour que les zéros de l'équation $\left(\dfrac{1+iz}{1-iz}\right)^n = a^n$ (inconnue $z \in \mathbb{C}$) soient tous réels, il faut et il suffit que $|a| = 1$. Dans ce cas, résoudre l'équation.

◇ **5.3.33** *a)* Soient $n \in \mathbb{N}$, $P_n = (X+i)^{2n+1} - (X-i)^{2n+1}$. Former la décomposition primaire de P_n dans $\mathbb{C}[X]$.

b) En déduire, pour $(n,a) \in \mathbb{N}^* \times \mathbb{C}$, la valeur de $\displaystyle\prod_{k=1}^{n}\left(a^2 + \operatorname{cotan}^2\frac{k\pi}{2n+1}\right)$.

◇ **5.3.34** *a)* Soient $n \in \mathbb{N}^*$, $P_n = \displaystyle\sum_{k=0}^{n} X^k$. Former la décomposition primaire de P_n dans $\mathbb{C}[X]$.

b) En déduire, pour $n \in \mathbb{N}^*$, la valeur de $\displaystyle\prod_{k=1}^{n}\sin\frac{k\pi}{n+1}$.

◇ **5.3.35** *a)* CNS sur $n \in \mathbb{N}^*$ pour que : $X^2 + X + 1 \mid (X^n+1)^n - X^n$.

b) CNS sur $n \in \mathbb{N}$ pour que : $X^3 - X^2 + X - 1 \mid (X^2 - X + 1)^n - X^{2n} + X^n - 1$.

c) CNS sur $(n,p,q) \in \mathbb{N}^* \times \mathbb{R} \times \mathbb{R}$ pour que : $X^8 + X^4 + 1 \mid X^{8n} + pX^{4n} + q$.

◇ **5.3.36** Soient $n,p \in \mathbb{N}^*$, $A = \displaystyle\sum_{k=0}^{p} X^k$. CNS pour que : $A \mid A(X^n)$.

◇ **5.3.37** Soit $(p,q,r) \in (\mathbb{N}^*)^3$ tel que $p \wedge q = p \wedge r = q \wedge r = 1$. Montrer :

$$(X^p - 1)(X^q - 1)(X^r - 1) \mid (X-1)^2(X^{pqr} - 1), \quad \text{dans} \quad \mathbb{C}[X].$$

◇ **5.3.38** Soit $(n,p) \in (\mathbb{N} - \{0,1\})^2$; montrer : $(X^n - 1)(X^p - 1) \mid (X^{n\wedge p} - 1)(X^{n\vee p} - 1)$.

◇ **5.3.39** Soient $n \in \mathbb{N} - \{0,1\}$, $M \in \mathbb{R}_+^*$, $(a_1,\ldots,a_n) \in \mathbb{C}^n$ tel que : $\big(\forall k \in \{1,\ldots,n\},\ |a_k| < M\big)$, $P = 1 + \displaystyle\sum_{k=1}^{n} a_k X^k$. Montrer que P n'a aucun zéro dans le disque ouvert de centre O et de rayon $\dfrac{1}{M+1}$.

◇ **5.3.40** *a)* Soient $n \in \mathbb{N}$, tel que $n \geqslant 3$, $a_0,\ldots,a_{n-3} \in \mathbb{R}$, $P = X^n + X^{n-1} + X^{n-2} + \sum_{k=0}^{n-3} a_k X^k$. Montrer que les zéros de P ne sont pas tous réels.

b) Même question pour $Q = 1 + X + X^2 + \sum_{k=3}^{n} b_k X^k$, où $b_3,\ldots,b_n \in \mathbb{R}$.

◇ **5.3.41** Soient $n \in \mathbb{N}^*$, $a_0,\ldots,a_n \in \mathbb{R}$, $P = \sum_{k=0}^{n} a_k X^k$. On suppose $a_n > 0$ et :

$$\{k \in \{0,\ldots,n-1\},\ a_k \leqslant 0\} \neq \varnothing.$$

On note $p = \text{Max}\{k \in \{0,\ldots,n-1\},\ a_k \leqslant 0\}$ et $M = \text{Max}\{|a_k|;\ a_k \leqslant 0\}$.

a) Montrer : $\forall x \in]1;+\infty[,\ P(x) \geqslant a_n x^n - M\dfrac{x^{p+1}-1}{x-1}$.

b) En déduire, pour tout zéro réel x de P : $x \leqslant 1 + \left(\dfrac{M}{a_n}\right)^{\frac{1}{n-p}}$.

c) Exemple : montrer que les zéros réels de $6X^{10} + 4X^9 - 7X^2 - X - 1$ sont tous $< 2{,}02$.

◇ **5.3.42*** Soient $N \in \mathbb{N}^*$, $n_0,n_1,\ldots,n_N$ des entiers tels que $0 = n_0 < n_1 < \ldots < n_N$, $P = \sum_{k=0}^{N} X^{n_k}$. Démontrer, pour tout zéro z de P dans $\mathbb{C}$: $|z| \geqslant \dfrac{\sqrt{5}-1}{2}$.

◇ **5.3.43** Soient $n \in \mathbb{N}^*$, $(a_0,\ldots,a_{n-1}) \in (\mathbb{R}_+)^n - \{(0,\ldots,0)\}$, $P = X^n - \sum_{k=0}^{n-1} a_k X^k$. Montrer que, dans $\mathbb{R}_+^*$, P admet un zéro et un seul.

◇ **5.3.44** Montrer que, pour tout n de $\mathbb{N}$, le polynôme $P_n = \sum_{k=0}^{2n} (-1)^k (k+1) X^{2n-k}$ n'a pas de zéro réel.

◇ **5.3.45*** Trouver tous les P de $\mathbb{R}[X]$ tels que : $P(X)P(X+1) = P(X^2+X+1)$.

◇ **5.3.46*** Trouver tous les P de $\mathbb{C}[X]$ tels que : $P(X)P(X+3) = P(X+1)P(X+2)$.

◇ **5.3.47** Soient $A = X^3 + X - 2$, α,β les zéros de A dans $\mathbb{C}$ autres que 1.

a) Montrer qu'il existe $B \in \mathbb{Q}_2[X]$ unique tel que : $B(1) = 1$, $B(\alpha) = \beta$, $B(\beta) = \alpha$, et calculer B.

b) Montrer : $A \mid B \circ B - X$.

◇ **5.3.48** Soient $P \in \mathbb{Q}[X]$, $a \in \mathbb{Q}$, $b \in \mathbb{Q}_+$ tel que : $\forall r \in \mathbb{Q}$, $b \neq r^2$. Montrer :

a) si $a + \sqrt{b}$ est zéro de P dans $\mathbb{R}$, alors $a - \sqrt{b}$ l'est aussi.

b) si $a + \sqrt{b}$ est un zéro au moins double de P dans $\mathbb{R}$, alors il existe $P_1, P_2 \in \mathbb{Q}[X]$ tels que $P = P_1 P_2^2$.

◇ **5.3.49** Soient $P,Q,R \in \mathbb{C}[X]$ tels que : $P(X^3) + XQ(X^3) = (1 + X + X^2)R(X)$. Montrer que $X - 1$ divise P,Q,R.

◇ **5.3.50** *a)* Soit p un nombre premier $\geqslant 5$. Montrer qu'il existe $A \in \mathbb{R}[X]$ à coefficients entiers tel que : $X^{2p} - X^p + 1 = (X^2 - X + 1)A$.

b) Soit $n \in \mathbb{N}^*$ admettant au moins un diviseur premier $\geqslant 5$; montrer que $2^{2n} - 2^n + 1$ est composé.

Dans les exercices suivants, $\mathbb{Z}[X]$ désigne l'anneau des polynômes à coefficients dans $\mathbb{Z}$; le lecteur pourra se convaincre qu'en remplaçant le corps K par un anneau commutatif A, l'étude de $K[X]$ est peu modifiée.

◇ **5.3.51** Soient $a,b,c \in \mathbb{Z}$ deux à deux distincts, $P \in \mathbb{Z}[X]$ tel que $P(a) = P(b) = P(c) = 2$. Démontrer : $\forall x \in \mathbb{Z}, \quad P(x) \neq 3$.

◇ **5.3.52** Soient $a,b,c, \in \mathbb{Z}$ deux à deux distincts, $P \in \mathbb{Z}[X]$. Montrer qu'on ne peut pas avoir :

$$P(a) = b, \quad P(b) = c, \quad P(c) = a.$$

◇ **5.3.53** Montrer que $X^3 + X + 3$ est irréductible dans $\mathbb{Q}[X]$.

◇ **5.3.54*** Soient $P \in \mathbb{Z}[X] - \{0\}$, $n = \deg(P)$. Montrer :

$$\forall a \in \mathbb{Z}, \quad \operatorname{pgcd}\left((P(k)\hat{)}_{0\leqslant k\leqslant n}\right) \Big| P(a).$$

◇ **5.3.55*** Soient $n \in \mathbb{N}^*$, $a_1,\ldots,a_n \in \mathbb{Z}$, $P = \left(\prod_{k=1}^{n}(X - a_k)\right) - 1$. Démontrer que P est irréductible dans $\mathbb{Z}[X]$.

5.3.5 Cas de $\mathbb{R}[X]$

Le corps $\mathbb{R}$ étant infini, nous confondons, ici polynôme P de $\mathbb{R}[X]$ et fonction polynomiale $\widetilde{P}$.

◆ **Proposition 1** Soit $P \in \mathbb{C}[X]$. On a :

$$P \in \mathbb{R}[X] \iff \left(\forall z \in \mathbb{C}, \quad \overline{P(z)} = P(\overline{z})\right).$$

Preuve :

Notons $P = \sum_{k=0}^{n} a_k X^k$, $(a_0, \ldots, a_n) \in \mathbb{C}^{n+1}$. On a, pour tout z de $\mathbb{C}$:

$$\overline{\overline{P(z)} - P(\overline{z})} = \sum_{k=0}^{n} (a_k - \overline{a_k}) z^k.$$

D'où : $\left(\forall z \in \mathbb{C}, \quad \overline{P(z)} = P(\overline{z})\right) \iff \left(\forall z \in \mathbb{C}, \quad \sum_{k=0}^{n} (a_k - \overline{a_k}) z^k = 0\right)$

$\iff (\forall k \in \{0, \ldots, n\}, \quad a_k - \overline{a_k} = 0) \iff P \in \mathbb{R}[X]$.

◆ **Proposition 2** Soient $P \in \mathbb{R}[X]$, $a \in \mathbb{C}$, $\alpha \in \mathbb{N}^*$. Pour que a soit zéro d'ordre α au moins (resp. exactement) de P, il faut et il suffit que $\overline{a}$ soit zéro d'ordre α au moins (resp. exactement) de P.

Preuve :

1) Supposons que a soit zéro d'ordre α au moins de P. D'après 5.3.3 Th. p. 176, on a :

$$\forall k \in \{0, \ldots, \alpha - 1\}, \quad P^{(k)}(a) = 0.$$

Comme $P, P', \ldots, P^{(\alpha-1)}$ sont dans $\mathbb{R}[X]$, d'après la Prop. 1, on a :

$$\forall k \in \{0, \ldots, \alpha - 1\}, \quad P^{(k)}(\overline{a}) = \overline{P^{(k)}(a)} = 0,$$

et donc (cf. 5.3.3 Th. p. 176) $\overline{a}$ est zéro d'ordre α au moins de P.

La réciproque se déduit de la partie directe en remplaçant a par $\overline{a}$.

2) Un raisonnement analogue permet de conclure dans le cas de l'ordre exact.

◆ **Proposition 3** Les polynômes irréductibles de $\mathbb{R}[X]$ sont :

- les polynômes du 1er degré
- les trinômes du 2nd degré à discriminant < 0.

Preuve :

1) Soit $P \in \mathbb{R}[X]$, irréductible, tel que $\deg(P) \geqslant 2$.

Comme $P \in \mathbb{C}[X]$, le théorème de d'Alembert montre que P admet au moins un zéro z dans $\mathbb{C}$.

Si $z \in \mathbb{R}$, alors $X - z$ divise P dans $\mathbb{R}[X]$, ce qui contredit l'irréductibilité de P dans $\mathbb{R}[X]$; donc $z \in \mathbb{C} - \mathbb{R}$.

D'après la Prop. 2, $\overline{z}$ est aussi un zéro de P. En notant $T = (X - z)(X - \overline{z})$, T divise P dans $\mathbb{C}[X]$.

Mais $T = X^2 - 2\,\text{Ré}\,(z)X + |z|^2 \in \mathbb{R}[X]$ et $P \in \mathbb{R}[X]$. Il s'ensuit (cf. 5.2.2 Rem. p. 157) que T divise P dans $\mathbb{R}[X]$.

Comme P est irréductible, il existe alors $\lambda \in \mathbb{R}^*$ tel que $P = \lambda T$, et donc P est un trinôme du 2nd degré, à discriminant < 0 : $\Delta' = (\text{Ré}(z))^2 - |z|^2 = -|\text{Im}(z)|^2 < 0$.

2) **Réciproque**

• Il est clair que les polynômes du 1cr degré sont irréductibles dans $\mathbb{R}[X]$ (c'est vrai plus généralement pour tout corps K au lieu de $\mathbb{R}$).

• Soient $(a,b,c) \in \mathbb{R}^3$ tel que $b^2 - 4ac < 0$, et $T = aX^2 + bX + c$.

S'il existe $(\alpha,\beta) \in \mathbb{R}^* \times \mathbb{R}$ tel que $\alpha X + \beta | T$, alors $T\left(-\dfrac{\beta}{\alpha}\right) = 0$, contradiction puisque $T = a\left(\left(X + \dfrac{b}{2a}\right)^2 + \dfrac{-\Delta}{4a^2}\right)$, qui ne s'annule en aucun réel.

Donc T n'admet (dans $\mathbb{R}[X]$) aucun diviseur de degré 1. Comme T est de degré 2, on conclut que T est irréductible. ■

Ainsi, la DP d'un polynôme quelconque P de $\mathbb{R}[X]$ (de degré $\geqslant 1$) est de la forme :

$$P = \lambda \prod_{i=1}^{N} (X - x_i)^{r_i} \prod_{j=1}^{N'} (X^2 + p_j X + q_j)^{s_j},$$

où :
$$\left|\begin{array}{l} \lambda \in \mathbb{R}^* \\ N, N' \in \mathbb{N} \\ x_1, \ldots, x_N \in \mathbb{R} \text{ deux à deux distincts} \\ (p_1,q_1), \ldots, (p_{N'},q_{N'}) \in \mathbb{R}^2 \text{ deux à deux distincts} \\ \forall\, j \in \{1, \ldots, N'\}, \quad p_j^2 - 4q_j < 0 \\ r_1, \ldots, r_N,\ s_1, \ldots, s_{N'} \in \mathbb{N}^* . \end{array}\right.$$

Remarques :

1) Il n'y a pas de lien logique, pour $P \in \mathbb{R}[X]$, entre l'existence d'au moins un zéro réel de P et l'irréductibilité de P dans $\mathbb{R}[X]$. En effet :

• Tout polynôme de degré 1 de $\mathbb{R}[X]$ est irréductible et admet un zéro réel. Exemple : $X - 1$.

• $X^4 + 2X^2 + 1$ n'admet pas de zéro réel (car : $\forall x \in \mathbb{R}$, $x^4 + 2x^2 + 1 \geqslant 1 > 0$) et $X^4 + 2X^2 + 1$ n'est pas irréductible, puisque $X^4 + 2X^2 + 1 = (X^2 + 1)^2$.

2) Tout polynôme P de $\mathbb{R}[X]$ de degré impair admet au moins un zéro réel, car l'application $P : \mathbb{R} \longrightarrow \mathbb{R}$, $x \longmapsto P(x)$ est continue sur l'intervalle $\mathbb{R}$ et de limites infinies de signes contraires en $-\infty$ et $+\infty$ (théorème des valeurs intermédiaires, Tome 1, 4.3.3).

3) Tout polynôme de $\mathbb{R}[X]$ de degré $\geqslant 3$ est non irréductible.

Factorisation des trinômes bicarrés réels

On appelle **trinômes bicarrés réels** les polynômes aX^4+bX^2+c, $(a,b,c,) \in \mathbb{R}^* \times \mathbb{R} \times \mathbb{R}$. En factorisant par a, on se ramène à l'étude de X^4+pX^2+q, $(p,q) \in \mathbb{R}^2$. Notons $\Delta = p^2-4q$.

1) Si $\Delta > 0$, la décomposition canonique d'un trinôme réel (Tome 1, 1.2.3 *2)*) donne :

$$X^4+pX^2+q = \left(X^2+\frac{p}{2}\right)^2 - \frac{\Delta}{4} = \left(X^2+\frac{p-\sqrt{\Delta}}{2}\right)\left(X^2+\frac{p+\sqrt{\Delta}}{2}\right)$$

et on pourra aisément en déduire la DP de X^4+pX^2+q dans $\mathbb{R}[X]$.

EXEMPLES : • $X^4-5X^2+4 = (X^2-4)(X^2-1) = (X-2)(X-1)(X+1)(X+2)$

• $X^4-2X^2-3 = (X^2-3)(X^2+1) = (X-\sqrt{3})(X+\sqrt{3})(X^2+1)$

• $X^4+5X^2+6 = (X^2+2)(X^2+3)$.

2) Si $\Delta < 0$, on regroupe X^4 et le terme constant ($q > 0$ car $p^2-4q < 0$) :

$$X^4+pX^2+q = \left(X^2+\sqrt{q}\right)^2 - (2\sqrt{q}-p)X^2.$$

De plus : $p^2-4q < 0 \Longrightarrow 2\sqrt{q} > p$,

d'où : $X^4+pX^2+q = \left(X^2-\sqrt{2\sqrt{q}-p}\,X+\sqrt{q}\right)\left(X^2+\sqrt{2\sqrt{q}-p}\,X+\sqrt{q}\right)$.

Les deux trinômes obtenus sont clairement iréductibles dans $\mathbb{R}[X]$.

EXEMPLES : • $X^4+1 = (X^2+1)^2-2X^2 = \left(X^2-\sqrt{2}\,X+1\right)\left(X^2+\sqrt{2}\,X+1\right)$.

• $X^4+X^2+1 = (X^2+1)^2-X^2 = (X^2-X+1)(X^2+X+1)$.

Remarque :

Pour factoriser un polynôme de $\mathbb{R}[X]$, on peut quelquefois «passer par» $\mathbb{C}[X]$.

EXEMPLE :

Pour $n \in \mathbb{N}-\{0,1\}$, factoriser X^n-1 dans $\mathbb{R}[X]$.

La DP de X^n-1 dans $\mathbb{C}[X]$ est : $X^n-1 = \prod_{k=0}^{n-1}(X-\omega_k)$, où $\omega_k = \exp\left(\frac{2\,i\,k\pi}{n}\right)$.

• Si n est pair, $n = 2p$ $(p \in \mathbb{N}^*)$, -1 et 1 sont zéros simples de X^n-1 et les autres zéros sont conjugués deux à deux et non réels : $\forall k \in \{1,\ldots,p-1\}$, $\omega_{2p-k} = \overline{\omega_k}$.

D'où :
$$X^{2p}-1 = (X-1)(X+1)\prod_{k=1}^{p-1}(X-\omega_k)(X-\overline{\omega_k})$$
$$= (X-1)(X+1)\prod_{k=1}^{p-1}\left(X^2-2\cos\frac{2k\pi}{2p}X+1\right),$$

ce qui constitue la DP de $X^{2p}-1$ dans $\mathbb{R}[X]$.

• De même, si n est impair, $n = 2p+1$ $(p \in \mathbb{N})$, on obtient :

$$X^{2p+1}-1 = (X-1)\prod_{k=1}^{p}\left(X^2-2\cos\frac{2k\pi}{2p+1}X+1\right).$$

Exercices

◇ **5.3.56** Factoriser dans $\mathbb{R}[X]$:

a) $X^3 - 5X^2 + 3X + 9$ *b)* $(X^2 - X + 2)^2 + (X - 2)^2$

c) $6X^5 + 15X^4 + 20X^3 + 15X^2 + 6X + 1$

d) $X^5 - 7X^3 - 2X^2 + 12X + 8$, sachant qu'il y a des zéros multiples

e) $X^5 + 1$ *f)* $X^6 + 4X^4 + 6X^2 + 9$

g) $X^6 + 3X^5 + 4X^4 + 4X^3 + 4X^2 + 3X + 1$ *h)* $X^8 + X^4 + 1$

i) $X^{12} + 1$

j) $X^{2n} - 2\cos a X^n + 1$, $(n,a) \in \mathbb{N}^* \times (\mathbb{R} - \pi\mathbb{Z})$.

◇ **5.3.57** Soit $P \in \mathbb{R}[X]$, $z_1, \ldots, z_n$ les zéros de P dans $\mathbb{C}$.

On suppose : $\forall k \in \{1, \ldots, n\}$, $\text{Ré}(z_k) \leqslant 0$.

Montrer que les coefficients de P sont tous du même signe.

◇ **5.3.58** Trouver tous les $(k, P) \in \mathbb{N} \times \mathbb{R}[X]$ tels que : $P \circ P = P^k$.

◇ **5.3.59*** Soient $n \in \mathbb{N}^*$, $P \in \mathbb{R}[X]$ tel que $\deg(P) = n$ et : $\forall k \in \{0, \ldots, n\}$, $P(k) = 2^k$.

Calculer $P(n + 1)$.

◇ **5.3.60*** Soient $n \in \mathbb{N}^*$, $P \in \mathbb{R}[X]$ tel que $\deg(P) = n$ et : $\forall k \in \{1, \ldots, n + 1\}$, $P(k) = \dfrac{1}{k}$.

Calculer $P(n + 2)$.

◇ **5.3.61** Soient $n \in \mathbb{N}^*$, $P \in \mathbb{R}[X]$ tel que $\deg(P) = n$ et : $\forall k \in \{0, \ldots, n\}$, $P(k) = \dfrac{1}{C_{n+1}^k}$.

Calculer $P(n + 1)$.

◇ **5.3.62** Soient $(P, Q) \in (\mathbb{R}[X])^2$ tel que :

$$\begin{cases} P \circ Q = Q \circ P \\ \text{l'équation } P(x) = Q(x) \text{ (inconnue } x \in \mathbb{R}) \text{ n'a pas de solution.} \end{cases}$$

Montrer que l'équation $P \circ P(x) = Q \circ Q(x)$ (inconnue $x \in \mathbb{R}$) n'a pas de solution.

◇ **5.3.63** Soient $A, B, C \in K[X] - \{0\}$ tels que : $A^2 + B^2 = C^2$ et $\text{pgcd}(A, B, C) = 1$.

Montrer que les zéros de $C + A$, $C - A$, $C + B$, $C - B$ sont tous de multiplicité paire.

◇ **5.3.64** Soient $P \in \mathbb{R}[X]$ scindé sur $\mathbb{R}$, $n = \deg(P) \in \mathbb{N}^*$, $x_1, \ldots, x_n$ les zéros de P, $x \in \mathbb{R}$ tel que : $\forall k \in \{2, \ldots, n\}$, $|x - x_1| \leqslant |x - x_k|$.

Montrer : $|P(x)| \geqslant 2^{-n+1} |P'(x_1)(x - x_1)|$.

◇ **5.3.65** Soit $P \in \mathbb{C}[X]$ tel que $\deg(P) \geqslant 2$. Montrer que $P : \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ x & \longmapsto & P(x) \end{array}$ n'est pas injective.

◇ **5.3.66*** Soient $P \in \mathbb{R}[X]$ scindé sur $\mathbb{R}$, $A \in \mathbb{R}[X]$ scindé sur $\mathbb{R}$, $n = \deg(A)$, $(a_0, \ldots, a_n) \in \mathbb{R}^{n+1}$ tel que $A = \sum_{k=0}^{n} a_k X^k$.

Démontrer que $\sum_{k=0}^{n} a_k P^{(k)}$ est scindé sur $\mathbb{R}$.

5.4 Fractions rationnelles

5.4.1 Corps $K(X)$

1) L'ensemble $K(X)$

Notons $E = K[X] \times (K[X] - \{0\})$ et considérons la relation $\mathcal{R}$ définie dans E par :

$$(A,S)\ \mathcal{R}\ (B,T) \Longleftrightarrow AT = BS.$$

La relation $\mathcal{R}$ est une relation d'équivalence dans E.

En effet, la réflexivité et la symétrie sont évidentes et, pour tous $(A,S),(B,T),(C,U)$ de E :

$$\begin{cases} (A,S)\ \mathcal{R}\ (B,T) \\ (B,T)\ \mathcal{R}\ (C,U) \end{cases} \Longleftrightarrow \begin{cases} AT = BS \\ BU = CT \end{cases}$$

$\Longrightarrow (AU)T = (AT)U = (BS)U = (BU)S = (CT)S = (CS)T \Longrightarrow AU = CS$,
car $T \neq 0$ et $K[X]$ est intègre. ■

L'ensemble-quotient $E/\mathcal{R}$ est noté $K(X)$ et ses éléments sont appelés les **fractions rationnelles à une indéterminée et à coefficients dans** K. Pour $(A,S) \in E$, on note $\dfrac{A}{S}$ la classe de (A,S) modulo $\mathcal{R}$. Ainsi, pour tous $(A,S),(B,T)$ de E, on a :

$$\frac{A}{S} = \frac{B}{T} \Longleftrightarrow AT = BS.$$

2) Addition dans $K(X)$

Définissons une loi interne, notée $+$, dans E par :

$$(A,S) + (B,T) = (AT + BS, ST)$$

(on a bien $ST \neq 0$, car $S \neq 0$ et $T \neq 0$).
Cette loi $+$ est compatible avec $\mathcal{R}$ (C.1.1 p. 37), c'est-à-dire :

$$\forall (A,S),(B,T),(C,U) \in E,\quad (A,S)\ \mathcal{R}\ (B,T) \Longrightarrow \big((A,S) + (C,U)\big)\ \mathcal{R}\ \big((B,T) + (C,U)\big).$$

En effet, si $(A,S)\ \mathcal{R}\ (B,T)$, alors $AT = BS$, d'où :

$$(AU + CS)TU = ATU^2 + CSTU = BSU^2 + CSTU = (BU + CT)SU,$$

et donc $(AU + CS, SU)\ \mathcal{R}\ (BU + CT, TU)$,
c'est-à-dire : $\big((A,S) + (C,U)\big)\ \mathcal{R}\ \big((B,T) + (C,U)\big)$. ■

On peut donc définir une loi, encore notée $+$, dans $K(X)$ par :

$$\forall (A,S),(B,T) \in E,\quad \frac{A}{S} + \frac{B}{T} = \frac{AT + BS}{ST}.$$

3) Multiplication dans $K(\mathrm{X})$

De même qu'en *2)*, on montre qu'on peut définir une loi interne dans $K(\mathrm{X})$, notée $\cdot$ (ou par l'absence de symbole) par :

$$\forall (A,S),(B,T) \in E, \quad \frac{A}{S} \cdot \frac{B}{T} = \frac{AB}{ST}.$$

◆ **Théorème - Définition**

$(K(\mathrm{X}),+,\cdot)$ est un corps commutatif, appelé **corps des fractions rationnelles à une indéterminée et à coefficients dans** K**.**

Preuve :

Le lecteur vérifiera aisément les propriétés suivantes :

a) $+$ est associative, commutative, admet $\frac{0}{1}$ (noté 0) pour neutre, et tout élément $\frac{A}{S}$ de $K(\mathrm{X})$ admet un opposé qui est $\frac{-A}{S}$, et qui est noté $-\frac{A}{S}$.

b) $\cdot$ est associative, commutative, distributive sur $+$, admet $\frac{1}{1}$ (noté 1) pour neutre et, pour tout élément $\frac{A}{S}$ de $K[\mathrm{X}] - \{0\}$, on a $A \neq 0$ et $\frac{A}{S}$ admet un inverse, qui est $\frac{S}{A}$.

4) Loi externe dans $K(\mathrm{X})$

De même qu'en *2)*, on montre qu'on peut définir une loi externe dans $K(\mathrm{X})$ (à coefficients dans K), notée par l'absence de symbole, par :

$$\forall \lambda \in K, \ \forall (A,S) \in E, \ \lambda \frac{A}{S} = \frac{\lambda A}{S}.$$

◆ **Proposition**

$(K(\mathrm{X}),+, \ ,\cdot)$ est une K-algèbre associative, commutative, unitaire.

Preuve :

Le lecteur vérifiera aisément les propriétés suivantes (dont certaines ont été acquises en *3)*) :

a) $(K(\mathrm{X}),+)$ est un groupe abélien.

b) $(K(\mathrm{X}),+, \ )$ est un K-ev.

c) $\forall \lambda \in K, \forall F,G \in K(\mathrm{X}), \quad (\lambda F)G = \lambda(FG)$.

d) $\cdot$ est associative, commutative, admet un neutre (1).

5) *Plongement de* $K[X]$ *dans* $K(X)$

L'application $\Psi : K[X] \longrightarrow K(X)$ est un morphisme injectif d'algèbres, c'est-à-dire :
$P \longmapsto \frac{P}{1}$

- $\forall P, Q \in K[X], \quad \Psi(P+Q) = \Psi(P) + \Psi(Q)$
- $\forall P, Q \in K[X], \quad \Psi(PQ) = \Psi(P)\Psi(Q)$
- $\forall \lambda \in K, \forall P \in K[X], \quad \Psi(\lambda P) = \lambda \Psi(P)$
- $\Psi(1) = 1$
- $\forall P \in K[X], \quad (\Psi(P) = 0 \Longrightarrow P = 0)$.

On peut donc confondre (identifier) un polynôme P et la fraction rationnelle $\frac{P}{1}$. Ainsi, $K[X]$ est considéré comme une sous-algèbre unitaire de $K(X)$; en particulier, $K[X]$ est un sous-anneau du corps $K(X)$, et $K[X]$ est un sous-espace vectoriel du K-ev $K(X)$.

6) *Degré d'une fraction rationnelle*

Pour tous (A,S), (B,T) de E tels que $\frac{A}{S} = \frac{B}{T}$, on a :

$$\deg(A) - \deg(S) = \deg(AT) - \deg(ST) = \deg(BS) - \deg(ST) = \deg(B) - \deg(T).$$

Ceci permet de définir le **degré d'une fraction rationnelle** par :

$$\forall (A,S) \in E, \quad \deg\left(\frac{A}{S}\right) = \deg(A) - \deg(S) \in \{-\infty\} \cup \mathbb{Z}.$$

Remarquons que l'application deg : $K(X) \longrightarrow \{-\infty\} \cup \mathbb{Z}$ prolonge l'application deg : $K[X] \longrightarrow \{-\infty\} \cup \mathbb{N}$ (définie en 5.1.1 Déf. 2 p. 140) car :

$$\forall P \in K[X], \quad \deg\left(\frac{P}{1}\right) = \deg(P) - \deg(1) = \deg(P).$$

Le lecteur pourra montrer, à titre d'exercice, les formules suivantes, pour tous k de K^* et F, G de $K(X)$:

1) $\deg(F+G) \leqslant \text{Max}\left(\deg(F), \deg(G)\right)$

2) $\deg(kF) = \deg(F)$

3) $\deg(FG) = \deg(F) + \deg(G)$.

7) *Forme irréductible d'une fraction rationnelle non nulle*

La démarche est la même que dans 4.3.4 *2)* p. 118.

On appelle **représentant irréductible** d'une fraction rationnelle F de $K(X)$ non nulle tout couple (A,S) de $(K[X] - \{0\})^2$ tel que :

$$F = \frac{A}{S} \quad \text{et} \quad A \wedge S = 1.$$

En raisonnant comme dans 4.3.4 *2)*, on montre :

a) Toute fraction rationnelle non nulle admet au moins un représentant irréductible.

b) Soient $F \in K(X)$ et (A,S) un représentant irréductible de F; tout représentant de F est de la forme (QA,QS), $Q \in K[X] - \{0\}$.

c) Soient $F \in K(X)$ et (A,S) un représentant irréductible de F; les représentants irréductibles de F sont les (kA,kS), $k \in K - \{0\}$.

8) Zéros et pôles d'une fraction rationnelle

♦ **Définition** Soient $F \in K(X) - \{0\}$, (A,S) un représentant irréductible de F.

1) On appelle **zéros** de F les zéros de A. Si a est un zéro de F, on appelle **ordre de multiplicité du zéro** a **de** F l'ordre de multiplicité de a en tant que zéro de A.

2) On appelle **pôles** de F les zéros de S. Si a est un pôle de F, on appelle **ordre de multiplicité du pôle** a **de** F l'ordre de multiplicité de a en tant que zéro de S.

EXEMPLE :

Pour $F = \dfrac{X^4 - X^2}{X^2 - 3X + 2} \in \mathbb{R}(X)$, la forme irréductible de F est $F = \dfrac{X^2(X+1)}{X-2}$, les zéros de F sont -1 (simple), 0 (double), et F admet un seul pôle, 2 (simple).

9) Dérivée d'une fraction rationnelle

Soient $F \in K(X)$, $(A,S) \in E$ tel que $F = \dfrac{A}{S}$.

On définit la **fraction rationnelle dérivée** de F, notée F' par : $F' = \dfrac{A'S - AS'}{S^2}$.

Cette définition est licite car, si $(A,S),(B,T)$ sont deux éléments de E tels que $F = \dfrac{A}{S} = \dfrac{B}{T}$, alors $AT = BS$, d'où $A'T + AT' = B'S + BS'$, et donc :

$$\begin{aligned}(A'S - AS')T^2 - (B'T - BT')S^2 &= (A'T - B'S)ST - AS'T^2 + BT'S^2 \\ &= (BS' - AT')ST - AS'T^2 + BT'S^2 \\ &= (BS - AT)(S'T + ST') = 0.\end{aligned}$$ ■

L'application $K(X) \xrightarrow[F \longmapsto F']{} K(X)$ prolonge l'application $K[X] \xrightarrow[P \longmapsto P']{} K[X]$ car :

$$\forall P \in K[X], \quad \left(\frac{P}{1}\right)' = \frac{P'1 - P \cdot 0}{1^2} = P'.$$

Le lecteur montrera aisément les formules suivantes, pour tous λ de K et F,G de $K(X)$:

$$(F+G)' = F' + G', \quad (\lambda F)' = \lambda F',$$
$$(FG)' = F'G + FG', \quad \left(\frac{F}{G}\right)' = \frac{F'G - FG'}{G^2} \text{ (si } G \neq 0).$$ ■

Il se peut que $\deg(F') \neq \deg(F) - 1$, comme le montrent les exemples :

- $F = 1, F' = 0$: $\deg(F) = 0$, $\deg(F') = -\infty$
- $F = \dfrac{X+1}{X}$, $F' = -\dfrac{1}{X^2}$: $\deg(F) = 0$, $\deg(F') = -2$.

On peut cependant remarquer : $\forall F \in K(X) - \{0\}$, $\deg(F') < \deg(F)$. ■

On définit, par récurrence, les **dérivées successives d'une fraction rationnelle** F :

$$\begin{cases} F^{(0)} = F, \quad F^{(1)} = F' \\ \forall n \in \mathbb{N}^*, \quad F^{(n)} = (F^{(n-1)})'. \end{cases}$$

Le lecteur pourra montrer les formules suivantes :

- $\forall F \in K(X)$, $\forall (i,j) \in \mathbb{N}^2$, $(F^{(i)})^{(j)} = F^{(i+j)}$
- $\forall n \in \mathbb{N}$, $\forall (F,G) \in (K(X))^2$, $(FG)^{(n)} = \displaystyle\sum_{k=0}^{n} C_n^k F^{(k)} G^{(n-k)}$ (**formule de Leibniz**).

◆ **Proposition** Soit $P \in K[X]$, scindé : $P = \lambda \displaystyle\prod_{i=1}^{n} (X - x_i)$, $\lambda \in K - \{0\}$, $n \in \mathbb{N}^*$, $x_1, \ldots, x_n \in K$. On a :

$$\frac{P'}{P} = \sum_{i=1}^{n} \frac{1}{X - x_i}.$$

Preuve :

Se déduit de $P' = \lambda \displaystyle\sum_{i=1}^{n} \left(\prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} (X - x_j) \right)$ en divisant par P.

10) Fonctions rationnelles

◆ **Définition** Soient $F \in K(X)$, (A,S) un représentant irréductible de F. On appelle **fonction rationnelle associée à** F la fonction, notée $\tilde{F}$, de K dans K, définie par : $\tilde{F}(x) = \dfrac{\tilde{A}(x)}{\tilde{S}(x)}$, pour tout x de K tel que $\tilde{S}(x) \neq 0$.

Cette définition est licite, puisque les représentants irréductibles de F sont les (kA, kS), $k \in K - \{0\}$ (cf. *7)* p. 189).

Avec les notations précédentes, l'ensemble de définition de $\tilde{F}$ est K privé des pôles de F.

EXEMPLE : $K = \mathbb{R}$, $F = \dfrac{X^3 - 2X^2 + X}{X^2 + X}$.

Sous forme irréductible : $F = \dfrac{X^2 - 2X + 1}{X + 1}$, donc $\tilde{F} : \mathbb{R} - \{-1\} \longrightarrow \mathbb{R}$, $x \longmapsto \dfrac{(x-1)^2}{x+1}$

On appelle **fonction rationnelle** (dans K) toute fonction f de K dans K telle qu'il existe une fraction rationnelle F de $K(X)$ telle que $f = \tilde{F}$.

EXEMPLE :

$f : \mathbb{C}^* \longrightarrow \mathbb{C}$, $z \longmapsto \frac{1}{z^2}$ est une fonction rationnelle, la fonction rationnelle associée à la fraction rationnelle $\frac{1}{X^2}$.

Exercices

◇ **5.4.1** Soient $n \in \mathbb{N} - \{0,1\}$, $P_n = \sum_{k=0}^{n-1}(k+1)X^k$.

Montrer que l'équation $P_n(x) = n^2$, d'inconnue $x \in \mathbb{Q}$, admet au moins une solution dans $]1;2[\cap\mathbb{Q}$.

◇ **5.4.2** Montrer qu'il n'existe pas de F de $K(X)$ telle que : $F^2 = X$.

◇ **5.4.3** Soit $P \in \mathbb{R}[X]$, de degré $n \in \mathbb{N}$, tel que : $P(-1) \neq 0$ et $-\frac{P'(-1)}{P(-1)} \leqslant \frac{n}{2}$. Démontrer que P admet au moins un zéro de module $\geqslant 1$.

5.4.2 Décomposition en éléments simples

1) Etude théorique

Le lecteur pourra omettre cette étude théorique et admettre le résultat d'existence et d'unicité de la décomposition en éléments simples d'une fraction rationnelle (Th. p. 196).

Le but de ce § *1)* est de décomposer une fraction rationnelle en une somme de fractions rationnelles «plus simples» en vue, entre autres, du calcul des primitives de cette fraction rationnelle (Tome 2, 9.5) et du développement en série entière de cette fraction rationnelle (lorsqu'elle n'admet pas 0 pour pôle; cf. Tome 4, 5.5.2 Prop. 4).

◆ **Lemme 1** Soient $F \in K(X)$, $(A,S) \in K[X] \times (K[X] - \{0\})$ tel que $F = \frac{A}{S}$.

Il existe un couple unique (E,R) de $(K[X])^2$ tel que :

$$F = E + \frac{R}{S} \quad \text{et} \quad \deg(R) < \deg(S).$$

De plus, si $A \wedge S = 1$, alors $R \wedge S = 1$.

Le polynôme E est appelé la **partie entière** de F; la fraction rationnelle $\frac{R}{S}$ est quelquefois appelée la **partie fractionnaire** de F.

Preuve :

1) **Existence**

Par division euclidienne de A par S, il existe $(E,R) \in (K[X])^2$ tel que :
$A = SE + R$ et $\deg(R) < \deg(S)$, d'où le résultat voulu.
De plus, d'après l'algorithme d'Euclide, si $A \wedge S = 1$, alors $R \wedge S = 1$.

2) **Unicité**

Soient (E_1,R_1), (E_2,R_2) convenant. Alors $E_1 - E_2 = \dfrac{R_2 - R_1}{S}$, donc :

$$\deg(E_1 - E_2) = \deg(R_2 - R_1) - \deg(S) < 0,$$

d'où $E_1 - E_2 = 0$, $E_1 = E_2$, $R_1 = R_2$.

EXEMPLE :

Pour $K = \mathbb{R}$, $F = \dfrac{X^4 + X^3 - 2X^2 + X - 1}{X^3 - 3X^2 + 1}$, on obtient à l'aide de la division euclidienne de $X^4 + X^3 - 2X^2 + X - 1$ par $X^3 - 3X^2 + 1$: $F = X + 4 + \dfrac{10X^2 - 5}{X^3 - 3X^2 + 1}$.

◆ **Lemme 2** Soient $A \in K[X]$, $n \in \mathbb{N}^*$, $S_1,\ldots,S_n \in K[X] - \{0\}$ tels que $S_1,\ldots,S_n$ soient premiers entre eux deux à deux.
Il existe alors $A_1,\ldots,A_n \in K[X]$ tels que : $\dfrac{A}{S_1\ldots,S_n} = \dfrac{A_1}{S_1} + \ldots + \dfrac{A_n}{S_n}$.

Preuve :

Récurrence sur n.

- La propriété est triviale pour $n = 1$.
- Cas $n = 2$

D'après le théorème de Bezout, puisque $S_1 \wedge S_2 = 1$, il existe $(U_1,U_2) \in (K[X])^2$ tel que $S_1U_1 + S_2U_2 = 1$. On a alors : $\dfrac{A}{S_1S_2} = \dfrac{A(S_1U_1 + S_2U_2)}{S_1S_2} = \dfrac{AU_2}{S_1} + \dfrac{AU_1}{S_2}$.

- Supposons la propriété vraie pour un n de $\mathbb{N}^*$, et soient $S_1,\ldots,S_{n+1} \in K[X] - \{0\}$ premiers entre eux deux à deux. D'après 5.2.4 *3)* Prop. 1 p. 165, on a alors :

$$(S_1 \ldots S_n) \wedge S_{n+1} = 1.$$

D'après l'étude du cas $n = 2$, il existe $C_1, A_{n+1} \in K[X]$ tels que :

$$\frac{A}{S_1 \ldots S_n S_{n+1}} = \frac{C_1}{S_1 \ldots S_n} + \frac{A_{n+1}}{S_{n+1}}.$$

Puis, d'après l'hypothèse de récurrence, il existe $A_1,\ldots,A_n \in K[X]$ tels que :

$$\frac{C_1}{S_1 \ldots S_n} = \frac{A_1}{S_1} + \ldots + \frac{A_n}{S_n},$$

d'où finalement : $\dfrac{A}{S_1 \ldots S_{n+1}} = \dfrac{A_1}{S_1} + \ldots + \dfrac{A_{n+1}}{S_{n+1}}$. ■

Nous allons maintenant combiner les lemmes 1 et 2 pour obtenir le résultat suivant.

♦ **Lemme 3** Soient $A \in K[X]$, $n \in \mathbb{N}^*$, $S_1, \ldots, S_n \in K[X] - \{0\}$ tels que $S_1, \ldots, S_n$ soient premiers entre eux deux à deux. Il existe $(E, R_1, \ldots, R_n) \in (K[X])^{n+1}$ unique tel que :

$$\begin{cases} \dfrac{A}{S_1 \ldots S_n} = E + \dfrac{R_1}{S_1} + \ldots + \dfrac{R_n}{S_n} \\ \forall i \in \{1, \ldots, n\},\ \deg(R_i) < \deg(S_i). \end{cases}$$

De plus, E est la partie entière de $\dfrac{A}{S_1 \ldots S_n}$.

Preuve :

1) **Existence**

D'après le Lemme 2 p. 192, il existe $A_1, \ldots, A_n \in K[X]$ tels que :

$$\frac{A}{S_1 \ldots S_n} = \frac{A_1}{S_1} + \ldots + \frac{A_n}{S_n}.$$

Puis, d'après le Lemme 1 p. 191, il existe $E_1, \ldots, E_n, R_1, \ldots, R_n \in K[X]$ tels que :

$$\forall i \in \{1, \ldots, n\},\quad \begin{cases} \dfrac{A_i}{S_i} = E_i + \dfrac{R_i}{S_i} \\ \deg(R_i) < \deg(S_i) \end{cases}.$$

En notant $E = E_1 + \ldots + E_n$, on obtient le résultat voulu.

2) **Unicité**

Récurrence sur n.

- Le cas $n = 1$ est déjà vu (Lemme 1).
- Cas $n = 2$.

Soient $(E, R_1, R_2), (D, P_1, P_2)$ convenant, c'est-à-dire :

$$\begin{cases} \dfrac{A}{S_1 S_2} = E + \dfrac{R_1}{S_1} + \dfrac{R_2}{S_2} = D + \dfrac{P_1}{S_1} + \dfrac{P_2}{S_2} \\ \forall i \in \{1,2\},\quad \begin{cases} \deg(R_i) < \deg(S_i) \\ \deg(P_i) < \deg(S_i) \end{cases} \end{cases}.$$

On a alors : $S_1(R_2 - P_2) = S_1 S_2 (D - E) + S_2(P_1 - R_1)$, et donc : $S_1 \mid S_2(P_1 - R_1)$.

Comme $S_1 \wedge S_2 = 1$, le théorème de Gauss montre : $S_1 \mid P_1 - R_1$.

Mais d'autre part : $\deg(P_1 - R_1) < \deg(S_1)$.

On déduit $P_1 - R_1 = 0$, $P_1 = R_1$, puis de même $P_2 = R_2$, et enfin $D = E$.

- Supposons la propriété vraie pour un n de $\mathbb{N}^*$.

Soient $E, R_1, \ldots, R_{n+1}, D, P_1, \ldots, P_{n+1} \in K[X]$ tels que :

$$\begin{cases} \dfrac{A}{S_1 \ldots S_{n+1}} = E + \displaystyle\sum_{i=1}^{n+1} \frac{R_i}{S_i} = D + \sum_{i=1}^{n+1} \frac{P_i}{S_i} \\ \forall i \in \{1, \ldots, n+1\},\quad \begin{cases} \deg(R_i) < \deg(S_i) \\ \deg(P_i) < \deg(S_i) \end{cases} \end{cases}.$$

En notant $T = S_1 \dots S_n$, $B = \sum_{i=1}^{n} \left(R_i \left(\prod_{\substack{i \leqslant j \leqslant n \\ j \neq i}} S_j \right) \right)$, $C = \sum_{i=1}^{n} \left(P_i \left(\prod_{\substack{i \leqslant j \leqslant n \\ j \neq i}} S_j \right) \right)$,

on a : $\begin{cases} T \wedge S_{n+1} = 1 \\ \dfrac{A}{TS_{n+1}} = E + \dfrac{B}{T} + \dfrac{R_{n+1}}{S_{n+1}} = D + \dfrac{C}{T} + \dfrac{P_{n+1}}{S_{n+1}} \cdot \end{cases}$

D'après l'étude du cas $n = 2$, on déduit :

$$D = E,\ C = B\ P_{n+1} = R_{n+1}.$$

Ainsi : $\begin{cases} \displaystyle\sum_{i=1}^{n} \frac{R_i}{S_i} = \sum_{i=1}^{n} \frac{P_i}{S_i} \\ \forall i \in \{1,\dots,n\}, \quad \begin{cases} \deg(R_i) < \deg(S_i) \\ \deg(P_i) < \deg(S_i), \end{cases} \end{cases}$

d'où, par l'hypothèse de récurrence : $P_1 = R_1, \dots, P_n = R_n$.

3) Avec les notations du Lemme, comme

$$\deg\left(\frac{R_1}{S_1} + \dots + \frac{R_n}{S_n}\right) \leqslant \operatorname{Max}\left(\left(\deg\left(\frac{R_i}{S_i}\right)\right)_{1 \leqslant i \leqslant n}\right) < 0,$$

d'après le Lemme 1, E est la partie entière de $\dfrac{A}{S_1 \dots S_n}$.

◆ **Lemme 4** Soient $A \in K[X]$, $S \in K[X]$ tel que $\deg(S) \geqslant 1$, $\alpha \in \mathbb{N}^*$.
Il existe $(E, C_1, \dots, C_\alpha) \in (K[X])^{\alpha+1}$ unique tel que :

$$\begin{cases} \dfrac{A}{S^\alpha} = E + \dfrac{C_\alpha}{S^\alpha} + \dfrac{C_{\alpha-1}}{S^{\alpha-1}} + \dots + \dfrac{C_1}{S} \\ \forall j \in \{1,\dots,\alpha\}, \quad \deg(C_j) < \deg(S). \end{cases}$$

De plus, E est la partie entière de $\dfrac{A}{S^\alpha}$.

Preuve :

1) **Existence**

Récurrence sur α.

• Le cas $\alpha = 1$ a été vu (lemme 1).

• Supposons la propriété vraie pour un α de $\mathbb{N}^*$; il existe donc $E_1, C_2, \dots, C_{\alpha+1} \in K[X]$ tels que :

$$\begin{cases} \dfrac{A}{S^\alpha} = E_1 + \dfrac{C_{\alpha+1}}{S^\alpha} + \dots + \dfrac{C_2}{S} \\ \forall j \in \{1,\dots,\alpha\}, \ \deg(C_{j+1}) < \deg(S) \end{cases}.$$

D'après le Lemme 1 p. 191, il existe $E, C_1 \in K[X]$ tels que :

$$\frac{E_1}{S} = E + \frac{C_1}{S} \quad \text{et} \quad \deg(C_1) < \deg(S).$$

On a alors :

$$\begin{cases} \dfrac{A}{S^{\alpha+1}} = \dfrac{A}{S^\alpha \cdot S} = E + \dfrac{C_{\alpha+1}}{S^{\alpha+1}} + \dots + \dfrac{C_1}{S} \\ \forall j \in \{1,\dots,\alpha+1\}, \ \deg(C_j) < \deg(S). \end{cases}$$

2) **Unicité**

Récurrence sur α.

- Le cas $\alpha = 1$ a été vu (cf. Lemme 1 p. 191).
- Supposons la propriété vraie pour un α de $\mathbb{N}^*$.

Soient $E_1, C_1, \ldots, C_{\alpha+1}$, $E_2, D_1, \ldots, D_{\alpha+1} \in K[X]$ tels que :

$$\begin{cases} \dfrac{A}{S^{\alpha+1}} = E_1 + \dfrac{C_{\alpha+1}}{S^{\alpha+1}} + \ldots + \dfrac{C_1}{S} = E_2 + \dfrac{D_{\alpha+1}}{S^{\alpha+1}} + \ldots + \dfrac{D_1}{S} \\ \forall j \in \{1, \ldots, \alpha+1\}, \quad \begin{cases} \deg(C_j) < \deg(S) \\ \deg(D_j) < \deg(S) \end{cases} . \end{cases}$$

En multipliant par S^α, on obtient :

$$\begin{aligned} \frac{A}{S} &= \left(E_1 + C_\alpha + C_{\alpha-1}S + \ldots + C_1 S^{\alpha-1}\right) + \frac{C_{\alpha+1}}{S} \\ &= \left(E_2 + D_\alpha + D_{\alpha-1}S + \ldots + D_1 S^{\alpha-1}\right) + \frac{D_{\alpha+1}}{S}. \end{aligned}$$

D'après le Lemme 1, on déduit $D_{\alpha+1} = C_{\alpha+1}$, puis, en appliquant l'hypothèse de récurrence :

$$D_\alpha = C_\alpha, \ldots, D_1 = C_1, \quad E_2 = E_1.$$

3) Avec les notations du lemme, comme

$$\deg\left(\frac{C_\alpha}{S^\alpha} + \ldots + \frac{C_1}{S}\right) \leqslant \operatorname{Max}\left(\left(\deg\left(\frac{C_j}{S_j}\right)\right)_{1 \leqslant j \leqslant \alpha}\right) < 0,$$

d'après le Lemme 1, E est la partie entière de $\dfrac{A}{S^\alpha}$.

◆ **Définition** On appelle **éléments simples** de $K(X)$:

- les monômes de $K[X]$
- les éléments de $K(X)$ de la forme $\dfrac{C}{S^\alpha}$ où :

$$\begin{cases} S \in K[X], \deg(S) \geqslant 1, \ S \text{ est irréductible} \\ \alpha \in \mathbb{N}^* \\ C \in K[X] - \{0\} \\ \deg(C) < \deg(S). \end{cases}$$

Les éléments simples de la forme $\dfrac{c}{S^\alpha}$ où $(S \in K[X], \deg(S) = 1, \alpha \in \mathbb{N}^*, c \in K - \{0\})$ sont appelés **éléments simples de 1ère espèce**.

Des lemmes précédents, on déduit le théorème suivant.

◆ **Théorème** **(Existence et unicité de la décomposition en éléments simples d'une fraction rationnelle)**

Soit $F = \dfrac{A}{S_1^{\alpha_1} \dots S_n^{\alpha_n}}$ où :

$n \in \mathbb{N}^*$

$S_1, \dots, S_n \in K[X] - \{0\}$ sont irréductibles et premiers entre eux deux à deux

$\alpha_1, \dots, \alpha_n \in \mathbb{N}^*$

$A \in K[X]$.

Il existe une famille unique de polynômes $\left(E, C_{\alpha_1,1}, \dots, C_{\alpha_1,\alpha_1}, C_{\alpha_2,1}, \dots, C_{\alpha_2,\alpha_2}, \dots, C_{\alpha_n,1}, \dots, C_{\alpha_n,\alpha_n}\right)$ de $K[X]$ telle que :

$$\begin{cases} F = E + \displaystyle\sum_{i=1}^{n} \sum_{j=1}^{\alpha_i} \frac{C_{\alpha_i,j}}{S_i^j} \\ \\ \forall i \in \{1, \dots, n\},\ \forall j \in \{1, \dots, \alpha_i\},\ \deg\left(C_{\alpha_i,j}\right) < \deg(S_i). \end{cases}$$

La formule ci-dessus s'appelle la **décomposition en éléments simples** (en abrégé : DES) **de la fraction rationnelle** F.

2) *Pratique de la* DES

a) Cas d'un pôle simple

Soient $(A,S) \in K[X] \times (K[X] - \{0\})$, $F = \dfrac{A}{S}$, a un zéro de S.

Supposons que a soit un zéro simple de S. Il existe alors $S_1 \in K[X]$ tel que :

$$S = (X - a)S_1 \quad \text{et} \quad \tilde{S}_1(a) \neq 0.$$

La DES de F contient le terme $\dfrac{\lambda}{X - a}$ $(\lambda \in K)$, pour lequel on cherche à calculer λ.

D'après le Lemme 2 p. 192, il existe $A_1 \in K[X]$ tel que : $F = \dfrac{A}{S} = \dfrac{\lambda}{X - a} + \dfrac{A_1}{S_1}$.

On a alors : $A = \lambda S_1 + (X - a)A_1$, d'où, en remplaçant X par a : $\tilde{A}(a) = \lambda \widetilde{S_1}(a)$.

Ainsi : $\lambda = \dfrac{\tilde{A}(a)}{\widetilde{S_1}(a)} = \widetilde{((X - a)F)}(a)$.

En résumé :

◆ **Proposition 1** Soient $(A,S) \in K[X] \times (K[X] - \{0\})$, $F = \dfrac{A}{S}$, a un zéro simple de S. Le coefficient λ du terme $\dfrac{\lambda}{X - a}$ de la DES de F est $\widetilde{((X - a)F)}(a)$.

Autrement dit, λ est obtenu par *multiplication* des deux membres de l'égalité $F = \dfrac{A}{S}$ par $X - a$, puis *remplacement* de X par a.

EXEMPLE :

Former la DES de $F = \dfrac{X}{(X - 1)(X - 2)}$ dans $\mathbb{R}(X)$.

La partie entière est nulle, et la DES est de la forme : $F = \dfrac{\lambda}{X-1} + \dfrac{\mu}{X-2}$, $(\lambda,\mu) \in \mathbb{R}^2$.

D'après la Prop. 1 : $\lambda = \widetilde{((X-1)F)}(1) = \left(\widetilde{\dfrac{X}{X-2}}\right)(1) = -1$

$$\mu = \widetilde{((X-2)F)}(2) = \left(\widetilde{\frac{X}{X-1}}\right)(2) = 2.$$

Ainsi : $F = \dfrac{-1}{X-1} + \dfrac{2}{X-2}$, ce qui peut être aisément vérifié par réduction au même dénominateur. ■

Dans certains cas, avec les notations de la Prop. 1, le calcul de $\widetilde{((X-a)F)}(a)$ peut donner des résultats apparemment compliqués ou inexploitables.

Puisque $S = (X-a)S_1$, on obtient, en dérivant :

$$S' = (X-a)S_1' + S_1, \quad \text{d'où} \quad \widetilde{S'}(a) = \widetilde{S_1}(a).$$

On a ainsi montré la Proposition suivante :

♦ **Proposition 2** Soient $(A,S) \in K[X] \times (K[X] - \{0\})$, $F = \dfrac{A}{S}$, a un zéro simple de S. Le coefficient λ du terme $\dfrac{\lambda}{X-a}$ de la DES de $\dfrac{A}{S}$ vaut $\dfrac{\widetilde{A}(a)}{\widetilde{S'}(a)}$.

EXEMPLE :

Former, pour $n \in \mathbb{N}^*$, la DES de $F = \dfrac{1}{X^n - 1}$ dans $\mathbb{C}(X)$.

La décomposition primaire de $X^n - 1$ (dans $\mathbb{C}[X]$) est : $X^n - 1 = \prod_{k=0}^{n-1}(X - \omega_k)$, où $\omega_k = \exp\left(\dfrac{2ik\pi}{n}\right)$, $0 \leqslant k \leqslant n-1$.

Les zéros de $X^n - 1$ sont tous simples, et la DES de F est de la forme :

$$F = \sum_{k=0}^{n-1} \frac{\lambda_k}{X - \omega_k}, \text{ où } \lambda_k \in \mathbb{C},\ 0 \leqslant k \leqslant n-1.$$

D'après la Prop. 2, pour tout k de $\{0,\ldots,n-1\}$:

$$\lambda_k = \left(\widetilde{\frac{1}{nX^{n-1}}}\right)(\omega_k) = \frac{1}{n\omega_k^{n-1}} = \frac{\omega_k}{n}.$$

D'où la DES : $\dfrac{1}{X^n - 1} = \sum_{k=0}^{n-1} \dfrac{\frac{\omega_k}{n}}{X - \omega_k}$.

L'application de la Prop. 1 aurait donné ici : $\lambda_k = \dfrac{1}{\prod\limits_{\substack{0\leqslant j\leqslant n-1\\ j\neq k}} (\omega_k - \omega_j)}$,

résultat exact, mais apparemment inutilisable.

b) Cas d'un pôle multiple

1) Cas du pôle 0

Intéressons-nous à une fraction rationnelle $F = \dfrac{A}{X^n T}$, où $A, T \in K[X]$, $\widetilde{T}(0) \neq 0$.

D'après le théorème de décomposition en éléments simples, il existe $\alpha_1, \ldots, \alpha_n \in K$, $B \in K[X]$ tels que : $F = \dfrac{\alpha_n}{X^n} + \ldots + \dfrac{\alpha_1}{X} + \dfrac{B}{T}$.

On a alors $A = \left(\alpha_n + \alpha_{n-1}X + \ldots + \alpha_1 X^{n-1}\right) T + X^n B$.

D'après le théorème de division suivant les puissances croissantes (cf. 5.2.6 p. 167), $\alpha_n + \alpha_{n-1}X + \ldots + \alpha_1 X^{n-1}$ est le **quotient de la division de A par T suivant les puissances croissantes jusqu'à l'ordre $n-1$** (et B en est le reste).

EXEMPLE :

Former la DES de $F = \dfrac{X^5 + 1}{X^3(X-2)}$ dans $\mathbb{R}(X)$.

La DES de F est de la forme : $F = E + \dfrac{\alpha_3}{X^3} + \dfrac{\alpha_2}{X^2} + \dfrac{\alpha_1}{X} + \dfrac{\lambda}{X-2}$,

où E est la partie entière de F, et α_3, α_2, α_1, $\lambda \in \mathbb{R}$.

• On calcule E comme quotient de la division euclidienne de $X^5 + 1$ par $X^4 - 2X^3$; on obtient $E = X + 2$.

• On calcule λ par multiplication et remplacement :

$$\lambda = \widetilde{((X-2)F)}(2) = \left(\widetilde{\frac{X^5+1}{X^3}}\right)(2) = \frac{33}{8}.$$

• On calcule α_3, α_2, α_1 par division de $1 + X^5$ par $-2 + X$ suivant les puissances croissantes jusqu'à l'ordre 2 :

$$\begin{array}{llll|l} 1 & & & +X^5 & -2+X \\ \cline{5-5} & \frac{1}{2}X & & +X^5 & -\frac{1}{2} - \frac{1}{4}X - \frac{1}{8}X^2 \\ & & \frac{1}{4}X^2 & +X^5 & \\ & & & \frac{1}{8}X^3 + X^5 & \end{array}$$

On obtient : $\alpha_3 = -\dfrac{1}{2}$, $\alpha_2 = -\dfrac{1}{4}$, $\alpha_1 = -\dfrac{1}{8}$.

On peut remarquer que, dans cette division, les termes de degré $\geqslant 3$ n'interviennent pas. On peut donc utiliser en pratique une division «tronquée » :

$$\begin{array}{l|l} 1 & -2+X \\ \frac{1}{2}X & \hline -\frac{1}{2}-\frac{1}{4}X-\frac{1}{8}X^2 \\ \frac{1}{4}X^2 & \\ 0 & \end{array}$$

Finalement : $\dfrac{X^5+1}{X^3(X-2)} = X+2+\dfrac{-\frac{1}{2}}{X^3}+\dfrac{-\frac{1}{4}}{X^2}+\dfrac{-\frac{1}{8}}{X}+\dfrac{\frac{33}{8}}{X-2}$.

2) Cas d'un pôle autre que 0

Si a est un zéro multiple de S, pour obtenir les coefficients relatifs au pôle a dans la DES de $\dfrac{A}{S}$, on effectuera un «changement d'indéterminée» $Y = X - a$, et on se ramènera au cas précédent (vis-à-vis de l'indéterminée Y).

EXEMPLE :

Former la DES de $F = \dfrac{1}{(X-1)^4(X+2)^3}$ dans $\mathbb{R}(X)$.

Il est clair que la partie entière est nulle. La DES de F est de la forme :

$$F = \frac{\alpha_4}{(X-1)^4}+\frac{\alpha_3}{(X-1)^3}+\frac{\alpha_2}{(X-1)^2}+\frac{\alpha_1}{X-1}+\frac{\beta_3}{(X+2)^3}+\frac{\beta_2}{(X+2)^2}+\frac{\beta_1}{X+2},$$

où $\alpha_4,\ldots,\alpha_1$, $\beta_3,\ldots,\beta_1$ sont des réels à calculer.

• *Calcul de* $\alpha_4,\ldots,\alpha_1$

Changement d'indéterminée $Y = X - 1$ (donc $X = 1 + Y$), $F = \dfrac{1}{(X-1)^4(X+2)^3} = \dfrac{1}{Y^4(3+Y)^3}$, puis division suivant les puissances croissantes jusqu'à l'ordre 3 $(= 4-1)$ de 1 par $(3+Y)^3$:

$$\begin{array}{l|l} 1 & 27+27Y+9Y^2+Y^3 \\ -Y-\frac{1}{3}Y^2-\frac{1}{27}Y^3 & \hline \frac{1}{27}-\frac{1}{27}Y+\frac{2}{81}Y^2-\frac{10}{729}Y^3 \\ \frac{2}{3}Y^2+\frac{8}{27}Y^3 & \\ -\frac{10}{27}Y^3 & \\ 0 & \end{array}$$

On obtient : $\alpha_4 = \dfrac{1}{27}$, $\alpha_3 = -\dfrac{1}{27}$, $\alpha_2 = \dfrac{2}{81}$, $\alpha_1 = -\dfrac{10}{729}$.

• *Calcul de $\beta_3,\dots,\beta_1$*

Changement d'indéterminée $Z = X + 2$ (donc $X = -2 + Z$),

$$F = \frac{1}{(X-1)^4(X+2)^3} = \frac{1}{(-3+Z)^4 Z^3},$$

puis division suivant les puissances croissantes jusqu'à l'ordre 2 ($= 3 - 1$) de 1 par $(3+Z)^4$:

$$\begin{array}{l|l} 1 & 81 - 108Z + 54Z^2 \\ \hline \frac{4}{3}Z - \frac{2}{3}Z^2 & \frac{1}{81} + \frac{4}{243}Z + \frac{10}{729}Z^2 \\ \frac{10}{9}Z^2 & \\ 0 & \end{array}$$

On obtient : $\beta_3 = \dfrac{1}{81}$, $\beta_2 = \dfrac{4}{243}$, $\beta_1 = \dfrac{10}{729}$.

Finalement :

$$\frac{1}{(X-1)^4(X+2)^3} = \frac{\frac{1}{27}}{(X-1)^4} + \frac{-\frac{1}{27}}{(X-1)^3} + \frac{\frac{2}{81}}{(X-1)^2} + \frac{-\frac{10}{729}}{X-1} + \frac{\frac{1}{81}}{(X+2)^3} + \frac{\frac{4}{243}}{(X+2)^2} + \frac{\frac{10}{729}}{X+2}.$$

c) Remarques de parité

En utilisant l'unicité de la DES d'une fraction rationnelle, on voit que, si la fraction rationnelle F est paire (resp. impaire) et si l'élément simple $\dfrac{C(X)}{(S(X))^k}$ figure dans la DES de F, alors l'élément simple $\dfrac{C(-X)}{(S(-X))^k}$ $\left(\text{resp. } -\dfrac{C(-X)}{(S(-X))^k}\right)$ figure dans la DES de F.

EXEMPLE :

Former la DES de $F = \dfrac{2X^2+5}{(X^2-1)^3}$ dans $\mathbb{R}(X)$.

La forme de la DES de F est :

$$F = \frac{a}{(X-1)^3} + \frac{b}{(X-1)^2} + \frac{c}{X-1} + \frac{\alpha}{(X+1)^3} + \frac{\beta}{(X+1)^2} + \frac{\gamma}{X+1},$$

où $a,\dots,\gamma$ sont des réels à trouver.

En remplacant X par $-X$:

$$F(-X) = \frac{-a}{(X+1)^3} + \frac{b}{(X+1)^2} + \frac{-c}{X+1} + \frac{-\alpha}{(X-1)^3} + \frac{\beta}{(X-1)^2} + \frac{-\gamma}{X-1}.$$

Comme F est paire, l'unicité de la DES de F montre : $a = -\alpha$, $b = \beta$, $c = -\gamma$.

Calcul de a,b,c

Changement d'indéterminée $Y = X - 1$ (donc $X = 1 + Y$),

$$F = \frac{2X^2+5}{(X-1)^3(X+1)^3} = \frac{2(1+Y)^2+5}{Y^3(2+Y)^3},$$

puis division suivant les puissances croissantes jusqu'à l'ordre 2 de $2(1+Y)^2+5$ par $(2+Y)^3$:

$$\begin{array}{l|l} 7+4Y+2Y^2 & 8+12Y+6Y^2 \\ \hline -\frac{13}{2}Y-\frac{13}{4}Y^2 & \frac{7}{8}-\frac{13}{16}Y+\frac{13}{16}Y^2 \\ \frac{13}{2}Y^2 & \\ 0 & \end{array}$$

On obtient : $a=\frac{7}{8}$, $b=-\frac{13}{16}$, $c=\frac{13}{16}$.

Finalement : $\dfrac{2X^2+5}{(X^2-1)^3}=\dfrac{\frac{7}{8}}{(X-1)^3}+\dfrac{-\frac{13}{16}}{(X-1)^2}+\dfrac{\frac{13}{16}}{(X-1)}+\dfrac{-\frac{7}{8}}{(X+1)^3}+\dfrac{-\frac{13}{16}}{(X+1)^2}+\dfrac{-\frac{13}{16}}{X+1}$.

d) Lorsqu'il ne reste plus qu'un ou deux coefficients à déterminer dans une DES, on peut envisager de remplacer X par une valeur particulière, ou de faire tendre X vers l'infini (rigoureusement : utiliser le changement d'indéterminée $Y=\frac{1}{X}$, puis remplacer Y par 0) après avoir éventuellement multiplié les deux membres de l'égalité par une puissance de X.

EXEMPLE :

Former la DES de $F=\dfrac{X}{(X-1)^2(X-2)}$ dans $\mathbb{R}(X)$.

La forme de la DES est : $F=\dfrac{a}{(X-1)^2}+\dfrac{b}{X-1}+\dfrac{\lambda}{X-2}$, où $a,b,\lambda\in\mathbb{R}$.

Par multiplication par $X-2$ puis remplacement de X par 2, on obtient : $\lambda=2$.

Par multiplication par $(X-1)^2$ puis remplacement de X par 1, on obtient : $a=-1$.

Par multiplication par X puis en faisant tendre X vers l'infini : $b+\lambda=0$, d'où $b=-2$.

Finalement : $\dfrac{X}{(X-1)^2(X-2)}=\dfrac{-1}{(X-1)^2}+\dfrac{-2}{X-1}+\dfrac{2}{X-2}$.

e) Cas de $\mathbb{C}(X)$

Soient $A\in\mathbb{C}[X]$, $S\in\mathbb{C}[X]$ unitaire tel que $\deg(S)\geqslant 1$, $F=\dfrac{A}{S}$. D'après le théorème de d'Alembert (5.3.4 Th. p. 177), S est scindé sur $\mathbb{C}$; il existe donc $n\in\mathbb{N}^*$, $z_1,\ldots,z_n\in\mathbb{C}$ deux à deux distincts, $\alpha_1,\ldots,\alpha_n\in\mathbb{N}^*$ tels que

$$F=\frac{A}{\prod_{i=1}^{n}(X-z_i)^{\alpha_i}}.$$

La DES de F est de la forme :

$$F=E+\sum_{i=1}^{n}\sum_{j=1}^{\alpha_i}\frac{\lambda_{\alpha_i,j}}{(X-z_i)^j},$$

où E est la partie entière de F et où les $\lambda_{\alpha_i,j}$ sont des complexes.

En pratique, pour calculer les $\lambda_{\alpha_i,j}$, on utilisera :

- la méthode de multiplication et remplacement, ou la formule utilisant une dérivée (5.4.2 *2) a)* p. 196-197) lorsque $\alpha_i = 1$.

- un changement d'indéterminée suivi d'une division suivant les puissances croissantes (cf. 5.4.2 *2) b)* p. 198) lorsque $\alpha_i > 1$.

f) Cas de $\mathbb{R}(X)$

Soient $A \in \mathbb{R}[X]$, $S \in \mathbb{R}[X]$ unitaire tel que $\deg(S) \geqslant 1$, $F = \dfrac{A}{S}$.

D'après 5.3.5 p. 183, la décomposition primaire de S est de la forme :

$$S = \prod_{i=1}^{N} (X - x_i)^{r_i} \prod_{k=1}^{N'} \left(X^2 + p_k X + q_k\right)^{s_k},$$

où :
$N, N' \in \mathbb{N}$
$x_1, \ldots, x_N \in \mathbb{R}$ deux à deux distincts
$(p_1, q_1), \ldots, (p_{N'}, q_{N'}) \in \mathbb{R}^2$ deux à deux distincts
$\forall k \in \{1, \ldots, N'\}, \quad p_k^2 - 4q_k < 0$
$r_1, \ldots, r_N, s_1, \ldots, s_{N'} \in \mathbb{N}^*$.

La DES de F est donc de la forme :

$$F = E + \sum_{i=1}^{N} \sum_{j=1}^{r_i} \frac{\lambda_{i,j}}{(X - x_i)^j} + \sum_{k=1}^{N'} \sum_{l=1}^{s_k} \frac{\mu_{k,l} X + \nu_{k,l}}{(X^2 + p_k X + q_k)^l},$$

où E est la partie entière de F, et les $\lambda_{i,j}$, $\mu_{k,l}$, $\nu_{k,l}$ des réels.

- Les éléments simples $\dfrac{\lambda_{i,j}}{(X - x_i)^j}$ sont dits **de 1ère espèce** (cf. 5.4.2 *1)* p. 195).

- Les éléments simples $\dfrac{\mu_{k,l} X + \nu_{k,l}}{(X^2 + p_k X + q_k)^l}$ sont dits **de 2nde espèce**.

Un cas particulier

Supposons que F soit de la forme $F = \dfrac{A}{T^s}$ où $A \in K[X]$, T est un trinôme irréductible, $s \in \mathbb{N}^*$. La DES de F est de la forme :

$$F = \frac{A}{T^s} = E + \frac{C_s}{T^s} + \frac{C_{s-1}}{T^{s-1}} + \ldots + \frac{C_1}{T}$$

où E est la partie entière de F, et $C_1, \ldots, C_s$ des polynômes de $\mathbb{R}[X]$ de degrés $\leqslant 1$.

On pourra calculer $C_s, C_{s-1}, \ldots, C_1$, E par des **divisions euclidiennes successives**. En effet, il existe des polynômes $Q_1, \ldots, Q_s, R_1, \ldots, R_s$ de $\mathbb{R}[X]$ tels que :

$$\begin{cases} A = Q_1 T + R_1, \quad Q_1 = Q_2 T + R_2, \ldots, Q_{s-1} = Q_s T + R_s \\ \forall j \in \{1, \ldots, s\}, \ \deg(R_j) < 2, \end{cases}$$

et on a alors :

$$\frac{A}{T^s} = \frac{R_1}{T^s} + \frac{Q_1}{T^{s-1}} = \ldots = \frac{R_1}{T^s} + \frac{R_2}{T^{s-1}} + \ldots + \frac{R_s}{T} + Q_s,$$

d'où, par unicité de la DES de F :

$$C_s = R_1,\ C_{s-1} = R_2, \ldots,\ C_1 = R_s,\ E = Q_s.$$

EXEMPLE :

Former la DES de $F = \dfrac{X^8 - X^4 + 2}{(X^2 + X + 1)^3}$ dans $\mathbb{R}(X)$.

$$\begin{array}{l|l}
X^8 - X^4 + 2 & X^2 + X + 1 \\
\hline
-X^7 - X^6 & X^6 - X^5 + X^3 - 2X^2 + X + 1 \\
X^5 & \\
-2X^4 - X^3 & \\
X^3 + 2X^2 & \\
X^2 - X + 2 & \\
-2X + 1 &
\end{array}$$

$$\begin{array}{l|l}
X^6 - X^5 + X^3 - 2X^2 + X + 1 & X^2 + X + 1 \\
\hline
-2X^5 - X^4 & X^4 - 2X^3 + X^2 + 2X - 5 \\
X^4 + 3X^3 & \\
2X^3 - 3X^2 & \\
-5X^2 - X & \\
4X + 6 &
\end{array}$$

$$\begin{array}{l|l}
X^4 - 2X^3 + X^2 + 2X - 5 & X^2 + X + 1 \\
\hline
-3X^3 & X^2 - 3X + 3 \\
3X^2 + 5X & \\
2X - 8 &
\end{array}$$

On conclut :

$$\frac{X^8 - X^4 + 2}{(X^2 + X + 1)^3} = X^2 - 3X + 3 + \frac{-2X + 1}{(X^2 + X + 1)^3} + \frac{4X + 6}{(X^2 + X + 1)^2} + \frac{2X - 8}{X^2 + X + 1}$$

■

Dans le cas général, on essaiera de combiner les méthodes précédemment évoquées. Cependant, le calcul d'une DES dans $\mathbb{R}(X)$ peut être long, lorsque le dénominateur contient plusieurs trinômes irréductibles, à des puissances élevées. Le passage par les complexes donne souvent des calculs compliqués.

À l'heure actuelle, on dispose de logiciels de calcul formel donnant les DES des fractions rationnelles de $\mathbb{C}(X)$ et $\mathbb{R}(X)$.

EXEMPLES :

1) Former la DES de $F = \dfrac{X}{(X-1)^2(X^2+1)^2}$ dans $\mathbb{R}(X)$.

La DES est de la forme :

$$F = \frac{\lambda}{(X-1)^2} + \frac{\mu}{X-1} + \frac{\alpha X+\beta}{(X^2+1)^2} + \frac{\gamma X+\delta}{X^2+1},$$

où $\lambda, \ldots, \delta$ sont des réels à calculer.

• *Calcul de* λ, μ

Changement d'indéterminée $Y = X - 1$ (donc $X = 1 + Y$) , $F = \dfrac{1+Y}{Y^2((1+Y)^2+1)^2}$, puis division suivant les puissances croissantes jusqu'à l'ordre 1 de $1 + Y$ par $((1 + Y)^2 + 1)^2$, ou encore par $4 + 8Y$:

$1+Y$	$4+8Y$
$-Y$	$\frac{1}{4} - \frac{1}{4}Y$
0	

D'où : $\lambda = \dfrac{1}{4}$, $\mu = -\dfrac{1}{4}$.

• *Calcul de* α, β

Multiplication par $(X^2 + 1)^2$ puis remplacement de X par i :

$$\alpha i + \beta = \frac{i}{(i-1)^2} = -\frac{1}{2}, \quad \text{d'où} \quad \alpha = 0, \ \beta = -\frac{1}{2}.$$

• *Calcul de* γ, δ

En remplaçant X par 0 : $0 = \lambda - \mu + \beta + \delta$, d'où $\delta = 0$.

En multipliant par X puis en faisant tendre X vers l'infini : $0 = \mu + \gamma$, d'où $\gamma = \dfrac{1}{4}$.

Finalement : $\dfrac{X}{(X-1)^2(X^2+1)^2} = \dfrac{\frac{1}{4}}{(X-1)^2} + \dfrac{-\frac{1}{4}}{X-1} + \dfrac{-\frac{1}{2}}{(X^2+1)^2} + \dfrac{\frac{1}{4}X}{X^2+1}$.

2) Former la DES de $F = \dfrac{X^2+2}{(X^2+1)^3(X^2+X+1)}$ dans $\mathbb{R}(X)$.

La DES de F est de la forme : $F = \dfrac{aX+b}{(X^2+1)^3} + \dfrac{cX+d}{(X^2+1)^2} + \dfrac{eX+f}{X^2+1} + \dfrac{\lambda X+\mu}{X^2+X+1}$,

où $a, \ldots, \mu$ sont des réels à calculer.

• *Calcul de* λ, μ

Multiplication par $X^2 + X + 1$ puis remplacement de X par j :

$$\lambda j + \mu = \frac{j^2+2}{(j^2+1)^3} = \frac{-j+1}{(-j)^3} = j - 1,$$

d'où $\lambda = 1$, $\mu = -1$, puisque $(1, j)$ est une base du $\mathbb{R}$-ev $\mathbb{C}$.

• *Calcul de* $a,\dots,f$

Considérons $G = F - \dfrac{X-1}{X^2+X+1} = \dfrac{X^2+2-(X-1)(X^2+1)^3}{(X^2+1)^3(X^2+X+1)}$.

On a : $(X^2+2)-(X-1)(X^2+1)^3 = -X^7+X^6-3X^5+3X^4-3X^3+4X^2-X+3$

$= (X^2+X+1)(-X^5+2X^4-4X^3+5X^2-4X+3)$.

D'où : $G = \dfrac{-X^5+2X^4-4X^3+5X^2-4X+3}{(X^2+1)^3}$.

Utilisons la méthode des divisions euclidiennes successives :

$$\begin{array}{l|l} -X^5+2X^4-4X^3+5X^2-4X+3 & X^2+1 \\ \hline 2X^4-3X^3 & -X^3+2X^2-3X+3 \quad \big| \quad X^2+1 \\ \hline -3X^3+3X^2 & 2X^2-2X \quad \big| \quad -X+2 \\ \hline 3X^2-X & -2X+1 \\ \hline -X & \end{array}$$

D'où : $G = \dfrac{-X}{(X^2+1)^3} + \dfrac{-2X+1}{(X^2+1)^2} + \dfrac{-X+2}{X^2+1}$, et finalement :

$$\frac{X^2+2}{(X^2+1)^3(X^2+X+1)} = \frac{-X}{(X^2+1)^3} + \frac{-2X+1}{(X^2+1)^2} + \frac{-X+2}{X^2+1} + \frac{X-1}{X^2+X+1}.$$

Exercices

◇ **5.4.4** *Exemples de décomposition en éléments simples de première espèce dans* $\mathbb{R}(X)$

a) $\dfrac{-X^3+5X^2-4X+1}{X^3(X-1)^4}$ *b)* $\dfrac{8X^4+8}{(X-1)^3(X+1)^3}$ *c)* $\dfrac{2X^4+5X^3+21X^2-X+5}{(X+1)^4(X-1)^3}$.

◇ **5.4.5** *Exemples de décomposition en éléments simples de première et de seconde espèces dans* $\mathbb{R}(X)$

a) $\dfrac{X^8-1}{(X^2+2X+2)^3}$ *b)* $\dfrac{X^2+1}{X^4+1}$ *c)* $\dfrac{X^3}{X^4+1}$

d) $\dfrac{1}{X^4+X^2+1}$ *e)* $\dfrac{X}{(X-1)(X^4-X^2+1)}$ *f)* $\dfrac{1}{(X^2+2X+3)(2X^2+3X+4)}$

g) $\dfrac{X^6-X^5+2X^4+X^2+1}{X^3(X^2+1)^2}$ *h)* $\dfrac{X^5+6X^4+17X^3+25X^2+19X+7}{(X+1)^2(X^2+X+1)}$

i) $\dfrac{3X^5+3X^4+5X^3+2X^2+X}{(X^2+1)^2(X^2+X+1)^2}$ *j)* $\dfrac{X^{2n}}{(X^2+1)^n}$, $n \in \mathbb{N}^*$.

◇ **5.4.6** Calculer, pour $N \in \mathbb{N}-\{0,1\}$, $\displaystyle\sum_{n=2}^{N} \frac{3n^2-1}{(n-1)^2n^2(n+1)^2}$.

◇ **5.4.7** Calculer $\displaystyle\sum_{k=1}^{4} \frac{z_k^3+2}{(z_k^2-1)^2}$, où $z_1,\dots,z_4$ sont les zéros de X^4-X^3+1 dans $\mathbb{C}$.

◇ **5.4.8** *a)* Décomposer $\dfrac{1}{(X-1)^3(X+1)^3}$ en éléments simples dans $\mathbb{R}(X)$.

b) En déduire un couple (U,V) de $(\mathbb{R}[X])^2$ tel que : $(X+1)^3U+(X-1)^3V=1$.

◇ **5.4.9** Soient $n\in\mathbb{N}^*$, $a\in\mathbb{C}-\{-1,0,1\}$. Simplifier

$$F_n=\sum_{k=0}^{n-1}\frac{a^k(X+a^{k+1})}{(X-a^k)(X-a^{k+1})(X-a^{k+2})}.$$

◇ **5.4.10** Soient $n\in\mathbb{N}-\{0,1\}$, $p\in\{0,\dots,n-1\}$, $\omega_k=\exp\left(\dfrac{2ik\pi}{n}\right)$ pour $k\in\{0,\dots,n-1\}$.

Mettre sous forme irréductible : $\displaystyle\sum_{k=0}^{n-1}\frac{\omega_k^p}{X-\omega_k}$.

◇ **5.4.11** Soient $a,b,c\in\mathbb{C}$, $d=\dfrac{a+b+c}{2}$; on suppose a,b,c,d deux à deux distincts.

a) Montrer que, pour tout polynôme P de $\mathbb{C}[X]$ de degré $\leqslant 2$, on a :

$$\frac{P}{(X-a)(X-b)(X-c)}=\sum\frac{P(a)}{(a-b)(a-c)}\cdot\frac{1}{X-a}$$

(où la somme comporte trois termes, par permutation circulaire).

b) En déduire la valeur de $\displaystyle\sum\frac{a^2}{(a-b)(a-c)(b+c-a)}$.

◇ **5.4.12*** Décomposer en éléments simples dans $\mathbb{R}(X)$ la fraction rationnelle associée à la fonction rationnelle définie par $x\mapsto\tan(n\operatorname{Arctan}x)$, $n\in\mathbb{N}-\{0,1\}$ fixé.

◇ **5.4.13** Soient $n\in\mathbb{N}^*$, $z_1,\dots,z_n\in\mathbb{C}$ deux à deux distincts, $Q=\displaystyle\prod_{k=1}^{n}(X-z_k)$.

a) Pour tout p de $\{0,\dots,n-1\}$ former la décomposition en éléments simples de $\dfrac{X^p}{Q}$.

b) En déduire, pour $p\in\{1,\dots,n-1\}$, la valeur de $\displaystyle\sum_{k=1}^{n}\frac{z_k^p}{Q'(z_k)}$.

◇ **5.4.14** Soient $P,Q\in\mathbb{C}[X]$, $n=\deg(Q)\geqslant 2$. On suppose :

$$\begin{cases}Q\text{ admet }n\text{ zéros simples }z_1,\dots,z_n\text{ dans }\mathbb{C}\\ \deg(P)\leqslant\deg(Q)-2.\end{cases}$$

Montrer : $\displaystyle\sum_{k=1}^{n}\frac{P(z_k)}{Q'(z_k)}=0$.

◇ **5.4.15*** Soient $n\in\mathbb{N}^*$, $a_0,\dots,a_{n-1}\in\mathbb{C}$, $P=X^n+a_{n-1}X^{n-1}+\dots+a_0$, $z_1,\dots z_n\in\mathbb{C}$ deux à deux distincts, $u_k=z_k-\dfrac{P(z_k)}{\displaystyle\prod_{\substack{1\leqslant i\leqslant n\\ i\neq k}}(z_k-z_i)}$ pour $k\in\{1,\dots,n\}$.

Démontrer : $\displaystyle\sum_{k=1}^{n}u_k=-a_{n-1}$.

Chapitre 6

Espaces vectoriels

Dans ce ch. 6, K désigne un corps commutatif. En pratique, $K = \mathbb{R}$ ou $\mathbb{C}$.

6.1 Structure d'espace vectoriel

♦ **Définition 1** On appelle K- **espace vectoriel** tout ensemble E muni d'une loi interne notée $+$, et d'une loi externe $\begin{array}{ccc} K \times E & \longrightarrow & E \\ (\lambda,x) & \longmapsto & \lambda x \end{array}$ telles que :

- $(E,+)$ est un groupe abélien
- *1)* $\forall(\lambda,\mu) \in K^2, \forall x \in E,\ (\lambda+\mu)x = \lambda x + \mu x$
  2) $\forall \lambda \in K, \forall (x,y) \in E^2,\ \lambda(x+y) = \lambda x + \lambda y$
  3) $\forall(\lambda,\mu) \in K^2, \forall x \in E,\ \lambda(\mu x) = (\lambda\mu)x$
  4) $\forall x \in E,\ 1x = x$.

Lorsqu'on ne change pas de corps K, on peut utiliser l'expression **espace vectoriel** au lieu de K-espace vectoriel.

Nous abrègerons K-espace vectoriel en K-ev, espace vectoriel en ev.

Les éléments d'un K-ev sont appelés **vecteurs**; les éléments de K sont appelés **scalaires**.

EXEMPLES :

1) Le corps K est un K-ev, en prenant pour loi interne $\begin{array}{ccc} K \times K & \longrightarrow & K \\ (x,y) & \longmapsto & x+y \end{array}$ et pour loi externe la multiplication dans K : $\begin{array}{ccc} K \times K & \longrightarrow & K \\ (\lambda,x) & \longmapsto & \lambda x \end{array}$. Ici, les éléments de K sont simultanément considérés comme des vecteurs et des scalaires.

2) Plus généralement, soit L un corps tel que K soit un sous-corps de L (on dit aussi que L est un **surcorps** de K). Alors L est un K-ev, pour les lois interne $\begin{array}{ccc} L \times L & \longrightarrow & L \\ (x,y) & \longmapsto & x+y \end{array}$ et externe $\begin{array}{ccc} K \times L & \longrightarrow & L \\ (\lambda,x) & \longmapsto & \lambda x \end{array}$ (multiplication dans L).

En particulier, $\mathbb{C}$ est un $\mathbb{R}$-ev pour les lois usuelles.

3) Soient $n \in \mathbb{N}^*$, $E_1,\dots,E_n$ des K-ev . Le produit $E = \prod_{i=1}^{n} E_i$ est alors un K-ev pour les lois interne et externe définies par :

- $\forall \big((x_1,\dots,x_n),(y_1,\dots,y_n)\big) \in E^2$, $(x_1,\dots,x_n)+(y_1,\dots,y_n) = (x_1+y_1,\dots,x_n+y_n)$
- $\forall \lambda \in K$, $\forall (x_1,\dots,x_n) \in E$, $\lambda(x_1,\dots,x_n) = (\lambda x_1,\dots,\lambda x_n)$.

En particulier, pour tout $n \in \mathbb{N}^*$, K^n est un K-ev pour les lois usuelles.

4) Soient X un ensemble non vide, E un K-ev. L'ensemble E^X des applications de X dans E est un K-ev pour les lois interne et externe définies par :

- $\forall (f,g) \in (E^X)^2$, $\forall x \in X$, $(f+g)(x) = f(x) + g(x)$
- $\forall \lambda \in K$, $\forall f \in E^X$, $\forall x \in X$, $(\lambda f)(x) = \lambda f(x)$.

Par exemple, l'ensemble $\mathbb{R}^{\mathbb{N}}$ des suites réelles est un $\mathbb{R}$-ev pour les lois usuelles.

5) Nous avons vu (5.1.4 Prop. 3 p. 144) que l'ensemble $K[X]$ des polynômes à une indéterminée et à coefficients dans K est un K-ev pour l'addition et la multiplication externe.

Souvent on montrera que E est un ev en montrant que E est un sev d'un ev connu (cf. 6.2 Prop.1 p. 211 et exercice 6.2.5 p. 215).

Remarque :

Changement de corps

Soit L un surcorps de K. Tout L-ev E peut être considéré comme un K-ev en le munissant de la loi $+$ déjà définie dans E et de la loi externe $\begin{array}{ccc} K \times E & \longrightarrow & E \\ (\lambda,x) & \longmapsto & \lambda x \end{array}$ restriction de la loi externe du L-ev E.

Par exemple, tout $\mathbb{C}$-ev peut être considéré comme un $\mathbb{R}$-ev.

◆ **Proposition 1** Soit E un K-ev. On a, pour tous λ,μ de K et tous x,y de E :

1) $\lambda x = 0 \iff (\lambda = 0 \text{ ou } x = 0)$

2) $(\lambda - \mu)x = \lambda x - \mu x$

3) $\lambda(x-y) = \lambda x - \lambda y$.

Nous notons ici 0 le neutre de l'addition dans K ainsi que le neutre de l'addition dans E; on peut noter 0_K et 0_E pour distinguer éventuellement ces deux objets.

Preuve :

1) • $0x = (0+0)x = 0x + 0x$, d'où $0x = 0$.

• $\lambda 0 = \lambda(0+0) = \lambda 0 + \lambda 0$, d'où $\lambda 0 = 0$.

• Si $\lambda x = 0$ et si $\lambda \neq 0$, alors, en notant λ^{-1} l'inverse de λ dans le corps K :

$$x = 1x = (\lambda^{-1}\lambda)x = \lambda^{-1}(\lambda x) = \lambda^{-1}0 = 0.$$

2) $\lambda x = \big((\lambda-\mu)+\mu\big)x = (\lambda-\mu)x + \mu x$, d'où $(\lambda-\mu)x = (\lambda x) - (\mu x)$, qui est noté $\lambda x - \mu x$.

3) $\lambda x = \lambda\big((x-y)+y\big) = \lambda(x-y) + \lambda y$, d'où $\lambda(x-y) = \lambda x - \lambda y$. ∎

La Proposition suivante est immédiate (par récurrence).

♦ **Proposition 2** **(Utilisation du symbole $\sum$ dans les ev)**

Soient E un K-ev, $n,p \in \mathbb{N}^*$, x,x_i,y_i,x_{ij} des éléments de E, $\lambda,\lambda_i,\ldots$ des éléments de K. On a :

1) $\left(\sum_{i=1}^{n} x_i\right) + \left(\sum_{i=n+1}^{p} x_i\right) = \sum_{i=1}^{p} x_i \qquad (\text{si } p \geqslant n+1)$

2) $\sum_{i=1}^{n}(x_i + y_i) = \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i$

3) $\sum_{i=1}^{n}\left(\sum_{j=1}^{p} x_{ij}\right) = \sum_{j=1}^{p}\left(\sum_{i=1}^{n} x_{ij}\right)$

4) $\forall \sigma \in \mathfrak{S}_n, \quad \sum_{i=1}^{n} x_{\sigma(i)} = \sum_{i=1}^{n} x_i$

5) $\sum_{i=1}^{n}(\lambda x_i) = \lambda \sum_{i=1}^{n} x_i$

6) $\sum_{i=1}^{n}(\lambda_i x) = \left(\sum_{i=1}^{n} \lambda_i\right) x.$

- Par convention, la somme d'une famille vide d'éléments de K (resp. E) vaut 0.
- D'après *5)* et *6)*, on peut noter $\sum_{i=1}^{n} \lambda x_i$ et $\sum_{i=1}^{n} \lambda_i x$ au lieu de $\sum_{i=1}^{n}(\lambda x_i)$ et $\sum_{i=1}^{n}(\lambda_i x)$ respectivement.

♦ **Définition 2** On appelle **K-algèbre** tout ensemble A muni d'une loi interne notée $+$, d'une loi externe $\begin{array}{ccc} K \times A & \longrightarrow & A \\ (\lambda,x) & \longmapsto & \lambda x \end{array}$, et d'une loi interne (appelée $3^{\text{ème}}$ loi) notée ici $*$, telles que :

1) $(A,+,\cdot)$ est un K-ev

2) $*$ est distributive sur $+$

3) $\forall \lambda \in K, \ \forall (x,y) \in A^2, \ \lambda(x * y) = (\lambda x) * y = x * (\lambda y).$

Une K-algèbre A est dite :

- **associative** si et ssi $*$ est associative
- **commutative** si et ssi $*$ est commutative
- **unitaire** (ou : **unifère**) si et ssi A admet un neutre pour $*$.

EXEMPLES :

1) Tout corps commutatif K est une K-algèbre associative, commutative, unitaire, en prenant pour $3^{\text{ème}}$ loi la multiplication.

2) Plus généralement, si L est un surcorps de K, L est une K-algèbre associative et unitaire, en prenant pour $3^{\text{ème}}$ loi la multiplication dans L.

Par exemple, $\mathbb{C}$ est une $\mathbb{R}$-algèbre associative, commutative, unitaire, pour les lois usuelles.

3) Soit X un ensemble non vide. Nous avons vu (Exemple 4 p. 208) que K^X est un K-ev pour les lois usuelles. En munissant K^X d'une 3ème loi, notée par l'absence de symbole, définie par :

$$\forall x \in X, \quad (fg)(x) = f(x)g(x),$$

K^X est une K-algèbre associative, commutative, unitaire, le neutre pour la 3ème loi étant l'application constante égale à 1.

4) Nous avons vu (5.1.4 Prop. 3 p. 144) que $K[X]$ est une K-algèbre associative, commutative, unitaire.

5) Nous verrons plus loin (7.2.2 Prop. 5 p. 247) l'algèbre $\mathcal{L}(E)$ des endomorphismes d'un K-ev E, dont la 3ème loi est la loi $\circ$ de composition, et (8.1.4 Prop.4 p. 269) l'algèbre $\mathbf{M}_n(K)$ des matrices carrées d'ordre n à coefficients dans K, dont la 3ème loi est la multiplication des matrices.

Souvent, on montrera que A est une algèbre en montrant que A est une sous-algèbre d'une algèbre connue (cf. 6.2 Prop. 6 p. 214 et exercice 6.4.10 p. 236).

6.2 Sous-espaces vectoriels

♦ **Définition 1** Soient E un K-ev, $F \in \mathfrak{P}(E)$. On dit que F est un **sous-espace vectoriel** de E si et seulement si :

$$\begin{cases} 1)\ F \neq \varnothing \\ 2)\ \forall (x,y) \in F^2,\ x+y \in F \\ 3)\ \forall \lambda \in K, \forall x \in F,\ \lambda x \in F. \end{cases}$$

Nous abrègerons sous-espace vectoriel en sev. Pour rappeler le corps K utilisé, on dit quelquefois sous-K-ev au lieu de sev.

La Proposition suivante est immédiate.

♦ **Proposition 1** Soient E un K-ev, $F \in \mathfrak{P}(E)$. Si F est un sev de E, alors F est un K-ev pour les lois $+ : F \times F \longrightarrow F$ et externe $K \times F \longrightarrow F$ induites par celles de E.
$\quad (x,y) \longmapsto x+y \qquad\qquad (\lambda,x) \longmapsto \lambda x$

EXEMPLES :

1) $\mathbb{R} \times \{0\}$ est un sev du $\mathbb{R}$-ev $\mathbb{R}^2$.

2) Pour tout n de $\mathbb{N}$, $K_n[X]$ est un sev du K-ev $K[X]$ (cf. 5.1.4 p. 146).

Remarques :

1) $\{0\}$ et E sont des sev du K-ev E.

2) Si F est un sev de l'ev E et si G est un sev de F, alors G est un sev de E ; on dit qu'il y a transitivité de la notion de sev.

♦ **Proposition 2** Soient E un K-ev , $(F_i)_{i \in I}$ une famille de sev de E ; alors $\bigcap_{i \in I} F_i$ est un sev de E.

Preuve :

Notons $F = \bigcap_{i \in I} F_i$.

1) $F \neq \varnothing$; en effet, $0 \in F$ puisque $(\forall i \in I, 0 \in F_i)$.

2) Soit $(x,y) \in F^2$. On a : $\big(\forall i \in I,\ (x \in F_i \text{ et } y \in F_i)\big)$, donc $(\forall i \in I,\ x+y \in F_i)$, d'où $x+y \in F$.

3) Soit $(\lambda,x) \in K \times F$.

On a : $(\forall i \in I, x \in F_i)$, donc $(\forall i \in I, \lambda x \in F_i)$, d'où $\lambda x \in F$. ■

En particulier, si F_1, F_2 sont deux sev de E, alors $F_1 \cap F_2$ est un sev de E.

◆ **Proposition - Définition 3**

Soient E un K-ev, F_1, F_2 deux sev de E.

On note $F_1 + F_2 = \{x \in E;\ \exists (x_1,x_2) \in F_1 \times F_2,\quad x = x_1 + x_2\}$

$= \{x_1 + x_2;\ \ (x_1,x_2) \in F_1 \times F_2\}$,

appelé **somme de F_1 et F_2** (cf. 2.1 Déf. 12, p. 43), et $F_1 + F_2$ est un sev de E.

Preuve :

1) $F_1 + F_2 \neq \varnothing$ car $0 = 0 + 0 \in F_1 + F_2$.

2) Soit $(x,y) \in (F_1 + F_2)^2$. Il existe $(x_1,x_2) \in F_1 \times F_2$, $(y_1,y_2) \in F_1 \times F_2$ tels que : $x = x_1 + x_2$ et $y = y_1 + y_2$.

On a alors : $x + y = (x_1 + x_2) + (y_1 + y_2) = (x_1 + y_1) + (x_2 + y_2) \in F_1 + F_2$.

3) Soit $(\lambda,x) \in K \times (F_1 + F_2)$. Il existe $(x_1,x_2) \in F_1 \times F_2$ tel que $x = x_1 + x_2$. On a :

$$\lambda x = \lambda(x_1 + x_2) = \lambda x_1 + \lambda x_2 \in F_1 + F_2.$$

◆ **Proposition 4** Soit E un K-ev; on a, pour tous sev F_1, F_2, F_3 de E :

1) $F_1 + F_2 = F_2 + F_1$	*1′)* $F_1 \cap F_2 = F_2 \cap F_1$
2) $F_1 \subset F_1 + F_2$	*2′)* $F_1 \cap F_2 \subset F_1$
3) $\begin{cases} F_1 \subset F_3 \\ F_2 \subset F_3 \end{cases} \iff F_1 + F_2 \subset F_3$	*3′)* $\begin{cases} F_3 \subset F_1 \\ F_3 \subset F_2 \end{cases} \iff F_3 \subset F_1 \cap F_2$
4) $F_1 \subset F_2 \Longrightarrow F_1 + F_3 \subset F_2 + F_3$	*4′)* $F_1 \subset F_2 \Longrightarrow F_1 \cap F_3 \subset F_2 \cap F_3$
5) $F_1 + F_1 = F_1$	*5′)* $F_1 \cap F_1 = F_1$
6) $F_1 + \{0\} = F_1$	*6′)* $F_1 \cap \{0\} = \{0\}$
7) $F_1 + E = E$	*7′)* $F_1 \cap E = F_1$
8) $(F_1 + F_2) + F_3 = F_1 + (F_2 + F_3)$	*8′)* $(F_1 \cap F_2) \cap F_3 = F_1 \cap (F_2 \cap F_3)$.

Preuve :

Les démonstrations sont (presque) immédiates. Par exemple, pour *2)* : pour tout x de F_1, on peut écrire $x = x + 0$, où $x \in F_1$ et $0 \in F_2$, donc $x \in F_1 + F_2$.

Remarque :

On note $\mathbf{V}(E)$ l'ensemble des sev de E.

Les lois internes $+$ et $\cap$ dans $\mathbf{V}(E)$ ne sont pas distributives l'une sur l'autre (sauf cas particulier de E), cf. exercice 6.2.1 p. 215.

◆ **Définition 2** Soient E un K-ev, F_1, F_2 deux sev de E. On dit que F_1 et F_2 **sont en somme directe** si et seulement si $F_1 \cap F_2 = \{0\}$.

Lorsque F_1 et F_2 sont deux sev en somme directe, on note $F_1 \oplus F_2$ au lieu de $F_1 + F_2$.

EXEMPLE :

Pour $K = \mathbb{R}$, $E = \mathbb{R}^3$, les sev $F_1 = \mathbb{R} \times \{0\} \times \{0\}$ et $F_2 = \{0\} \times \mathbb{R} \times \{0\}$ sont en somme directe.

Remarque :

La notation $F_1 \oplus F_2$ n'est définie que si F_1 et F_2 sont en somme directe; $\oplus$ n'est pas une nouvelle opération.

◆ **Proposition 5** Pour que deux sev F_1, F_2 d'un K-ev E soient en somme directe, il faut et il suffit que tout élément de $F_1 + F_2$ se décompose d'une façon unique en somme d'un élément de F_1 et d'un élément de F_2.

Preuve :

1) Supposons que F_1 et F_2 soient en somme directe, et soit $x \in F_1 + F_2$.

- Par définition de $F_1 + F_2$, il existe $(x_1, x_2) \in F_1 \times F_2$ tel que $x = x_1 + x_2$.
- Soient $(x_1, x_2) \in F_1 \times F_2$, $(y_1, y_2) \in F_1 \times F_2$ tels que $x = x_1 + x_2 = y_1 + y_2$.

Alors : $x_1 - y_1 = y_2 - x_2$.

Comme $(x_1 - y_1 \in F_1,\ y_2 - x_2 \in F_2, \quad F_1 \cap F_2 = \{0\})$, on déduit $x_1 - y_1 = y_2 - x_2 = 0$, donc $x_1 = y_1, x_2 = y_2$.

Ainsi, x se décompose d'une façon unique sur F_1 et F_2.

2) Réciproquement, supposons que tout élément de $F_1 + F_2$ se décompose d'une façon unique sur F_1 et F_2.

Soit $x \in F_1 \cap F_2$. On dispose de deux décompositions de 0 sur F_1 et F_2 : $0 = 0 + 0$ et $0 = x + (-x)$, d'où $x = 0$. Ainsi $F_1 \cap F_2 = \{0\}$, F_1 et F_2 sont en somme directe.

◆ **Définition 3** Deux sev F_1, F_2 d'un K-ev E sont dits **supplémentaires dans** E si et seulement si : $F_1 \cap F_2 = \{0\}$ et $F_1 + F_2 = E$.

Ceci revient à : F_1 et F_2 sont en somme directe et $F_1 \oplus F_2 = E$.

EXEMPLES :

1) $K = \mathbb{R}$, $E = \mathbb{R}^2$, $F_1 = \mathbb{R} \times \{0\}$, $F_2 = \{0\} \times \mathbb{R}$; F_1 et F_2 sont deux sev de E supplémentaires dans E.

2) $K = \mathbb{R}$, $E = \mathbb{R}^{\mathbb{R}}$, F_1 (resp. F_2) est l'ensemble des applications paires (resp. impaires) de $\mathbb{R}$ dans $\mathbb{R}$; F_1 et F_2 sont deux sev de E supplémentaires dans E. En effet :

- Si $f \in F_1 \cap F_2$, alors f est paire et impaire, donc $(\forall x \in \mathbb{R},\ f(x) = -f(x))$, d'où $f = 0$
- Tout f de E se décompose en $f = g + h$ où $g \in F_1, h \in F_2$ sont définies par :

$$\forall x \in \mathbb{R}, \quad g(x) = \frac{1}{2}\big(f(x) + f(-x)\big),\ h(x) = \frac{1}{2}\big(f(x) - f(-x)\big).$$

(cf. Tome 1, 4.1.3 Prop.).

Remarques :

1) Un sev F de E peut admettre plusieurs supplémentaires dans E. Par exemple, si $K = \mathbb{R}$ et $E = \mathbb{R}^2$, le sev $F = \mathbb{R} \times \{0\}$ de E admet une infinité de supplémentaires dans E, qui sont tous les $\mathbb{R}x$, $x \in E - F$.

2) Nous montrerons plus loin (6.4 Prop. 6 p. 231) que, si E est de dimension finie, alors tout sev de E admet au moins un supplémentaire dans E.

3) L'existence d'un moins un supplémentaire pour tout sev d'un ev quelconque est logiquement équivalente à l'*axiome du choix*, dont l'étude dépasse le cadre de cet ouvrage.

◆ **Définition 4** Soit A une K-algèbre, de $3^{\text{ème}}$ loi notée $*$, $B \in \mathfrak{P}(A)$. On dit que B est une **sous-algèbre** de A si et seulement si :

$$\begin{cases} B \text{ est un sev du } K\text{-ev } A \\ \forall (x,y) \in B^2,\ x * y \in B. \end{cases}$$

Autrement dit, une partie B d'une algèbre A est une sous-algèbre de A si et seulement si :

$$\begin{cases} B \neq \varnothing \\ \forall (x,y) \in B^2,\ x + y \in B \\ \forall (\lambda,x) \in K \times B,\ \lambda x \in B \\ \forall (x,y) \in B^2,\ x * y \in B. \end{cases}$$

■

La Proposition suivante est immédiate.

◆ **Proposition 6** Soient A une K-algèbre, $B \in \mathfrak{P}(A)$. Si B est une sous-algèbre de A, alors B est une K-algèbre pour les lois $+ : B \times B \longrightarrow B$, $(x,y) \longmapsto x+y$ externe $K \times B \longrightarrow B$, $(\lambda,x) \longmapsto \lambda x$ $\quad * : B \times B \longrightarrow B$ induites par celles de A. $(x,y) \longmapsto x*y$

EXEMPLE :

$\mathbb{R}^{\mathbb{R}}$ est une $\mathbb{R}$-algèbre pour les lois usuelles (la $3^{\text{ème}}$ loi étant la multiplication) et l'ensemble B des applications bornées de $\mathbb{R}$ dans $\mathbb{R}$ est une sous-algèbre de A (cf. Tome 1, 4.1.8 Prop. 3).

Exercices

◊ **6.2.1** Soient E un K-ev, F,G,H des sev de E.

a) 1) Montrer : $(F \cap G) + (F \cap H) \subset F \cap (G + H)$.

2) Montrer : $(G \subset F \text{ ou } H \subset F) \Longrightarrow (F \cap G) + (F \cap H) = F \cap (G + H)$.

3) Donner un exemple de K,E,F,G,H pour lequel il n'y a pas égalité dans le résultat de *a) 1)*.

b) 1) Montrer : $F + (G \cap H) \subset (F + G) \cap (F + H)$.

2) Montrer : $(F \subset G \text{ ou } F \subset H) \Longrightarrow F + (G \cap H) = (F + G) \cap (F + H)$.

3) Donner un exemple de K,E,F,G,H pour lequel il n'y a pas égalité dans le résultat de *b) 1)*.

◊ **6.2.2** Soient E un K-ev, F,G deux sev de E tels que $F \cup G = E$. Montrer : $F = E$ ou $G = E$.

◊ **6.2.3** Soient E un K-ev, I un ensemble non vide , $(F_i)_{i\in I}$ une famille de sev de E.
On suppose : $\forall (i,j) \in I^2, \exists k \in I,\ F_i \cup F_j \subset F_k$. Montrer que $\bigcup_{i\in I} F_i$ est un sev de E.

◊ **6.2.4** Donner un exemple de corps fini K, de K-ev E, du sev F_1,F_2,F_3 de E tels que :
$$F_1 \cup F_2 \cup F_3 = E \quad \text{et} \quad (\forall i \in \{1,2,3\},\ F_i \neq E).$$

◊ **6.2.5** Soit E l'ensemble des applications $f : \mathbb{R} \longrightarrow \mathbb{R}$ telles qu'il existe $A \in \mathbb{R}_+^*$ et $g,h : \mathbb{R} \longrightarrow \mathbb{R}$ croissantes tels que : $\forall x \in \mathbb{R},\ (|x| \geqslant A \Longrightarrow f(x) = g(x) - h(x))$.
Montrer que E est un $\mathbb{R}$-ev pour les lois usuelles.

◊ **6.2.6** Soient $N \in \mathbb{N}^*$, $a_0,\ldots,a_N \in \mathbb{R}$ deux à deux distincts, $E = \mathbb{R}^{\mathbb{R}}$, $F = \{f \in \mathbb{R}^{\mathbb{R}};\ \forall i \in \{0,\ldots,N\},\ f(a_i) = 0\}$, G l'ensemble des applications polynomiales de $\mathbb{R}$ dans $\mathbb{R}$ de degré $\leqslant N$. Etablir que F et G sont deux sev de E, supplémentaires dans E (E étant muni des lois usuelles).

◊ **6.2.7** Soit A une K-algèbre. Pour toute partie X de A, on appelle **commutant** de X la partie de A, noté X', définie par : $X' = \{y \in A;\ \forall x \in X,\ xy = yx\}$.

a) Montrer que, si A est associative, alors X' est une sous-algèbre de A. En particulier, le **centre** de A, qui est par définition A', est une sous-algèbre de A (si A est associative).

b) Montrer : *1)* $\forall (X,Y) \in (\mathfrak{P}(A))^2,\ (X \subset Y \Longrightarrow X' \supset Y')$

2) $\forall X \in \mathfrak{P}(A),\ X \subset X''$.

6.3 Dépendance et indépendance linéaires

6.3.1 Familles liées, familles libres

◆ **Définition 1** Soient E un K-ev, $n \in \mathbb{N}^*$, $(x_1,\ldots,x_n) \in E^n$. On appelle **combinaison linéaire** de $x_1,\ldots,x_n$ tout élément de E tel qu'il existe $(\lambda_1,\ldots,\lambda_n) \in K^n$ tel que $x = \lambda_1 x_1 + \ldots + \lambda_n x_n = \sum_{i=1}^{n} \lambda_i x_i$.

Plus généralement, si $(x_i)_{i\in I}$ est une famille (éventuellement infinie) d'éléments d'un K-ev E, on appelle **combinaison linéaire** de la famille $(x_i)_{i\in I}$ tout élément x de E tel qu'il existe une partie finie J de I et une famille $(\lambda_i)_{i\in J}$ d'éléments de K telles que $x = \sum_{i\in J} \lambda_i x_i$.

Par convention : $\sum_{i\in\varnothing} x_i = 0$ (cf. 6.1 p. 209).

◆ **Proposition** Soient E un K-ev, $F \in \mathfrak{P}(E)$.
Pour que F soit un sev de E, il faut et il suffit que F soit non vide et que F soit stable par combinaison linéaire
(c'est-à-dire : $\forall(\lambda,\mu) \in K^2,\quad \forall(x,y) \in F^2,\quad \lambda x + \mu y \in F$).

Preuve :

1) Si F est un sev de E, alors $F \neq \varnothing$ et, pour tous (λ,μ) de K^2 et (x,y) de F^2, λx et μy sont dans F, puis $\lambda x + \mu y \in F$.

2) Réciproquement supposons $F \neq \varnothing$ et : $\forall(\lambda,\mu) \in K^2, \forall(x,y) \in F^2, \lambda x + \mu y \in F$. En choisissant $\mu = 0$, puis $\lambda = \mu = 1$, on conclut que F est un sev de E.

Remarque : Pour qu'une partie F d'un ev E soit un sev de E, il faut et il suffit que :

$$\begin{cases} F \neq \varnothing \\ \forall \lambda \in K, \forall (x,y) \in F^2,\ \lambda x + y \in F. \end{cases}$$

◆ **Définition 2** Soient E un K-ev, $n \in \mathbb{N}^*$, $(x_1,\ldots,x_n) \in E^n$.

1) On dit que la famille finie $(x_1,\ldots,x_n)$ est **liée** si et seulement si :

$$\exists(\lambda_1,\ldots,\lambda_n) \in K^n - \{(0,\ldots,0)\},\quad \sum_{i=1}^{n} \lambda_i x_i = 0.$$

2) On dit que la famille finie $(x_1,\ldots,x_n)$ est **libre** si et seulement si elle n'est pas liée, c'est-à-dire :

$$\forall(\lambda_1,\ldots,\lambda_n) \in K^n,\ \left(\sum_{i=1}^{n} \lambda_i x_i = 0 \Longrightarrow (\forall i \in \{1,\ldots,n\},\ \lambda_i = 0)\right).$$

Une famille finie d'éléments de E est aussi appellée **système** d'éléments de E.

Plus généralement, soit $(x_i)_{i\in I}$ une famille (éventuellement infinie) d'éléments de E.

1) On dit que $(x_i)_{i\in I}$ est **liée** si et seulement s'il existe une sous-famille finie de $(x_i)_{i\in I}$ qui soit liée, c'est-à-dire si et seulement s'il existe une partie finie J de I telle que $(x_i)_{i\in J}$ soit liée.

2) On dit que $(x_i)_{i\in I}$ est **libre** si et seulement si elle n'est pas liée, c'est-à-dire si et seulement si toute sous-famille finie de $(x_i)_{i\in I}$ est libre. ■

Pour rappeler le corps K utilisé, on dit quelquefois K- **libre** (resp. K-**lié**) au lieu de libre (resp. lié).

On dit que deux vecteurs x, y de $E - \{0\}$ sont **colinéaires** si et seulement si (x,y) est lié, c'est-à-dire si et seulement s'il existe $\lambda \in K$ tel que $y = \lambda x$.

Remarques :

1) Pour qu'une famille (x) à un seul élément soit liée, il faut et il suffit que : $x = 0$.

2) Pour tout x de E, la famille (x,x) est liée, puisque : $1x + (-1)x = 0$ et $(1,-1) \neq (0,0)$.

3) Si une famille $(x_i)_{i\in I}$ d'éléments de E est liée, alors toute **surfamille** de $(x_i)_{i\in I}$ (c'est-à-dire : toute famille d'éléments de E dont $(x_i)_{i\in I}$ est une sous-famille) est liée. Par exemple, toute famille contenant 0 est liée.

4) Si une famille $(x_i)_{i\in I}$ d'éléments de E est libre, alors toute sous-famille de $(x_i)_{i\in I}$ est libre.

5) Si une famille $(x_i)_{i\in I}$ d'éléments de E est libre, alors les $x_i (i \in I)$ sont deux à deux distincts. En effet, soit $(i,j) \in I^2$ tel que $i \neq j$; d'après *3)*, la famille (x_i, x_j) à deux éléments est libre, donc (cf. *2)*) : $x_i \neq x_j$.

6) La liaison ou la liberté d'une famille $(x_i)_{i\in I}$ ne dépend pas de l'« ordre » des éléments x_i. Autrement dit, si $\sigma : I \longrightarrow I$ est une permutation de I, la famille $(x_{\sigma(i)})_{i\in I}$ est liée (resp. libre) si et seulement si la famille $(x_i)_{i\in I}$ est liée (resp. libre).

La remarque *6)* précédente permet la Définition suivante.

◆ Définition 3

Une partie A de E est dite **libre** si et seulement si la famille $(x)_{x\in A}$ est libre.

En particulier, une partie finie $\{x_1,\ldots,x_n\}$ de E (où, $n \in \mathbb{N}^*$ et $x_1,\ldots,x_n$ sont deux à deux distincts) est libre si et seulement si la famille $(x_1,\ldots,x_n)$ est libre.

EXEMPLE :

1) $E = \mathbb{R}^3$, $n = 2$, $x_1 = (1,0,1)$, $x_2 = (2,1,-1)$; la famille (x_1,x_2) est libre.

2) $E = \mathbb{R}^2$, $n = 3$, $x_1 = (1,1)$, $x_2 = (2,1)$, $x_3 = (-1,0)$; la famille (x_1,x_2,x_3) est liée, puisque $x_1 - x_2 - x_3 = 0$.

3) $E = \mathbb{R}^{\mathbb{R}}$ et, pour $\alpha \in \mathbb{R}$, $f_\alpha : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & e^{\alpha x} \end{array}$, la famille $(f_\alpha)_{\alpha\in\mathbb{R}}$ est libre (cf. exercice 6.3.4 *d)* p. 218).

Exercices

◇ **6.3.1** Soient E un $\mathbb{R}$-ev, $x,y,z \in E$ tels que (x,y,z) soit libre, $u = x+y$, $v = y+z$, $w = z+x$. Montrer que (u,v,w) est libre.

◇ **6.3.2** Soit $(N,n) \in (\mathbb{N} - \{0,1\})^2$ tel que : $\forall k \in \mathbb{N}$, $N \neq k^n$.

a) Démontrer : $\sqrt[n]{N} \notin \mathbb{Q}$.

b) Etablir que $\left(1, \sqrt[n]{N}\right)$ est $\mathbb{Q}$- libre.

◇ **6.3.3** Soient $n \in \mathbb{N}$, $z_0,\ldots,z_n \in \mathbb{C}$ deux à deux distincts. Montrer que $\left((X - z_k)^n\right)_{0\leqslant k\leqslant n}$ est libre dans $\mathbb{C}[X]$.

◇ **6.3.4** Montrer que les familles de fonctions suivantes sont libres (pour les lois usuelles) :

a) $\left(\begin{array}{l} f_a :]0,1[\longrightarrow \mathbb{R} \\ \quad x \longmapsto \dfrac{1}{1-ax} \end{array}\right)_{a \in]0;\,1[}$

b) $\left(\begin{array}{l} f_a : \mathbb{R} \longrightarrow \mathbb{R} \\ \quad x \longmapsto \dfrac{1}{x^2+a^2+1} \end{array}\right)_{a \in [0;\,+\infty[}$

c) $\left(\begin{array}{l} f_a :]0,1[\longrightarrow \mathbb{R} \\ \quad x \longmapsto \begin{cases} 1 & \text{si } x \geqslant a \\ 0 & \text{si } x < a \end{cases} \end{array}\right)_{a \in \mathbb{R}}$

d) $\left(\begin{array}{l} f_a : \mathbb{R} \longrightarrow \mathbb{R} \\ \quad x \longmapsto \mathrm{e}^{ax} \end{array}\right)_{a \in \mathbb{R}}$

e) $\left(\begin{array}{l} f_{a,b} : \mathbb{R}^2 \longrightarrow \mathbb{R} \\ \quad (x,y) \longmapsto \mathrm{e}^{ax+by} \end{array}\right)_{(a,b) \in \mathbb{R}^2}$

f) $\left(\begin{array}{l} f_a :]0;\,+\infty[\longrightarrow \mathbb{R} \\ \quad x \longmapsto x^a \end{array}\right)_{a \in \mathbb{R}}$

g) $\left(\begin{array}{l} f_{a,b} :]0;\,+\infty[^2 \longrightarrow \mathbb{R} \\ \quad (x,y) \longmapsto x^a y^b \end{array}\right)_{(a,b) \in \mathbb{R}^2}$

h) $\left(\begin{array}{l} f_n : \mathbb{R} \longrightarrow \mathbb{R} \\ \quad x \longmapsto \sin(x^n) \end{array}\right)_{n \in \mathbb{N}^*}$

i) $(f, f\circ f, f\circ f\circ f)$, où $\begin{array}{l} f : \mathbb{R} \longrightarrow \mathbb{R} \\ \quad x \longmapsto \sin x \end{array}$.

◇ **6.3.5** Pour tout (a,h) de $\mathbb{R} \times \mathbb{R}_+^*$, on note $f_{a,h} : \mathbb{R} \longrightarrow \mathbb{R}$ l'application définie par :

$$f_{a,h}(x) = \begin{cases} 0 & \text{si } x \leqslant a \\ \dfrac{1}{h}(x-a) & \text{si } a \leqslant x \leqslant a+h \\ 1 & \text{si } a+h \leqslant x. \end{cases}$$

La famille $(f_{a,h})_{(a,h)\in\mathbb{R}\times\mathbb{R}_+^*}$ est-elle libre (pour les lois usuelles)?

6.3.2 Sous-espace engendré par une partie

♦ **Définition 1** Soient E un K-ev, $A \in \mathfrak{P}(E)$. On appelle **sev engendré par** A, et on note Vect (A), l'intersection de tous les sev de E contenant A :

$$\text{Vect}(A) = \bigcap_{\substack{F \in \mathbf{V}(E) \\ F \supset A}} F.$$

♦ **Proposition 1** Soient E un K-ev, $A \in \mathfrak{P}(E)$.

1) Vect (A) est le plus petit (au sens de l'inclusion) sev de E contenant A.

2) • Si $A \neq \varnothing$, alors Vect (A) est l'ensemble des combinaisons linéaires d'éléments de A.

• Vect $(\varnothing) = \{0\}$.

Preuve :

1) • D'après 6.2 Prop. 2 p. 219, Vect (A) est un sev de E, comme intersection de sev de E.

• Par la définition de Vect (A), on a : $A \subset$ Vect (A).

• Soit F un sev de E contenant A. Par la définition de Vect (A), on a : Vect $(A) \subset F$.

Ainsi, Vect (A) est un sev de E contenant A, et il est inclus dans tout sev de E contenant A.

2) Le singleton $\{0\}$ est à l'évidence le plus petit sev de E contenant $\varnothing$.

Supposons $A \neq \varnothing$ et notons C l'ensemble des combinaisons linéaires d'éléments de A :

$$C = \left\{ x \in E;\ \exists n \in \mathbb{N}^*, \exists (a_1,\ldots,a_n) \in A^n,\ \exists (\lambda_1,\ldots,\lambda_n) \in K^n,\ x = \sum_{i=1}^{n} \lambda_i a_i \right\}.$$

Montrons que C est le plus petit sev de E contenant A.

a) • Il est clair que $C \neq \varnothing$.

• Soit $(x,y) \in C^2$. Il existe $n \in \mathbb{N}^*$, $(a_1,\ldots,a_n) \in A^n$, $(\lambda_1,\ldots,\lambda_n) \in K^n$ tels que $x = \sum_{i=1}^{n} \lambda_i a_i$, et $p \in \mathbb{N}^*, (b_1,\ldots,b_p) \in A^p$, $(\mu_1,\ldots,\mu_p) \in K^p$ tels que $y = \sum_{j=1}^{p} \mu_j b_j$.

En notant $c_k = \begin{cases} a_k & \text{si } 1 \leqslant k \leqslant n \\ b_{k-n} & \text{si } n+1 \leqslant k \leqslant n+p \end{cases}$ et $\nu_k = \begin{cases} \lambda_k & \text{si } 1 \leqslant k \leqslant n \\ \mu_{k-n} & \text{si } n+1 \leqslant k \leqslant n+p, \end{cases}$

on a : $\left| \begin{array}{l} \forall k \in \{1,\ldots,n+p\},\ c_k \in A \\ x + y = \sum_{i=1}^{n} \lambda_i a_i + \sum_{j=1}^{p} \mu_j b_j = \sum_{k=1}^{n+p} \nu_k c_k \end{array} \right|$, donc $x + y \in C$.

• On montre de même : $\forall \lambda \in K, \forall x \in C,\ x \in C$.

Ainsi, C est un sev de E.

b) Comme tout élément de A est combinaison linéaire d'éléments de A (il suffit d'écrire $a = 1a$), Vect (A) contient A.

c) Soient G un sev de E contenant A, et $x \in C$. Il existe $n \in \mathbb{N}^*$, $(a_1,\ldots,a_n) \in A^n$, $(\lambda_1,\ldots,\lambda_n) \in K^n$ tels que $x = \sum_{i=1}^{n} \lambda_i a_i$. Comme G contient A et que G est un sev, on déduit $x \in G$, ce qui montre $C \subset G$.

Ceci établit que C est le plus petit sev de E contenant A, et finalement : $C =$ Vect (A). ■

En particulier, le sev engendré par un singleton $\{x\}$ (où $x \in E$) est Kx, c'est-à-dire $\{\lambda x;\ \lambda \in K\}$.

◆ **Définition 2** Soient E un K-ev, $(x_i)_{i\in I}$ une famille d'éléments de E. On appelle **sev engendré par** $(x_i)_{i\in I}$, et on note ici Vect $((x_i)_{i\in I})$ le sev engendré par la partie $\{x_i;\ i \in I\}$ de E.

En particulier, le sev de E engendré par une famille finie non vide $(x_1,\ldots,x_n)$ d'éléments de E est $\left\{\sum_{i=1}^{n} \lambda_i x_i;\ \ (\lambda_1,\ldots,\lambda_n) \in K^n\right\}$.

◆ **Proposition 2** Soient E un K-ev, $A, B \in \mathfrak{P}(E)$. On a :

1) $A \subset B \Longrightarrow$ Vect $(A) \subset$ Vect (B)

2) A est un sev de E si et seulement si Vect $(A) = A$

3) Vect (Vect (A)) = Vect (A)

4) Vect $(A \cup B) =$ Vect $(A) +$ Vect (B).

Preuve :

Les démonstrations de *1), 2), 3)* sont immédiates. Montrons *4)*.

• $\left\{\begin{array}{l} A \subset A \cup B \\ B \subset A \cup B \end{array}\right. \overset{1)}{\Longrightarrow} \left\{\begin{array}{l} \text{Vect}\,(A) \subset \text{Vect}\,(A \cup B) \\ \text{Vect}\,(B) \subset \text{Vect}\,(A \cup B) \end{array}\right. \Longrightarrow \text{Vect}\,(A)+\text{Vect}\,(B) \subset \text{Vect}\,(A \cup B)$,

cf. 6.2 Prop. 4 *3)* p. 212.

• Réciproquement, soit $x \in$ Vect $(A \cup B)$. Il existe $n \in \mathbb{N}^*$, $(c_1,\ldots,c_n) \in (A \cup B)^n$, $(\lambda_1,\ldots,\lambda_n) \in K^n$ tels que $x = \sum_{i=1}^{n} \lambda_i c_i$. En groupant les termes de A d'une part, ceux de B d'autre part, on en déduit qu'il existe $a \in A$, $b \in B$ tels que $x = a + b$.

Ceci montre : Vect $(A \cup B) \subset$ Vect $(A) +$ Vect (B).

6.3.3 Somme de plusieurs sev

Nous allons généraliser ici l'étude de la somme de deux sev faite en 6.2 p. 211.

♦ **Définition 1** Soient E un K-ev, $n \in \mathbb{N}^*$, $F_1,\ldots,F_n$ des sev de E. On définit la **somme** de $F_1,\ldots,F_n$, notée $F_1+\ldots+F_n$ (ou $\sum_{i=1}^{n} F_i$) :

$$F_1+\ldots+F_n = \{x \in E;\ \exists (x_1,\ldots,x_n) \in F_1\times\ldots\times F_n,\quad x = x_1+\ldots+x_n\}$$
$$= \{x_1+\ldots+x_n;\quad (x_1,\ldots,x_n) \in F_1\times\ldots\times F_n\}.$$

On convient de : $\sum_{i\in\varnothing} F_i = \{0\}$.

La Proposition suivante est immédiate (par récurrence).

♦ **Proposition** Soient E un K-ev, $n \in \mathbb{N}^*$, $F_1,\ldots,F_n$ des sev de E. On a :

1) $\forall \sigma \in \mathfrak{S}_n,\ \sum_{i=1}^{n} F_{\sigma(i)} = \sum_{i=1}^{n} F_i$

2) Pour toute partition Π de $\{1,\ldots,n\}$: $\sum_{J\in\Pi}\left(\sum_{i\in J} F_i\right) = \sum_{i=1}^{n} F_i$.

Autrement dit :

1) la somme de plusieurs sev ne dépend pas de l'ordre de ces sev

2) dans une somme de plusieurs sev, on peut « grouper » des sev par paquets.

En particulier, pour tous sev F_1, F_2, F_3 de E :

$$(F_1+F_2)+F_3 = F_1+(F_2+F_3) = F_1+F_2+F_3.$$

Remarque :

Pour tous sev $F_1,\ldots,F_n$ d'un K-ev E, on a : $\sum_{i=1}^{n} F_i = \text{Vect}\left(\bigcup_{i=1}^{n} F_i\right)$.

En particulier, pour tout $(x_1,\ldots,x_n)$ de E^n : $\text{Vect}\,(x_1,\ldots,x_n) = \sum_{i=1}^{n} Kx_i$.

♦ **Définition 2** Soient E un K-ev, $n \in \mathbb{N}^*$, $F_1,\ldots,F_n$ des sev de E. On dit que $F_1,\ldots,F_n$ **sont en somme directe** si et seulement si :

$$\forall (x_1,\ldots,x_n) \in F_1\times\ldots\times F_n,\quad (x_1+\ldots+x_n = 0 \Longrightarrow x_1 = \ldots = x_n = 0).$$

Lorsque $F_1,\ldots,F_n$ sont des sev en somme directe, on note $F_1\oplus\ldots\oplus F_n$, ou $\bigoplus_{i=1}^{n} F_i$, au lieu de $F_1+\ldots+F_n$.

Au lieu de $F_1,\ldots,F_n$ sont en somme directe, on dit aussi : $F_1,\ldots,F_n$ **ont une somme directe**, ou : $F_1+\ldots+F_n$ **est directe**, ou : $F_1,\ldots,F_n$ **sont linéairement indépendants**.

◆ **Théorème** Soient E un K-ev, $n \in \mathbb{N}^*$, $F_1, \ldots, F_n$ des sev de E. Les propriétés suivantes sont deux à deux équivalentes :

1) $F_1, \ldots, F_n$ sont en somme directe

2) Tout élément de $\sum_{i=1}^{n} F_i$ se décompose de façon unique en une somme d'éléments de $F_1, \ldots, F_n$

3) $\forall i \in \{1, \ldots, n\}, \quad F_i \cap \left(\sum_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} F_j \right) = \{0\}$

4) $\forall i \in \{2, \ldots, n\}, \quad F_i \cap \left(\sum_{1 \leqslant j \leqslant i-1} F_j \right) = \{0\}$

5) Pour tout $(x_1, \ldots, x_n)$ de $(F_1 - \{0\}) \times \ldots \times (F_n - \{0\})$, $(x_1, \ldots, x_n)$ est libre (en supposant $F_1, \ldots, F_n$ tous $\neq \{0\}$).

Preuve :

1) $\Longrightarrow$ *2)* : On suppose que $F_1, \ldots, F_n$ sont en somme directe.

Soient $x \in F_1 + \ldots + F_n$, $(x_1, \ldots, x_n) \in F_1 \times \ldots \times F_n$, $(y_1, \ldots, y_n) \in F_1 \times \ldots \times F_n$ tels que : $x = \sum_{i=1}^{n} x_i = \sum_{i=1}^{n} y_i$.

Alors : $\left\{ \begin{array}{l} \forall i \in \{1, \ldots, n\}, \; x_i - y_i \in F_i \\ \sum_{i=1}^{n} (x_i - y_i) = 0 \end{array} \right.$, d'où, puisque $F_1 + \ldots + F_n$ est directe :

$\forall i \in \{1, \ldots, n\}, \; x_i - y_i = 0$, et donc $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$.

2) $\Longrightarrow$ *3)* : Supposons que tout élément de $\sum_{i=1}^{n} F_i$ se décompose d'une façon unique en une somme d'éléments de $F_1, \ldots, F_n$.

Soient $i \in \{1, \ldots, n\}$ et $x \in F_i \cap \left(\sum_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} F_j \right)$.

Alors $x \in F_i$ et il existe $(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \in F_1 \times \ldots \times F_{i-1} \times F_{i+1} \times \ldots \times F_n$ tel que : $x = \sum_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} x_j$. En notant $x_i = -x$, on obtient : $\left\{ \begin{array}{l} \forall j \in \{1, \ldots, n\}, \; x_j \in F_j \\ \sum_{j=1}^{n} x_j = 0 \end{array} \right.$.

D'après *2)*, comme 0 se décompose aussi en $0 = 0 + \ldots + 0$ ($0 \in F_j$), on déduit :

$$\forall j \in \{1, \ldots, n\}, \; x_j = 0.$$

En particulier, $x = -x_i = 0$ et donc $F_i \cap \left(\sum_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} F_j \right) = \{0\}$.

3) $\Longrightarrow$ *4)* : Immédiat, puisque : $\sum_{1\leqslant j\leqslant i-1} F_j \subset \sum_{\substack{1\leqslant j\leqslant n \\ j\neq i}} F_j$.

4) $\Longrightarrow$ *5)* : Supposons *4)* vérifié.

Soient $x_1 \in F_1 - \{0\}, \ldots, x_n \in F_n - \{0\}, (\lambda_1, \ldots, \lambda_n) \in K^n$ tels que $\sum_{i=1}^{n} \lambda_i x_i = 0$.

• On a : $\lambda_n x_n \in F_n$ et $\lambda_n x_n = -\sum_{i=1}^{n-1} \lambda_i x_i \in \sum_{1\leqslant j\leqslant n-1} F_j$, d'où d'après *4)* : $\lambda_n x_n = 0$, puis, comme $x_n \neq 0$: $\lambda_n = 0$.

• En réitérant, on déduit : $\lambda_n = 0$, $\lambda_{n-1} = 0, \ldots, \lambda_1 = 0$. Finalement, $(x_1, \ldots, x_n)$ est libre.

5) $\Longrightarrow$ *1)* : Supposons $F_1, \ldots, F_n$ tous $\neq \{0\}$ et la condition *5)* satisfaite.

Soit $(x_1, \ldots, x_n) \in F_1 \times \ldots \times F_n$ tel que $\sum_{i=1}^{n} x_i = 0$. Notons $I = \{i \in \{1, \ldots, n\};\ x_i \neq 0\}$.

Supposons $I \neq \varnothing$ et notons $J = \{1, \ldots, n\} - I$.

Puisque $F_1, \ldots, F_n$ sont tous $\neq \{0\}$, il existe $(y_1, \ldots, y_n)$ dans $(F_1 - \{0\}) \times \ldots \times (F_n - \{0\})$.

Notons, pour $i \in \{1, \ldots, n\}$: $z_i = \begin{cases} x_i & \text{si } i \in I \\ y_i & \text{si } i \in J \end{cases}$.

La famille $(z_1, \ldots, z_n)$ est liée car c'est une sur-famille de $(X_i)_{i\in I}$ qui est elle-même liée $\left(\sum_{i\in I} x_i = 0\right)$. De plus : $\forall i \in I,\ z_i \in F_i - \{0\}$. Ceci contredit l'hypothèse *5)*.

Il en résulte $I = \varnothing$, c'est-à-dire : $\forall i \in \{1, \ldots, n\},\ x_i = 0$.

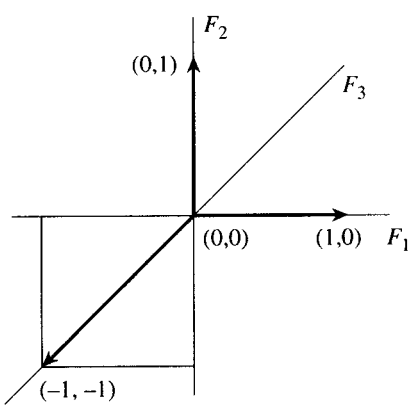
Remarques :

1) Si F_1, F_2, F_3 sont des sev d'un ev E, on peut avoir $F_1 \cap F_2 = F_1 \cap F_3 = F_2 \cap F_3 = \{0\}$ sans que F_1, F_2, F_3 soient en somme directe, comme le montre l'exemple :

$K = \mathbb{R}$, $E = \mathbb{R}^2$, $F_1 = \mathbb{R} \times \{0\}$,

$F_2 = \{0\} \times \mathbb{R}$, $F_3 = \{(x,x);\ x \in \mathbb{R}\}$.

Dans cet exemple, F_1, F_2, F_3 ne sont pas en somme directe car $(1,0) \in F_1$, $(0,1) \in F_2$, $(-1,-1) \in F_3$ sont tous non nuls et de somme $(0,0)$.



2) Si F_1, F_2, F_3 sont des sev d'un ev E, on peut avoir $F_1 \cap F_2 \cap F_3 = \{0\}$ sans que F_1, F_2, F_3 soient en somme directe (même exemple que ci-dessus).

3) Le fait que des sev $F_1, \ldots, F_n$ soient en somme directe ne dépend pas de l'ordre de $F_1, \ldots, F_n$. Autrement dit, si des sev $F_1, \ldots, F_n$ de E sont en somme directe, alors, pour toute permutation σ de $\mathfrak{S}_n$, $F_{\sigma(1)}, \ldots, F_{\sigma(n)}$ sont en somme directe.

4) Si des sev $F_1, \ldots, F_n$ de E sont en somme directe, alors, pour tout p de $\{1, \ldots, n\}$, les sev $F_1, \ldots, F_p$ sont en somme directe.

Exercices

◇ **6.3.6** Soient E un K-ev, F, G, F', G' des sev de E tels que :

$$\begin{cases} F \text{ et } G \text{ sont supplémentaires dans } E \\ F' \text{ et } G' \text{ sont supplémentaires dans } E \\ F' \subset G. \end{cases}$$

Montrer que $F, F', G \cap G'$ sont en somme directe et : $F \oplus F' \oplus (G \cap G') = E$.

◇ **6.3.7** Soient E un K-ev, $n \in \mathbb{N}^*$, $x_1, \ldots, x_n \in E^n$. Montrer que $(x_1, \ldots, x_n)$ est libre si et seulement si :

$$\begin{cases} \forall i \in \{1, \ldots, n\},\ x_i \neq 0 \\ \sum_{i=1}^{n} Kx_i \text{ est directe.} \end{cases}$$

◇ **6.3.8** Soient E un K-ev, $n \in \mathbb{N}^*$, $F_1, \ldots, F_n$, $G_1, \ldots, G_n$ des sev de E tels que :

$$\begin{cases} F_1, \ldots, F_n \text{ sont en somme directe} \\ \forall i \in \{1, \ldots, n\},\ G_i \subset F_i \end{cases}$$

Montrer que $G_1, \ldots, G_n$ sont en somme directe.

6.3.4 Familles génératrices, bases

♦ **Définition 1** Soient E un K-ev, $\mathcal{G}$ une famille d'éléments de E. On dit que $\mathcal{G}$ est une **famille génératrice de** E (ou : $\mathcal{G}$ **engendre** E) si et seulement si :

$$\text{Vect}\,(\mathcal{G}) = E.$$

La Proposition suivante est immédiate.

♦ **Proposition 1** Si $\mathcal{G} = (x_1,\ldots,x_n)$ est une famille finie d'éléments d'un K-ev E, $\mathcal{G}$ engendre E si et seulement si :

$$\forall x \in E,\ \exists\,(\lambda_1,\ldots,\lambda_n) \in K^n,\ x = \sum_{i=1}^{n} \lambda_i x_i.$$

Une partie G d'un K-ev E est dite **génératrice de** E si et seulement si : Vect $(G) = E$. Ceci revient à ce que la famille $(x)_{x\in G}$ des éléments de G engendre E au sens de la Déf. 1.

♦ **Définition 2** On dit qu'une famille $\mathcal{B}$ d'éléments d'un K-ev est une **base** de E si et seulement si : $\mathcal{B}$ est libre et génératrice de E.

Remarque :

$\varnothing$ est une base de $\{0\}$.

La Proposition suivante est immédiate.

♦ **Proposition - Définition 2** Une famille finie $\mathcal{B} = (e_1,\ldots,e_n)$ d'éléments d'un K-ev E est une base de E si et seulement si :

$$\forall x \in E,\ \exists\,!(x_1,\ldots,x_n) \in K^n,\ x = \sum_{i=1}^{n} x_i e_i.$$

Si E admet une base finie $\mathcal{B} = (e_1,\ldots,e_n)$, pour tout x de E, les éléments $x_1,\ldots,x_n$ définis ci-dessus s'appellent les **coordonnées** (ou : **composantes**) **de** x **sur la base** $\mathcal{B}$; x_i s'appelle la $i^{\text{ème}}$ **coordonnée** (ou : **composante**) **de** x **dans la base** $\mathcal{B}$.

Exercice

◇ **6.3.9** Soient E un K-ev, $n \in \mathbb{N}^*$, $F_1,\ldots F_n$ des sev de E.

a) Montrer que, si $F_1,\ldots,F_n$ sont en somme directe et si, pour tout i de $\{1,\ldots,n\}$, $\mathcal{L}_i$ est une famille libre dans F_i, alors $\bigcup_{i=1}^{n} \mathcal{L}_i$ est libre dans E.

b) Montrer que, si $F_1 + \ldots + F_n = E$ et si, pour tout i de $\{1,\ldots,n\}$, $\mathcal{G}_i$ est une famille génératrice de F_i, alors $\bigcup_{i=1}^{n} \mathcal{G}_i$ est génératrice de E.

c) Montrer que, si $F_1,\ldots,F_n$ sont en somme directe et de somme égale à E et si, pour tout i de $\{1,\ldots,n\}$, $\mathcal{B}_i$ est une base de F_i, alors $\bigcup_{i=1}^{n} \mathcal{B}_i$ est une base de E.

6.4 Théorie de la dimension

Dans ce § 6.4, E désigne un K-ev.

◆ **Proposition 1** Soient $(n,p) \in (\mathbb{N}^*)^2$, $(x_1,\ldots,x_{n+p}) \in E^{n+p}$, $\mathcal{F} = (x_1,\ldots,x_p)$, $\mathcal{F}' = (x_1,\ldots,x_p,x_{p+1},\ldots,x_{n+p})$.
1) Si $\mathcal{F}'$ est libre, alors $\mathcal{F}$ est libre
2) Si $\mathcal{F}$ est génératrice de E, alors $\mathcal{F}'$ est génératrice de E.

Preuve :

1) Cf. 6.3.1 Rem. *4)* p. 217.

2) Soit $x \in E$. Puisque $\mathcal{F}$ engendre E, il existe $(\lambda_1,\ldots,\lambda_p) \in K^p$ tel que $x = \sum_{i=1}^{p} \lambda_i x_i$.

En notant $\lambda_{p+1} = \ldots = \lambda_{n+p} = 0$, on a alors $x = \sum_{i=1}^{n+p} \lambda_i x_i$.

Ceci montre que $\mathcal{F}'$ engendre E. ∎

La Proposition précédente se généralise à des familles quelconques (non nécessairement finies) :

1) Si $\mathcal{F} \subset \mathcal{F}'$ et si $\mathcal{F}'$ est libre, alors $\mathcal{F}$ est libre

2) Si $\mathcal{F} \subset \mathcal{F}'$ et si $\mathcal{F}$ est génératrice de E, alors $\mathcal{F}'$ est génératrice de E.

(où $\mathcal{F} \subset \mathcal{F}'$ signifie que $\mathcal{F}$ est une sous-famille de $\mathcal{F}'$).

◆ **Proposition 2** Soient $n \in \mathbb{N}^*$, $(x_1,\ldots,x_{n+1}) \in E^{n+1}$, $\mathcal{F} = (x_1,\ldots,x_n)$, $\mathcal{F}' = (x_1,\ldots,x_n,x_{n+1})$.
1) Si $\mathcal{F}$ est libre et si $x_{n+1} \notin \text{Vect}(\mathcal{F})$, alors $\mathcal{F}'$ est libre
2) Si $\mathcal{F}'$ est génératrice de E et si $x_{n+1} \in \text{Vect}(\mathcal{F})$, alors $\mathcal{F}$ est génératrice de E.

Preuve :

1) Soit $(\lambda_1,\ldots,\lambda_{n+1}) \in K^{n+1}$ tel que $\sum_{i=1}^{n+1} \lambda_i x_i = 0$. Si $\lambda_{n+1} \neq 0$, alors on déduit $x_{n+1} = \sum_{i=1}^{n} \left(-\lambda_{n+1}^{-1}\lambda_i\right) x_i \in \text{Vect}(\mathcal{F})$, contradiction.

Donc $\lambda_{n+1} = 0$, d'où $\sum_{i=1}^{n} \lambda_i x_i = 0$, puis $\lambda_1 = \ldots = \lambda_n = 0$ puisque $\mathcal{F}$ est libre.

2) Soit $x \in E$. Puisque $\mathcal{F}'$ est génératrice de E, il existe $(\lambda_1,\ldots,\lambda_{n+1}) \in K^{n+1}$ tel que : $x = \sum_{i=1}^{n+1} \lambda_i x_i$.

Comme $x_{n+1} \in \text{Vect}(\mathcal{F})$, il existe $(\mu_1,\ldots,\mu_n) \in K^n$ tel que : $x_{n+1} = \sum_{i=1}^{n} \mu_i x_i$.

On déduit : $x = \left(\sum_{i=1}^{n} \lambda_i x_i\right) + \lambda_{n+1} x_{n+1} = \sum_{i=1}^{n} (\lambda_i + \lambda_{n+1}\mu_i) x_i \in \text{Vect}(\mathcal{F})$,

ce qui montre que $\mathcal{F}$ est génératrice de E. ■

La Proposition précédente se généralise à des familles quelconques (non nécessairement finies) :

1) Si $\mathcal{F}$ est libre et si $x \notin \text{Vect}(\mathcal{F})$, alors $\mathcal{F} \cup \{x\}$ est libre (où $\mathcal{F} \cup \{x\}$ est obtenue en rajoutant x à la famille $\mathcal{F}$).

2) Si $\mathcal{F} \cup \{x\}$ est génératrice de E et si $x \in \text{Vect}(\mathcal{F})$, alors $\mathcal{F}$ est génératrice de E. ■

On peut énoncer la Proposition précédente sous la forme :

1) En rajoutant à une famille libre un vecteur qui ne se décompose pas sur cette famille, on obtient une nouvelle famille libre

2) En enlevant à une famille génératrice de E un vecteur qui se décompose sur les autres éléments de cette famille, on obtient une nouvelle famille génératrice de E.

♦ **Lemme (Théorème de l'échange)**

Soient $\mathcal{G} = (x_1,\ldots,x_p)$, $\mathcal{L} = (y_1,\ldots,y_r)$ deux familles finies d'éléments de E. Si $\mathcal{G}$ est génératrice de E et si $\mathcal{L}$ est libre, alors :

1) $r \leqslant p$

2) On peut remplacer d'au moins une façon r des vecteurs de $\mathcal{G}$ par ceux de $\mathcal{L}$ pour obtenir une famille génératrice de E.

Preuve :

• Puisque $\mathcal{G}$ engendre E, il existe $(\lambda_{1,1},\ldots,\lambda_{1,p}) \in K^p$ tel que $y_1 = \sum_{j=1}^{p} \lambda_{1,j} x_j$.

On a : $(\lambda_{1,1},\ldots,\lambda_{1,p}) \neq (0,\ldots,0)$, car, sinon $y_1 = 0$, ce qui contredit la liberté de $\mathcal{L}$.

Quitte à permuter $x_1,\ldots,x_p$ (et $\lambda_{1,1},\ldots,\lambda_{1,p}$), on peut se ramener à : $\lambda_{1,1} \neq 0$.

Alors, en notant $\mathcal{G}_1 = (y_1,x_2,\ldots,x_p)$, on a : $x_1 = \lambda_{1,1}^{-1} y_1 - \sum_{j=2}^{p} \lambda_{1,1}^{-1}\lambda_{1,j} x_j \in \text{Vect}(\mathcal{G}_1)$.

Puisque $\mathcal{G}$ engendre E, $(y_1,x_1,x_2,\ldots,x_p)$ engendre E (cf. Prop. 1 *2)* p. 226), puis , comme $x_1 \in \text{Vect}(\mathcal{G}_1)$, $\mathcal{G}_1$ engendre E (cf. Prop. 2 *2)* p. 226).

On a ainsi remplacé un des vecteurs de $\mathcal{G}$ par y_1 pour obtenir une famille génératrice $\mathcal{G}_1 = (y_1,x_2,\ldots,x_p)$.

• Soit $s \in \mathbb{N}^*$ tel que $s \leqslant \text{Min}(p-1, r-1)$. Supposons (après une éventuelle permutation de $x_1,\ldots,x_p$) que la famille $\mathcal{G}_s = (y_1,\ldots,y_s,x_{s+1},\ldots,x_p)$ soit génératrice de E.

Il existe $(\lambda_{s+1,1},\ldots,\lambda_{s+1,p}) \in K^p$ tel que : $y_{s+1} = \sum_{j=1}^{s} \lambda_{s+1,j} y_j + \sum_{j=s+1}^{p} \lambda_{s+1,j} x_j$.

Si $(\lambda_{s+1,s+1},\ldots,\lambda_{s+1,p}) = (0,\ldots,0)$, alors $y_{s+1} = \sum_{j=1}^{s} \lambda_{s+1,j} y_j$, ce qui contredit la liberté de $(y_1,\ldots,y_{s+1})$ (donc de $\mathcal{L}$). Quitte à permuter $x_{s+1},\ldots,x_p$ (et $\lambda_{s+1,s+1},\ldots,\lambda_{s+1,p}$), on peut se ramener à : $\lambda_{s+1,s+1} \neq 0$. Alors, en notant $\mathcal{G}_{s+1} = (y_1,\ldots,y_s,y_{s+1},x_{s+2},\ldots,x_p)$, la même argumentation que plus haut montre que $\mathcal{G}_{s+1}$ est génératrice de E.

On a ainsi remplacé des vecteurs de $\mathcal{G}$ par des vecteurs de $\mathcal{L}$ pour obtenir une famille génératrice.

• Supposons $r > p$.

Avec les notations précédentes, $\mathcal{G}_p = (y_1,\ldots,y_p)$ est génératrice de E, donc $y_{p+1} \in \text{Vect}\,(\mathcal{G}_p)$, ce qui contredit la liberté de $(y_1,\ldots,y_{p+1})$, donc de $\mathcal{L}$.

Donc $r \leqslant p$, et $\mathcal{G}_r = (y_1,\ldots,y_r,x_{r+1},\ldots,x_p)$ est génératrice de E.

◆ **Définition 1** Un K-ev E est dit **de dimension finie** si et seulement si E admet au moins une famille génératrice finie.

EXEMPLE :

1) $\{0\}$ et $K^n (n \in \mathbb{N}^*)$ sont des K-ev de dimension finie.

2) $K[X]$ est un K-ev qui n'est pas de dimension finie, car si $K[X]$ admettait une famille génératrice finie $(P_1,\ldots,P_n)$, alors, pour tout P de $K[X]$, on aurait $\deg(P) \leqslant \underset{1\leqslant i\leqslant n}{\text{Max}}\,(\deg(P_i))$.

◆ **Théorème - Définition 1** Soit E un K-ev de dimension finie. Alors :

1) E admet au moins une base finie

2) Toutes les bases de E sont finies et ont le même cardinal.

Le cardinal d'une base de E est appelé la **dimension** de E et noté $\dim_K(E)$, ou $\dim(E)$.

Preuve :

1) Puisque E est de dimension finie, E admet au moins une famille génératrice $\mathcal{G} = (x_1,\ldots,x_p)$. Si $\mathcal{G}$ est libre, alors $\mathcal{G}$ est une base finie de E.

Supposons que $\mathcal{G}$ soit liée; il existe $(\lambda_1,\ldots,\lambda_p) \in K^p - \{(0,\ldots,0)\}$ tel que $\sum_{i=1}^{p} \lambda_i x_i = 0$.

Quitte à permuter $x_1,\ldots,x_p$ (et $\lambda_1,\ldots,\lambda_p$), on peut se ramener à $\lambda_p \neq 0$, d'où, en notant $\mathcal{G}_1 = (x_1,\ldots,x_{p-1})$: $\quad x_p = -\sum_{i=1}^{p-1} \lambda_p^{-1}\lambda_i x_i \in \text{Vect}\,(\mathcal{G}_1)$.

D'après la Prop. 2 *2)* p. 226, $\mathcal{G}_1$ est génératrice de E.

On réitère le procédé.

S'il existe $r \in \{1,\ldots,p\}$ tel que la famille génératrice $\mathcal{G}_r = (x_1,\ldots,x_{p-r})$ soit libre, alors $\mathcal{G}_r$ est une base de E.

Sinon, $\mathcal{G}_1 = (x_1)$ est liée et génératrice, d'où $E = \{0\}$, et $\varnothing$ est une base finie de E.

2) D'après *1)*, E admet au moins une basse finie $\mathcal{B}$; notons n le nombre d'éléments de $\mathcal{B}$.

Soit $\mathcal{B}'$ une (autre) base de E. Si $\mathcal{B}'$ est infinie ou finie de cardinal $> n$, alors $\mathcal{B}'$ contient au moins une famille finie libre $\mathcal{L}$ ayant $n+1$ éléments. Mais $\mathcal{B}$ est génératrice à n éléments et $\mathcal{L}$ libre à $n+1$ éléments, ce qui contredit le résultat *1)* du théorème de l'échange.

Donc $\mathcal{B}'$ est finie de cardinal $\leqslant n$.

De même, $\mathcal{B}$ étant libre à n éléments et $\mathcal{B}'$ génératrice, le résultat *1)* du théorème de l'échange montre : $n \leqslant \text{Card}(\mathcal{B}')$.

Finalement, $\mathcal{B}'$ est finie et a n éléments. ∎

Remarque :

La preuve précédente établit plus précisément que toute famille génératrice finie d'un K-ev de dimension finie contient au moins une base. ■

On dit qu'un sev F d'un ev E est **de dimension finie** si et seulement si l'ev F est de dimension finie.

On dit quelquefois qu'un ev qui n'est pas de dimension finie est «**de dimension infinie** ».

Remarques :

1) Pour tout ev E de dimension finie : $\dim(E) = 0 \iff E = \{0\}$.

2) La dimension d'un K-ev de dimension finie «dépend» du corps K. Par exemple :

$\dim_{\mathbb{C}}(\mathbb{C}^2) = 2$, mais $\dim_{\mathbb{R}}(\mathbb{C}^2) = 4$.

3) L'existence, pour tout ev (non nécessairement de dimension finie) d'au moins une base est logiquement équivalente à l'*axiome du choix*, dont l'étude dépasse le cadre de cet ouvrage.

♦ **Théorème 2** (**Théorème de la base incomplète**)

Soient E un K-ev de dimension finie, $\mathcal{L} = (y_1, \ldots, y_r)$ une famille libre dans E.

1ère forme (forme forte)

Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base de E. Il y a au moins une façon de compléter $\mathcal{L}$ par $n - r$ vecteurs de $\mathcal{B}$ pour obtenir une base de E.

2ème forme (forme faible)

Il y a au moins une façon de compléter $\mathcal{L}$ par $n - r$ vecteurs de E pour obtenir une base de E.

Preuve :

Pour la 1ère forme, il suffit d'appliquer le théorème de l'échange à la famille génératrice $\mathcal{B}$ et à la famille libre $\mathcal{L}$.

La 2ème forme se déduit trivialement de la 1ère forme et de l'existence d'au moins une base finie de E.

♦ **Proposition 3** Soient E un K-ev de dimension finie, $n = \dim(E)$.

1) Toute famille libre de E est finie et a au plus n éléments

2) Toute famille de E ayant au moins $n + 1$ éléments est liée

3) Toute famille génératrice de E a au moins n éléments.

Preuve :

D'après Th.- Def. 1 p. 228, E admet au moins une base $\mathcal{B} = (e_1, \ldots, e_n)$.

1) Soit $\mathcal{L}$ une famille libre dans E. Si $\mathcal{L}$ est infinie ou est finie de cardinal $> n$, il y a alors contradiction avec le résultat *1)* du théorème de l'échange, puisque $\mathcal{B}$ est génératrice.

2) Se déduit de *1)* par contre-apposition.

3) Soit $\mathcal{G}$ une famille génératrice de E. D'après le résultat *1)* du théorème de l'échange, et puisque $\mathcal{B}$ est libre, $\mathcal{G}$ a au moins n éléments.

◆ **Proposition 4** Soient E un K-ev de dimension finie, $n = \dim(E)$, $\mathcal{F}$ une famille finie d'éléments de E. Deux quelconques des trois propriétés suivantes entraînent la troisième :

1) $\mathcal{F}$ a n éléments

2) $\mathcal{F}$ est libre

3) $\mathcal{F}$ est génératrice de E.

Preuve :

• (1 et 2) $\Longrightarrow$ 3 :

Supposons $\text{Card}(\mathcal{F}) = n$ et $\mathcal{F}$ libre; E admet au moins une base $\mathcal{B} = (e_1,\ldots,e_n)$. D'après le théorème de l'échange, comme $\mathcal{B}$ est génératrice et $\mathcal{F}$ libre, on peut remplacer d'au moins une façon n des vecteurs de $\mathcal{B}$ par ceux de $\mathcal{F}$ pour obtenir une famille génératrice. Mais, comme $\mathcal{B}$ a n éléments, la famille génératrice obtenue est $\mathcal{F}$.

• (1 et 3) $\Longrightarrow$ 2 :

Supposons $\text{Card}(\mathcal{F}) = n$ et $\mathcal{F}$ génératrice. Raisonnons par l'absurdre : supposons $\mathcal{F}$ liée.

Il existe $(\lambda_1,\ldots,\lambda_n) \in K^n - \{(0,\ldots,0)\}$ tel que $\sum_{i=1}^{n} \lambda_i x_i = 0$.

Quitte à permuter $x_1,\ldots,x_n$ (et $\lambda_1,\ldots,\lambda_n$), on peut se ramener à $\lambda_n \neq 0$, d'où :

$$x_n = -\sum_{i=1}^{n-1} \lambda_n^{-1}\lambda_i x_i \in \text{Vect}\,(x_1,\ldots,x_{n-1}).$$

D'après Prop. 2, *2)* p. 226, $(x_1,\ldots,x_{n-1})$ est génératrice de E, ce qui contredit Prop. 3 *3)* p. 229.

Ceci prouve que $\mathcal{F}$ est libre.

• (2 et 3) $\Longrightarrow$ 1 : Résulte de Th.- Déf. 1 p. 228.

◆ **Proposition 5** Soit E un K-ev de dimension finie. Tout sev F de E est de dimension finie, et :

$$\dim(F) \leqslant \dim(E).$$

Preuve :

Le résultat est évident lorsque $F = \{0\}$.

Supposons $F \neq \{0\}$. Il existe $x_1 \in F$ tel que $x_1 \neq 0$; notons $\mathcal{L}_1 = (x_1)$, qui est libre.

Si $\mathcal{L}_1$ engendre F, alors F est de dimension finie et $\dim(F) = 1$.

Sinon, il existe $x_2 \in F$ tel que $x_2 \notin \text{Vect}\,(\mathcal{L}_1)$.

D'après Prop. 2, *1)*, p. 226, la famille $\mathcal{L}_2 = (x_1,x_2)$ est libre, et on réitère le raisonnement.

Soit $p \in \mathbb{N}^*$; supposons définis $x_1,\ldots,x_p$ dans F tels que $\mathcal{L}_p = (x_1,\ldots,x_p)$ soit libre.

Si $\mathcal{L}_p$ engendre F, alors F est de dimension finie et $\dim(F) = p$.

Sinon, il existe $x_{p+1} \in F$ tel que $x_{p+1} \notin \text{Vect}\,(\mathcal{L}_p)$, et la famille $\mathcal{L}_{p+1} = (x_1,\ldots,x_{p+1})$ est libre dans F.

En notant $n = \dim(E)$, comme toute famille de E ayant au moins $n+1$ éléments est liée, il existe $p \in \{1,\ldots,n\}$ tel que $\mathcal{L}_p$ engendre F.

Ainsi, F est de dimension finie et $\dim(F) \leqslant n$. ∎

♦ **Définition 2** On appelle **droite vectorielle** (resp. **plan vectoriel**) tout ev ou sev de dimension 1 (resp. 2). Une droite vectorielle est engendrée (on dit aussi : **dirigée**) par n'importe lequel de ses vecteurs $\neq 0$.

Dans un ev de dimension finie n ($n \geqslant 1$), on appelle **hyperplan** tout sev de dimension $n-1$.

♦ **Proposition 6** Soient E un K-ev de dimension finie, $n = \dim(E)$, F un sev de E, $p = \dim(F)$.

1) F admet au moins un supplémentaire dans E.

2) Tout supplémentaire de F dans E est de dimension $n-p$.

Preuve :

1) D'après Th.- Déf. 1 p. 228 et Prop. précédente, E admet au moins une base $\mathcal{B} = (e_1,\ldots,e_n)$, F admet au moins une base $\mathcal{C} = (f_1,\ldots,f_p)$, et $p \leqslant n$.

D'après le théorème de la base incomplète, forme forte (Th. 2 p. 229), quitte à permuter dans $\mathcal{B}$ et dans $\mathcal{C}$, la famille $\mathcal{B}' = (f_1,\ldots,f_p, e_{p+1},\ldots,e_n)$ est une base de E.

Notons $G = \text{Vect}\,(e_{p+1},\ldots,e_n)$, et montrons que G est un supplémentaire de F dans E.

• Soit $x \in E$. Il existe $(\lambda_1,\ldots,\lambda_n) \in K^n$ tel que $x = \sum_{i=1}^{p} \lambda_i f_i + \sum_{i=p+1}^{n} \lambda_i e_i$, d'où $x \in F + G$. Ceci montre : $F + G = E$.

• Soit $x \in F \cap G$. Il existe $(\lambda_1,\ldots,\lambda_n) \in K^n$ tel que $x = \sum_{i=1}^{p} \lambda_i f_i = \sum_{i=p+1}^{n} \lambda_i e_i$. On a alors $\sum_{i=1}^{p} \lambda_i f_i + \sum_{i=p+1}^{n} (-\lambda_i) e_i = 0$, d'où, puisque $\mathcal{B}'$ est libre :

$\lambda_1 = \ldots = \lambda_p = \lambda_{p+1} = \ldots = \lambda_n = 0$, et donc $x = 0$. Ceci montre : $F \cap G = \{0\}$.

Finalement, G est un supplémentaire de F dans E.

2) Soit H un supplémentaire de F dans E.

D'après Prop. 5 p. 230, H est de dimension finie. D'après Th.- Déf. 1 p. 228, F (resp. H) admet au moins une base $(F_1,\ldots,f_p)$ (resp. $(h_{p+1},\ldots,h_q)$).

Montrons que $\mathcal{F} = (f_1,\ldots,f_p,h_{p+1},\ldots,h_q)$ est une base de E.

• Soit $(\lambda_1,\ldots,\lambda_q) \in K^q$ tel que $\sum_{i=1}^{p} \lambda_i f_i + \sum_{i=p+1}^{q} \lambda_i h_i = 0$.

Alors : $\sum_{i=1}^{p} \lambda_i f_i = -\sum_{i=p+1}^{q} \lambda_i h_i \in F \cap G = \{0\}$, donc : $\sum_{i=1}^{p} \lambda_i f_i = 0$ et $\sum_{i=p+1}^{q} \lambda_i h_i = 0$, d'où $\lambda_1 = \ldots = \lambda_p = \lambda_{p+1} = \ldots = \lambda_q = 0$, puisque $(f_1,\ldots,f_p)$ et $(h_{p+1},\ldots,h_q)$ sont libres.

Ceci établit que $\mathcal{F}$ est libre.

• Soit $x \in E$. Puisque $E = F + H$, il existe $(f,h) \in F \times H$ tel que $x = f + h$. Puis il existe $(\lambda_1,\ldots,\lambda_p) \in K^p$ et $(\lambda_{p+1},\ldots,\lambda_q) \in K^{q-p}$ tels que $f = \sum_{i=1}^{p} \lambda_i f_i$ et $h = \sum_{i=p+1}^{q} \lambda_i h_i$.

On obtient $x = \sum_{i=1}^{p} \lambda_i f_i + \sum_{i=p+1}^{q} \lambda_i h_i$ ce qui montre que $\mathcal{F}$ engendre E. ∎

Remarque :

La preuve précédente établit plus précisément :

$$\text{Si } \left\{ \begin{array}{l} E \text{ est un } K\text{-ev de dimension finie} \\ F, G \text{ sont deux sev de } E \text{ supplémentaires dans } E \\ \mathcal{B} \text{ (resp. } \mathcal{C}) \text{ est une base de } F \text{ (resp. } G) \end{array} \right. , \text{ alors } \mathcal{B} \cup \mathcal{C} \text{ est une base de } E.$$

◆ **Corollaire 1** Soient E un K-ev de dimension finie, F, G deux sev de E en somme directe. On a alors :

$$\dim(F \oplus G) = \dim(F) + \dim(G).$$

Preuve :

Résulte de la Prop. 6 p. 231 appliquée à $F \oplus G$ au lieu de E.

Remarque :

Dans le Cor. 1, on peut remplacer l'hypothèse E de dimension finie par : F et G sont de dimension finie (la locution «de dimension finie» est invariable).

◆ **Corollaire 2** Soient E un K-ev de dimension finie, $n \in \mathbb{N}^*$, $F_1, \ldots, F_n$ des sev de E en somme directe. On a alors : $\dim\left(\bigoplus_{i=1}^{n} F_i\right) = \sum_{i=1}^{n} \dim(F_i)$.

Preuve :

Récurrence sur n.

- Le cas $n = 1$ est trivial, le cas $n = 2$ est le Cor. 1.
- Supposons la propriété établie pour un entier n, et soient $F_1, \ldots, F_{n+1}$ des sev de E en somme directe. Alors (cf. 6.3.3 Rem. *4)* p. 224) $F_1, \ldots, F_n$ sont en somme directe, et $\bigoplus_{i=1}^{n} F_i$ et F_{n+1} sont en somme directe, d'où : $\dim\left(\bigoplus_{i=1}^{n+1} F_i\right) = \dim\left(\left(\bigoplus_{i=1}^{n} F_i\right) \oplus F_{n+1}\right)$

$$\dim\left(\bigoplus_{i=1}^{n} F_i\right) + \dim(F_{n+1}) = \sum_{i=1}^{n} \dim(F_i) + \dim(F_{n+1}) = \sum_{i=1}^{n+1} \dim(F_i).$$

◆ **Corollaire 3** Soient E un K-ev de dimension finie, F, G deux sev de E.

$$\text{Si } \left\{ \begin{array}{l} F \subset G \\ \dim(F) = \dim(G) \end{array} \right. , \text{ alors } F = G.$$

Preuve :

F admet au moins un supplémentaire H dans G, et $\dim(H) = \dim(G) - \dim(F) = 0$, d'où $H = \{0\}$, $G = F + H = F$.

♦ **Théorème 3** Soit E un K-ev de dimension finie.
On a, pour tous sev F, G de E :

$$\dim(F+G) = \dim(F) + \dim(G) - \dim(F \cap G).$$

Preuve :
D'après Prop. 6 p. 231, $F \cap G$ admet au moins un supplémentaire F' dans F.

1) Montrons que F' et G sont en somme directe et que $F' \oplus G = F + G$.

- $F' \subset F$ d'où $F' \cap G = (F' \cap F) \cap G = F' \cap (F \cap G) = \{0\}$.
- $F + G = \big(F' + (F \cap G)\big) + G = F' + \big((F \cap G) + G\big) = F' + G$.

2) D'après Cor. 1 p. 232 : $\left\{ \begin{array}{l} \dim(F+G) = \dim(F' \oplus G) = \dim(F') + \dim G \\ \dim(F) = \dim\big(F' \oplus (F \cap G)\big) = \dim(F') + \dim(F \cap G) \end{array} \right.$,
d'où la relation voulue.

Remarque :
Dans le Th. précédent, on peut remplacer l'hypothèse E de dimension finie par : F et G sont de dimension finie.

♦ **Proposition 7** Soient E, F deux K-ev de dimension finie. Alors $E \times F$ est de dimension finie et : $\dim(E \times F) = \dim(E) + \dim(F)$.

Preuve :
D'après Th.- Déf. 1 p. 228, E et F admettent des bases finies $(e_1,\ldots,e_n)$, $(f_1,\ldots,f_p)$ respectivement, où $n = \dim(E)$, $p = \dim(F)$.
Montrons que $\mathcal{B} = \big((e_1,0),\ldots,(e_n,0),(0,f_1),\ldots,(0,f_p)\big)$ est une base de $E \times F$.

1) Soit $(\lambda_1,\ldots,\lambda_n,\mu_1,\ldots,\mu_p) \in K^{n+p}$ tel que $\sum_{i=1}^{n} \lambda_i (e_i,0) + \sum_{j=1}^{p} \mu_j (0,f_j) = 0$.

On a alors : $\left(\sum_{i=1}^{n} \lambda_i e_i, \sum_{j=1}^{p} \mu_j f_j\right) = (0,0)$, d'où : $\sum_{i=1}^{n} \lambda_i e_i = 0$ et $\sum_{j=1}^{p} \mu_j f_j = 0$,

et donc $\lambda_1 = \ldots = \lambda_n = \mu_1 = \ldots = \mu_p = 0$, puisque $(e_1,\ldots,e_n)$ et $(f_1,\ldots,f_p)$ sont libres.
Ceci montre que $\mathcal{B}$ est libre.

2) Soit $(x,y) \in E \times F$. puisque $(e_1,\ldots,e_n)$ et $(f_1,\ldots,f_p)$ engendrent respectivement E et F, il existe $(\lambda_1,\ldots,\lambda_n) \in K^n$ et $(\mu_1,\ldots,\mu_p) \in K^p$ tels que : $x = \sum_{i=1}^{n} \lambda_i e_i$, $y = \sum_{j=1}^{p} \mu_j f_j$.

On a alors : $(x,y) = \left(\sum_{i=1}^{n} \lambda_i e_i, \sum_{j=1}^{p} \mu_j f_j\right) = \sum_{i=1}^{n} \lambda_i (e_i,0) + \sum_{j=1}^{p} \mu_j (0,f_j)$.

Ceci montre que $\mathcal{B}$ engendre E.
Ainsi, $\mathcal{B}$ est une base de $E \times F$, donc $E \times F$ est de dimension finie et :

$$\dim(E \times F) = \mathrm{Card}(\mathcal{B}) = n + p = \dim(E) + \dim(F).$$

◆ **Corollaire** Soient $n \in \mathbb{N}^*, E_1, \ldots, E_n$ des K-ev de dimension finie. Alors $\prod_{i=1}^{n} E_i$ est de dimension finie et : $\dim\left(\prod_{i=1}^{n} E_i\right) = \sum_{i=1}^{n} \dim(E_i)$.

Preuve :

Récurrence immédiate à partir de la Prop. précédente. ∎

En particulier, pour tout n de $\mathbb{N}^*$, K^n est un K-ev de dimension finie et $\dim(K^n) = n$. La famille $(e_1, \ldots, e_n)$ d'éléments de K^n définie par $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ où le « 1 » est à la $i^{\text{ème}}$ place, $1 \leqslant i \leqslant n$, est une base de K^n, appelée base canonique de K^n.

Rang d'une famille finie de vecteurs

◆ **Définition 3** Soient E un K-ev, $\mathcal{F}$ une famille finie d'éléments de E. On appelle **rang** de $\mathcal{F}$, et on note $\text{rg}(\mathcal{F})$, l'entier naturel : $\text{rg}(\mathcal{F}) = \dim(\text{Vect}(\mathcal{F}))$.

◆ **Proposition 8** Pour toutes familles finies $\mathcal{F}, \mathcal{F}'$ d'éléments de E :

1) $\mathcal{F} \subset \mathcal{F}' \Longrightarrow \text{rg}(\mathcal{F}) \leqslant \text{rg}(\mathcal{F}')$

2) $\text{Max}\left(\text{rg}(\mathcal{F}), \text{rg}(\mathcal{F}')\right) \leqslant \text{rg}(\mathcal{F} \cup \mathcal{F}') \leqslant \text{rg}(\mathcal{F}) + \text{rg}(\mathcal{F}')$.

Preuve :

1) $\mathcal{F} \subset \mathcal{F}' \Longrightarrow \text{Vect}(\mathcal{F}) \subset \text{Vect}(\mathcal{F}') \Longrightarrow \dim(\text{Vect}(\mathcal{F})) \leqslant \dim\left(\text{Vect}(\mathcal{F}')\right)$.

2) $\begin{cases} \mathcal{F} \subset \mathcal{F} \cup \mathcal{F}' \\ \mathcal{F}' \subset \mathcal{F} \cup \mathcal{F}' \end{cases} \Longrightarrow \begin{cases} \text{rg}(\mathcal{F}) \leqslant \text{rg}(\mathcal{F} \cup \mathcal{F}') \\ \text{rg}(\mathcal{F}') \leqslant \text{rg}(\mathcal{F} \cup \mathcal{F}') \end{cases} \Longrightarrow \text{Max}\left(\text{rg}(\mathcal{F}), \text{rg}(\mathcal{F}')\right) \leqslant \text{rg}(\mathcal{F} \cup \mathcal{F}')$.

3) $\text{rg}(\mathcal{F} \cup \mathcal{F}') = \dim\left(\text{Vect}(\mathcal{F} \cup \mathcal{F}')\right) = \dim\left(\text{Vect}(\mathcal{F}) + \text{Vect}(\mathcal{F}')\right)$
$\leqslant \dim\left(\text{Vect}(\mathcal{F})\right) + \dim\left(\text{Vect}(\mathcal{F}')\right)$, en utilisant 6.3.2 Prop. 2 *4)* p. 220.

◆ **Proposition 9** Soient E un K-ev, $\mathcal{F}$ une famille finie d'éléments de E.

1) Le rang de $\mathcal{F}$ est le plus grand cardinal des sous-familles libres de $\mathcal{F}$

2) $\mathcal{F}$ est libre si et seulement si : $\text{Card}(\mathcal{F}) = \text{rg}(\mathcal{F})$.

Preuve :

1) • Puisque $\mathcal{F}$ est finie, Vect $(\mathcal{F})$ est de dimension finie. D'après Rem. p. 229, il existe une sous-famille $\mathcal{B}$ de $\mathcal{F}$ qui soit une base de Vect $(\mathcal{F})$, donc telle que $\text{Card}(\mathcal{B}) = \text{rg}(\mathcal{F})$.

• Soit $\mathcal{L}$ une sous-famille libre de $\mathcal{F}$. D'après Prop. 3 *1)* p. 229 :

$$\text{Card}(\mathcal{L}) \leqslant \dim\left(\text{Vect}(\mathcal{F})\right) = \text{rg}(\mathcal{F}).$$

2) • Si $\mathcal{F}$ est libre, d'après *1)* : $\text{rg}(\mathcal{F}) = \text{Card}(\mathcal{F})$.

• Réciproquement, si $\text{Card}(\mathcal{F}) = \text{rg}(\mathcal{F})$, comme $\mathcal{F}$ engendre Vect $(\mathcal{F})$, d'après Prop. 4 p. 230, $\mathcal{F}$ est une base de Vect $(\mathcal{F})$, et donc est libre.

EXEMPLE :

$K = \mathbb{R}$, $E = \mathbb{R}^3$, $\mathcal{F} = (V_i)_{1 \leqslant i \leqslant 4}$ où :

$$V_1 = (1,-1,1),\ V_2 = (-1,1,-1),\ V_3 = (0,1,1),\ V_4 = (1,0,2).$$

Comme (V_1, V_3) est libre et que $V_2 = -V_1$ et $V_4 = V_1 + V_3$, on a : $\operatorname{rg}(\mathcal{F}) = 2$.

Nous verrons plus loin (8.1.7 p. 281) un algorithme (*méthode de Gauss*) permettant de calculer le rang d'une famille finie de vecteurs.

Exercices

◇ **6.4.1** Montrer que l'ensemble F défini par $F = \left\{(x,y,z) \in \mathbb{C}^3;\ \begin{cases} x+y+z=0 \\ x+\mathrm{i}y-z=0 \end{cases}\right\}$ est un sev de $\mathbb{C}^3$, et en déterminer une base et la dimension.

◇ **6.4.2** Déterminer une base et la dimension du sev F de $\mathbb{R}^{]-1;1[}$ engendré par $(f_i)_{1 \leqslant i \leqslant 4}$ où, pour tout x de $]-1;1[$:

$$f_1(x) = \sqrt{\frac{1-x}{1+x}},\ f_2(x) = \sqrt{\frac{1+x}{1-x}},\ f_3(x) = \frac{1}{\sqrt{1-x^2}},\ f_4(x) = \frac{x}{\sqrt{1-x^2}}.$$

◇ **6.4.3** Dans $\mathbb{R}^4$, soient $u = (1,0,1,0)$, $v = (0,1,-1,0)$, $w = (1,1,1,1)$, $x = (0,0,1,0)$, $y = (1,1,0,-1)$, $F = \text{Vect}\,(u,v,w)$, $G = \text{Vect}\,(x,y)$. Quelles sont les dimensions de F, G, $F+G$, $F \cap G$?

◇ **6.4.4** Soient E un K-ev de dimension finie, F un sev de E tel que $F \neq \{0\}$ et $F \neq E$. Montrer que F admet au moins deux supplémentaires différents dans E.

◇ **6.4.5** Soient E un K-ev de dimension finie, F, G deux sev de E. Montrer que deux quelconques des trois propriétés suivantes entraînent la troisième :

1) $F \cap G = \{0\}$ *2)* $F + G = E$ *3)* $\dim(F) + \dim(G) = \dim(E)$.

◇ **6.4.6** Soient E, F deux K-ev. Montrer que, si $E \times F$ est de dimension finie, alors E et F sont de dimension finie.

◇ **6.4.7** Pour $a \in \mathbb{R}$, on note $f_a : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \cos(x+a) \end{array}$.

Soit $(a_1,a_2,a_3) \in \mathbb{R}^3$; déterminer le rang de $(f_{a_1}, f_{a_2}, f_{a_3})$ dans $\mathbb{R}^{\mathbb{R}}$ muni des lois usuelles.

◇ **6.4.8** Soient E un K-ev de dimension finie, $\mathcal{F}$ une famille finie d'éléments de E. Montrer que les propriétés suivantes sont équivalentes :

1) $\mathcal{F}$ est une base de E

2) $\begin{cases} \mathcal{F} \text{ est génératrice de } E \\ \text{Pour toute famille génératrice } \mathcal{G} \text{ de } E : \quad \mathcal{G} \subset \mathcal{F} \Longrightarrow \mathcal{G} = \mathcal{F} \\ \text{(on dit que } \mathcal{F} \text{ est une } \textit{famille génératrice minimale} \text{ de } E) \end{cases}$

3) $\begin{cases} \mathcal{F} \text{ est libre} \\ \text{Pour toute famille libre } \mathcal{L} \text{ de } E : \quad \mathcal{F} \subset \mathcal{L} \Longrightarrow \mathcal{F} = \mathcal{L} \\ \text{(on dit que } \mathcal{F} \text{ est une } \textit{famille libre maximale} \text{ de } E). \end{cases}$

◇ **6.4.9** Soit E un K-ev de dimension finie.

a) Montrer que, pour toute famille génératrice finie $\mathcal{G}$ de E, il existe une base $\mathcal{B}_1$ de E telle que $\mathcal{B}_1 \subset \mathcal{G}$.

b) Montrer que, pour toute famille libre $\mathcal{L}$ de E, il existe une base $\mathcal{B}_2$ de E telles que $\mathcal{L} \subset \mathcal{B}_2$.

c) Montrer que, pour toute famille génératrice finie $\mathcal{G}$ de E et toute famille libre $\mathcal{L}$ de E telles que $\mathcal{L} \subset \mathcal{G}$, il existe une base $\mathcal{B}_3$ de E telle que $\mathcal{L} \subset \mathcal{B}_3 \subset \mathcal{G}$.

d) Montrer que, pour toute famille génératrice finie $\mathcal{G}$ de E et toute famille libre $\mathcal{L}$ de E, il existe une base $\mathcal{B}_4$ de E telle que $\mathcal{L} \subset \mathcal{B}_4 \subset \mathcal{L} \cup \mathcal{G}$.

◇ **6.4.10** On note $A = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6};\ (a,b,c,d) \in \mathbb{Q}^4\}$.

a) Montrer que A est une $\mathbb{Q}$-algèbre pour les lois usuelles (la 3$^{\text{ème}}$ loi étant la multiplication).

b) Montrer que A est un $\mathbb{Q}$-ev de dimension finie et que $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ en est une base.

c) Démontrer que A est un sous-corps de $\mathbb{R}$.

Exemple : décomposer l'inverse de $4 + 3\sqrt{2} - 2\sqrt{3} - \sqrt{6}$ sur la base $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ de A.

Chapitre 7

Applications linéaires

Dans ce ch.7, K désigne un corps commutatif. En pratique : $K = \mathbb{R}$ ou $\mathbb{C}$.
On abrège espace vectoriel en ev, et sous-espace vectoriel en sev.

7.1 Généralités

7.1.1 Définitions

♦ **Définition 1**

1) Soient E, F deux K-ev; une application $f : E \longrightarrow F$ est dite **linéaire** (ou : **K-linéaire**; ou : est un **morphisme de K-ev**) si et seulement si :

$$\begin{cases} \forall (x,y) \in E^2, & f(x+y) = f(x) + f(y) \\ \forall \lambda \in K, \forall x \in E, & f(\lambda x) = \lambda f(x). \end{cases}$$

On note $\mathcal{L}(E,F)$ (ou : $\mathcal{L}_K(E,F)$) l'ensemble des applications linéaires de E dans F.

2) Soient E un K-ev, $f : E \longrightarrow E$ une application. On dit que f est un **endomorphisme** de E si et seulement si f est linéaire.
On note $\mathcal{L}(E)$ (ou : $\mathcal{L}_K(E)$) l'ensemble des endomorphismes de E.

On a donc : $\mathcal{L}(E) = \mathcal{L}(E,E)$.

Remarque :
Pour toute f de $\mathcal{L}(E,F)$, $f(0) = 0$ car : $f(0) = f(0+0) = f(0) + f(0)$; cf. aussi 2. 2. 3 Prop. 1 *1)* p. 52.

♦ **Définition 2**

1) Soient E, F deux K-ev, $f : E \longrightarrow F$ une application. On dit que f est un **isomorphisme** de E sur F si et seulement si f est linéaire et bijective.

2) Soient E un K-ev, $f : E \longrightarrow E$ une application. On dit que f est un **automorphisme** de E si et seulement si f est linéaire et bijective.
On note $\mathcal{GL}(E)$ (ou : $\mathcal{GL}_K(E)$) l'ensemble des automorphismes de l'ev E.

◆ **Définition 3** Soient E un K-ev. On appelle **forme linéaire** sur E toute application linéaire φ de E dans K. On note E^* l'ensemble des formes linéaires sur E; E^* est appelé le **dual** de E.

On a donc : $E^* = \mathcal{L}(E,K)$.

◆ **Proposition 1** Soient E,F deux K-ev, $f : E \longrightarrow F$ une application; f est linéaire si et seulement si :

$$\forall \lambda \in K, \forall (x,y) \in E^2, \ f(\lambda x + y) = \lambda f(x) + f(y).$$

Preuve :

1) Si f est linéaire, alors, pour tout (λ,x,y) de $K \times E \times E$:

$$f(\lambda x + y) = f(\lambda x) + f(y) = \lambda f(x) + f(y).$$

2) Réciproquement, si la condition précédente est satisfaite, alors :

- en prenant $\lambda = 1$, on obtient $f(x + y) = f(x) + f(y)$
- en prenant $y = 0$, on obtient $f(\lambda x) = \lambda f(x)$, et donc f est linéaire.

◆ **Proposition 2** Soient E,F deux K-ev, $f \in \mathcal{L}(E,F)$. On a, pour tous n de $\mathbb{N}^*$, $(\lambda_1,\ldots,\lambda_n)$ de K^n, $(x_1,\ldots,x_n)$ de E^n :

$$f\left(\sum_{i=1}^{n} \lambda_i x_i\right) = \sum_{i=1}^{n} \lambda_i f(x_i).$$

Preuve :

Récurrence sur n.

La propriété est immédiate pour $n = 1$; et pour $n = 2$:

$$f(\lambda_1 x_1 + \lambda_2 x_2) = f(\lambda_1 x_1) + f(\lambda_2 x_2) = \lambda_1 f(x_1) + \lambda_2 f(x_2).$$

Si la propriété est vraie pour un n de $\mathbb{N}^*$, alors, pour tous $(\lambda_1,\ldots,\lambda_{n+1})$ de K^{n+1} et $(x_1,\ldots,x_{n+1})$ de E^{n+1} :

$$\begin{aligned} f\left(\sum_{i=1}^{n+1} \lambda_i x_i\right) &= f\left(\sum_{i=1}^{n} \lambda_i x_i + \lambda_{n+1} x_{n+1}\right) \\ &= f\left(\sum_{i=1}^{n} \lambda_i x_i\right) + f\left(\lambda_{n+1} x_{n+1}\right) \\ &= \sum_{i=1}^{n} \lambda_i f(x_i) + \lambda_{n+1} f(x_{n+1}) = \sum_{i=1}^{n+1} \lambda_i f(x_i). \end{aligned}$$

■

On déduit le Corollaire suivant :

♦ **Corollaire** Soient E un K-ev de dimension finie, F un K-ev, $\mathcal{B} = (e_1,\ldots,e_n)$ une base de E, $f \in \mathcal{L}(E,F)$, $x \in E$, $(x_1,\ldots,x_n)$ les composantes de x dans la base $\mathcal{B}$ (c'est-à-dire : $x = \sum_{i=1}^{n} x_i e_i$). On a alors :

$$f(x) = \sum_{i=1}^{n} x_i f(e_i).$$

Autrement dit, une application linéaire est entièrement déterminée par les images des vecteurs d'une base.

Remarque :

Le Corollaire précédent se généralise au cas où E n'est pas de dimension finie, en utilisant la notion de «somme à support fini», ce qui dépasse le cadre de cet ouvrage. ■

EXEMPLES :

1) **Homothéties**

Soit E un K-ev. Pour tout α de K, on appelle **homothétie (vectorielle) de rapport** α l'application $h_\alpha : \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & \alpha x \end{array}$; il est clair que : $h_\alpha \in \mathcal{L}(E)$.

En particulier : $h_0 = 0$, $h_1 = \mathrm{Id}_E$. Pour alléger les écritures, on notera souvent e au lieu de Id_E.

2) **Projecteurs**

Soient E un K-ev, F,G deux sev de E supplémentaires dans E : $E = F \oplus G$.

Pour tout x de E, il existe $(x',x'') \in F \times G$ unique tel que $x = x' + x''$.

L'application $p : \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & x' \end{array}$ est un endomorphisme de E. En effet, si $\lambda \in K$ et $(x,y) \in E^2$, il existe $(x',x'') \in F \times G$ et $(y',y'') \in F \times G$ tels que $x = x' + x''$ et $y = y' + y''$, d'où :

$$\begin{cases} \lambda x + y = \lambda(x' + x'') + (y' + y'') = (\lambda x' + y') + (\lambda x'' + y'') \\ (\lambda x' + y',\ \lambda x'' + y'') \in F \times G, \end{cases}$$

et donc $p(\lambda x + y) = \lambda x' + y' = \lambda p(x) + p(y)$.

L'application $p : \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & x' \end{array}$ est appelée le **projecteur sur** F **parallèlement à** G.

Il est clair que l'application $q : \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & x'' \end{array}$ est le projecteur sur G parallèlement à F.

On a : $q = e - p$, c'est-à-dire : $\forall x \in E,\ q(x) = x - p(x)$.

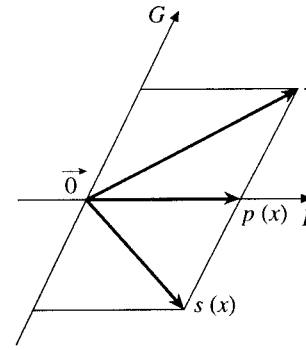
3) **Symétries**

Soient E un K-ev, F, G deux sev de E supplémentaires dans E : $E = F \oplus G$. Notons p le projecteur sur F parallèlement à G.

L'application $s = 2p - e$, définie par :

$$\begin{array}{rcl} s : E & \longrightarrow & E \\ x & \longmapsto & 2p(x) - x \end{array}$$

est un endomorphisme de E, appelé **symétrie par rapport à F parallèlement à G.**



4) **Inclusion canonique**

Soient E un K-ev , F un sev de E. L'**inclusion** (ou : **injection canonique**) $\mathrm{i}_{F,E} : \begin{array}{c} F \longrightarrow E \\ x \longmapsto x \end{array}$ (cf. 1.3.1 Exemple *2)* p. 24) est linéaire.

5) **Projections canoniques**

Soient $n \in \mathbb{N}^*$, $E_1, \ldots, E_n$ des K-ev. Pour chaque i de $\{1, \ldots, n\}$, la $i^{\text{ème}}$ **projection canonique** $\mathrm{pr}_i : \begin{array}{c} E_1 \times \ldots \times E_n \longrightarrow E_i \\ (x_1, \ldots, x_n) \longmapsto x_i \end{array}$ (cf. 1.3.1 Exemple *6)* p. 25) est linéaire.

6) **Evaluations**

Soient X un ensemble non vide, F un K-ev. Pour chaque a de X, l'application $E_a : \begin{array}{c} F^X \longrightarrow F \\ \varphi \longmapsto \varphi(a) \end{array}$, appelée **évaluation en a**, est linéaire car :

$$\forall \lambda \in K, \forall \varphi, \psi \in F^X, \; E_a(\lambda\varphi + \psi) = (\lambda\varphi + \psi)(a) = \lambda\varphi(a) + \psi(a) = \lambda E_a(\varphi) + E_a(\psi).$$

7) **Opérateur de dérivation**

Soient I un intervalle de $\mathbb{R}$, non vide et non réduit à un point, $D^1(I, \mathbb{R})$ le $\mathbb{R}$-ev des applications de I dans $\mathbb{R}$ dérivables sur I. L'application $D : \begin{array}{c} D^1(I,\mathbb{R}) \longrightarrow \mathbb{R}^I \\ f \longmapsto f' \end{array}$ est linéaire (cf. Tome 1, 5.1.3 Th. 1).

8) **Intégration**

Soient $(a,b) \in \mathbb{R}^2$ tel que $a \leqslant b$, $\mathcal{CM}$ le $\mathbb{R}$-ev des applications de $[a;b]$ dans $\mathbb{R}$ continues par morceaux (cf. Tome 1, 6.2.1 Prop. 1). L'application $\mu : \begin{array}{c} \mathcal{CM} \longrightarrow \mathbb{R} \\ f \longmapsto \int_a^b f \end{array}$ est linéaire (cf. Tome 1, 6.2.4 Prop.).

Algèbres

♦ **Définition 4**

1) Soient A, B deux K- algèbres (la $3^{\text{ème}}$ loi étant notée multiplicativement); une application $f : A \longrightarrow B$ est appelée **morphisme d'algèbres** si et seulement si :

$$\begin{cases} \forall (x,y) \in A^2, & f(x+y) = f(x) + f(y) \\ \forall \lambda \in K, \forall x \in A, & f(\lambda x) = \lambda f(x) \\ \forall (x,y) \in A^2, & f(xy) = f(x) f(y). \end{cases}$$

2) Soient A un K-algèbre, $f : A \longrightarrow A$ une application. On dit que f est un **endomorphisme de l'algèbre** A si et seulement si f est un morphisme d'algèbres de A dans A.

Remarque :

Avec les notations de *1)* ci-dessus, f est un morphisme d'algèbres si et seulement si :

$$\begin{cases} f \text{ est linéaire (de l'ev } A \text{ dans l'ev } B) \\ f \text{ est un morphisme pour la } 3^{\text{ème}} \text{ loi.} \end{cases}$$

♦ **Définition 5**

1) Soient A, B deux K-algèbres, $f : A \longrightarrow B$ une application. On dit que f est un **isomorphisme d'algèbres** de A sur B si et seulement si f est un morphisme d'algèbres et est bijective.

2) Soient A une K-algèbre, $f : A \longrightarrow A$ une application. On dit que f est un **automorphisme de l'algèbre** A si et seulement si f est un endomorphisme de l'algèbre A et est bijective.

7.1.2 Noyau, image

♦ **Proposition 1** Soient E, F deux K-ev, $f \in \mathcal{L}(E,F)$.

1) Pout tout sev F_1 de F, l'image réciproque $f^{-1}(F_1)$ est un sev de E.

2) Pour tout sev E_1 de E, l'image directe $f(E_1)$ est un sev de F.

Rappelons (cf. 1.3.5 Déf. p. 32) :

- $f^{-1}(F_1) = \{x \in E;\ f(x) \in F_1\}$
- $f(E_1) = \{y \in F;\ \exists x \in E_1,\ y = f(x)\}$.

Preuve :

1) • $f^{-1}(F_1) \neq \varnothing$: $0 \in f^{-1}(F_1)$ car $f(0) = 0 \in F_1$.

• Soient $\lambda \in K$, $(x,y) \in \left(f^{-1}(F_1)\right)^2$. On a : $(f(x), f(y)) \in (F_1)^2$ d'où : $f(\lambda x + y) = \lambda f(x) + f(y) \in F_1$, et donc $\lambda x + y \in f^{-1}(F_1)$.

2) • $f(E_1) \neq \varnothing$: $0 \in f(E_1)$ car $0 = f(0)$.

• Soient $\lambda \in K$, $(x',y') \in (f(E_1))^2$. Il existe $(x,y) \in (E_1)^2$ tel que $x' = f(x)$ et $y' = f(y)$. On a alors $\lambda x' + y' = \lambda f(x) + f(y) = f(\lambda x + y) \in f(E_1)$. ∎

Rappelons que, d'après 1.3.1 Déf. 3 p. 25, un sev V d'un ev E est dit **stable** par un endomorphisme f de E si et seulement si : $f(V) \subset V$. ∎

◆ **Définition** Soient E,F deux K-ev, $f \in \mathcal{L}(E,F)$. On appelle **noyau** de f, et on note $\mathrm{Ker}(f)$, le sev de E définie par :

$$\mathrm{Ker}(f) = f^{-1}(\{0\}) = \{x \in E;\ f(x) = 0\}.$$

On appelle **image** de f, et on note $\mathrm{Im}(f)$, le sev de F défini par :

$$\mathrm{Im}(f) = f(E) = \{y \in F; \exists x \in E,\ y = f(x)\}.$$

◆ **Proposition 2** Soient E,F deux K-ev, $f \in \mathcal{L}(E,F)$.

1) f est injective si et seulement si $\mathrm{Ker}(f) = \{0\}$.

2) f est surjective si et seulement si $\mathrm{Im}(f) = F$.

Preuve :

1) • Supposons f injective, et soit $x \in \mathrm{Ker}(f)$. Alors $f(x) = 0 = f(0)$, d'où, puisque f est injective : $x = 0$. Ainsi : $\mathrm{Ker}(f) = \{0\}$.

• Réciproquement, supposons $\mathrm{Ker}(f) = \{0\}$, et soit $(x,y) \in E^2$ tel que $f(x) = f(y)$. Alors : $f(x-y) = f(x) - f(y) = 0$, donc $x - y \in \mathrm{Ker}(f) = \{0\}$, d'où $x = y$.

Ceci montre que f est injective.

2) (f surjective) $\iff \big(\forall y \in F,\ \exists x \in E,\ y = f(x)\big) \iff f(E) = F \iff \mathrm{Im}(f) = F$.

7.1.3 Applications linéaires et familles de vecteurs

Dans ce § 7.1.3 :

- E,F désignent deux K-ev
- $f \in \mathcal{L}(E,F)$
- $\mathcal{F} = (x_1,\ldots,x_n)$ est une famille finie d'éléments de E.

◆ **Proposition 1** Pour toute f de $\mathcal{L}(E,F)$ et toute famille finie $\mathcal{F}$ d'éléments de E :

$$f\big(\mathrm{Vect}\,(\mathcal{F})\big) = \mathrm{Vect}\,\big(f(\mathcal{F})\big).$$

Preuve :

1) Soit $y \in f\big(\mathrm{Vect}\,(\mathcal{F})\big)$. Il existe $x \in \mathrm{Vect}\,(\mathcal{F})$ tel que $y = f(x)$, puis il existe $(\lambda_i)_{1 \leqslant i \leqslant n} \in K^n$ tel que $x = \sum_{i=1}^{n} \lambda_i x_i$. On a alors :

$$y = f(x) = f\left(\sum_{i=1}^{n} \lambda_i x_i\right) = \sum_{i=1}^{n} \lambda_i f(x_i) \in \mathrm{Vect}\,(f(\mathcal{F})).$$

Ceci montre : $f\big(\mathrm{Vect}\,(\mathcal{F})\big) \subset \mathrm{Vect}\,\big(f(\mathcal{F})\big)$.

2) L'inclusion réciproque se montre de façon analogue.

♦ **Corollaire** Si $f \in \mathcal{L}(E,F)$ est surjective et si $\mathcal{F}$ engendre E, alors $f(\mathcal{F})$ engendre F.

Preuve : $F = f(E) = f\big(\text{Vect}\,(\mathcal{F})\big) = \text{Vect}\,\big(f(\mathcal{F})\big)$.

♦ **Proposition 2** Soient $f \in \mathcal{L}(E,F)$ et $\mathcal{F}$ une famille d'éléments de E.

1) Si $\mathcal{F}$ est liée, alors $f(\mathcal{F})$ est liée.

2) Si $f(\mathcal{F})$ est libre, alors $\mathcal{F}$ est libre.

Preuve :

1) Puisque $\mathcal{F}$ est liée, il existe $(\lambda_1,\ldots,\lambda_n) \in K^n - \{(0,\ldots,0)\}$ tel que $\sum_{i=1}^{n} \lambda_i x_i = 0$.

On a alors : $\sum_{i=1}^{n} \lambda_i f(x_i) = f\left(\sum_{i=1}^{n} \lambda_i x_i\right) = f(0) = 0$, et donc $f(\mathcal{F})$ est liée.

2) Se déduit de *1)* par contre-apposition.

♦ **Proposition 3** Soient $f \in \mathcal{L}(E,F)$, $\mathcal{F}$ une famille d'éléments de E. Si f est injective et si $\mathcal{F}$ est libre, alors $f(\mathcal{F})$ est libre.

Preuve :

Soit $(\lambda_1,\ldots,\lambda_n) \in K^n$ tel que $\sum_{i=1}^{n} \lambda_i f(x_i) = 0$. Alors : $f\left(\sum_{i=1}^{n} \lambda_i x_i\right) = \sum_{i=1}^{n} \lambda_i f(x_i) = 0$,

d'où, puisque f est injective : $\sum_{i=1}^{n} \lambda_i x_i = 0$. Enfin, comme $\mathcal{F}$ est libre : $\forall i \in \{1,\ldots,n\}, \lambda_i = 0$.

♦ **Proposition 4** Soient E un K-ev de dimension finie, F un K-ev, $f \in \mathcal{L}(E,F)$. Les propriétés suivantes sont deux à deux équivalentes :

(i) f est bijective

(ii) Pour toute base $\mathcal{B}$ de E, $f(\mathcal{B})$ est une base de F

(iii) Il existe une base $\mathcal{B}$ de E telle que $f(\mathcal{B})$ soit une base de F.

Preuve :

(i) $\Longrightarrow$ (ii) :

On suppose f bijective. Soit $\mathcal{B}$ une base de E. Puisque f est surjective et $\mathcal{B}$ génératrice de E, $f(\mathcal{B})$ est génératrice de F (cf. Cor.). Puisque f est injective et $\mathcal{B}$ libre, $f(\mathcal{B})$ est libre (cf. Prop. 3).

(ii) $\Longrightarrow$ (iii) :

Résulte de l'existence d'une base de E (cf. 6.4 Th.- Déf. 1 p. 228).

(iii) $\Longrightarrow$ (i) :

Supposons qu'il existe une base $\mathcal{B} = (e_1,\ldots,e_n)$ de E telle que $f(\mathcal{B}) = \big(f(e_1),\ldots,f(e_n)\big)$ soit une base de F.

• Soit $x \in \text{Ker}(f)$. Il existe $(x_1,\ldots,x_n) \in K^n$ tel que $x = \sum_{i=1}^{n} x_i e_i$. On a :

$$0 = f(x) = f\left(\sum_{i=1}^{n} x_i e_i\right) = \sum_{i=1}^{n} x_i f(e_i),$$

donc, puisque $f(\mathcal{B})$ est libre : $\forall i \in \{1,\ldots,n\}, x_i = 0$, d'où $x = 0$.
Ainsi, $\text{Ker}(f) = \{0\}$, et donc f est injective.

• Soit $y \in F$.

Puisque $f(\mathcal{B})$ engendre F, il existe $(x_1,\ldots,x_n) \in K^n$ tel que $y = \sum_{i=1}^{n} x_i f(e_i)$, d'où $y = f\left(\sum_{i=1}^{n} x_i e_i\right) \in \text{Im}(f)$.

Ceci montre que f est surjective. Finalement, f est bijective. ∎

Remarque :

Les résultats de ce § 7.1.3 sont valables plus généralement pour toute famille $\mathcal{F}$ d'éléments de E (non nécessairement finie).

Exercices

◇ **7.1.1** Soient E, F deux K-ev, $f \in \mathcal{L}(E,F)$, A, B deux sev de E. Montrer :

$$f(A) \subset f(B) \Longleftrightarrow A + \text{Ker}(f) \subset B + \text{Ker}(f).$$

◇ **7.1.2** Soient E, F deux K-ev, G un sev de $E \times F$ tel que : $\forall a \in E, \exists! b \in F, (a,b) \in G$.
On note $f : \begin{array}{ccc} E & \longrightarrow & F \\ a & \longmapsto & b \end{array}$ définie ci-dessus.
Montrer que f est linéaire.

◇ **7.1.3** Montrer que $f : \begin{array}{ccc} \mathbb{R}[X] & \longrightarrow & \mathbb{R}[X] \\ P & \longmapsto & P - XP' \end{array}$ est linéaire, et déterminer $\text{Ker}(f)$ et $\text{Im}(f)$.

◇ **7.1.4** Soient $n \in \mathbb{N}$, $E = K_n[X]$ le K-ev des polynômes de degré $\leqslant n$, $f : \begin{array}{ccc} E & \longrightarrow & E \\ P & \longmapsto & P - P' \end{array}$.
Montrer que f est un automorphisme de E et exprimer f^{-1}.

◇ **7.1.5** Soient $T \in \mathbb{R}_+^*$, E l'ensemble des applications de $\mathbb{R}$ dans $\mathbb{R}$, T-périodiques et de classe C^∞.
a) Vérifier que E est un $\mathbb{R}$-ev (pour les lois usuelles) et que : $\forall f \in E, f' \in E$.
b) On note $\phi : \begin{array}{ccc} E & \longrightarrow & E \\ f & \longmapsto & f' \end{array}$. Vérifier que ϕ est linéaire, et déterminer $\text{Ker}(\phi)$ et $\text{Im}(\phi)$.

◇ **7.1.6*** Soient E un K-ev, $f \in \mathcal{L}(E)$ tel que, pour tout x de E, $(x, f(x))$ est liée. Démontrer que f est une homothétie.

◇ **7.1.7** Soient E un K-ev, $f \in \mathcal{L}(E)$, $n \in \mathbb{N}^*$, $\lambda_1,\ldots,\lambda_n \in K$ deux à deux distincts; on note $N_i = \text{Ker}(f - \lambda_i e)$ pour $1 \leqslant i \leqslant n$, où $e = \text{Id}_E$.
Démontrer que les sev N_i ($1 \leqslant i \leqslant n$) sont linéairement indépendants (c'est-à-dire :

$$\forall (x_1,\ldots,x_n) \in F_1 \times \ldots \times F_n, \quad (x_1 + \ldots + x_n = 0 \Longrightarrow x_1 = \ldots = x_n = 0),$$

cf. 6.3.3 Déf. 2 p. 221).

7.2 Opérations sur les applications linéaires

7.2.1 L'espace vectoriel $\mathcal{L}(E,F)$

♦ **Proposition**

$\mathcal{L}(E,F)$ est un K-ev pour les lois usuelles.

Rappelons (cf. 6.1 Exemple *4)* p. 208) que les lois usuelles sur F^E sont définies par :

$$\begin{cases} \forall f,g \in F^E, \forall x \in E, \ (f+g)(x) = f(x) + g(x) \\ \forall \lambda \in K, \ \forall f \in F^E, \ (\lambda f)(x) = \lambda f(x). \end{cases}$$

Preuve :

Nous allons montrer que $\mathcal{L}(E,F)$ est un sev de F^E.

1) $\mathcal{L}(E,F) \neq \varnothing$, puisque l'application nulle $0 : \begin{array}{ccc} E & \longrightarrow & F \\ x & \longmapsto & 0 \end{array}$ est à l'évidence linéaire.

2) Soient $\alpha \in K$, $f,g \in \mathcal{L}(E,F)$. On a, pour tous λ de K et x,y de E :

$$\begin{aligned} (\alpha f + g)(\lambda x + y) &= \alpha f(\lambda x + y) + g(\lambda x + y) = \alpha\big(\lambda f(x) + f(y)\big) + \big(\lambda g(x) + g(y)\big) \\ &= \lambda\big(\alpha f(x) + g(x)\big) + \big(\alpha f(y) + g(y)\big) = \lambda(\alpha f + g)(x) + (\alpha f + g)(y). \end{aligned}$$

Ceci montre que $\alpha f + g$ est linéaire, donc $\alpha f + g \in \mathcal{L}(E,F)$.

7.2.2 Composition

♦ **Proposition 1** Soient E,F,G trois K-ev. On a :

$$\forall f \in \mathcal{L}(E,F), \forall g \in \mathcal{L}(F,G), \ g \circ f \in \mathcal{L}(E,G).$$

Preuve : $\forall \lambda \in K, \forall (x,y) \in E^2$,

$$\begin{aligned} (g \circ f)(\lambda x + y) &= g\big(f(\lambda x + y)\big) = g\big(\lambda f(x) + f(y)\big) \\ &= \lambda g\big(f(x)\big) + g\big(f(y)\big) = \lambda(g \circ f)(x) + (g \circ f)(y) \end{aligned}$$ ■

Autrement dit : la composée de deux applications linéaires est linéaire.

♦ **Proposition 2** Soient E,F,G trois K-ev. On a :

1) $\forall f_1, f_2 \in \mathcal{L}(E,F), \forall g \in \mathcal{L}(F,G), \ g \circ (f_1 + f_2) = g \circ f_1 + g \circ f_2$
(pseudo-distributivité à gauche)

2) $\forall f \in \mathcal{L}(E,F), \ \forall g_1, g_2 \in \mathcal{L}(F,G), (g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f$
(pseudo-distributivité à droite)

3) $\forall \alpha \in K, \forall f \in \mathcal{L}(E,F), \forall g \in \mathcal{L}(F,G), \ (\alpha g) \circ f = g \circ (\alpha f) = \alpha(g \circ f)$.

Preuve :

Les vérifications sont «automatiques »

1) $\forall x \in E$,

$$\begin{aligned}(g\circ(f_1+f_2))(x) &= g\big((f_1+f_2)(x)\big) = g\big(f_1(x)\big)+g\big(f_2(x)\big)\\ &= (g\circ f_1)(x)+(g\circ f_2)(x) = (g\circ f_1+g\circ f_2)(x).\end{aligned}$$

2) $\forall x \in E$,

$$\begin{aligned}\big((g_1+g_2)\circ f\big)(x) &= (g_1+g_2)\big(f(x)\big) = g_1\big(f(x)\big)+g_2\big(f(x)\big)\\ &= (g_1\circ f)(x)+(g_2\circ f)(x) = (g_1\circ f+g_2\circ f)(x).\end{aligned}$$

3) $\forall x \in E$,

$$\begin{cases}\big((\alpha g)\circ f\big)(x) = (\alpha g)\big(f(x)\big) = \alpha g\big(f(x)\big) = \alpha(g\circ f)(x) = \big(\alpha(g\circ f)\big)(x)\\ \big(g\circ(\alpha f)\big)(x) = g\big(\alpha f(x)\big) = \alpha g\big(f(x)\big).\end{cases}$$

■

Remarque :

- La formule *1)* utilise la linéarité de g, mais non celles de f_1 et f_2
- La formule *2)* n'utilise pas de linéarité (de g_1, g_2, f)
- La formule $(\alpha g)\circ f = \alpha(g\circ f)$ n'utilise pas de linéarité
- La formule $g\circ(\alpha f) = \alpha(g\circ f)$ utilise la linéarité de g mais non celle de f.

◆ **Proposition 3** Soient E, F deux K-ev, $f \in \mathcal{L}(E,F)$. Si f est un isomorphisme de E sur F, alors f^{-1} est un isomorphisme de F sur E.

Preuve :

Supposons que f soit linéaire et bijective, et montrons que $f^{-1} : F \longrightarrow E$, qui est déjà bijective (cf. 1.3.2 Prop. 3 p. 28), est linéaire.

Soient $\lambda \in K, (x', y') \in F^2$. On a :

$$\begin{aligned}f^{-1}(\lambda x'+y') &= f^{-1}\left(\lambda f(f^{-1}(x'))+f(f^{-1}(y'))\right)\\ &= f^{-1}\left(f\left(\lambda f^{-1}(x')+f^{-1}(y')\right)\right) = \lambda f^{-1}(x')+f^{-1}(y'),\end{aligned}$$

et donc f^{-1} est linéaire. Cf. aussi 2.1 Prop. 5 *3)* p. 43.

◆ **Définition 1** Deux K-ev E, F sont dits **isomorphes** si et seulement s'il existe un isomorphisme de K-ev de E sur F.

Remarque :

La relation «être isomorphe à » entre K-ev est une relation d'équivalence dans tout ensemble de K-ev (mais il n'existe pas d'*ensemble* de tous les K-ev).

◆ **Proposition 4**

1) Soient E, F deux K-ev de dimension finie. Pour que E et F soient isomorphes, il faut et il suffit que : $\dim(E) = \dim(F)$.

2) Soit $n \in \mathbb{N}^*$. Tout K-ev de dimension finie n est isomorphe à K^n.

Preuve :

1) • Supposons E et F isomorphes. Il existe un isomorphisme f de E sur F. L'ev E admet au moins une base $\mathcal{B}$ et donc (cf. 7.1.3 Prop. 4 p. 243), $f(\mathcal{B})$ est une base de F, d'où :

$$\dim(F) = \mathrm{Card}\big(f(\mathcal{B})\big) = \mathrm{Card}(\mathcal{B}) = \dim(E).$$

• Réciproquement, supposons $\dim(E) = \dim(F)$. Alors E (resp. F) admet une base $\mathcal{B} = (e_1,\ldots,e_n)$ (resp. $\mathcal{C} = (e'_1,\ldots,e'_n)$), où $n = \dim(E) \in \mathbb{N}$.

Considérons $f \in \mathcal{L}(E,F)$, $g \in \mathcal{L}(F,E)$ définies par :

$$\forall i \in \{1,\ldots,n\},\ (f(e_i) = e'_i \quad \text{et} \quad g(e'_i) = e_i).$$

Il est clair que : $g \circ f = \mathrm{Id}_E$ et $f \circ g = \mathrm{Id}_F$, donc (cf. 1.3.2 Prop. 5 p. 28), f et g sont bijectives, réciproques l'une de l'autre. Ainsi, f est un isomorphisme de K-ev de E sur F.

2) Résulte de *1)*, puisque $\dim(E) = \dim(K^n) = n$.

♦ **Proposition 5**

$(\mathcal{L}(E),+,\cdot,\circ)$ est une K-algèbre associative unitaire.

Preuve :

1) Nous avons déjà vu que $(\mathcal{L}(E),+,\cdot)$ est un K-ev, cf. 7.2.1 Prop. p. 245.

2) La loi $\circ$ est interne dans $\mathcal{L}(E)$ (cf. Prop. 1 p. 245), distributive sur $+$ (cf. Prop. 2, *1)* et *2)* p. 245), et vérifie la formule $(\alpha g) \circ f = g \circ (\alpha f) = \alpha(g \circ f)$ (cf. Prop. 2, *3)* p. 245).

3) La loi $\circ$ est associative (dans E^E).

4) $\mathrm{Id}_E \in \mathcal{L}(E)$ et Id_E est neutre pour $\circ$.

Remarques :

1) D'après la Prop. 5, $\mathcal{L}(E),+,\circ)$ est un anneau.

2) La loi $\circ$ n'est pas commutative dans $\mathcal{L}(E)$, sauf si : E est de dimension finie et $\dim(E) \leqslant 1$.

En effet, supposons qu'il existe $e_1,e_2 \in E$ tels que (e_1,e_2) soit libre, et *admettons* que le sev Vect (e_1,e_2) ait au moins un supplémentaire F dans E. Considérons les applications $f,g : E \longrightarrow E$ définies de la façon suivante. Pour tout x de E, il existe $(\lambda_1,\lambda_2,y) \in K \times K \times F$ unique tel que $x = \lambda_1 e_1 + \lambda_2 e_2 + y$, et on pose : $f(x) = \lambda_2 e_1$ et $g(x) = \lambda_1 e_2$.

Il est clair que f,g sont linéaires, $g \circ f(e_1) = 0$ et $(f \circ g)(e_1) = e_1$, donc $g \circ f \neq f \circ g$.

L'écriture matricielle éclairera cet exemple (cf. 8.1.3 Prop. 2 p. 265). ■

♦ **Définition 2** Un endomorphisme f d'un K-ev E est dit **nilpotent** si et seulement s'il existe $p \in \mathbb{N}^*$ tel que $f^p = 0$.

Ici, f^p désigne $f \circ \ldots \circ f$ (p facteurs).

Si f est nilpotent, l'ensemble $\{k \in \mathbb{N}^*;\ f^k = 0\}$ est une partie non vide de $\mathbb{N}^*$, donc admet un plus petit élément, noté ici $\nu(f)$, et appelé **indice de nilpotence** de f. On a :

• $\forall k \in \mathbb{N}^*, (k < \nu(f) \Longrightarrow f^k \neq 0)$, par définition de $\nu(f)$

• $\forall k \in \mathbb{N}^*, (k \geqslant \nu(f) \Longrightarrow f^k = 0)$, car $f^k = f^{k-\nu(f)} \circ f^{\nu(f)} = f^{k-\nu(f)} \circ 0 = 0$. ■

◆ **Proposition 6** **(Recollement d'applications linéaires)**

Soient E, F deux K-ev, $n \in \mathbb{N}^*$, $E_1, \ldots, E_n$ des sev de E en somme directe et tels que $E = \bigoplus_{i=1}^{n} E_i$, $f_i \in \mathcal{L}(E_i, F)$ $(1 \leqslant i \leqslant n)$.

Il existe un élément et un seul f de $\mathcal{L}(E,F)$ tel que : $\forall i \in \{1,\ldots,n\}$, $f|_{E_i} = f_i$, et on a : $f = \sum_{i=1}^{n} f_i \circ p_i$ où, pour tout i de $\{1,\ldots,n\}$, $p_i : E \longrightarrow E_i$ est définie par : $\forall (x_1,\ldots,x_n) \in E_1 \times \ldots \times E_n$, $p_i(x_1 + \ldots + x_n) = x_i$.

Preuve :

1) Soit $f \in \mathcal{L}(E,F)$ telle que : $\forall i \in \{1,\ldots,n\}, f|_{E_i} = f_i$. On a, pour tout x de E :

$$f(x) = f\left(\sum_{i=1}^{n} p_i(x)\right) = \sum_{i=1}^{n} f(p_i(x)) = \sum_{i=1}^{n} f_i(p_i(x)) = \left(\sum_{i=1}^{n} f_i \circ p_i\right)(x),$$

et donc : $f = \sum_{i=1}^{n} f_i \circ p_i$.

2) Réciproquement, $\sum_{i=1}^{n} f_i \circ p_i \in \mathcal{L}(E,F)$ et, en notant $j_i : E_i \longrightarrow E$ l'injection canonique $(1 \leqslant i \leqslant n)$, on a, pour tout k de $\{1,\ldots,n\}$:

$$\left(\sum_{i=1}^{n} f_i \circ p_i\right)\Big|_{E_k} = \left(\sum_{i=1}^{n} f_i \circ p_i\right) \circ j_k = \sum_{i=1}^{n} f_i \circ (p_i \circ j_k) = f_k, \text{ car } p_i \circ j_k = \begin{cases} \mathrm{Id}_{E_k} & \text{si } i = k \\ 0 & \text{si } i \neq k \end{cases}.$$

Schématiquement :

si $i = k$: $E_i \xrightarrow{j_i} E \xrightarrow{p_i} E_i$, Id_{E_i} ; si $i \neq k$: $E_k \xrightarrow{j_k} E \xrightarrow{p_i} E_i$, 0. ■

Projecteurs

Soit E un K-ev.

1) On a vu (7.1.1 Exemple *2)* p. 239) que, pour tout couple (F,G) de sev de E supplémentaires dans E, on appelle projecteur sur F parallèlement à G l'application linéaire $p : E \underset{x \longmapsto x'}{\longrightarrow} E$ où $(x',x'') \in F \times G$ est tel que $x = x' + x''$.

• Avec les notations ci-dessus, $x' = x' + 0$ et $(x',0) \in F \times G$, d'où $p(x') = x'$, autrement dit : $(p \circ p)(x) = p(x)$.

• Déterminons $\mathrm{Im}(p)$.

Avec les notations précédentes : $p(x) = x' \in F$, d'où $\mathrm{Im}(p) \subset F$.

D'autre part, pour tout x de F, on a $x = x + 0$ et $(x,0) \in F \times G$, donc $x = p(x) \in \mathrm{Im}(p)$.

Ainsi : $\mathrm{Im}(p) = F$.

• Déterminons $\mathrm{Ker}(p)$.

Pour tout x de G, $x = 0 + x$ et $(0,x) \in F \times G$, donc $p(x) = 0$, d'où $G \subset \mathrm{Ker}(p)$.

D'autre part, pour tout x de E, on a, avec les notations précédentes :

$$p(x) = 0 \Longleftrightarrow x' = 0 \Longleftrightarrow x = x'' \Longrightarrow x \in G,$$

donc $\mathrm{Ker}(p) \subset G$.

Ainsi : $\mathrm{Ker}(p) = G$.

2) Réciproquement, soit $p \in \mathcal{L}(E)$ tel que $p \circ p = p$ (on dit que p est un *idempotent* de l'anneau $\mathcal{L}(E)$). Montrons que $\mathrm{Im}(p)$ et $\mathrm{Ker}(p)$ sont deux sev de E supplémentaires dans E et que p est le projecteur sur $\mathrm{Im}(p)$ parallèlement à $\mathrm{Ker}(p)$.

• Soit $x \in \mathrm{Ker}(p) \cap \mathrm{Im}(p)$. Alors $p(x) = 0$, et il existe $y \in E$ tel que $x = p(y)$, d'où :

$$0 = p(x) = p(p(y)) = (p \circ p)(y) = p(y) = x.$$

Ceci montre : $\mathrm{Im}(p) \cap \mathrm{Ker}(p) = \{0\}$.

• Soit $x \in E$. On dispose de la décomposition : $x = p(x) + \big(x - p(x)\big)$

et : $\begin{cases} p(x) \in \mathrm{Im}(p) \\ x - p(x) \in \mathrm{Ker}(p), \text{ car } p\big(x - p(x)\big) = p(x) - (p \circ p)(x) = 0. \end{cases}$

Ceci montre : $E = \mathrm{Im}(p) + \mathrm{Ker}(p)$.

• Puisque, pour tout x de E : $\begin{cases} x = p(x) + \big(x - p(x)\big) \\ p(x) \in \mathrm{Im}(p) \\ x - p(x) \in \mathrm{Ker}(p) \end{cases}$,

p est le projecteur sur $\mathrm{Im}(p)$ parallèlement à $\mathrm{Ker}(p)$.

Résumons l'étude :

♦ **Proposition 7**

1) Soient F, G deux sev de E supplémentaires dans E, p le projecteur sur F parallèlement à G. On a : $p \circ p = p$, $\mathrm{Im}(p) = F$, $\mathrm{Ker}(p) = G$.

2) Réciproquement, si $p \in \mathcal{L}(E)$ est tel que $p \circ p = p$, alors $\mathrm{Im}(p)$ et $\mathrm{Ker}(p)$ sont deux sev de E supplémentaires dans E, et p est le projecteur sur $\mathrm{Im}(p)$ parallèlement à $\mathrm{Ker}(p)$.

De plus, pour tout x de E :

$$x = p(x) + \big(x - p(x)\big), \quad p(x) \in \mathrm{Im}(p), \quad x - p(x) \in \mathrm{Ker}(p).$$

Remarque :

Soit p un projecteur de E. Notons $e = \mathrm{Id}_E$.

1) $e - p$ est un projecteur de E, puisque $(e-p)^2 = e - 2p + p^2 = e - p$, dit **projecteur associé** au projecteur p.

Il est clair que : $\mathrm{Im}(e-p) = \mathrm{Ker}(p)$ et $\mathrm{Ker}(e-p) = \mathrm{Im}(p)$.

2) $s = 2p - e$ est la symétrie par rapport à $\mathrm{Im}(p)$ parallèlement à $\mathrm{Ker}(p)$ (cf. 7.1.1 Exemple *3)* p. 240); on a : $s^2 = (2p-e)^2 = 4p^2 - 4p + e = e$.

En supposant $2 \neq 0$ dans K, on montre facilement $\mathrm{Ker}(s-e) = \mathrm{Im}(p)$ et $\mathrm{Ker}(s+e) = \mathrm{Ker}(p)$, et donc, pour tout (x',x'') de $\mathrm{Im}(p) \times \mathrm{Ker}(p)$: $s(x'+x'') = x' - x''$,

$\big($puisque $s(x') = 2p(x') - x' = x'$ et $s(x'') = 2p(x'') - x'' = -x''\big)$.

7.2.3 Le groupe $\mathcal{GL}(E)$

◆ **Proposition - Définition**

Soit E un K-ev. L'ensemble $\mathcal{GL}(E)$ des automorphismes de E est un groupe pour $\circ$, appelé **groupe linéaire** de E.

Preuve :

1) La loi $\circ$ est interne dans $\mathcal{GL}(E)$ car, si $f,g : E \longrightarrow E$ sont linéaires et bijectives, alors $g \circ f$ est linéaire (cf. 7.2.2 Prop. 1 p. 245) et bijective (cf. 1.3.2 Prop. 1 p. 27).

2) $\mathrm{Id}_E \in \mathcal{GL}(E)$ et Id_E est neutre pour $\circ$.

3) La loi $\circ$ est associative (dans E^E).

4) Soit $f \in \mathcal{GL}(E)$. D'après 7.2.2 Prop. 3 p. 246, f^{-1} est un automorphisme de E, c'est-à-dire $f^{-1} \in \mathcal{GL}(E)$.

Remarques :

1) Le groupe $\mathcal{GL}(E)$ n'est pas commutatif, sauf si : E est de dimension finie et $\dim(E) \leqslant 1$; raisonner comme dans 7.2.2 Rem *2)* p. 247 avec :

$$f(x) = \lambda_1(e_1 + e_2) + \lambda_2 e_2 + y, \quad g(x) = \lambda_1 e_1 + \lambda_2(e_1 + e_2) + y.$$

L'écriture matricielle éclairera cet exemple (cf. 8.1.4 Rem *1)* p. 269).

2) Si E est de dimension finie et $\dim(E) = 1$, alors $(\mathcal{GL}(E),\circ)$ est un groupe isomorphe au groupe $(K - \{0\},\cdot)$ par l'isomorphisme de groupes $K - \{0\} \longrightarrow \mathcal{GL}(E)$, où $h_\alpha : E \longrightarrow E$
$\alpha \longmapsto h_\alpha$ $\quad x \longmapsto \alpha x$
est l'homothétie de rapport α.

3) $\mathcal{GL}(E)$ est aussi l'ensemble des éléments inversibles de l'anneau $(\mathcal{L}(E),+,\circ)$ (cf. 7.2.2 Prop. 3 p. 246).

Exercices

◊ **7.2.1** Soient E le $\mathbb{R}$-ev des applications de $\mathbb{R}$ dans $\mathbb{R}$ de classe C^∞ sur $\mathbb{R}$, $\varphi : \begin{array}{c} E \longrightarrow E, \\ f \longmapsto f' \end{array}$

$\psi : E \longrightarrow E$ définie par : $\forall f \in E,\ \forall x \in \mathbb{R},\ \big(\psi(f)\big)(x) = \displaystyle\int_0^x f(t)\,dt$.

a) Vérifier que φ et ψ sont linéaires.

b) Exprimer $\psi \circ \varphi$ et $\varphi \circ \psi$.

c) Etudier l'injectivité, la surjectivité, la bijectivité de φ et de ψ.

◊ **7.2.2** Soient E un K-ev, $n \in \mathbb{N}^*$, $f \in \mathcal{L}(E)$ tel que $f^n = e$ (où $e = \mathrm{Id}_E$), $\alpha \in K$ tel que $\alpha^n \neq 1$, et $g = f - \alpha e$. Montrer que g est bijective, et calculer g^{-1}.

◊ **7.2.3** Soient E, F deux K-ev, $g \in \mathcal{L}(F,E)$, $\varphi : \begin{array}{c} E \times F \longrightarrow E \times F \\ (x,y) \longmapsto (x + g(y), y) \end{array}$. Montrer que φ est un automorphisme de $E \times F$.

◊ **7.2.4** Soient E un K-ev, $f \in \mathcal{L}(E)$. On suppose qu'il existe un unique g de $\mathcal{L}(E)$ tel que $f \circ g = \mathrm{Id}_E$. Démontrer : $f \in \mathcal{GL}(E)$.

◊ **7.2.5** Soient E un K-ev, $E \neq \{0\}$, $f \in \mathcal{L}(E)$ nilpotent, p l'indice de nilpotence de f (c'est-à-dire : $p \in \mathbb{N}^*$, $f^p = 0, f^{p-1} \neq 0$). Montrer que la famille $(\mathrm{Id}_E, f, \ldots, f^{p-1})$ est libre.

◊ **7.2.6** Soient E un K-ev, $n \in \mathbb{N}^*$, $E_1, \ldots, E_n$ des sev de E, $f : E_1 \times \ldots \times E_n \longrightarrow E$.
$(x_1, \ldots, x_n) \longmapsto \displaystyle\sum_{i=1}^{n} x_i$

Montrer que $E_1, \ldots, E_n$ sont linéairement indépendants si et seulement si f est injective.

◊ **7.2.7** Soient E un K-ev, $n \in \mathbb{N}^*$, $E_1, \ldots, E_n$ des sev de E linéairement indépendants et tels que $\displaystyle\bigoplus_{i=1}^{n} E_i = E$, $f_i \in \mathcal{L}(E_i)$ pour $i \in \{1, \ldots, n\}$, $f : E \longrightarrow E$ définie par : pour tout x de E, il existe $(x_1, \ldots, x_n) \in E_1 \times \ldots \times E_n$ unique tel que $x = x_1 + \ldots + x_n$, et on pose $f(x) = \displaystyle\sum_{i=1}^{n} f_i(x_i)$.

Montrer : *a)* $\mathrm{Ker}(f) = \displaystyle\bigoplus_{i=1}^{n} \mathrm{Ker}(f_i)$ *b)* $\mathrm{Im}(f) = \displaystyle\bigoplus_{i=1}^{n} \mathrm{Im}(f_i)$.

◊ **7.2.8** Soient E un K-ev, $f, g \in \mathcal{L}(E)$ tels que $f \circ g = g \circ f$. Montrer que $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$ sont stables par g.

◊ **7.2.9** Soient E, F, G trois K-ev, $f \in \mathcal{L}(E,F)$, $g \in \mathcal{L}(F,G)$. Montrer :

a) $\mathrm{Ker}(g \circ f) = f^{-1}(\mathrm{Ker} g)$ et $\mathrm{Ker}(g \circ f) \supset \mathrm{Ker}(f)$

b) $\mathrm{Im}(g \circ f) = g(\mathrm{Im}(f))$ et $\mathrm{Im}(g \circ f) \subset \mathrm{Im}(g)$.

◊ **7.2.10** Soient E, F, G trois K-ev, $f \in \mathcal{L}(E,F)$, $g, h \in \mathcal{L}(F,G)$. Montrer :
$\mathrm{Ker}(g \circ f) = \mathrm{Ker}(h \circ f) \Longleftrightarrow \mathrm{Im}(f) \cap \mathrm{Ker}(g) = \mathrm{Im}(f) \cap \mathrm{Ker}(h)$.

◇ **7.2.11** Soient E un K-ev, $f,g \in \mathcal{L}(E)$, $\lambda \in K$, V un sev de E.

a) Montrer que, si V est stable par f et par g, alors V est stable par $f+g$, λf, $g \circ f$.

b) Montrer que, si V est stable par f, alors, pour tout n de $\mathbb{N}^*$, V est stable par f^n.

c) Donner un exemple d'ev E sur $\mathbb{R}$, de $f \in \mathcal{L}(E)$ et de sev V de E tels que :
f est bijective, $f(V) \subset V$, $f(V) \neq V$.

◇ **7.2.12** Soient E un K-ev, p,q deux projecteurs de E tels que : $p \neq 0$, $q \neq 0$, $p \neq q$. Montrer que (p,q) est libre dans $\mathcal{L}(E)$.

◇ **7.2.13** Soient E un K-ev, p,q deux projecteurs de E tels que $p \circ q = q \circ p$ et $\mathrm{Ker}(p) = \mathrm{Ker}(q)$. Montrer $p = q$.

◇ **7.2.14** Soient E un $\mathbb{K}$-ev (où $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$), p,q deux projecteurs de E. Montrer que $p+q$ est un projecteur si et seulement si : $p \circ q = q \circ p = 0$.

◇ **7.2.15** Soient E un K-ev, $f,g \in \mathcal{L}(E)$. Montrer que les deux propriétés suivantes sont équivalentes :

(i) $f \circ g = g$ et $g \circ f = f$

(ii) f,g sont des projecteurs et $\mathrm{Im}(f) = \mathrm{Im}(g)$.

◇ **7.2.16** Soient E un K-ev, p un projecteur de E, $q = e - p$ (où $e = \mathrm{Id}_E$),
$L = \{f \in \mathcal{L}(E);\ \exists u \in \mathcal{L}(E),\ f = u \circ p\}$, $M = \{g \in \mathcal{L}(E);\ \exists v \in \mathcal{L}(E),\ g = v \circ q\}$.
Montrer que L et M sont des sev de $\mathcal{L}(E)$ supplémentaires dans $\mathcal{L}(E)$.

Dans les exercices 7.2.17 à 7.2.22, *on admettra que tout sev d'un ev admet au moins un supplémentaire.*

◇ **7.2.17*** Soient E,F deux K-ev , $f \in \mathcal{L}(E,F)$.

a) Montrer que f est surjective si et seulement s'il existe $g \in \mathcal{L}(F,E)$ telle que $f \circ g = \mathrm{Id}_F$.

b) Montrer que f est injective si et seulement s'il existe $h \in \mathcal{L}(F,E)$ telle que $h \circ f = \mathrm{Id}_E$.

◇ **7.2.18*** **Factorisation d'une application linéaire**
Soient E,F,G trois K-ev.

a) Soient $f \in \mathcal{L}(E,F)$, $g \in \mathcal{L}(E,G)$.
Montrer : $\mathrm{Ker}(f) \subset \mathrm{Ker}(g) \iff \big(\exists h \in \mathcal{L}(F,G),\ g = h \circ f\big)$.

b) Soient $f \in \mathcal{L}(F,G)$, $g \in \mathcal{L}(E,G)$.
Montrer : $\mathrm{Im}(f) \supset \mathrm{Im}(g) \iff \big(\exists k \in \mathcal{L}(E,F),\ g = f \circ k\big)$.

◇ **7.2.19*** Soient E,F,G trois K-ev tels que $E \neq \{0\}$ et $G \neq \{0\}$. On note :
$\phi : \mathcal{L}(E,F) \longrightarrow \mathcal{L}\big(\mathcal{L}(F,G),\mathcal{L}(E,G)\big)$ et $\Psi : \mathcal{L}(F,G) \longrightarrow \mathcal{L}\big(\mathcal{L}(E,F),\mathcal{L}(E,G)\big)$
les applications linéaires définies par :

$$\forall f \in \mathcal{L}(E,F),\ \forall g \in \mathcal{L}(F,G),\ (\phi(f))(g) = (\Psi(g))(f) = g \circ f.$$

Montrer, pour tout (f,g) de $\mathcal{L}(E,F) \times \mathcal{L}(F,G)$:

a) $\phi(f)$ injective $\iff$ f surjective

b) $\phi(f)$ surjective $\iff$ f injective

c) $\Psi(g)$ injective $\iff$ g injective

d) $\Psi(g)$ surjective $\iff$ g surjective.

(On pourra utiliser l'exercice 7.2.18 p. 252).

◊ **7.2.20*** Soient E un K-ev, F, G deux sev de E. Montrer que les deux propriétés suivantes sont équivalentes :

(i) $\exists f \in \mathcal{L}(E)$, $\mathrm{Im}(f) = F$ et $\mathrm{Ker}(f) = G$

(ii) Il existe un supplémentaire H de G dans E tel que H soit isomorphe à F.

◊ **7.2.21*** Soient E, F' deux K-ev, E' un sev de E, F un sev de F', $\phi : \mathcal{L}(E,F) \longrightarrow \mathcal{L}(E',F')$ l'application définie par :

$$\forall f \in \mathcal{L}(E,F),\ \forall x' \in E',\ (\phi(f))(x') = f(x').$$

a) Vérifier que ϕ est linéaire.

b) Déterminer $\mathrm{Ker}(\phi)$ et $\mathrm{Im}(\phi)$.

◊ **7.2.22*** Soient E, F deux K-ev, $f \in \mathcal{L}(E,F)$. Démontrer qu'il existe $g \in \mathcal{L}(F,E)$ tel que :

$$f \circ g \circ f = f \quad \text{et} \quad g \circ f \circ g = g.$$

◊ **7.2.23*** Soient E un K-ev, E_1, E_2 deux sev de E supplémentaires dans E ; on note :

$$G = \{f \in \mathcal{L}(E);\ \mathrm{Ker}(f) = E_1 \text{ et } \mathrm{Im}(f) = E_2\}.$$

a) Soit $f \in G$. Montrer que E_2 est stable par f et que l'endomorphisme f' de E_2 induit par f (c'est-à-dire : $\forall x \in E_2,\ f'(x) = f(x)$) est un automorphisme de E_2.

b) Démontrer que G est un groupe (pour $\circ$), isomorphe à $\mathcal{GL}(E_2)$.

7.3 Cas de la dimension finie

Dans ce § 7.3, les ev envisagés sont supposés (sauf mention expresse du contraire) de dimension finie.

Si E, F sont deux K-ev de dimension finie et $f \in \mathcal{L}(E,F)$, en vue de l'étude des matrices (ch. 8 p. 261), il est préférable de noter n la dimension de F et p celle de E (au lieu du contraire).

7.3.1 Le théorème du rang et ses conséquences

◆ **Définition** Soient E, F deux K-ev de dimension finie, $f \in \mathcal{L}(E,F)$. On appelle **rang** de f, et on note $\mathrm{rg}(f)$, l'entier naturel défini par :

$$\mathrm{rg}(f) = \dim\big(\mathrm{Im}(f)\big).$$

Remarques :

1) $\mathrm{Im}(f)$ est bien de dimension finie, puisque $\mathrm{Im}(f)$ est un sev de F et que F est de dimension finie, ou bien, autrement, parce que E est de dimension finie. Plus généralement, soient E, F deux K-ev (non nécessairement de dimension finie), $f \in \mathcal{L}(E,F)$. On dit que f est **de rang fini** si et seulement si $\mathrm{Im}(f)$ est de dimension finie, et, dans ce cas, on appelle **rang** de f l'entier naturel, noté $\mathrm{rg}(f)$, défini par :

$$\mathrm{rg}(f) = \dim\big(\mathrm{Im}(f)\big).$$

2) Si $\mathcal{B}$ est une base de E, alors, pour toute f de $\mathcal{L}(E,F)$:

$$\mathrm{rg}(f) = \dim\big(f(\mathrm{Vect}\,(\mathcal{B}))\big) = \dim\big(\mathrm{Vect}\,(f(\mathcal{B}))\big) = \mathrm{rg}\big(f(\mathcal{B})\big),$$

cf. 6.4 Déf. 3 p. 234 et 7.1.3 Prop. 1 p. 242.

3) Pour toute f de $\mathcal{L}(E,F)$: $\mathrm{rg}(f) \leqslant \mathrm{Min}\big(\dim(E), \dim(F)\big)$. En effet :

- E admet au moins une base $\mathcal{B}$, et on a :

$$\mathrm{rg}(f) = \mathrm{rg}\big(f(\mathcal{B})\big) \text{ et } \mathrm{Card}\big(f(\mathcal{B})\big) \leqslant \dim(E)$$

- $\mathrm{rg}(f) = \dim\big(\mathrm{Im}(f)\big) \leqslant \dim(F)$.

◆ **Théorème 1** (Théorème du rang)

Soient E, F deux K-ev, $f \in \mathcal{L}(E,F)$. On a :

$$\mathrm{rg}(f) = \dim(E) - \dim\big(\mathrm{Ker}(f)\big).$$

Preuve :

Notons $p = \dim(E)$, $n = \dim(F)$; le sev $\mathrm{Ker}(f)$ de E admet au moins une base $(e_1, \ldots, e_q)$ où $q = \dim(\mathrm{Ker}(f)) \in \mathbb{N}$. D'après le théorème de la base incomplète, forme faible (6.4 Th. 2 p. 229), on peut compléter $(e_1, \ldots, e_q)$ en une base $(e_1, \ldots, e_q, e_{q+1}, \ldots, e_p)$ de E. Nous allons montrer que $\big(f(e_{q+1}), \ldots, f(e_p)\big)$ est une base de $\mathrm{Im}(f)$.

1) $f(e_{q+1}),\ldots,f(e_p)$ sont à l'évidence dans $\mathrm{Im}(f)$.

2) Soit $(\lambda_{q+1},\ldots,\lambda_p) \in K^{p-q}$ tel que $\sum_{i=q+1}^{p} \lambda_i f(e_i) = 0$.

Alors : $f\left(\sum_{i=q+1}^{p} \lambda_i e_i\right) = \sum_{i=q+1}^{p} \lambda_i f(e_i) = 0$, donc $\sum_{i=q+1}^{p} \lambda_i e_i \in \mathrm{Ker}(f)$.

Il existe donc $(\mu_1,\ldots,\mu_q) \in K^q$ tel que $\sum_{i=q+1}^{p} \lambda_i e_i = \sum_{i=1}^{q} \mu_i e_i$,

d'où : $\mu_1 e_1 + \ldots + \mu_q e_q - \lambda_{q+1} e_{q+1} - \ldots - \lambda_p e_p = 0$.

Comme $(e_1,\ldots,e_p)$ est libre, on déduit (entre autres) : $\lambda_{q+1} = \ldots = \lambda_p = 0$.

Ceci montre que $\big(f(e_{q+1}),\ldots,f(e_p)\big)$ est libre.

3) Soit $y \in \mathrm{Im}(f)$. Il existe $x \in E$ tel que $y = f(x)$; puis, comme $(e_1,\ldots,e_p)$ engendre E, il existe $(\alpha_1,\ldots,\alpha_p) \in K^p$ tel que $x = \sum_{i=1}^{p} \alpha_i e_i$.

On a : $y = f(x) = f\left(\sum_{i=1}^{p} \lambda_i e_i\right) = \sum_{i=1}^{p} \lambda_i f(e_i) = \sum_{i=q+1}^{p} \lambda_i f(e_i)$,

puisque $f(e_1) = \ldots = f(e_q) = 0$.

Ceci montre que $\big(f(e_{q+1}),\ldots,f(e_p)\big)$ engendre $\mathrm{Im}(f)$.

Puisque $\big(f(e_{q+1}),\ldots,f(e_p)\big)$ est une base de $\mathrm{Im}(f)$, on conclut :

$$\mathrm{rg}(f) = \dim\big(\mathrm{Im}(f)\big) = p - q = \dim(E) - \dim\big(\mathrm{Ker}(f)\big). \qquad \blacksquare$$

Remarques :

1) La preuve précédente montre aussi que, pour tout supplémentaire E_1 de $\mathrm{Ker}(f)$ dans E, l'application linéaire $\begin{array}{ccc} E_1 & \longrightarrow & \mathrm{Im}(f) \\ x & \longmapsto & f(x) \end{array}$ est un isomorphisme d'ev.

Ainsi, tout supplémentaire de $\mathrm{Ker}(f)$ dans E est isomorphe à $\mathrm{Im}(f)$.

2) Bien que $\dim\big(\mathrm{Ker}(f)\big) + \dim\big(\mathrm{Im}(f)\big) = \dim(E)$, «en général» $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$ ne sont pas supplémentaires dans E.

En effet, d'abord, $\mathrm{Im}(f)$ est un sev de F et non de E (a priori).

Et puis, même si $F = E$, $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$ peuvent ne pas être supplémentaires dans E, comme le montre l'exemple : $K = \mathbb{R}$, $E = F = \mathbb{R}^2$, $\begin{array}{ccc} f : \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ (x,y) & \longmapsto & (y,0) \end{array}$, dans lequel on a :

$\mathrm{Ker}(f) = \mathrm{Im}(f) = \mathrm{Vect}\big((1,0)\big)$.

♦ **Proposition** Soient E, F deux K-ev de dimension finie, $f \in \mathcal{L}(E,F)$. On a :

1) (f injective) $\iff \mathrm{rg}(f) = \dim(E)$

2) (f surjective) $\iff \mathrm{rg}(f) = \dim(F)$.

Preuve :

1) En utilisant le théorème du rang :

(f injective) $\iff \mathrm{Ker}(f) = \{0\} \iff \dim\big(\mathrm{Ker}(f)\big) = 0 \iff \mathrm{rg}(f) = \dim(E)$.

1) $f(e_{q+1}),\ldots,f(e_p)$ sont à l'évidence dans $\mathrm{Im}(f)$.

2) Soit $(\lambda_{q+1},\ldots,\lambda_p) \in K^{p-q}$ tel que $\sum_{i=q+1}^{p} \lambda_i f(e_i) = 0$.

Alors : $f\left(\sum_{i=q+1}^{p} \lambda_i e_i\right) = \sum_{i=q+1}^{p} \lambda_i f(e_i) = 0$, donc $\sum_{i=q+1}^{p} \lambda_i e_i \in \mathrm{Ker}(f)$.

Il existe donc $(\mu_1,\ldots,\mu_q) \in K^q$ tel que $\sum_{i=q+1}^{p} \lambda_i e_i = \sum_{i=1}^{q} \mu_i e_i$,

d'où : $\mu_1 e_1 + \ldots + \mu_q e_q - \lambda_{q+1} e_{q+1} - \ldots - \lambda_p e_p = 0$.

Comme $(e_1,\ldots,e_p)$ est libre, on déduit (entre autres) : $\lambda_{q+1} = \ldots = \lambda_p = 0$.

Ceci montre que $\big(f(e_{q+1}),\ldots,f(e_p)\big)$ est libre.

3) Soit $y \in \mathrm{Im}(f)$. Il existe $x \in E$ tel que $y = f(x)$; puis, comme $(e_1,\ldots,e_p)$ engendre E, il existe $(\alpha_1,\ldots,\alpha_p) \in K^p$ tel que $x = \sum_{i=1}^{p} \alpha_i e_i$.

On a : $y = f(x) = f\left(\sum_{i=1}^{p} \lambda_i e_i\right) = \sum_{i=1}^{p} \lambda_i f(e_i) = \sum_{i=q+1}^{p} \lambda_i f(e_i)$,

puisque $f(e_1) = \ldots = f(e_q) = 0$.

Ceci montre que $\big(f(e_{q+1}),\ldots,f(e_p)\big)$ engendre $\mathrm{Im}(f)$.

Puisque $\big(f(e_{q+1}),\ldots,f(e_p)\big)$ est une base de $\mathrm{Im}(f)$, on conclut :

$$\mathrm{rg}(f) = \dim\big(\mathrm{Im}(f)\big) = p - q = \dim(E) - \dim\big(\mathrm{Ker}(f)\big). \qquad \blacksquare$$

Remarques :

1) La preuve précédente montre aussi que, pour tout supplémentaire E_1 de $\mathrm{Ker}(f)$ dans E, l'application linéaire $\begin{array}{ccc} E_1 & \longrightarrow & \mathrm{Im}(f) \\ x & \longmapsto & f(x) \end{array}$ est un isomorphisme d'ev.

Ainsi, tout supplémentaire de $\mathrm{Ker}(f)$ dans E est isomorphe à $\mathrm{Im}(f)$.

2) Bien que $\dim\big(\mathrm{Ker}(f)\big) + \dim\big(\mathrm{Im}(f)\big) = \dim(E)$, «en général» $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$ ne sont pas supplémentaires dans E.

En effet, d'abord, $\mathrm{Im}(f)$ est un sev de F et non de E (a priori).

Et puis, même si $F = E$, $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$ peuvent ne pas être supplémentaires dans E, comme le montre l'exemple : $K = \mathbb{R}$, $E = F = \mathbb{R}^2$, $f : \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ (x,y) & \longmapsto & (y,0) \end{array}$, dans lequel on a : $\mathrm{Ker}(f) = \mathrm{Im}(f) = \mathrm{Vect}\big((1,0)\big)$.

♦ **Proposition** Soient E, F deux K-ev de dimension finie, $f \in \mathcal{L}(E,F)$. On a :

1) (f injective) $\iff \mathrm{rg}(f) = \dim(E)$

2) (f surjective) $\iff \mathrm{rg}(f) = \dim(F)$.

Preuve :

1) En utilisant le théorème du rang :

(f injective) $\iff \mathrm{Ker}(f) = \{0\} \iff \dim\big(\mathrm{Ker}(f)\big) = 0 \iff \mathrm{rg}(f) = \dim(E)$.

2) (f surjective) $\iff \mathrm{Im}(f) = F \iff \mathrm{rg}(f) = \dim(F)$
(cf. 6.4 Cor. 3 p. 232).

Un élément f de $\mathcal{L}(E)$ est dit :

- **inversible à gauche** pour $\circ$ dans $\mathcal{L}(E)$ si et seulement si :

$$\exists\, f' \in \mathcal{L}(E),\ f' \circ f = \mathrm{Id}_E$$

- **inversible à droite** pour $\circ$ dans $\mathcal{L}(E)$ si et seulement si :

$$\exists f'' \in \mathcal{L}(E),\ f \circ f'' = \mathrm{Id}_E$$

- **inversible** pour $\circ$ dans $\mathcal{L}(E)$ si et seulement si :

$$\exists\, f' \in \mathcal{L}(E),\ f' \circ f = f \circ f' = \mathrm{Id}_E$$

(cf. 2.1 Déf. 8 p. 41).

Rappelons qu'un élément f de $\mathcal{L}(E)$ est dit :

- **régulier à gauche** pour $\circ$ dans $\mathcal{L}(E)$ si et seulement si :

$$\forall\, (g,h) \in (\mathcal{L}(E))^2,\ (f \circ g = f \circ h \Longrightarrow g = h)$$

- **régulier à droite** pour $\circ$ dans $\mathcal{L}(E)$ si et seulement si :

$$\forall\, (g,h) \in (\mathcal{L}(E))^2,\ (g \circ f = h \circ f \Longrightarrow g = h)$$

- **régulier** pour $\circ$ dans $\mathcal{L}(E)$ si et seulement si f est régulier à gauche et régulier à droite pour $\circ$ dans $\mathcal{L}(E)$ (cf. 2.1 Déf. 5 p. 40).

◆ **Théorème 2** Soient E un K-ev de dimension finie, $f \in \mathcal{L}(E)$. Les propriétés suivantes sont deux à deux équivalentes :

1. f est inversible à gauche pour $\circ$ dans $\mathcal{L}(E)$
2. f est inversible à droite pour $\circ$ dans $\mathcal{L}(E)$
3. f est inversible pour $\circ$ dans $\mathcal{L}(E)$
4. f est régulier à gauche pour $\circ$ dans $\mathcal{L}(E)$
5. f est régulier à droite pour $\circ$ dans $\mathcal{L}(E)$
6. f est régulier pour $\circ$ dans $\mathcal{L}(E)$
7. f est injectif
8. f est surjectif
9. f est bijectif.

Preuve :

1 $\Longrightarrow$ **4** :

Supposons f inversible à gauche pour $\circ$ dans $\mathcal{L}(E)$; il existe $f' \in \mathcal{L}(E)$ tel que $f' \circ f = e$ $(= \mathrm{Id}_E)$. Alors : $\forall (g,h) \in (\mathcal{L}(E))^2$, $\big(f \circ g = f \circ h \Longrightarrow f' \circ f \circ g = f' \circ f \circ h \Longrightarrow g = h\big)$, donc f est régulier à gauche pour $\circ$ dans $\mathcal{L}(E)$.

On montre de même : **2** $\Longrightarrow$ **5**, et on déduit : **3** $\Longrightarrow$ **6**.

4 $\Longrightarrow$ **7** :

Supposons f régulier à gauche pour $\circ$ dans $\mathcal{L}(E)$. Le sev $\mathrm{Ker}(f)$ de l'ev de dimension finie E admet au moins un supplémentaire E_1 dans E.

Considérons le projecteur p sur E_1 parallèlement à $\mathrm{Ker}(f)$. On a :

$$\forall x \in E,\ f(x) = f\big(p(x) + (x - p(x))\big) = f\big(p(x)\big) + f\big(x - p(x)\big) = f\big(p(x)\big),$$

puisque : $x - p(x) \in \mathrm{Ker}(f)$.

Ainsi : $f \circ e = f \circ p$, d'où, puisque f est régulier à gauche : $e = p$, et donc $E = e(E) = p(E) = E_1$, $\mathrm{Ker}(f) = \{0\}$, f est injective.

5 $\Longrightarrow$ **8** :

Supposons f régulier à droite pour $\circ$ dans $\mathcal{L}(E)$. Le sev $\mathrm{Im}(f)$ de l'ev de dimension finie E admet au moins un supplémentaire E_2 dans E. Considérons le projecteur q sur $\mathrm{Im}(f)$ parallèlement à E_2. On a : $\forall x \in E$, $f(x) = q\big(f(x)\big)$, puisque : $f(x) \in \mathrm{Im}(f)$.

Ainsi : $e \circ f = g \circ f$, d'où, puisque f est régulier à droite : $e = q$, et donc $E = e(E) = q(E) = \mathrm{Im}(f)$, f est surjective.

Comme ((**4** $\Longrightarrow$ **7**) et (**5** $\Longrightarrow$ **8**)), on déduit : **6** $\Longrightarrow$ **9**.

7 $\Longrightarrow$ **8** :

En utilisant le théorème du rang et 6.4 Cor. 3 p. 232, on obtient :

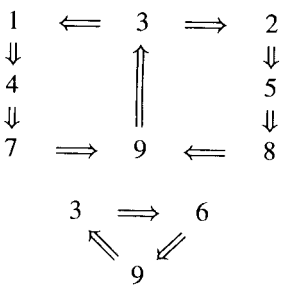
$$\begin{aligned}(f \text{ injective}) &\Longleftrightarrow \mathrm{Ker}(f) = \{0\} \Longleftrightarrow \dim\big(\mathrm{Ker}(f)\big) = 0 \Longleftrightarrow \mathrm{rg}(f) = \dim(E)\\ &\Longleftrightarrow \dim\big(\mathrm{Im}(f)\big) = \dim(E) \Longleftrightarrow \mathrm{Im}(f) = E \Longleftrightarrow (f \text{ surjective}).\end{aligned}$$

De l'équivalence **7** $\Longleftrightarrow$ **8**, on déduit trivialement : (**7** $\Longrightarrow$ **9**) et (**8** $\Longrightarrow$ **9**).

9 $\Longrightarrow$ **3** :

Si f est linéaire et bijective, alors f^{-1} est linéaire (cf. 7.2.2 Prop. 3 p. 246), donc f admet un inverse pour $\circ$ dans $\mathcal{L}(E)$.

(**3** $\Longrightarrow$ **1**) et (**3** $\Longrightarrow$ **2**) : évident.



Le «cycle » $1 \Rightarrow 4 \Rightarrow 7 \Rightarrow 9 \Rightarrow 3 \Rightarrow 1$ montre que les propriétés 1, 4, 7, 9, 3 sont deux à deux équivalentes.

De même, 2, 5, 8, 9, 3 sont deux à deux équivalentes, et 3, 6, 9 sont deux à deux équivalentes.

Finalement, les neuf propriétés envisagées sont deux à deux équivalentes.

Remarques :

1) • Les implications $3 \Rightarrow 1, 3 \Rightarrow 2, 6 \Rightarrow 4, 6 \Rightarrow 5, 9 \Rightarrow 7, 9 \Rightarrow 8$ sont triviales.

• Les implications $1 \Rightarrow 4, 2 \Rightarrow 5, 3 \Rightarrow 6$ sont vraies même si E n'est pas de dimension finie.

• Les implications $4 \Rightarrow 7, 5 \Rightarrow 8, 6 \Rightarrow 9, 7 \Rightarrow 1, 8 \Rightarrow 2, 9 \Rightarrow 3$ sont vraies même si E n'est pas de dimension finie, à condition d'admettre, pour tout sev F de E, l'existence d'un supplémentaire de F dans E, ce qui utilise l'*axiome du choix* (voir exercice 7.2.17 p. 252).

• Les implications $1 \Rightarrow 2, 2 \Rightarrow 1, 4 \Rightarrow 5, 5 \Rightarrow 4, 7 \Rightarrow 8, 8 \Rightarrow 7$ peuvent être fausses si E n'est pas de dimension finie.

2) Nous verrons plus loin (8.1.5 Th. p. 273) d'autres caractérisations, en termes de matrices.

7.3.2 Dimension de $\mathcal{L}(E,F)$

◆ **Proposition** Soient E, F deux K-ev de dimension finie. Alors $\mathcal{L}(E,F)$ est de dimension finie et : $\dim(\mathcal{L}(E,F)) = \dim(E) \cdot \dim(F)$.

Preuve :

On va construire une base de $\mathcal{L}(E,F)$ associée à la donnée d'une base de E et d'une base de F.

Notons $p = \dim(E), n = \dim(F), \mathcal{B} = (e_1,\ldots,e_p)$ une base de $E, \mathcal{C} = (e'_1,\ldots,e'_n)$ une base de F.

Pour chaque (i,j) de $\{1,\ldots,n\} \times \{1,\ldots,p\}$, notons φ_{ij} l'application linéaire de E dans F définie par : $\forall k \in \{1,\ldots,p\}$, $\varphi_{ij}(e_k) = \delta_{kj} e'_i$, où δ_{kj} est le *symbole de Kronecker*, défini par : $\delta_{kj} = \begin{cases} 1 & \text{si } k = j \\ 0 & \text{si } k \neq j. \end{cases}$

Montrons que la famille $\Phi = (\varphi_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}}$ est une base de $\mathcal{L}(E,F)$.

1) Soit $(\lambda_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}} \in K^{np}$ tel que $\sum_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}} \lambda_{ij} \varphi_{ij} = 0.$

On a alors, pour tout k de $\{1,\ldots,p\}$:

$$0 = \left(\sum_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}} \lambda_{ij} \varphi_{ij} \right)(e_k) = \sum_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}} \lambda_{ij} \varphi_{ij}(e_k) = \sum_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}} \lambda_{ij} \delta_{kj} e'_i = \sum_{i=1}^{n} \lambda_{ik} e'_i.$$

Comme $(e'_1,\dots,e'_n)$ est libre, on déduit : $\forall k \in \{1,\dots,p\}, \forall i \in \{1,\dots,n\}, \lambda_{ik} = 0$.
Ceci montre que Φ est libre.

2) Soit $f \in \mathcal{L}(E,F)$.
Pour chaque j de $\{1,\dots,p\}$, $f(e_j)$ se décompose sur la base $(e'_1,\dots,e'_n)$ de F, et il existe donc $(\lambda_{1j},\dots,\lambda_{nj}) \in K^n$ tel que : $f(e_j) = \sum_{i=1}^{n} \lambda_{ij} e'_i$.

On a alors, comme dans *1)* : $\forall k \in \{1,\dots,p\}$, $\left(\sum_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant p}} \lambda_{ij}\varphi_{ij} \right)(e_k) = \sum_{i=1}^{n} \lambda_{ik} e'_i = f(e_k)$,

d'où $f = \sum_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant p}} \lambda_{ij}\varphi_{ij}$.

Ceci montre que Φ engendre $\mathcal{L}(E,F)$.
Finalement, Φ est une base de $\mathcal{L}(E,F)$, et :
$\dim(\mathcal{L}(E,F)) = \mathrm{Card}(\Phi) = pn = \dim(E) \cdot \dim(F)$.

Remarque :
La preuve précédente (construction des φ_{ij}) s'éclairera par le point de vue matriciel (cf. 8.1.3 Prop. 2 p. 265) .

Exercices

◊ **7.3.1** Soient $n \in \mathbb{N}^*$, $E_n = \mathbb{R}_n[X]$ le $\mathbb{R}$-ev des polynômes de $\mathbb{R}[X]$ de degré $\leqslant n$. Montrer :

$$\forall Q \in E_n, \exists ! P \in E_n,\ Q = \sum_{i=0}^{n} P^{(i)}\left(\frac{X}{2^i}\right).$$

◊ **7.3.2** Soient E un K-ev de dimension 2, D_1, D_2, D_3 (resp. Δ_1, Δ_2, Δ_3) trois droites vectorielles deux à deux distinctes. Montrer : $\exists f \in \mathcal{GL}(E), \forall i \in \{1,2,3\},\ f(D_i) = \Delta_i$.

◊ **7.3.3** Soient E un K-ev de dimension finie, $f \in \mathcal{L}(E)$ tel que : $\forall x \in E, \exists p_x \in \mathbb{N}^*,\ f^{p_x}(x) = x$.
Montrer : $\exists p \in \mathbb{N}^*,\ f^p = \mathrm{Id}_E$.

◊ **7.3.4** Soient E un K-ev de dimension finie, $e = \mathrm{Id}_E$, $f,g \in \mathcal{L}(E)$. On suppose qu'il existe $h \in \mathcal{L}(E)$ tel que : $e - f\circ g = f\circ h$ et $f\circ h = h\circ f$. Montrer : $f\circ g = g\circ f$.

◊ **7.3.5*** Soient $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, E un $\mathbb{K}$-ev de dimension finie, L_1, L_2 deux sev de $\mathcal{L}(E)$ tels que :

$$\begin{cases} L_1 \oplus L_2 = \mathcal{L}(E) \\ \forall (f_1,f_2) \in L_1 \times L_2,\ f_1\circ f_2 + f_2\circ f_1 = 0. \end{cases}$$

Démontrer : $L_1 = \{0\}$ ou $L_2 = \{0\}$.

◊ **7.3.6** Soient E un K-ev de dimension finie, $f \in \mathcal{L}(E)$. Montrer : $\dim\left(\mathrm{Ker}(f^2)\right) \leqslant 2\dim\left(\mathrm{Ker}(f)\right)$.

◇ **7.3.7** Soient E un K-ev de dimension finie, $\lambda \in K$, $f \in \mathcal{L}(E)$. Calculer $\mathrm{rg}(\lambda f)$ en fonction de $\mathrm{rg}(f)$.

◇ **7.3.8** Soient E_1, E_2, F_1, F_2 des K-ev de dimension finie, $f_1 \in \mathcal{L}(E_1, F_1)$, $f_2 \in \mathcal{L}(E_2, F_2)$,
$\varphi : E_1 \times E_2 \longrightarrow F_1 \times F_2$, $(x_1, x_2) \longmapsto (f_1(x_1), f_2(x_2))$. Montrer que φ est linéaire et : $\mathrm{rg}(\varphi) = \mathrm{rg}(f_1) + \mathrm{rg}(f_2)$.

◇ **7.3.9** Soient E un K-ev de dimension finie, $f, g \in \mathcal{L}(E)$ tels que :

$$f + g = \mathrm{Id}_E \text{ et } \mathrm{rg}(f) + \mathrm{rg}(g) \leqslant \dim(E).$$

Montrer que f et g sont des projecteurs.

◇ **7.3.10*** Soient E, F deux K-ev de dimension finie, $f, g \in \mathcal{L}(E, F)$. Montrer :

$$\mathrm{rg}(f+g) = \mathrm{rg}(f) + \mathrm{rg}(g) \Longleftrightarrow \begin{cases} \mathrm{Im}(f) \cap \mathrm{Im}(g) = \{0\} \\ \mathrm{Ker}(f) + \mathrm{Ker}(g) = E. \end{cases}$$

◇ **7.3.11** Soient E, F, G trois K-ev de dimension finie, $f \in \mathcal{L}(E, F)$, $g \in \mathcal{L}(F, G)$.

a) Montrer : $\mathrm{Ker}\left(g\,|_{\mathrm{Im}(f)}\right) = \mathrm{Ker}(g) \cap \mathrm{Im}(f)$.

b) En déduire : $\mathrm{rg}(g \circ f) = \mathrm{rg}(f) - \dim\left(\mathrm{Ker}(g) \cap \mathrm{Im}(f)\right)$.

c) Montrer : $\mathrm{rg}(g \circ f) \geqslant \mathrm{rg}(f) + \mathrm{rg}(g) - \dim(F)$.

Complément

◇ **C 7.1** **Sev stables par les endomorphismes de permutation**

Soient $n \in \mathbb{N} - \{0, 1\}$, E un $\mathbb{C}$-ev de dimension n, $\mathcal{B} = (e_1, \ldots, e_n)$ une base de E.

Pour toute σ de $\mathfrak{S}_n$, on note f_σ l'endomorphisme de E défini par : $\forall i \in \{1, \ldots, n\}$, $f_\sigma(e_i) = e_{\sigma(i)}$.

On note $s = \sum_{i=1}^{n} e_i$, D la droite vectorielle engendrée par s, H l'hyperplan d'équation $\sum_{i=1}^{n} x_i = 0$,

$\mathfrak{F}$ l'ensemble des sev F de E tels que : $\forall \sigma \in \mathfrak{S}_n$, $f_\sigma(F) \subset F$.

1) Montrer : $D \in \mathfrak{F}$ et $H \in \mathfrak{F}$.

2) Etablir que D et H sont supplémentaires dans E et qu'en notant p le projecteur sur D parallèlement à H, on a : $p = \dfrac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} f_\sigma$.

3) Soit $F \in \mathfrak{F}$ tel que $F \not\subset D$. Démontrer : $F \supset H$.

4) Conclure : $\mathfrak{F} = \{\{0\}, D, H, E\}$.

Chapitre 8

Matrices

Dans ce ch.8, K désigne un corps commutatif.

Tous les K-ev considérés sont supposés de dimension finie et de dimension $\geqslant 1$.

8.1 Calcul matriciel

8.1.1 Notion de matrice

Soient $n, p \in \mathbb{N}^*$.

♦ **Définition** On appelle **matrice à n lignes, p colonnes, et à éléments** (ou : **coefficients**) **dans** K toute application de $\{1,\ldots,n\} \times \{1,\ldots,p\}$ dans K.

Une application $A : \{1,\ldots,n\} \times \{1,\ldots,p\} \longrightarrow K$ est notée sous la forme d'un
$(i,j) \longmapsto a_{ij}$ (ou : $a_{i,j}$)

tableau :

$$A = (a_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant p}} = (a_{ij})_{1\leqslant i\leqslant n,\ 1\leqslant j\leqslant p} = (a_{ij})_{ij} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1p} \\ a_{21} & a_{22} & \ldots & a_{2p} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{np} \end{pmatrix}.$$

Dans cette notation, les indices extérieurs au parenthésage désignent, dans l'ordre, les numéros de ligne et de colonne.

Le couple (n,p) est appelé le **format** de la matrice A; n est le **nombre de lignes** de A, p est le **nombre de colonnes** de A.

Pour $(i,j) \in \{1,\ldots,n\} \times \{1,\ldots,p\}$, le terme a_{ij} située à la $i^{\text{ème}}$ ligne et $j^{\text{ème}}$ colonne s'appelle le $(i,j)^{\text{ème}}$ **terme** (ou : **coefficient**) de A.

On dit que :

- A est une matrice **carrée** si et seulement si $n = p$; on dit alors que A est une matrice **carrée d'ordre** n
- A est une **matrice-colonne** (ou : **matrice unicolonne**) si et seulement si $p = 1$
- A est une **matrice-ligne** (ou : **matrice uniligne**) si et seulement si $n = 1$.

Si $A = (a_{ij})_{1\leqslant i,\ j\leqslant n}$ est carrée d'ordre n, les $a_{ii}\ (1 \leqslant i \leqslant n)$ sont appelés les **éléments diagonaux** de A, et $(a_{11},\ldots,a_{nn})$ est appelé la **diagonale** de A.

◆ **Notation** Pour $(n,p) \in (\mathbb{N}^*)^2$, on note :

$\mathbf{M}_{n,p}(K)$ l'ensemble des matrices à n lignes, p colonnes, et à éléments dans K

$\mathbf{M}_n(K) = \mathbf{M}_{n,n}(K)$ l'ensemble des matrices carrées d'ordre n à éléments dans K.

Soit $A = (a_{ij})_{1\leqslant i\leqslant n,\ 1\leqslant j\leqslant p} \in \mathbf{M}_{n,p}(K)$.

• Pour $i \in \{1,\ldots,n\}$, la matrice-ligne $(a_{ij})_{1\leqslant j\leqslant p} = (a_{i1}\ldots a_{ip})$ de $\mathbf{M}_{1,p}(K)$ est appelée la $i^{\text{ème}}$ **ligne** de A

• Pour $j \in \{1,\ldots,p\}$, la matrice-colonne $(a_{ij})_{1\leqslant i\leqslant n} = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix}$ de $\mathbf{M}_{n,1}(K)$ est appelée la $j^{\text{ème}}$ **colonne** de A.

8.1.2 Matrices et applications linéaires

◆ **Définition 1** Soient E un K-ev, $n = \dim(E)$, $\mathcal{B} = (e_1,\ldots,e_n)$ une base de E, $x \in E$, $(x_1,\ldots,x_n)$ les composantes de x dans $\mathcal{B}$: $x = \sum_{i=1}^{n} x_i e_i$.

La matrice colonne $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ s'appelle la **matrice-colonne des composantes de** x **dans** $\mathcal{B}$ et est notée $\text{Mat}_{\mathcal{B}}(x)$.

Ainsi : $\text{Mat}_{\mathcal{B}}(x) \in \mathbf{M}_{n,1}(K)$.

Il est clair que l'application $\begin{array}{ccc} \text{Mat}_{\mathcal{B}} : E & \longrightarrow & \mathbf{M}_{n,1}(K) \\ x & \longmapsto & \text{Mat}_{\mathcal{B}}(x) \end{array}$ est une bijection.

Lorsque $X = \text{Mat}_{\mathcal{B}}(x)$, on dit que x **est représenté par** X dans la base $\mathcal{B}$, ou que X **représente** x **dans** $\mathcal{B}$.

◆ **Définition 2** Soient E un K-ev, $n = \dim(E)$, $\mathcal{B} = (e_1,\ldots,e_n)$ une base de E, $p \in \mathbb{N}^*$, $\mathcal{F} = (V_1,\ldots,V_p)$ une famille finie de p éléments de E, et, pour chaque j de $\{1,\ldots,p\}$, $(a_{1j},\ldots,a_{nj})$ les composantes de V_j dans $\mathcal{B}$:

$$\forall\, j \in \{1,\ldots,p\},\ V_j = \sum_{i=1}^{n} a_{ij} e_i.$$

La matrice $(a_{ij})_{1\leqslant i\leqslant n,\ 1\leqslant j\leqslant p} = \begin{pmatrix} a_{11} & \ldots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{np} \end{pmatrix}$ de $\mathbf{M}_{n,p}(K)$ s'appelle la **matrice de la famille** $(V_1,\ldots,V_p)$ **relativement à la base** $\mathcal{B}$ et est notée $\text{Mat}_{\mathcal{B}}(\mathcal{F})$.

Remarque :

$\text{Mat}_{\mathcal{B}}(V_1,\ldots,V_p)$ est obtenue en mettant «côte-à-côte» les matrices-colonnes $\text{Mat}_{\mathcal{B}}(V_1),\ldots,$ $\text{Mat}_{\mathcal{B}}(V_p)$.

♦ **Définition 3**

1) Soient $\left|\begin{array}{l} E,F \text{ deux } K\text{-ev},\ p=\dim(E),\ n=\dim(F) \\ \mathcal{B}=(e_1,\ldots,e_p) \text{ une base de } E,\ \mathcal{C}=(f_1,\ldots,f_n) \text{ une base de } F \\ f\in\mathcal{L}(E,F). \end{array}\right.$

Pour chaque j de $\{1,\ldots,p\}$, notons $(a_{1j},\ldots,a_{nj})$ les composantes de $f(e_j)$ dans $\mathcal{C}$:

$$f(e_j)=\sum_{i=1}^{n} a_{ij} f_i.$$

On appelle **matrice de f relativement aux bases $\mathcal{B}$ et $\mathcal{C}$**, et on note $\text{Mat}_{\mathcal{B},\mathcal{C}}(f)$, la matrice de $\mathbf{M}_{n,p}(K)$ définie par :

$$\text{Mat}_{\mathcal{B},\mathcal{C}}(f)=(a_{ij})_{1\leqslant i\leqslant n,\ 1\leqslant j\leqslant p}.$$

2) Soient E un K-ev, $n=\dim(E)$, $\mathcal{B}=(e_1,\ldots,e_n)$ une base de E, $f\in\mathcal{L}(E)$. On appelle **matrice de f relativement à la base $\mathcal{B}$**, et on note $\text{Mat}_{\mathcal{B}}(f)$, la matrice de $\mathbf{M}_n(K)$ définie par :

$$\text{Mat}_{\mathcal{B}}(f)=\text{Mat}_{\mathcal{B},\mathcal{B}}(f).$$

Il est clair que l'application $\begin{array}{rcl}\text{Mat}_{\mathcal{B},\mathcal{C}} : \mathcal{L}(E,F) & \longrightarrow & \mathbf{M}_{n,p}(K) \\ f & \longmapsto & \text{Mat}_{\mathcal{B},\mathcal{C}}(f)\end{array}$ est une bijection.

Lorsque $A=\text{Mat}_{\mathcal{B},\mathcal{C}}(f)$, on dit que f **est représentée par A dans les bases $\mathcal{B},\mathcal{C}$**, ou que A **représente f dans les bases $\mathcal{B},\mathcal{C}$.**

8.1.3 L'espace vectoriel $\mathbf{M}_{n,p}(K)$

Nous allons « transporter » la structure vectorielle de $\mathcal{L}(E,F)$ sur $\mathbf{M}_{n,p}(K)$, grâce à la bijection Mat $_{\mathcal{B},\mathcal{C}}$, où $\mathcal{B}=(e_1,\ldots,e_p)$ et $\mathcal{C}=(f_1,\ldots,f_n)$ sont des bases fixées de E,F respectivement.
Soient $\lambda\in K$, $f,g\in\mathcal{L}(E,F)$, $A=(a_{ij})_{ij}=\text{Mat}_{\mathcal{B},\mathcal{C}}(f)$, $B=(b_{ij})_{ij}=\text{Mat}_{\mathcal{B},\mathcal{C}}(g)$.
On a donc :

$$\forall j\in\{1,\ldots,p\},\quad \begin{cases} f(e_j)=\sum_{i=1}^{n} a_{ij}f_i \\ g(e_j)=\sum_{i=1}^{n} b_{ij}f_i \end{cases},$$

d'où : $\forall j\in\{1,\ldots,p\}$, $(\lambda f+g)(e_j)=\sum_{i=1}^{n}(\lambda a_{ij}+b_{ij})f_i$.
Ceci nous amène à la Définition suivante.

◆ **Définition**

1) On appelle **addition** dans $\mathbf{M}_{n,p}(K)$ la loi interne, notée $+$, définie par :
$\forall (a_{ij})_{ij}\in\mathbf{M}_{n,p}(K),\forall (b_{ij})_{ij}\in\mathbf{M}_{n,p}(K)$, $(a_{ij})_{ij}+(b_{ij})_{ij}=\left(a_{ij}+b_{ij}\right)_{ij}$.

2) On appelle **multiplication** par les scalaires la loi externe
$K\times\mathbf{M}_{n,p}(K)\longrightarrow\mathbf{M}_{n,p}(K)$, notée par l'absence de symbole (ou par un point), définie par : $\forall\alpha\in K$, $\forall (a_{ij})_{ij}\in\mathbf{M}_{n,p}(K)$, $\alpha(a_{ij})_{ij}=(\alpha a_{ij})_{ij}$.

Remarque :
On ne peut additionner que des matrices de même format.

◆ **Proposition 1**

1) $(\mathbf{M}_{n,p}(K),+,\cdot)$ est un K-ev.

2) Pour tous K-ev E (de dimension p) et F (de dimension n) et pour toutes bases $\mathcal{B}$ de E et $\mathcal{C}$ de F, l'application $\text{Mat}_{\mathcal{B},\mathcal{C}}$: $\mathcal{L}(E,F)\longrightarrow\mathbf{M}_{n,p}(K)$, $f\longmapsto\text{Mat}_{\mathcal{B},\mathcal{C}}(f)$ est un isomorphisme de K-ev.

Preuve :
L'application Mat $_{\mathcal{B},\mathcal{C}}$ est bijective et :

$$\forall\alpha\in K,\ \forall (f,g)\in(\mathcal{L}(E,F))^2,\ \text{Mat}_{\mathcal{B},\mathcal{C}}(\alpha f+g)=\alpha\text{Mat}_{\mathcal{B},\mathcal{C}}(f)+\text{Mat}_{\mathcal{B},\mathcal{C}}(g).$$

Il en résulte aisément, par transport de structure, que $\mathbf{M}_{n,p}(K)$ est un K-ev et que Mat $_{\mathcal{B},\mathcal{C}}$ est un isomorphisme de K-ev. ∎

De même, pour tout K-ev E de dimension n et toute base $\mathcal{B}$ de E, l'application
Mat $_{\mathcal{B}}$: $E\longrightarrow\mathbf{M}_{n,1}(K)$ est un isomorphisme de K-ev.
$x\longmapsto\text{Mat}_{\mathcal{B}}(x)$

♦ **Notation**

1) On note $0_{n,p}$ ou, plus simplement, 0 (ou : $\mathsf{0}$) la matrice de $\mathbf{M}_{n,p}(K)$ dont tous les termes sont nuls.

2) Pour $(n,p) \in (\mathbb{N}^*)^2$ et $(i,j) \in \{1,\dots,n\} \times \{1,\dots,p\}$, on note E_{ij} la matrice de $\mathbf{M}_{n,p}(K)$ dont le $(i,j)^{\text{ème}}$ terme vaut 1 et tous les autres sont nuls. Les matrices E_{ij} sont appelées les **matrices élémentaires**.

Remarques :

1) Dans la notation E_{ij}, on omet de rappeler le format (n,p).

2) En notant δ le **symbole de Kronecker**, défini par $\delta_{xy} = \begin{cases} 1 & \text{si } x = y \\ 0 & \text{si } x \neq y \end{cases}$, on a clairement : $E_{ij} = \left(\delta_{ki}\delta_{lj}\right)_{\substack{1 \leqslant k \leqslant n \\ 1 \leqslant l \leqslant p}}$.

♦ **Proposition 2**

1) $\left(E_{ij}\right)_{(i,j) \in \{1,\dots,n\} \times \{1,\dots,p\}}$ est une base de $\mathbf{M}_{n,p}(K)$, appelée **base canonique** de $\mathbf{M}_{n,p}(K)$.

2) $\dim\left(\mathbf{M}_{n,p}(K)\right) = np$.

Preuve :

1) Il est clair que, pour toute matrice $A = (a_{ij})_{ij}$ de $\mathbf{M}_{n,p}(K)$ on a : $A = \sum_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}} a_{ij}E_{ij}$, ce qui montre que $\left(E_{ij}\right)_{ij}$ engendre $\mathbf{M}_{n,p}(K)$.

2) Si $(a_{ij})_{ij}$ vérifie $\sum_{i,j} a_{ij}E_{ij} = 0$, alors $(a_{ij})_{ij} = 0$, ce qui montre que $\left(E_{ij}\right)_{ij}$ est libre.

Voir aussi 7.3.2 Prop. p. 258. ■

EXEMPLE :

La base canonique de $\mathbf{M}_2(K)$ est $(E_{11},E_{12},E_{21},E_{22})$ où $E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, $E_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, et on a, pour toute matrice $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ de $\mathbf{M}_2(K)$:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}E_{11} + a_{12}E_{12} + a_{21}E_{21} + a_{22}E_{22}.$$

8.1.4 Multiplication des matrices

Soient
- E, F, G trois K-ev, de dimensions respectives q, p, n
- $\mathcal{B} = (e_1, \ldots, e_q)$, $\mathcal{C} = (f_1, \ldots, f_p)$, $\mathcal{D} = (g_1, \ldots, g_n)$ des bases de E, F, G respectivement
- $f \in \mathcal{L}(E, F)$, $g \in \mathcal{L}(F, G)$
- $A = (a_{jk})_{jk} = \text{Mat}_{\mathcal{B},\mathcal{C}}(f)$, $\mathcal{B} = (b_{ij})_{ij} = \text{Mat}_{\mathcal{C},\mathcal{D}}(g)$.

Nous allons déterminer la matrice de $g \circ f$ relativement aux bases $\mathcal{B}$ et $\mathcal{D}$.

Soit $k \in \{1, \ldots, q\}$. On a, par définition de A : $f(e_k) = \sum_{j=1}^{p} a_{jk} f_j$.

D'où : $(g \circ f)(e_k) = g\left(\sum_{j=1}^{p} a_{jk} f_j\right) = \sum_{j=1}^{p} a_{jk} g(f_j)$.

Par définition de B : $\forall j \in \{1, \ldots, p\}$, $g(f_j) = \sum_{i=1}^{n} b_{ij} g_i$.

Donc : $(g \circ f)(e_k) = \sum_{j=1}^{p} a_{jk} \left(\sum_{i=1}^{n} b_{ij} g_i\right) = \sum_{j=1}^{p} \sum_{i=1}^{n} b_{ij} a_{jk} g_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{p} b_{ij} a_{jk}\right) g_i$.

Donc $\text{Mat}_{\mathcal{B},\mathcal{D}}(g \circ f) = (c_{ik})_{ik}$, où : $\forall (i,k) \in \{1, \ldots, n\} \times \{1, \ldots, q\}$, $c_{ik} = \sum_{j=1}^{p} b_{ij} a_{jk}$.

Ceci nous amène à la Définition suivante, après échange de A et B.

◆ **Définition 1** Soient $A = (a_{ij})_{ij} \in \mathbf{M}_{n,p}(K)$, $B = (b_{jk})_{jk} \in \mathbf{M}_{p,q}(K)$. On appelle **produit de A par B**, et on note AB, la matrice de $\mathbf{M}_{n,q}(K)$ définie par

$AB = (c_{ik})_{ik}$, où : $\forall (i,k) \in \{1, \ldots, n\} \times \{1, \ldots, q\}$, $c_{ik} = \sum_{j=1}^{p} a_{ij} b_{jk}$.

L'application $\begin{array}{ccc} \mathbf{M}_{n,p}(K) \times \mathbf{M}_{p,q}(K) & \longrightarrow & \mathbf{M}_{n,q}(K) \\ (A, B) & \longmapsto & AB \end{array}$ s'appelle la **multiplication des matrices**.

Remarque :

Le produit AB existe si et seulement si le nombre de colonnes de A est égal au nombre de lignes de B. ■

Nous avons montré le résultat suivant :

♦ **Proposition 1**

Soient | E, F, G trois K-ev
| $\mathcal{B}, \mathcal{C}, \mathcal{D}$ des bases de E, F, G respectivement
| $f \in \mathcal{L}(E,F)$, $g \in \mathcal{L}(F,G)$.

On a : $\operatorname{Mat}_{\mathcal{B},\mathcal{D}}(g \circ f) = \left(\operatorname{Mat}_{\mathcal{C},\mathcal{D}}(g)\right)\left(\operatorname{Mat}_{\mathcal{B},\mathcal{C}}(f)\right)$.

Autrement dit : (dans des bases convenables) la matrice d'une composée de deux applications linéaires est le produit des matrices de ces applications linéaires (dans le même ordre). ■

♦ **Proposition 2**

Soient | E, F deux K-ev
| $\mathcal{B}, \mathcal{C}$ des bases de E, F respectivement
| $f \in \mathcal{L}(E,F)$, $x \in E$.

On a : $\operatorname{Mat}_{\mathcal{C}}\left(f(x)\right) = \left(\operatorname{Mat}_{\mathcal{B},\mathcal{C}}(f)\right)\left(\operatorname{Mat}_{\mathcal{B}}(x)\right)$.

Preuve :

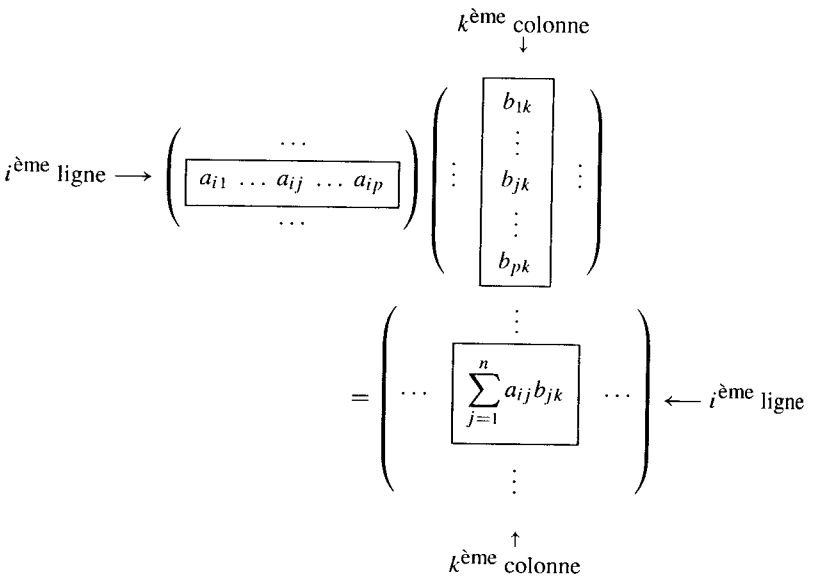
Notons $\mathcal{B} = (e_1, \ldots, e_p)$, $\mathcal{C} = (f_1, \ldots, f_n)$, $X = \operatorname{Mat}_{\mathcal{B}}(x) = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$,

$A = \operatorname{Mat}_{\mathcal{B},\mathcal{C}}(f) = (a_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}}$.

On a :
$$f(x) = f\left(\sum_{j=1}^{p} x_j e_j\right) = \sum_{j=1}^{p} x_j f(e_j) = \sum_{j=1}^{p}\left(x_j \sum_{i=1}^{n} a_{ij} f_i\right)$$
$$= \sum_{j=1}^{p}\sum_{i=1}^{n} a_{ij} x_j f_i = \sum_{i=1}^{n}\left(\sum_{j=1}^{p} a_{ij} x_j\right) f_i,$$

d'où $\operatorname{Mat}_{\mathcal{C}}\left(f(x)\right) = \left(\sum_{j=1}^{p} a_{ij} x_j\right)_{1 \leqslant i \leqslant n} = AX.$ ■

En pratique, pour effectuer le produit AB de deux matrices, on dispose de la façon suivante :



Remarque :

Si $A \in \mathbf{M}_{n,p}(K)$ et $B \in \mathbf{M}_{p,q}(K)$, alors $AB \in \mathbf{M}_{n,q}(K)$. Ainsi le format (n,q) de AB est obtenu à partir des formats (n,p) de A, et (p,q) de B «comme par la relation de Chasles».

EXEMPLES :

1) • $(2 \quad 3)\begin{pmatrix} 1 \\ 11 \end{pmatrix} = (3 \quad 5)$.

• Plus généralement : $(x_1 \ldots x_n)\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \left(\sum_{i=1}^{n} x_i y_i\right)$.

2) • $\begin{pmatrix} 1 \\ 11 \end{pmatrix}(2 \quad 3) = \begin{pmatrix} 2 & 3 \\ 22 & 33 \end{pmatrix}$.

• Plus généralement : $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}(y_1 \ldots y_p) = \begin{pmatrix} x_1 y_1 & \ldots & x_1 y_p \\ \vdots & & \vdots \\ x_n y_1 & \ldots & x_n y_p \end{pmatrix}$.

3) $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$.

4) $(u \quad v)\begin{pmatrix} \alpha & \alpha' & \alpha'' \\ \beta & \beta' & \beta'' \end{pmatrix} = (u\alpha + v\beta \quad u\alpha' + v\beta' \quad u\alpha'' + v\beta'')$.

5) $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x & y \\ z & t \end{pmatrix} = \begin{pmatrix} ax + bz & ay + bt \\ cx + dz & cy + dt \end{pmatrix}$.

6) $\begin{pmatrix} 1 & -2 \\ 3 & 7 \\ -4 & 6 \end{pmatrix}\begin{pmatrix} 4 & 1 & -3 & 2 \\ 6 & -5 & 9 & 0 \end{pmatrix} = \begin{pmatrix} -8 & 11 & -21 & 2 \\ 54 & -32 & 54 & 6 \\ 20 & -34 & 66 & -8 \end{pmatrix}$. ■

À partir des propriétés connues sur les opérations algébriques pour les applications linéaires, on déduit des propriétés sur les opérations algébriques pour les matrices :

♦ **Proposition 3**

1) **(Pseudo-distributivité à gauche)**

$$\forall A \in \mathbf{M}_{n,p}(K),\ \forall B,C \in \mathbf{M}_{p,q}(K),\ \ A(B+C) = AB + AC.$$

2) **(Pseudo-distributivité à droite)**

$$\forall A,B \in \mathbf{M}_{n,p}(K),\ \forall C \in \mathbf{M}_{p,q}(K),\ \ (A+B)C = AC + BC.$$

3) $\forall \lambda \in K,\ \forall A \in \mathbf{M}_{n,p}(K),\ \forall B \in \mathbf{M}_{p,q}(K)$

$$(\lambda A)B = \lambda(AB) = A(\lambda B).$$

4) **(Pseudo-associativité)**

$$\forall A \in \mathbf{M}_{n,p}(K),\ \forall B \in \mathbf{M}_{p,q}(K),\ \forall C \in \mathbf{M}_{q,r}(K)$$

$$(AB)C = A(BC).$$

Pour des matrices A,B,C de formats respectifs (n,p), (p,q), (q,r), on pourra noter ABC au lieu de $(AB)C$ ou $A(BC)$. ■

♦ **Proposition 4**

1) $(\mathbf{M}_n(K),+,\cdot,\times)$ est une K-algèbre associative et unitaire.

2) Pour tout K-ev E de dimension n et toute base $\mathcal{B}$ de E, l'application $\mathrm{Mat}_{\mathcal{B}} : \mathcal{L}(E) \longrightarrow \mathbf{M}_n(K)$ est un isomorphisme de K-algèbres unitaires.
$f \longmapsto \mathrm{Mat}_{\mathcal{B}}(f)$

Preuve :

On a déjà vu que $(\mathbf{M}_n(K),+,\cdot)$ est un K-ev (8.1.3 Prop. 1 p. 264) et que la multiplication est interne dans $\mathbf{M}_n(K)$.

Comme $\mathrm{Mat}_{\mathcal{B}}$ est bijective, que :

$$\forall (f,g) \in \big(\mathcal{L}(E)\big)^2,\ \ \mathrm{Mat}_{\mathcal{B}}(g \circ f) = \big(\mathrm{Mat}_{\mathcal{B}}(g)\big)\big(\mathrm{Mat}_{\mathcal{B}}(f)\big),$$

et que $\big(\mathcal{L}(E),+,\cdot,\circ\big)$ est une K-algèbre associative et unitaire, par transport de structure, $\big(\mathbf{M}_n(K),+,\cdot,\times\big)$ est aussi une K-algèbre associative et unitaire, et $\mathrm{Mat}_{\mathcal{B}}$ est un isomorphisme de K-algèbres unitaires.

♦ **Notation** On note $\mathrm{I}_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in \mathbf{M}_n(K)$, qui est l'élément neutre de la multiplication dans $\mathbf{M}_n(K)$.

Remarques :

1) Si $n \geqslant 2$, l'algèbre $\mathbf{M}_n(K)$ n'est pas commutative, comme le montre (pour $n = 2$) l'exemple : $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

2) Si $n \geqslant 2$, il se peut que le produit de deux matrices de $\mathbf{M}_n(K)$ soit nul sans qu'aucune des deux matrices ne soit nulle, comme le montre (pour $n = 2$) l'exemple :

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

3) On confond souvent un élément x de K et la matrice (x) de $\mathbf{M}_1(K)$.

- Soit $A \in \mathbf{M}_{n,1}(K)$; on a $A \cdot (x) = xA$, mais $(x)A$ n'est pas définie (si $n \geqslant 2$).
- Soit $B \in \mathbf{M}_{1,n}(K)$; on a $(x)B = xB$, mais $B \cdot (x)$ n'est pas définie (si $n \geqslant 2$).

◆ **Définition 2** Une matrice carrée A de $\mathbf{M}_n(K)$ est dite **nilpotente** si et seulement s'il existe $k \in \mathbb{N}^*$ tel que $A^k = 0$.

EXEMPLES :

1) $A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ de $\mathbf{M}_3(\mathbb{R})$ est nilpotente, car $A^2 = 0$.

2) $A = \begin{pmatrix} -9 & 7 & 3 \\ -13 & 10 & 4 \\ 4 & -3 & -1 \end{pmatrix}$ de $\mathbf{M}_3(\mathbb{R})$ est nilpotente, car $A^3 = 0$.

◆ **Proposition - Définition 5** Soit $A \in \mathbf{M}_n(K)$ nilpotente.

L'ensemble $\{k \in \mathbb{N}^* ;\ A^k = 0\}$ admet un plus petit élément $\nu(A)$ appelé **indice de nilpotence** de A, et on a : $\forall k \in \mathbb{N}^*,\ (k \geqslant \nu(A) \Longrightarrow A^k = 0)$.

Preuve :

- $\{k \in \mathbb{N}^* ;\ A^k = 0\}$ est une partie non vide de $\mathbb{N}^*$, donc admet un plus petit élément $\nu(A)$.
- Pour tout k tel que $k \geqslant \nu(A)$: $A^k = A^{k-\nu(A)}A^{\nu(A)} = 0$.

◆ **Définition 3** Soit $A \in \mathbf{M}_{n,p}(K)$.

1) On appelle **noyau** de A le sev de $\mathbf{M}_{p,1}(K)$, noté $\mathrm{Ker}(A)$, défini par :

$$\mathrm{Ker}(A) = \{X \in \mathbf{M}_{p,1}(K) ;\ AX = 0\}.$$

2) On appelle **image** de A le sev de $\mathbf{M}_{n,1}(K)$, noté $\mathrm{Im}(A)$, défini par :

$$\mathrm{Im}(A) = \{Y \in \mathbf{M}_{n,1}(K) ; \exists\, X \in \mathbf{M}_{p,1}(K),\ Y = AX\} = \{AX ;\ X \in \mathbf{M}_{p,1}(K)\}.$$

Soit $A \in \mathbf{M}_{n,p}(K)$. En notant $f : \begin{array}{ccc} \mathbf{M}_{p,1}(K) & \longrightarrow & \mathbf{M}_{n,1}(K) \\ X & \longmapsto & AX \end{array}$, f est linéaire et :

$\mathrm{Ker}(f) = \mathrm{Ker}(A)$ et $\mathrm{Im}(f) = \mathrm{Im}(A)$.

Les notations $\mathrm{Ker}(A)$, $\mathrm{Im}(A)$ incitent à considérer A comme une application linéaire. ∎

Nous verrons dans le Tome 6 les notions de *décomposition en blocs*, et de *polynômes de matrices*.

Exercices

◊ **8.1.1** Soient $n,p,q \in \mathbb{N}^*$, $i \in \{1,\ldots,n\}$, $j,k \in \{1,\ldots,p\}$, $l \in \{1,\ldots,q\}$, E_{ij}, E_{kl} les matrices élémentaires de $\mathbf{M}_{n,p}(K)$ et $\mathbf{M}_{p,q}(K)$. Calculer $E_{ij}E_{kl}$.

◊ **8.1.2** Soit $A \in \mathbf{M}_n(K)$ telle que : $\forall X \in \mathbf{M}_n(K)$, $(XA)^2 = 0$. Montrer : $A = 0$.

◊ **8.1.3** Soient $A,B \in \mathbf{M}_n(K)$ telles qu'il existe $(\alpha,\beta) \in (K - \{0\})^2$ tel que $AB + \alpha A + \beta B = 0$. Montrer : $AB = BA$.

◊ **8.1.4** Résoudre l'équation $X^2 - 2X = \begin{pmatrix} -1 & 0 \\ 6 & 3 \end{pmatrix}$ d'inconnue $X \in \mathbf{M}_2(\mathbb{R})$.

◊ **8.1.5** Résoudre le système d'équations $\begin{cases} XYZ = I_2 \\ YXY = I_2 \end{cases}$ d'inconnue $(X,Y) \in (\mathbf{M}_2(\mathbb{R}))^2$.

◊ **8.1.6** Soient $U = \begin{pmatrix} 1 & -1 & 1 \\ 1 & 1 & 1 \\ 1 & -1 & 1 \end{pmatrix} \in \mathbf{M}_n(\mathbb{C})$, $E = \{aU ; a \in \mathbb{C}\}$. Montrer que E est un corps pour les lois usuelles; E est-il un sous-corps de l'anneau $\mathbf{M}_n(\mathbb{C})$?

◊ **8.1.7** Soit $E = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} ; a \in K \right\}$.

a) Montrer que E est un sous-pseudo-anneau de l'anneau $\mathbf{M}_2(K)$.

b) Est-ce que E est un sous-anneau de l'anneau $\mathbf{M}_2(K)$?

◊ **8.1.8** Soit $E = \left\{ \begin{pmatrix} a & b & b & c \\ b & a & c & b \\ b & c & a & b \\ c & b & b & a \end{pmatrix} ; (a,b,c) \in \mathbb{C}^3 \right\}$.

a) Montrer que E est une sous-algèbre commutative et unitaire de $\mathbf{M}_4(\mathbb{C})$, et $\dim(E) = 3$.

b) Résoudre l'équation $X^2 = I_4$, d'inconnue $X \in E$.

◊ **8.1.9** Soient $a,b \in K$, $M_{a,b} = \begin{pmatrix} a & & b \\ & \ddots & \\ b & & a \end{pmatrix} \in \mathbf{M}_n(\mathbb{C})$, $k \in \mathbb{N}^*$. Calculer $M_{a,b}^k$.

◊ **8.1.10** Soient $A = \begin{pmatrix} 1 & & 1 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in \mathbf{M}_n(K)$, $k \in \mathbb{N}^*$. Calculer A^k.

◊ **8.1.11** Trouver toutes les matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\mathbf{M}_2(\mathbb{R})$ telles que :

$$\forall k \in \mathbb{N}^*,\ A^k = \begin{pmatrix} a^k & b^k \\ c^k & d^k \end{pmatrix}.$$

8.1.5 Le groupe $\mathbf{GL}_n(K)$

Soit $n \in \mathbb{N}^*$.

◆ **Définition** Une matrice A de $\mathbf{M}_n(K)$ est dite **inversible** si et seulement s'il existe $A' \in \mathbf{M}_n(K)$ telle que $AA' = A'A = \mathrm{I}_n$.

Si A est inversible, alors A' est unique et appelée **inverse** de A, notée A^{-1}.

On note $\mathbf{GL}_n(K)$ l'ensemble des matrices inversibles de $\mathbf{M}_n(K)$.

◆ **Proposition - Définition**

1) La multiplication est interne dans $\mathbf{GL}_n(K)$, et $(\mathbf{GL}_n(K),\cdot)$ est un groupe, appelé **groupe linéaire.**

2) Pour tout K-ev E de dimension n et toute base $\mathcal{B}$ de E, l'application $f \longmapsto \mathrm{Mat}_{\mathcal{B}}(f)$ est un isomorphisme du groupe $(\mathcal{GL}(E),\circ)$ sur le groupe $\big(\mathbf{GL}_n(K),\cdot\big)$.

Preuve :

1) • Pour tout (A,B) de $(\mathbf{GL}_n(K))^2$, $(AB)(B^{-1}A^{-1}) = (B^{-1}A^{-1})(AB) = \mathrm{I}_n$, donc $AB \in \mathbf{GL}_n(K)$.

• $\mathrm{I}_n \in \mathbf{GL}_n(K)$.

• Pour toute A de $\mathbf{GL}_n(K)$, $A^{-1}A = AA^{-1} = \mathrm{I}_n$, donc $A^{-1} \in \mathbf{GL}_n(K)$.

2) • Pour toute f de $\mathcal{GL}(E)$, comme

$$\big(\mathrm{Mat}_{\mathcal{B}}(f)\big)\big(\mathrm{Mat}_{\mathcal{B}}(f^{-1})\big) = \big(\mathrm{Mat}_{\mathcal{B}}(f^{-1})\big)\big(\mathrm{Mat}_{\mathcal{B}}(f)\big) = \mathrm{Mat}_{\mathcal{B}}(\mathrm{Id}_E) = \mathrm{I}_n,$$

on a : $\mathrm{Mat}_{\mathcal{B}}(f) \in \mathbf{GL}_n(K)$.

• Réciproquement, pour toute A de $\mathbf{GL}_n(K)$, il existe $(f,g) \in \big(\mathcal{L}(E)\big)^2$ unique tel que $\mathrm{Mat}_{\mathcal{B}}(f) = A$ et $\mathrm{Mat}_{\mathcal{B}}(g) = A^{-1}$, et on a

$$\begin{cases} \mathrm{Mat}_{\mathcal{B}}(g\circ f) = \big(\mathrm{Mat}_{\mathcal{B}}(g)\big)\big(\mathrm{Mat}_{\mathcal{B}}(f)\big) = A^{-1}A = \mathrm{I}_n \\ \mathrm{Mat}_{\mathcal{B}}(f\circ g) = \big(\mathrm{Mat}_{\mathcal{B}}(f)\big)\big(\mathrm{Mat}_{\mathcal{B}}(g)\big) = AA^{-1} = \mathrm{I}_n, \end{cases}$$

donc $g\circ f = f\circ g = \mathrm{Id}_E$, d'où $f \in \mathcal{GL}(E)$.

• Enfin : $\forall (f,g) \in \big(\mathcal{GL}(E)\big)^2$, $\mathrm{Mat}_{\mathcal{B}}(g\circ f) = \big(\mathrm{Mat}_{\mathcal{B}}(g)\big)\big(\mathrm{Mat}_{\mathcal{B}}(f)\big)$. ∎

Remarque :

Pour $n \geqslant 2$, le groupe $\mathbf{GL}_n(K)$ n'est pas commutatif, comme le montre (pour $n = 2$) l'exemple suivant :

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}. \qquad ∎$$

Du Théorème 2 de 7.3.1 p. 256, on déduit le Théorème suivant.

♦ **Théorème** Soient $A \in \mathbf{M}_n(K)$, f un endomorphisme représenté par A dans une base. Les propriétés suivantes, sont deux à deux équivalentes :

1) f est bijective

2) A est inversible à gauche

3) A est inversible à droite

4) A est inversible

5) A est régulière à gauche

6) A est régulière à droite

7) A est régulière.

Rappelons (cf. 2.1 Déf. 5 p. 40) que A est dite :

- **régulière à gauche** si et seulement si : $\forall (B,C) \in \left(\mathbf{M}_n(K)\right)^2$, $(AB = AC \Longrightarrow B = C)$
- **régulière à droite** si et seulement si : $\forall (B,C) \in \left(\mathbf{M}_n(K)\right)^2$, $(BA = CA \Longrightarrow B = C)$
- **régulière** si et seulement si A est régulière à gauche et régulière à droite.

Remarque :

Une matrice A de $\mathbf{M}_n(K)$ est inversible si et seulement si :

$\forall X \in \mathbf{M}_{n,1}(K)$, $(AX = 0 \Longrightarrow X = 0)$ (cf. par exemple, C 8.1 I, p. 300).

Nous verrons plus loin d'autres caractérisations de l'inversibilité d'une matrice carrée faisant intervenir le rang (8.1.6 Prop. 3 p. 277), le déterminant (9.4 Prop. 2 *4)* p. 310), les valeurs propres (Tome 6, 2.1 p. 35).

Une matrice carrée est quelquefois dite **singulière** si et seulement si elle n'est pas régulière. ■

Calcul pratique de A^{-1}

En notant $AX = Y$, où $X, Y \in \mathbf{M}_{n,1}(K)$, on exprime X en fonction de Y par résolution d'un système linéaire (car, si A est inversible : $AX = Y \Longleftrightarrow X = A^{-1}Y$).

EXEMPLE : Montrer que $A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \in \mathbf{M}_4(\mathbb{R})$ est inversible et calculer A^{-1}.

En notant $X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$ et $Y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix}$, on a : $AX = Y \Longleftrightarrow \begin{cases} x_2 + x_3 + x_4 = y_1 \\ x_1 + x_3 + x_4 = y_2 \\ x_1 + x_2 + x_4 = y_3 \\ x_1 + x_2 + x_3 = y_4. \end{cases}$

On peut rajouter à ce système linéaire l'équation obtenue par addition des quatre équations :

$$3(x_1 + x_2 + x_3 + x_4) = y_1 + y_2 + y_3 + y_4,$$

et donc : $AX = Y \iff \begin{cases} 3x_1 = (y_1 + y_2 + y_3 + y_4) - 3y_1 \\ 3x_2 = (y_1 + y_2 + y_3 + y_4) - 3y_2 \\ 3x_3 = (y_1 + y_2 + y_3 + y_4) - 3y_3 \\ 3x_4 = (y_1 + y_2 + y_3 + y_4) - 3y_4. \end{cases}$

Ceci montre que A est inversible et : $A^{-1} = \frac{1}{3}\begin{pmatrix} -2 & 1 & 1 & 1 \\ 1 & -2 & 1 & 1 \\ 1 & 1 & -2 & 1 \\ 1 & 1 & 1 & -2 \end{pmatrix}$. ∎

Pour des matrices carrées de grand ordre, ou à termes numériques, on utilisera un logiciel de calcul d'inverse des matrices inversibles.

Exercices

◇ **8.1.12** Montrer que $E = \left\{ \begin{pmatrix} x+y & 3y \\ -y & x-y \end{pmatrix} ; (x,y) \in \mathbb{R}^2 \right\}$ est un sous-corps de l'anneau $\mathbf{M}_2(\mathbb{R})$, isomorphe à $\mathbb{C}$.

◇ **8.1.13** Soient $\alpha \in \mathbb{R}$, $E_\alpha = \left\{ \begin{pmatrix} x & \alpha y \\ y & x \end{pmatrix} ; (x,y) \in \mathbb{R}^2 \right\}$.

a) Montrer que E_α est une sous-algèbre commutative et unitaire de $\mathbf{M}_2(\mathbb{R})$.

b) Montrer :

- si $\alpha < 0$, alors E_α est un corps isomorphe à $\mathbb{C}$
- si $\alpha \geqslant 0$, alors E_α est un anneau non intègre.

◇ **8.1.14** Dans les exemples suivants, montrer que la matrice est inversible (dans $\mathbf{M}_n(\mathbb{R})$, $n \geqslant 2$) et calculer son inverse :

a) $A = \begin{pmatrix} 1 & 1 & 0 \\ & \ddots & 1 \\ 0 & & 1 \end{pmatrix}$ *b)* $A = \begin{pmatrix} 1 & & 1 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ *c)* $A = \begin{pmatrix} 1 & 2 & \dots & n \\ & \ddots & \ddots & \vdots \\ & & \ddots & 2 \\ 0 & & & 1 \end{pmatrix}$.

◇ **8.1.15** Soient $t \in K$, $A = (a_{ij})_{ij}$, $B = (b_{ij})_{ij} \in \mathbf{M}_n(K)$ définies par :

$$a_{ij} = \begin{cases} t^{j-i}\mathrm{C}_j^i & \text{si } i \leqslant j \\ 0 & \text{si } i > j \end{cases}, \qquad b_{ij} = \begin{cases} (-1)^{i+j} t^{j-i}\mathrm{C}_j^i & \text{si } i \leqslant j \\ 0 & \text{si } i > j \end{cases}.$$

Montrer que A et B sont inverses l'une de l'autre.

◇ **8.1.16** Soient $A, B \in \mathbf{M}_n(K)$ telles que B et $B - AB^{-1}A$ soient inversibles. Résoudre le système d'équations $\begin{cases} AX + BY = 0 \\ BX - AY = \mathrm{I}_n \end{cases}$, d'inconnue $(X,Y) \in \left(\mathbf{M}_n(K)\right)^2$.

◇ **8.1.17** Résoudre dans $\left(\mathbf{M}_2(\mathbb{R})\right)^3$: $XY = \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}$, $YZ = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix}$, $ZX = \begin{pmatrix} 2 & 0 \\ 2 & 0 \end{pmatrix}$.

◇ **8.1.18** Soient $S \in \mathbf{M}_n(K)$, $E = \{M \in \mathbf{M}_n(K);\ MS = 0\}$, $F = \{\mathrm{I}_n + M;\ M \in E\}$.

a) Montrer que E est un sev de $\mathbf{M}_n(K)$.

b α) Montrer que F est stable pour la multiplication.

β) Etablir : $\forall A \in F \cap \mathbf{GL}_n(K)$, $A^{-1} \in F$.

◇ **8.1.19** *a)* Montrer : $\forall (i,j) \in \{1,\dots,n\}^2$, $\left(i \neq j \Longrightarrow \mathrm{I}_n + \mathrm{E}_{ij} \in \mathbf{GL}_n(K)\right)$.

b) En déduire que $\{A \in \mathbf{M}_n(K);\ \forall X \in \mathbf{GL}_n(K),\ AX = XA\}$, appelé **commutant** de $\mathbf{GL}_n(K)$ dans $\mathbf{M}_n(K)$, est égal à $K\mathrm{I}_n$.

8.1.6 Rang d'une matrice

◆ **Définition** Soit $A \in \mathbf{M}_{n,p}(K)$. On appelle **rang** de A, et on note $\text{rg}(A)$ le rang de la famille des colonnes de A dans $\mathbf{M}_{n,1}(K)$.

Ainsi, en notant $A = \begin{pmatrix} a_{11} & \dots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{np} \end{pmatrix}$ et $C_1 = \begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix}, \dots, C_p = \begin{pmatrix} a_{1p} \\ \vdots \\ a_{np} \end{pmatrix}$ les colonnes de A, on a : $\text{rg}(A) = \text{rg}(C_1, \dots, C_p)$.

◆ **Proposition 1** Soient E, F deux K-ev, $\mathcal{B}, \mathcal{C}$ des bases de E, F respectivement, $f \in \mathcal{L}(E,F)$, $A = \text{Mat}_{\mathcal{B},\mathcal{C}}(f)$. On a : $\text{rg}(f) = \text{rg}(A)$.

Preuve :

Notons $\mathcal{B} = (e_1, \dots, e_p)$, $\mathcal{C} = (f_1, \dots, f_n)$, $A = (a_{ij})_{ij}$, $C_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix}$ pour $1 \leqslant j \leqslant p$.

On a : $\forall j \in \{1, \dots, p\}$, $f(e_j) = \sum_{i=1}^{n} a_{ij} f_i$.

Puisque θ : $\mathbf{M}_{n,1}(K) \longrightarrow F$ est un isomorphisme de K-ev, on a :

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \longmapsto \sum_{i=1}^{n} x_i f_i$$

$$\begin{aligned} \text{rg}(A) &= \dim\big(\text{Vect}\,(C_1, \dots, C_p)\big) = \dim\big(\text{Vect}\,(\theta(C_1), \dots, \theta(C_p))\big) \\ &= \dim\big(\text{Vect}\,(f(e_1), \dots, f(e_p))\big) = \text{rg}(f). \end{aligned}$$ ∎

Ainsi :

- Le rang d'une matrice A est le rang de n'importe quelle application linéaire représentée par A
- Le rang d'une application linéaire f est le rang de n'importe quelle matrice représentant f
- Le rang d'une famille finie $\mathcal{F}$ de vecteurs d'un K-ev E est le rang de la matrice de $\mathcal{F}$ dans n'importe quelle base de E. ∎

◆ **Proposition 2**

$$\forall A \in \mathbf{M}_{n,p}(K), \quad \text{rg}(A) \leqslant \text{Min}(n,p).$$

Preuve : Avec les notations précédentes :

- $\text{rg}(A) = \text{rg}(C_1, \dots, C_p) \leqslant p$
- $\text{rg}(A) = \dim\big(\text{Vect}\,(C_1, \dots, C_p)\big) \leqslant \dim\big(\mathbf{M}_{n,1}(K)\big) = n.$ ∎

♦ **Proposition 3**

$$\forall A \in \mathbf{M}_n(K),\ \big(\mathrm{rg}(A) = n \iff A \in \mathbf{GL}_n(K)\big).$$

Preuve :

Soit f l'endomorphisme de $\mathbf{M}_{n,1}(K)$ représenté par A dans la base canonique de $\mathbf{M}_{n,1}(K)$. Comme $(C_1,\ldots,C_n)$ est une base de $\mathbf{M}_{n,1}(K)$ si et seulement si f est bijective, on conclut : $\mathrm{rg}(A) = n \iff A \in \mathbf{GL}_n(K)$. ■

♦ **Proposition 4**

$$\forall A \in \mathbf{M}_{n,p}(K),\ \begin{cases} \forall P \in \mathbf{GL}_p(K), & \mathrm{rg}(AP) = \mathrm{rg}(A) \\ \forall Q \in \mathbf{GL}_n(K), & \mathrm{rg}(QA) = \mathrm{rg}(A) \end{cases}.$$

Preuve :

1) Il est clair que $\mathrm{Im}(AP) \subset \mathrm{Im}(A)$, d'où $\mathrm{rg}(AP) \leqslant \mathrm{rg}(A)$. En remplaçant (A,P) par (AP,P^{-1}), on déduit : $\mathrm{rg}(A) = \mathrm{rg}\big((AP)P^{-1}\big) \leqslant \mathrm{rg}(AP)$.

2) Il est clair que $\mathrm{Ker}(A) \subset \mathrm{Ker}(QA)$, d'où, d'après le théorème du rang :

$$\mathrm{rg}(A) = p - \dim\big(\mathrm{Ker}(A)\big) \geqslant p - \dim\big(\mathrm{Ker}(QA)\big) = \mathrm{rg}(QA).$$

En remplaçant (A,Q) par (QA,Q^{-1}), on déduit :

$$\mathrm{rg}(QA) \geqslant \mathrm{rg}\big(Q^{-1}(QA)\big) = \mathrm{rg}(A).$$ ■

Autrement dit, on ne modifie pas le rang d'une matrice en multipliant celle-ci par une matrice inversible.

Remarque :

On montre de façon analogue :

$$\forall (A,B,C) \in \mathbf{M}_{n,p}(K) \times \mathbf{M}_{p,q}(K) \times \mathbf{M}_{q,r}(K),\ \mathrm{rg}(ABC) \leqslant \mathrm{rg}(B).$$

Exercices

◇ **8.1.20** Pour $(a,b) \in \mathbb{C}^2$, déterminer le rang de $M_{a,b} = \begin{pmatrix} a & & b \\ & \ddots & \\ b & & a \end{pmatrix} \in \mathbf{M}_n(\mathbb{C})$.

◇ **8.1.21** Soient $A \in \mathbf{M}_{n,p}(K), C_1, \ldots, C_p$ les colonnes de A. Montrer :

a) $\text{rg}(A) = n \iff \big((C_1, \ldots, C_p) \text{ engendre } \mathbf{M}_{n,1}(K)\big)$

b) $\text{rg}(A) = p \iff \big((C_1, \ldots, C_p) \text{ est libre}\big)$.

◇ **8.1.22** Soient $A \in \mathbf{M}_{n,p}(K)$, E, F deux K-ev de dimensions respectives p,n, $\mathcal{B}$ (resp. $\mathcal{C}$) une base de E(resp. F), $f \in \mathcal{L}(E,F)$ telle que $\text{Mat}_{\mathcal{B},\mathcal{C}}(f) = A$. Montrer :

a) $\text{rg}(A) = n \iff f$ surjective

b) $\text{rg}(A) = p \iff f$ injective.

◇ **8.1.23** Soient $A \in \mathbf{M}_{n,p}(K)$, $s \in \mathbb{N}$. Démontrer :

$$\text{rg}(A) \leqslant s \iff \left(\exists q \in \mathbb{N}^*, \exists B \in \mathbf{M}_{p,q}(K), \begin{cases} AB = 0 \\ \text{rg}(B) \geqslant p - s \end{cases} \right).$$

◇ **8.1.24** Soient $A \in \mathbf{M}_{n,p}(K)$, $B \in \mathbf{M}_{p,q}(K)$, $C \in \mathbf{M}_{q,r}(K)$ telles que $\text{rg}(B) = \text{rg}(AB)$. Démontrer : $\text{rg}(BC) = \text{rg}(ABC)$.

◇ **8.1.25*** Soient $A \in \mathbf{M}_{3,4}(\mathbb{R})$, $B \in \mathbf{M}_{4,2}(\mathbb{R})$, $C \in \mathbf{M}_{2,3}(\mathbb{R})$ telles que

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

Calculer CAB et montrer $(BCA)^2 = BCA$.

◇ **8.1.26*** *a)* Soient $A, B \in \mathbf{M}_n(K)$ telles que : A est nilpotente, $AB = BA$, $B \neq 0$.
Montrer : $\text{rg}(AB) \leqslant \text{rg}(B) - 1$.

b) Soient $p \in \mathbb{N}^*$, $A_1, \ldots, A_p \in \mathbf{M}_n(K)$ nilpotentes et qui commutent deux à deux.
Montrer : $\text{rg}\left(\prod_{i=1}^{p} A_i\right) \leqslant (n-p)^+ = \begin{cases} n-p & \text{si } n-p \geqslant 0 \\ 0 & \text{si } n-p < 0 \end{cases}$.

c) En déduire que, si $A_1, \ldots, A_n \in \mathbf{M}_n(K)$ sont nilpotentes et commutent deux à deux, alors $\prod_{i=1}^{n} A_i = 0$.

8.1.7 Opérations élémentaires

Soient $(n,p) \in (\mathbb{N}-\{0,1\})^2$, $A=(a_{ij})_{ij} \in \mathbf{M}_{n,p}(K)$.

On appelle **opérations élémentaires sur les colonnes** de A les transformations suivantes (où C_j désigne la $j^{\text{ème}}$ colonne de A, $1 \leqslant j \leqslant p$) :

- Echange (entre elles) de deux colonnes de A
- Remplacement d'une colonne C_j de A par αC_j, où $\alpha \in K-\{0\}$
- Remplacement d'une colonne C_j de A par $C_j+\alpha C_k$ où $\alpha \in K$ et $k \in \{1,\ldots,p\}-\{j\}$.

On définit de manière analogue les **opérations élémentaires sur les lignes** de A (qui sont les opérations élémentaires sur les colonnes de la transposée de A , cf. 8.1.8 Déf. p. 283).

Nous allons interpréter les opérations élémentaires sur les colonnes ou les lignes de A comme des multiplications par certaines matrices carrées inversibles. Rappelons (cf. ex. 8.1.1 p. 271) :

$$\forall (i,j,k,l) \in \{1,\ldots p\}^4,\ \mathrm{E}_{ij}\mathrm{E}_{kl}=\delta_{jk}\mathrm{E}_{il}.$$

1) Pour $(j,k) \in \{1,\ldots,p\}^2$ tel que $j<k$, en notant

$$\mathrm{P}_{jk}=\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & \cdots & 1 & & \\ & & \vdots & \ddots & \vdots & & \\ & & 1 & \cdots & 0 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} = \mathrm{I}_p+\left(\mathrm{E}_{jk}+\mathrm{E}_{kj}-\mathrm{E}_{jj}-\mathrm{E}_{kk}\right) \in \mathbf{M}_p(K),$$

($j^{\text{ème}}$ colonne, $k^{\text{ème}}$ colonne)

$$\text{on a : } AP_{jk}=\begin{pmatrix} a_{1\,1} & \cdots & a_{1\,j-1} & a_{1\,k} & a_{1\,j+1} & \cdots & a_{1\,k-1} & a_{1\,j} & a_{1\,k+1} & \cdots & a_{1\,p} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n\,1} & \cdots & a_{n\,j-1} & a_{n\,k} & a_{n\,j+1} & \cdots & a_{n\,k-1} & a_{n\,j} & a_{n\,k+1} & \cdots & a_{n\,p} \end{pmatrix}.$$

De plus, P_{jk} est inversible, car $\mathrm{P}_{jk}^2=\mathrm{I}_p$.

Ainsi, l'échange des colonnes n^{os} j et k de A revient à la multiplication à droite (on dit aussi **postmultiplication**) par la matrice inversible P_{jk}.

2) Pour $j \in \{1,\dots,p\}$ et $\alpha \in K - \{0\}$, en notant

$$D_{j,\alpha} = \begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & \alpha & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix} = I_p + (\alpha - 1)E_{jj} \in \mathbf{M}_p(K),$$

(α en position (j,j))

$j^{\text{ème}}$ colonne

on a : $AD_{j,\alpha} = \begin{pmatrix} a_{11} & \dots & \alpha a_{1j} & \dots & a_{1p} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \dots & \alpha a_{nj} & \dots & a_{np} \end{pmatrix}$.

De plus $D_{j,\alpha}$ est inversible, car $D_{j,\alpha}\, D_{j,\alpha^{-1}} = I_p$.

Ainsi, le remplacement de la $j^{\text{ème}}$ colonne de A par le produit de cette colonne par α ($\alpha \in K$ et $\alpha \neq 0$) revient à la postmultiplication par la matrice inversible $D_{j,\alpha}$.

3) Pour $(j,k) \in \{1,\dots,p\}^2$ tel que $j \neq k$, et $\alpha \in K$, en notant

$$T_{j\,k,\alpha} = \begin{pmatrix} 1 & & & & & 0 \\ & \ddots & & & & \\ & & 1 & \dots & 0 & \\ & & \vdots & \ddots & \vdots & \\ & & \alpha & \dots & 1 & \\ 0 & & & & & \ddots \\ & & & & & & 1 \end{pmatrix} = I_n + \alpha\, E_{jk} \in \mathbf{M}_p(K),$$

(α en position (k,j))

$k^{\text{ème}}$ colonne $\quad$ $j^{\text{ème}}$ colonne

on a : $AT_{j,k,\alpha} = \begin{pmatrix} a_{11} & \dots & a_{1k} + \alpha a_{1j} & \dots & a_{1p} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \dots & a_{nk} + \alpha a_{nj} & \dots & a_{np} \end{pmatrix}$.

$k^{\text{ème}}$ colonne

De plus, $T_{j,k,\alpha}$ est inversible, car : $T_{j,k,\alpha}T_{j,k,-\alpha} = (I_n + \alpha E_{jk})(I_n - \alpha E_{jk}) = I_n$.

Ainsi, le remplacement de C_k par $C_k + \alpha C_j$ ($k \neq j$) revient à la postmultiplication par la matrice inversible $T_{j,k,\alpha}$. ■

De même, les opérations élémentaires sur les lignes ($L_j \longleftrightarrow L_k$, $L_j \longleftarrow \alpha L_j$, $L_k \longleftarrow L_k + \alpha L_j$) reviennent à des **prémultiplications** par des matrices inversibles $\mathrm{P}_{j,k}$, $\mathrm{D}_{j,\alpha}$, $\mathrm{T}_{k,j,\alpha}$. ■

D'après 8.1.6 Prop. 4 p. 277, on en déduit le résultat suivant.

♦ **Proposition**

Les opérations élémentaires sur les colonnes ou les lignes ne changent pas le rang.

Autrement dit, si $B \in \mathbf{M}_{n,p}(K)$ se déduit de $A \in \mathbf{M}_{n,p}(K)$ par des opérations élémentaires, alors $\mathrm{rg}(B) = \mathrm{rg}(A)$.

Méthode de Gauss

Soit $A \in \mathbf{M}_{n,p}(K)$.

Nous allons, par des opérations élémentaires, construire une matrice T de même rang que A et telle que le rang de T soit évident.

Si la $1^{\text{ère}}$ ligne de A est nulle, la matrice de $\mathbf{M}_{n-1,p}(K)$ obtenue en supprimant dans A la $1^{\text{ère}}$ ligne a le même rang que A. On peut donc supposer que la $1^{\text{ère}}$ ligne de A n'est pas nulle.

Par permutation de colonnes, on se ramène à une matrice de même rang que A, et dont le $(1,1)^{\text{ème}}$ terme est $\neq 0$. En multipliant la $1^{\text{ère}}$ colonne par l'inverse de cet élément, on se ramène à une matrice $A_1 = (\alpha_{ij})_{ij}$ telle que $\alpha_{11} = 1$.

Pour chaque j de $\{2,\dots,p\}$, le remplacement de la colonne C_j par $C_j - \alpha_{1j}C_1$ fait apparaître une matrice A_2, de même rang que A, et dont la $1^{\text{ère}}$ ligne est $(1,0,\dots,0)$:

$$A_1 = \underset{\begin{matrix} C_1 & C_2 & \dots & C_p \end{matrix}}{\begin{pmatrix} 1 & \alpha_{12} & \dots & \alpha_{1p} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2p} \\ \vdots & \vdots & & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{np} \end{pmatrix}} \rightsquigarrow A_2 = \underset{\begin{matrix} C_1 & C_2 - \alpha_{12}C_1 & \dots & C_p - \alpha_{1p}C_1 \end{matrix}}{\begin{pmatrix} 1 & 0 & \text{———} & 0 \\ \alpha_{21} & \alpha_{22} - \alpha_{12}\alpha_{21} & \dots & \alpha_{2p} - \alpha_{1p}\alpha_{21} \\ \vdots & \vdots & & \vdots \\ \alpha_{n1} & \alpha_{n2} - \alpha_{12}\alpha_{n1} & \dots & \alpha_{np} - \alpha_{1p}\alpha_{n1} \end{pmatrix}}.$$

En réitérant le procédé sur la matrice à $n-1$ lignes et $p-1$ colonnes située en bas à droite dans A_2, on arrive, au bout d'un nombre fini d'opérations élémentaires sur les colonnes de A et de suppressions d'éventuelles lignes ou colonnes nulles, à une matrice T (qui a donc le même rang que A) de la forme :

$$T = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ & & 1 \\ & \dots & \end{pmatrix}$$

Il est clair que, puisque les colonnes de T forment une famille libre, le rang de T est le nombre de colonnes de T (qui n'est pas nécessairement le nombre de colonnes de A).

EXEMPLE :

Calculer le rang de la matrice $A = \begin{pmatrix} 2 & 3 & 5 \\ 1 & 4 & 0 \\ -1 & -3 & -1 \\ 3 & 6 & 6 \end{pmatrix} \in \mathbf{M}_{4,3}(\mathbb{R})$,

$$A \rightsquigarrow \begin{pmatrix} 1 & 3 & 5 \\ \frac{1}{2} & 4 & 0 \\ -\frac{1}{2} & -3 & -1 \\ \frac{3}{2} & 6 & 6 \end{pmatrix} \text{ par } C_1 \longleftarrow \frac{1}{2}C_1$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{2} & \frac{5}{2} & -\frac{5}{2} \\ -\frac{1}{2} & -\frac{3}{2} & \frac{3}{2} \\ \frac{3}{2} & \frac{3}{2} & -\frac{3}{2} \end{pmatrix} \text{ par } C_2 \longleftarrow C_2 - 3C_1 \text{ et } C_3 \longleftarrow C_3 - 5C_1$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & 1 \\ -\frac{1}{2} & -\frac{3}{5} \\ \frac{3}{2} & \frac{3}{5} \end{pmatrix} \text{ par } C_2 \longleftarrow \frac{2}{5}C_2,$$

la dernière colonne, colinéaire à C_2, pouvant être supprimée.

Finalement : $\text{rg}(A) = 2$.

Remarques :

1) La méthode de Gauss peut être appliquée aux lignes (à la place des colonnes). On peut aussi utiliser un mélange d'opérations élémentaires sur lignes et sur colonnes.

2) Si A est inversible (donc carrée), des opérations élémentaires sur lignes et colonnes permettent de passer de A à $\mathbf{I}_n$, donc de calculer A^{-1}.

8.1.8 Transposition

♦ **Définition** Pour toute matrice $A = (a_{ij})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}} = \begin{pmatrix} a_{11} & \dots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{np} \end{pmatrix}$ de $\mathbf{M}_{n,p}(K)$, on appelle **transposée** de A la matrice, notée ${}^tA$, de $\mathbf{M}_{p,n}(K)$ définie par : ${}^tA = (a_{ij})_{\substack{1\leqslant j\leqslant p\\1\leqslant i\leqslant n}} = \begin{pmatrix} a_{11} & \dots & a_{n1} \\ \vdots & & \vdots \\ a_{1p} & \dots & a_{np} \end{pmatrix}$.

Autrement dit, ${}^tA$ est obtenue à partir de A par symétrie par rapport à la «diagonale« (bien que A soit rectangulaire).

Par exemple, si $A = \begin{pmatrix} a & b & c \\ \alpha & \beta & \gamma \end{pmatrix}$, alors ${}^tA = \begin{pmatrix} a & \alpha \\ b & \beta \\ c & \gamma \end{pmatrix}$.

On peut aussi dire que ${}^tA$ s'obtient à partir de A en échangeant les notions de ligne et de colonne.

En particulier, la transposée d'une matrice-ligne est une matrice-colonne et réciproquement :

$$ {}^t\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (x_1 \ \dots \ x_n), \quad {}^t(x_1 \ \dots \ x_n) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}. $$

♦ **Proposition**

1) $\forall A \in \mathbf{M}_{n,p}(K)$, ${}^t({}^tA) = A$.

2) $\forall \alpha \in K, \forall (A,B) \in (\mathbf{M}_{n,p}(K))^2$, ${}^t(\alpha A + B) = \alpha\, {}^tA + {}^tB$.

3) $\forall A \in \mathbf{M}_{n,p}(K), \forall B \in \mathbf{M}_{p,q}(K)$, ${}^t(AB) = {}^tB\, {}^tA$.

4) $\forall A \in \mathbf{GL}_n(K)$, $\left({}^tA \in \mathbf{GL}_n(K) \text{ et } ({}^tA)^{-1} = {}^t(A^{-1})\right)$.

Preuve :

1) Immédiat.

2) En notant $A = (a_{ij})_{ij}$, $B = (b_{ij})_{ij}$, on a $\alpha A + B = (\alpha a_{ij} + b_{ij})_{ij}$, donc ${}^t(\alpha A + B) = (\alpha a_{ij} + b_{ij})_{ji}$, et $\alpha\, {}^tA + {}^tB = \alpha(a_{ij})_{ji} + (b_{ij})_{ji} = (\alpha a_{ij} + b_{ij})_{ji}$, d'où ${}^t(\alpha A + B) = \alpha\, {}^tA + {}^tB$.

3) En notant $A = (a_{ij})_{ij}$, $B = (b_{jk})_{jk}$, on a ${}^tA = (\alpha_{ji})_{ji}$, ${}^tB = (\beta_{kj})_{kj}$ où $\alpha_{ji} = a_{ij}$ et $\beta_{kj} = b_{jk}$, et $AB = (c_{ik})_{ik}$, ${}^tB\, {}^tA = (\gamma_{ki})_{ki}$ où $c_{ik} = \sum_{j=1}^{p} a_{ij}b_{jk}$ et :

$$ \gamma_{ki} = \sum_{j=1}^{p} \beta_{kj}\alpha_{ji} = \sum_{J=1}^{p} b_{jk}a_{ij} = c_{ik}. $$

Ainsi : ${}^tB\, {}^tA = {}^t(AB)$.

4) Soit $A \in \mathbf{GL}_n(K)$.

Puisque ${}^tA\, {}^t(A^{-1}) = {}^t(A^{-1}A) = {}^t\mathrm{I}_n = \mathrm{I}_n$, ${}^tA$ est inversible et $({}^tA)^{-1} = {}^t(A^{-1})$. ■

D'après *4)* ci-dessus, pour $A \in \mathbf{GL}_n(K)$, on pourra noter ${}^tA^{-1}$ au lieu de $({}^tA)^{-1}$ ou ${}^t(A^{-1})$.

Exercice

◇ **8.1.27** Soient $a \in K - \{0\}$, $A = \begin{pmatrix} 0 & a & \cdots & a^{n-1} \\ \frac{1}{a} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & a \\ \frac{1}{a^{n-1}} & \cdots & \frac{1}{a} & 0 \end{pmatrix} \in \mathbf{M}_n(K)$,

c'est-à-dire $A = U\,{}^tV - \mathrm{I}_n$, où $U = \begin{pmatrix} 1 \\ \frac{1}{a} \\ \vdots \\ \frac{1}{a^{n-1}} \end{pmatrix}$, $V = \begin{pmatrix} 1 \\ a \\ \vdots \\ a^{n-1} \end{pmatrix}$.

a) Calculer A^k pour $k \in \mathbb{N}^*$.

b) Montrer que A est inversible et calculer A^{-1}.

c) Calculer A^k pour $k \in \mathbb{Z}$.

8.1.9 Trace d'une matrice carrée

◆ **Définition** Pour toute matrice carrée $A = (a_{ij})_{ij} \in \mathbf{M}_n(K)$, on définit la **trace** de A, notée $\mathrm{tr}(A)$, par : $\mathrm{tr}(A) = \sum_{i=1}^{n} a_{ii}$.

Autrement dit, $\mathrm{tr}(A)$ est la somme des éléments diagonaux de A.

◆ **Proposition**

1) L'application $\mathrm{tr} : \begin{array}{ccc} \mathbf{M}_n(K) & \longrightarrow & K \\ A & \longmapsto & \mathrm{tr}(A) \end{array}$ est une forme linéaire.

2) $\forall A \in \mathbf{M}_{n,p}(K), \forall B \in \mathbf{M}_{p,n}(K), \quad \mathrm{tr}(AB) = \mathrm{tr}(BA)$.

Preuve :

1) En notant $A = (a_{ij})_{ij}$, $B = (b_{ij})_{ij}$:

$$\mathrm{tr}(\alpha A + B) = \sum_{i=1}^{n} (\alpha a_{ii} + b_{ii}) = \alpha \sum_{i=1}^{n} a_{ii} + \sum_{i=1}^{n} b_{ii} = \alpha \mathrm{tr}(A) + \mathrm{tr}(B).$$

2) Remarquer d'abord que AB et BA sont carrées.

En notant $A = (a_{ij})_{ij}$, $B = (b_{jk})_{jk}$, on a :

$$\mathrm{tr}(AB) = \sum_{i=1}^{n} \left(\sum_{j=1}^{p} a_{ij} b_{ji} \right) = \sum_{j=1}^{p} \left(\sum_{i=1}^{n} b_{ji} a_{ij} \right) = \mathrm{tr}(BA).$$

Exercices

◇ **8.1.28** **Egalité de Wagner**

Montrer : $\forall A,B,C \in \mathbf{M}_2(K),\ (AB-BA)^2C - C(AB-BA)^2 = 0.$

◇ **8.1.29** Montrer qu'il n'existe pas $(A,B,C,D) \in \left(\mathbf{M}_n(\mathbb{R})\right)^4$ tel que : $\begin{cases} AC+DB = \mathrm{I}_n \\ CA+BD = 0 \end{cases}$.

◇ **8.1.30** Résoudre (S) $\begin{cases} \mathrm{tr}(X)Y + \mathrm{tr}(Y)X = \begin{pmatrix} 4 & 8 \\ 4 & -4 \end{pmatrix} \\ XY = \begin{pmatrix} 1 & 1 \\ 4 & -2 \end{pmatrix} \end{cases}$, d'inconnue $(X,Y) \in \left(\mathbf{M}_2(\mathbb{R})\right)^2$.

◇ **8.1.31** Soit $H \in \mathbf{M}_n(K)$ telle que $\mathrm{rg}(H) \leqslant 1$.

a) Montrer qu'il existe $U,V \in \mathbf{M}_{n,1}(K)$ tels que : $H = U\,{}^tV$ et $\mathrm{tr}(H) = {}^tVU$.

b) En déduire : $H^2 = \mathrm{tr}(H)H$.

◇ **8.1.32** Montrer, pour toute A de $\mathbf{M}_3(\mathbb{C})$: $A^2 = 0 \iff \begin{cases} \mathrm{rg}(A) \leqslant 1 \\ \mathrm{tr}(A) = 0 \end{cases}$.

(On pourra utiliser l'exercice 8.1.31).

◇ **8.1.33** Soient $A \in \mathbf{M}_{n,p}(K)$, $B \in \mathbf{M}_{q,n}(K)$. Montrer :

$$\left(\forall X \in \mathbf{M}_{p,q}(K),\ \mathrm{tr}(AXB) = 0\right) \iff BA = 0.$$

◇ **8.1.34** *a)* Trouver toutes les applications linéaires $f : \mathbf{M}_n(K) \longrightarrow \mathbf{M}_n(K)$ telles que :

$$\forall A,B \in \mathbf{M}(K),\quad f(AB) = f(BA).$$

b) Trouver toutes les applications linéaires $f : \mathbf{M}_n(K) \longrightarrow \mathbf{M}_n(K)$ telles que :

$$\forall A,B,C \in \mathbf{M}_n(K),\quad f(ABC) = f(BAC).$$

8.2 Changement de bases

8.2.1 Matrices de passage

◆ **Définition** Soient E un K-ev de dimension n, $\mathcal{B}$, $\mathcal{B}'$ deux bases de E.

On appelle **matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$**, et on note Pass $(\mathcal{B},\mathcal{B}')$, la matrice de $\mathbf{M}_n(K)$ dont les colonnes sont formées des composantes des vecteurs de $\mathcal{B}'$ exprimés sur la base $\mathcal{B}$, c'est-à-dire :

$$\text{Pass}\,(\mathcal{B},\mathcal{B}') = \text{Mat}_{\mathcal{B}}(\mathcal{B}').$$

EXEMPLE :

Soient $\mathcal{B} = (e_1,e_2)$ la base canonique de K^2, c'est-à-dire $e_1 = (1,0)$ et $e_2 = (0,1)$, et $u = (2,4)$, $v = (3,-1)$. Alors $\mathcal{B}' = (u,v)$ est une base de K^2 et la matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$ est $\begin{pmatrix} 2 & 3 \\ 4 & -1 \end{pmatrix}$, puisque $u = 2e_1 + 4e_2$, $v = 3e_1 - e_2$.

◆ **Proposition 1**

Pour toutes bases $\mathcal{B}$, $\mathcal{B}'$ de E : Pass $(\mathcal{B},\mathcal{B}') = \text{Mat}_{\mathcal{B}',\mathcal{B}}(\text{Id}_E)$.

Preuve :

Notons $\mathcal{B}' = (e'_1,\ldots,e'_n)$. Pour chaque j de $\{1,\ldots,n\}$, la $j^{\text{ème}}$ colonne de Mat $_{\mathcal{B}',\mathcal{B}}(\text{Id}_E)$ est formée par les composantes de $\text{Id}_E(e_j)$, c'est-à-dire e_j, sur la base $\mathcal{B}$. ∎

On remarquera qu'on exprime ici la matrice d'un endomorphisme (l'identité) par rapport à deux bases a priori différentes pour le départ et l'arrivée, ce qui est peu fréquent.

◆ **Proposition 2** Soient E un K-ev, $\mathcal{B}$, $\mathcal{B}'$, $\mathcal{B}''$ des bases de E. On a :

1) Pass $(\mathcal{B},\mathcal{B}'') = $ Pass $(\mathcal{B},\mathcal{B}')$Pass $(\mathcal{B}',\mathcal{B}'')$

2) Pass $(\mathcal{B},\mathcal{B}) = \mathrm{I}_n$

3) Pass $(\mathcal{B},\mathcal{B}')$ est inversible et $\big(\text{Pass}\,(\mathcal{B},\mathcal{B}')\big)^{-1} = $ Pass $(\mathcal{B}',\mathcal{B})$.

Preuve :

1) Pass $(\mathcal{B},\mathcal{B}'') = \text{Mat}_{\mathcal{B}'',\mathcal{B}}(\text{Id}_E) = \big(\text{Mat}_{\mathcal{B}',\mathcal{B}}(\text{Id}_E)\big)\big(\text{Mat}_{\mathcal{B}'',\mathcal{B}'}(\text{Id}_E)\big)$
$= $ Pass $(\mathcal{B},\mathcal{B}')$ Pass $(\mathcal{B}',\mathcal{B}'')$.

2) Pass $(\mathcal{B},\mathcal{B}) = \text{Mat}_{\mathcal{B},\mathcal{B}}(\text{Id}_E) = \mathrm{I}_n$.

3) Pass $(\mathcal{B},\mathcal{B}')$ Pass $(\mathcal{B}',\mathcal{B}) = $ Pass $(\mathcal{B},\mathcal{B}) = \mathrm{I}_n$.

Remarque :

Soient E un K-ev de dimension n,$\mathcal{B}$ une base de E. L'application $\mathcal{B}' \longmapsto$ Pass $(\mathcal{B},\mathcal{B}')$ est clairement une bijection de l'ensemble des bases de E sur $\mathbf{GL}_n(K)$. Ainsi :

- Toute matrice de passage est inversible
- Toute matrice inversible peut être considérée comme matrice de passage (on peut même choisir la base de départ, ou d'arrivée).

8.2.2 Changement de base pour un vecteur

♦ **Proposition** Soient E un K-ev, $\mathcal{B},\mathcal{B}'$ deux bases de E, $P = \text{Pass}(\mathcal{B},\mathcal{B}')$, $x \in E$, $X = \text{Mat}_{\mathcal{B}}(x)$, $X' = \text{Mat}_{\mathcal{B}'}(x)$. Alors :

$$\boxed{X = PX'}$$

Preuve :

$$X = \text{Mat}_{\mathcal{B}}(x) = \left(\text{Mat}_{\mathcal{B}',\mathcal{B}}(\text{Id}_E)\right)\left(\text{Mat}_{\mathcal{B}'}(x)\right) = PX'.$$

EXEMPLE :

Dans K^2, soient (e_1,e_2) la base canonique, $u_1 = (-2,1)$, $u_2 = (3,-2)$, $x = (x_1,x_2) \in K^2$. Il est clair que (u_1,u_2) est une base de K^2. En notant X_1, X_2 les composantes de x dans la base (u_1,u_2), on a :

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -2 & 3 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = \begin{pmatrix} -2X_1 + 3X_2 \\ X_1 - 2X_2 \end{pmatrix}.$$

Remarque :

Dans un changement de base pour un vecteur, on exprime donc naturellement les *anciennes coordonnées* (coordonnées de x dans $\mathcal{B}$) en fonction des *nouvelles coordonnées* (coordonnées de x dans $\mathcal{B}'$). Si l'on veut exprimer les nouvelles coordonnées de x en fonction des anciennes coordonnées de x, on dispose de la formule $X' = P^{-1}X$, dont l'emploi nécessite le calcul de l'inverse de P.

8.2.3 Changement de bases pour une application linéaire

1) Formule de changement de bases

♦ **Proposition**

Soient E, F deux K-ev

$\mathcal{B},\mathcal{B}'$ deux bases de E, $P = \text{Pass}(\mathcal{B},\mathcal{B}')$

$\mathcal{C},\mathcal{C}'$ deux bases de F, $Q = \text{Pass}(\mathcal{C},\mathcal{C}')$

$f \in \mathcal{L}(E,F)$, $A = \text{Mat}_{\mathcal{B},\mathcal{C}}(f)$, $A' = \text{Mat}_{\mathcal{B}',\mathcal{C}'}(f)$.

Alors :

$$\boxed{A' = Q^{-1}AP}.$$

Preuve :

$$\begin{aligned} A' &= \text{Mat}_{\mathcal{B}',\mathcal{C}'}(f) = \text{Mat}_{\mathcal{B}',\mathcal{C}'}(\text{Id}_E \circ f \circ \text{Id}_E) \\ &= \left(\text{Mat}_{\mathcal{C},\mathcal{C}'}(\text{Id}_E)\right)\left(\text{Mat}_{\mathcal{B},\mathcal{C}}(f)\right)\left(\text{Mat}_{\mathcal{B}',\mathcal{B}}(\text{Id}_E)\right) = Q^{-1}AP. \end{aligned}$$

2) *Matrices équivalentes*

◆ **Définition** Soient $A, B \in \mathbf{M}_{n,p}(K)$. On dit que A est **équivalente** à B, et on note A eq B, si et seulement si :

$$\exists\, (P,Q) \in \mathbf{GL}_p(K) \times \mathbf{GL}_n(K), \quad B = Q^{-1}AP.$$

D'après la Prop. précédente, A eq B si et seulement si A et B représentent (dans des bases) une même application linéaire.

◆ **Proposition 1**

La relation eq est une relation d'équivalence dans $\mathbf{M}_{n,p}(K)$.

Preuve :

1) Réflexivité : $\forall A \in \mathbf{M}_{n,p}(K)$, $A = \mathrm{I}_n A \mathrm{I}_p$.

2) Symétrie :

S'il existe $(P,Q) \in \mathbf{GL}_p(K) \times \mathbf{GL}_n(K)$ tel que $B = Q^{-1}AP$, alors $A = (Q^{-1})^{-1}BP^{-1}$ et $(P^{-1}, Q^{-1}) \in \mathbf{GL}_p(K) \times \mathbf{GL}_n(K)$, donc B eq A.

3) Transitivité :

Supposons A eq B et B eq C. Il existe $P \in \mathbf{GL}_p(K)$, $Q \in \mathbf{GL}_n(K)$, $R \in \mathbf{GL}_p(K)$, $S \in \mathbf{GL}_n(K)$ telles que : $B = Q^{-1}AP$ et $C = S^{-1}BR$.

Alors : $C = S^{-1}Q^{-1}APR = (QS)^{-1}A(PR)$ et $(PR, QS) \in \mathbf{GL}_p(K) \times \mathbf{GL}_n(K)$, d'où A eq C. ■

Puisque la relation eq est symétrique, on peut exprimer A eq B par : A et B **sont équivalentes**.

◆ **Proposition 2** Soient $A \in \mathbf{M}_{n,p}(K)$, $r = \mathrm{rg}(A)$. Alors A est équivalente à la matrice $\mathrm{J}_{n,p,r}$ définie par : $\mathrm{J}_{n,p,r} = \begin{pmatrix} 1 & & 0 & 0 \\ & \ddots & & \\ 0 & & 1 & \\ & & & \\ 0 & & 0 & 0 \end{pmatrix} \begin{matrix} \updownarrow r \\ \updownarrow n-r \\ \\ \\ \end{matrix} = \begin{pmatrix} \mathrm{I}_r & 0_{r,p-r} \\ 0_{n-r,r} & 0_{n-r,p-r} \end{pmatrix}$

$r \quad p-r$

(en particulier : $\mathrm{J}_{n,p,0} = 0$).

Preuve :

Soient E, F deux K-ev de dimensions respectives p,n (il en existe), $\mathcal{B}$ et $\mathcal{C}$ des bases de E et F, respectivement (il en existe), $f \in \mathcal{L}(E,F)$ représentée par A dans les bases $\mathcal{B}$ et $\mathcal{C}$: $\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f) = A$.

D'après le théorème du rang (7.3.1 Th. 1 p. 254), le sev $\mathrm{Ker}(f)$ de E est de dimension $p-r$, donc admet au moins une base $(e_{r+1}, \ldots, e_p)$.

D'après le théorème de la base incomplète, forme faible (6.4 Th. 2 p. 229), il existe $e_1, \ldots, e_r \in E$ tels que $\mathcal{B}' = (e_1, \ldots, e_r, e_{r+1}, \ldots, e_p)$ soit une base de E.

Notons $f_1 = f(e_1), \ldots, f_r = f(e_r)$.

La famille $(f_1, \ldots, f_r)$ est libre; en effet, si $(\lambda_1, \ldots, \lambda_r) \in K^r$ est tel que $\sum_{i=1}^{r} \lambda_i f_i = 0$,

alors : $\sum_{i=1}^{r} \lambda_i e_i \in \text{Ker}(f) \cap \text{Vect}(e_1, \ldots, e_r) = \{0\}$,

donc $\lambda_1 = \ldots = \lambda_r = 0$ (cf. aussi 7.3.1 p. 255).

D'après le théorème de la base incomplète, forme faible, il existe $f_{r+1}, \ldots, f_n \in F$ tels que $\mathcal{C}' = (f_1, \ldots, f_r, f_{r+1}, \ldots, f_n)$ soit une base de F.

Puisque $f(e_1) = f_1, \ldots, f(e_r) = f_r$, $f(e_{r+1}) = 0, \ldots, f(e_p) = 0$, la matrice de f dans $\mathcal{B}'$ et $\mathcal{C}'$ est $J_{n,p,r}$, et donc A eq $J_{n,p,r}$.

♦ **Corollaire 1**

$$\forall (A, B) \in \left(\mathbf{M}_{n,p}(K)\right)^2, \left(A \text{ eq } B \iff \text{rg}(A) = \text{rg}(B)\right).$$

Preuve :

1) Si A eq B, alors A et B représentent une même application linéaire (dans des bases), donc ont le même rang.

2) Réciproquement, si $\text{rg}(A) = \text{rg}(B)$, alors A et B sont équivalentes à $J_{n,p,r}$, donc sont équivalentes entre elles.

♦ **Corollaire 2**

$$\forall A \in \mathbf{M}_{n,p}(K), \ \text{rg}({}^tA) = \text{rg}(A).$$

Preuve :

En notant $r = \text{rg}(A)$, il existe $(P, Q) \in \mathbf{GL}_p(K) \times \mathbf{GL}_n(K)$ tel que $A = Q^{-1} J_{n,p,r} P$. On a alors : ${}^tA = {}^tP \, {}^tJ_{n,p,r} \, {}^t(Q^{-1}) = ({}^tP^{-1})^{-1} J_{p,n,r} \, {}^tQ^{-1}$,

et donc $\text{rg}({}^tA) = \text{rg}(J_{n,p,r}) = r$.

Exercices

◇ **8.2.1** Soient $A \in \mathbf{M}_{n,p}(K)$, $r = \mathrm{rg}(A)$. Montrer qu'il existe $A_1, \ldots, A_r \in \mathbf{M}_{n,p}(K)$ telles que :

$$\begin{cases} A = \sum_{k=1}^{r} A_k \\ \forall k \in \{1, \ldots, r\},\ \mathrm{rg}(A_k) = 1. \end{cases}$$

◇ **8.2.2** Etablir : $\forall A \in \mathbf{M}_n(\mathbb{C}),\ \exists (B,C) \in (\mathbf{GL}_n(\mathbb{C}))^2,\ A = B + C$.

◇ **8.2.3** Soient $A \in \mathbf{M}_{n,p}(K)$ et $r \in \mathbb{N}^*$ tel que $r \leqslant \mathrm{Min}(n,p)$. Démontrer :

$$\mathrm{rg}(A) \leqslant r \iff \big(\exists (B,C) \in \mathbf{M}_{n,r}(K) \times \mathbf{M}_{r,p}(K),\ A = BC\big).$$

En particulier : $\mathrm{rg}A \leqslant 1 \iff \big(\exists (U,V) \in \mathbf{M}_{n,1}(K) \times \mathbf{M}_{p,1}(K),\ A = U\,{}^tV\big)$.

◇ **8.2.4*** *a)* Soit $A \in \mathbf{M}_{n,p}(K)$. Montrer que, par une suite finie d'opérations élémentaires sur les colonnes et sur les lignes, on peut passer de A à $J_{n,p,r}$, où $r = \mathrm{rg}(A)$.

b) En déduire que, pour tout (A,B) de $\big(\mathbf{M}_{n,p}(K)\big)^2$, les deux propriétés suivantes sont équivalentes :

(i) $\mathrm{rg}(A) = \mathrm{rg}(B)$

(ii) On peut passer de A à B par une suite finie d'opérations élémentaires sur les colonnes et sur les lignes.

c) Montrer que la partie de $\mathbf{GL}_n(K)$ formée par les matrices des opérations élémentaires (c'est-à-dire : les $P_{j,k}$, $D_{j,\alpha}$, $T_{j,k,\alpha}$, cf. 8.1.7 pp. 279-280) engendre le groupe $\mathbf{GL}_n(K)$.

◇ **8.2.5*** Soient E, F deux K-ev de dimension finie, $f, g \in \mathcal{L}(E,F)$.

a) On suppose $\mathrm{rg}(g) \leqslant \mathrm{rg}(f)$. Montrer :

$\alpha)$ $\exists h \in \mathcal{GL}(F),\ \exists k \in \mathcal{L}(E),\ h \circ g = f \circ k$

$\beta)$ $\exists u \in \mathcal{GL}(E),\ \exists v \in \mathcal{L}(F),\ g \circ u = v \circ f$.

b) On suppose $\mathrm{rg}(g) = \mathrm{rg}(f)$. Montrer : $\exists h \in \mathcal{GL}(F),\ \exists k \in \mathcal{GL}(E),\ h \circ g = f \circ k$.

8.2.4 Changement de base pour un endomorphisme

La Prop. suivante est un cas particulier de la Prop. de 8.2.3 *1)* p. 287.

♦ **Proposition 1**

Soient | E un K-ev de dimension n
| $\mathcal{B},\mathcal{B}'$ deux bases de E, $P = \text{Pass}(\mathcal{B},\mathcal{B}')$
| $f \in \mathcal{L}(E)$, $A = \text{Mat}_{\mathcal{B}}(f)$, $A' = \text{Mat}_{\mathcal{B}'}(f)$.

Alors : $\boxed{A' = P^{-1}AP}$.

♦ **Définition 1** Soient $A,B \in \mathbf{M}_n(K)$. On dit que A est **semblable** à B, et on note $A \sim B$, si et seulement s'il existe $P \in \mathbf{GL}_n(K)$ telle que : $B = P^{-1}AP$.

♦ **Proposition 2**

La relation $\sim$ est une relation d'équivalence dans $\mathbf{M}_n(K)$.

Preuve :

1) Réflexivité : $\forall A \in \mathbf{M}_n(K)$, $A = \mathrm{I}_n A \mathrm{I}_n$.

2) Symétrie :

S'il existe $P \in \mathbf{GL}_n(K)$ telle que $B = P^{-1}AP$,

alors $A = (P^{-1})^{-1}BP^{-1}$ et $P^{-1} \in \mathbf{GL}_n(K)$, donc $B \sim A$.

3) Transitivité :

Supposons $A \sim B$ et $B \sim C$. Il existe $P,Q \in \mathbf{GL}_n(K)$ telles que $B = P^{-1}AP$ et $C = Q^{-1}BQ$.

Alors, $C = Q^{-1}P^{-1}APQ = (PQ)^{-1}A(PQ)$ et $PQ \in \mathbf{GL}_n(K)$, donc $A \sim C$. ■

Puisque la relation $\sim$ est symétrique, on peut exprimer $A \sim B$ par : A et B **sont semblables**.

La relation $\sim$ est appelée la **similitude des matrices carrées**.

♦ **Proposition 3**

$$\forall (A,B) \in \big(\mathbf{M}_n(K)\big)^2, \quad \big(A \sim B \Longrightarrow \text{tr}(A) = \text{tr}(B)\big).$$

Preuve :

Supposons $A \sim B$. Il existe $P \in \mathbf{GL}_n(K)$ telle que $B = P^{-1}AP$, d'où (cf. 8.1.9 Prop. *2)* p. 284) :

$$\text{tr}(B) = \text{tr}\big(P^{-1}(AP)\big) = \text{tr}\big((AP)P^{-1}\big) = \text{tr}(A).$$

Remarques :

1) Il est clair que, si deux matrices carrées sont semblables, alors elles sont équivalentes.

2) Mais (si $n \geqslant 2$) deux matrices équivalentes peuvent ne pas être semblables. Par exemple, pour $n = 2$, les matrices $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ sont équivalentes puisqu'elles sont de même rang 1, mais ne sont pas semblables puisqu'elles n'ont pas la même trace.

3) Soit $A \in \mathbf{M}_n(K)$. S'il existe $\alpha \in K$ tel que $A \sim \alpha \mathrm{I}_n$, alors $A = \alpha \mathrm{I}_n$. En effet, pour toute P de $\mathbf{GL}_n(K)$: $P(\alpha \mathrm{I}_n)P^{-1} = \alpha \mathrm{I}_n$.

4) Si $n \geqslant 2$, deux matrices carrées peuvent avoir la même trace sans être semblables. Par exemple, pour $n = 2$, les matrices $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ont la même trace, mais ne sont pas semblables, puisqu'elles ne sont même pas équivalentes (la $1^{\text{ère}}$ est de rang 0, la 2^{nde} de rang 1).

◆ **Définition 2** Soient E un K-ev, $f \in \mathcal{L}(E)$. On appelle **trace** de f, et on note $\mathrm{tr}(f)$, la trace de n'importe quelle matrice représentant l'endomorphisme f.

Cette définition est correcte puisque, d'après la Prop. précédente, toutes les matrices représentant l'endomorphisme f ont la même trace. ∎

Des propriétés de la trace d'une matrice carrée, on déduit aisément la Prop. suivante.

◆ **Proposition 4** Soit E un K-ev.

1) L'application $\mathrm{tr} : \begin{array}{ccc} \mathcal{L}(E) & \longrightarrow & K \\ f & \longmapsto & \mathrm{tr}(f) \end{array}$ est une forme linéaire.

2) $\forall (f,g) \in \big(\mathcal{L}(E)\big)^2, \quad \mathrm{tr}(g \circ f) = \mathrm{tr}(f \circ g)$

3) $\forall f \in \mathcal{L}(E), \forall h \in \mathcal{GL}(E), \quad \mathrm{tr}(h^{-1} \circ f \circ h) = \mathrm{tr}(f)$.

Exercices

◇ **8.2.6** On note S : $\begin{array}{ccc} \mathbf{M}_n(K) & \longrightarrow & K \\ A = (a_{ij})_{ij} & \longmapsto & \displaystyle\sum_{1 \leqslant i,j \leqslant n} a_{ij}a_{ji} \end{array}$

Montrer : $\forall A, B \in \mathbf{M}_n(K), \ \big(A \sim B \Longrightarrow S(A) = S(B)\big)$.

◇ **8.2.7** Les matrices $A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ de $\mathbf{M}_4(\mathbb{R})$ sont-elles semblables ?

8.3 Matrices remarquables

8.3.1 Matrices symétriques, matrices antisymétriques

Dans ce § 8.3.1, on suppose $2 \cdot 1_K \neq 0$ (où 1_K est le neutre de K pour la multiplication); ainsi 2 (confondu avec $2 \cdot 1_K$) admet dans K un inverse, noté $\frac{1}{2}$. On dit aussi que K est **de caractéristique** $\neq 2$ (cf. exercice 2.3.4 p. 58). C'est le cas si $K = \mathbb{R}$ ou $\mathbb{C}$.

Soit $n \in \mathbb{N}^*$.

1) Matrices symétriques

♦ **Définition**

Une matrice carrée A de $\mathbf{M}_n(K)$ est dite **symétrique** si et seulement si : ${}^tA = A$.

On note $\mathbf{S}_n(K)$ l'ensemble des matrices symétriques d'ordre n à coefficients dans K.

♦ **Proposition 1**

$\mathbf{S}_n(K)$ est un sev de $\mathbf{M}_n(K)$.

Preuve :

1) $0 \in \mathbf{S}_n(K)$.

2) Soient $\alpha \in K$, $A, B \in \mathbf{S}_n(K)$. On a : ${}^t(\alpha A + B) = \alpha\, {}^tA + {}^tB = \alpha A + B$, donc $\alpha A + B \in \mathbf{S}_n(K)$.

Remarques :

1) Il est clair que la famille $(\mathrm{E}_{ii})_{1 \leqslant i \leqslant n} \cup (\mathrm{E}_{ij} + \mathrm{E}_{ji})_{1 \leqslant i < j \leqslant n}$ est une base de $\mathbf{S}_n(K)$, et donc $\dim\left(\mathbf{S}_n(K)\right) = \dfrac{n(n+1)}{2}$.

Par exemple, pour $n = 2$, $\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)$ est une base de $\mathbf{S}_2(K)$; toute matrice symétrique d'ordre 2 s'écrit d'une manière unique $\begin{pmatrix} a & b \\ b & d \end{pmatrix}$ (où $(a,b,d) \in K^3$), c'est-à-dire : $a\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + d\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

2) Si $n \geqslant 2$, le produit de deux matrices symétriques peut ne pas être symétrique, comme le montre (pour $n = 2$) l'exemple :

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

Cependant, la formule ${}^t(AB) = {}^tB\, {}^tA$ montre la Prop. suivante.

♦ **Proposition 2**

$$\forall (A,B) \in \left(\mathbf{S}_n(K)\right)^2,\ \left(AB \in \mathbf{S}_n(K) \iff AB = BA\right). \qquad \blacksquare$$

◆ **Proposition 3**

$$\forall A \in \mathbf{S}_n(K) \cap \mathbf{GL}_n(K),\ A^{-1} \in \mathbf{S}_n(K).$$

Preuve :

Soit $A \in \mathbf{S}_n(K) \cap \mathbf{GL}_n(K)$; on a alors ${}^t(A^{-1}) = ({}^tA)^{-1} = A^{-1}$, donc $A^{-1} \in \mathbf{S}_n(K)$.

2) *Matrices antisymétriques*

◆ **Définition** Une matrice carrée A de $\mathbf{M}_n(K)$ est dite **antisymétrique** si et seulement si : ${}^tA = -A$. On note $\mathbf{A}_n(K)$ l'ensemble des matrices antisymétriques d'ordre n à coefficients dans K.

◆ **Proposition 1**

$\mathbf{A}_n(K)$ est un sev de $\mathbf{M}_n(K)$.

Preuve :

1) $0 \in \mathbf{A}_n(K)$.

2) Soient $\alpha \in K$, $A, B \in \mathbf{A}_n(K)$. On a : ${}^t(\alpha A+B) = \alpha\,{}^tA + {}^tB = -\alpha A - B = -(\alpha A+B)$, donc $\alpha A + B \in \mathbf{A}_n(K)$.

Remarques :

1) Il est clair que la famille $(E_{ij} - E_{ji})_{1 \leqslant i < j \leqslant n}$ est une base de $\mathbf{A}_n(K)$, et donc $\dim(\mathbf{A}_n(K)) = \dfrac{n(n-1)}{2}$.

Par exemple, pour $n = 3$, $\left(\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}\right)$

est une base de $\mathbf{A}_3(K)$; toute matrice antisymétrique d'ordre 3 s'écrit d'une manière unique $\begin{pmatrix} 0 & -a & -b \\ a & 0 & -c \\ b & c & 0 \end{pmatrix}$ (où $(a,b,c) \in K^3$), c'est-à-dire

$$a\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + b\begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} + c\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}.$$

2) Si $n \geqslant 3$, le produit de deux matrices antisymétriques peut n'être ni symétrique ni antisymétrique, comme le montre (pour $n = 3$) l'exemple :

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

Cependant, soient $A, B \in \mathbf{M}_n(K)$ telles que $AB = BA$. Si A et B sont symétriques ou antisymétriques (quatre cas), alors AB est symétrique ou antisymétrique « suivant une règle des signes » car, comme ${}^tA = \varepsilon A$, ${}^tB = \varepsilon' B$, $(\varepsilon, \varepsilon') \in \{-1,1\}^2$, on a :

$${}^t(AB) = {}^tB\,{}^tA = \varepsilon'\varepsilon BA = \varepsilon'\varepsilon AB.$$

♦ **Proposition 2**

Les sev $\mathbf{S}_n(K)$ et $\mathbf{A}_n(K)$ sont supplémentaires dans $\mathbf{M}_n(K)$.

Preuve :

1) Soit $A \in \mathbf{S}_n(K) \cap \mathbf{A}_n(K)$. On a alors ${}^tA = A$ et ${}^tA = -A$, d'où $2A = 0$, donc $A = 0$. Ainsi : $\mathbf{S}_n(K) \cap \mathbf{A}_n(K) = \{0\}$.

2) Soit $M \in \mathbf{M}_n(K)$. Il est clair que :

$$\begin{cases} M = \dfrac{1}{2}(M + {}^tM) + \dfrac{1}{2}(M - {}^tM) \\ \dfrac{1}{2}(M + {}^tM) \in \mathbf{S}_n(K), \quad \dfrac{1}{2}(M - {}^tM) \in \mathbf{A}_n(K) \end{cases},$$

ce qui montre : $\mathbf{S}_n(K) + \mathbf{A}_n(K) = \mathbf{M}_n(K)$.

Pour $M \in \mathbf{M}_n(K)$, la matrice symétrique $\dfrac{1}{2}(M + {}^tM)$ s'appelle la **partie symétrique** de M, et la matrice antisymétrique $\dfrac{1}{2}(M - {}^tM)$ s'appelle la **partie antisymétrique** de M. Remarquer l'analogie avec les notions de partie paire et partie impaire d'une fonction (Tome 1, 4.1.3).

8.3.2 Matrices triangulaires

Soit $n \in \mathbb{N}^*$.

♦ **Définition** Soit $A \in \mathbf{M}_n(K)$.

1) On dit que A est **triangulaire** (ou : **trigonale**) **supérieure** si et seulement si :

$$\forall (i,j) \in \{1,\ldots,n\}^2, \quad (i > j \Longrightarrow a_{ij} = 0).$$

On note $\mathbf{T}_{n,s}(K)$ l'ensemble des matrices triangulaires supérieures d'ordre n à coefficients dans K.

2) On dit que A est **triangulaire** (ou : **trigonale**) **inférieure** si et seulement si :

$$\forall (i,j) \in \{1,\ldots,n\}^2, \ (i < j \Longrightarrow a_{ij} = 0).$$

On note $\mathbf{T}_{n,i}(K)$ l'ensemble des matrices triangulaires inférieures d'ordre n à coefficients dans K.

3) On dit que A est **triangulaire** (ou : **trigonale**) si et seulement si A est triangulaire supérieure ou triangulaire inférieure.

EXEMPLES :

• $\begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}$ est triangulaire supérieure • $\begin{pmatrix} 3 & 0 & 0 \\ -1 & 0 & 0 \\ 4 & 1 & 2 \end{pmatrix}$ est triangulaire inférieure.

Remarque : $\forall A \in \mathbf{M}_n(K), \ \big(A \in \mathbf{T}_{n,i}(K) \Longleftrightarrow {}^tA \in \mathbf{T}_{n,s}(K)\big)$.

La Prop. suivante est immédiate.

◆ **Proposition 1**

$\mathbf{T}_{n,s}(K)$ et $\mathbf{T}_{n,i}(K)$ sont des sev de $\mathbf{M}_n(K)$.

Remarque :

Il est clair que la famille $(E_{ij})_{1\leqslant i\leqslant j\leqslant n}$ est une base de $\mathbf{T}_{n,s}(K)$, et donc :

$$\dim\left(\mathbf{T}_{n,s}(K)\right) = \frac{n(n+1)}{2}.$$

◆ **Proposition 2**

$\mathbf{T}_{n,s}(K)$ est une sous-algèbre unitaire de l'algèbre unitaire $\mathbf{M}_n(K)$.

Preuve :

1) $\mathbf{T}_{n,s}(K)$ est un sev de $\mathbf{M}_n(K)$.

2) Soient $A = (a_{ij})_{ij}$, $B = (b_{ij})_{ij}$ deux éléments de $\mathbf{T}_{n,s}(K)$. Soit $(i,j) \in \{1,\ldots,n\}^2$ tel que $i > j$. Le $(i,j)^{\text{ème}}$ terme de AB vaut $\sum_{k=1}^{n} a_{ik}b_{kj}$. Pour chaque k de $\{1,\ldots,n\}$:

- si $i > k$, alors $a_{ik} = 0$ (car $A \in \mathbf{T}_{n,s}(K)$)
- si $k \geqslant i$, alors $k > j$ et donc $b_{kj} = 0$ (car $B \in \mathbf{T}_{n,s}(K)$).

Ainsi : $\forall k \in \{1,\ldots,n\}$, $a_{ik}b_{kj} = 0$, et donc : $\sum_{k=1}^{n} a_{ik}b_{kj} = 0$, ce qui montre : $AB \in \mathbf{T}_{n,s}(K)$.

3) $I_n \in \mathbf{T}_{n,s}(K)$. ∎

Remarques :

1) Les termes diagonaux du produit de deux matrices triangulaires supérieures sont les produits des termes diagonaux de ces deux matrices :

$$\begin{pmatrix} a_{11} & & \cdots \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix}\begin{pmatrix} b_{11} & & \cdots \\ & \ddots & \\ 0 & & b_{nn} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & & \cdots \\ & \ddots & \\ 0 & & a_{nn}b_{nn} \end{pmatrix}.$$

2) En particulier, les termes diagonaux d'une puissance d'une matrice triangulaire sont les puissances des termes diagonaux de cette matrice :

$$\begin{pmatrix} a_{11} & & \cdots \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix}^k = \begin{pmatrix} a_{11}^k & & \cdots \\ & \ddots & \\ 0 & & a_{nn}^k \end{pmatrix}.$$

♦ **Proposition 3**

$\forall A \in \mathbf{T}_{n,s}(K) \cap \mathbf{GL}_n(K),\ A^{-1} \in \mathbf{T}_{n,s}(K).$

Preuve :

Soit $A \in \mathbf{T}_{n,s}(K) \cap \mathbf{GL}_n(K)$.

D'après la Prop. 2 p. 296, pour toute M de $\mathbf{T}_{n,s}(K)$, AM est dans $\mathbf{T}_{n,s}(K)$, ce qui permet de considérer l'application $f_A : \begin{array}{ccc} \mathbf{T}_{n,s}(K) & \longrightarrow & \mathbf{T}_{n,s}(K) \\ M & \longmapsto & AM \end{array}$.

1) f_A est linéaire :

$$\forall \alpha \in K, \forall (M,N) \in \left(\mathbf{T}_{n,s}(K)\right)^2,\ f_A(\alpha M + N) = A(\alpha M + N)$$
$$= \alpha AM + AN = \alpha f_A(M) + f_A(N).$$

2) f_A est injective car, pour toute M de $\mathbf{T}_{n,s}(K)$:

$$f_A(M) = 0 \Longleftrightarrow AM = 0 \Longrightarrow A^{-1}(AM) = 0 \Longrightarrow M = 0.$$

3) Puisque f_A est un endomorphisme injectif d'un ev de dimension finie, f_A est bijectif (cf. 7.3.1 Th.2 p. 256). Comme $\mathrm{I}_n \in \mathbf{T}_{n,s}(K)$, il existe donc $B \in \mathbf{T}_{n,s}(K)$ telle que $f_A(B) = \mathrm{I}_n$. Alors $A^{-1} = B \in \mathbf{T}_{n,s}(K)$.

♦ **Proposition 4** Soit $A = \begin{pmatrix} a_{11} & & \cdots \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix} \in \mathbf{T}_{n,s}(K)$.

On a :

$$A \in \mathbf{GL}_n(K) \Longleftrightarrow \left(\forall i \in \{1,\ldots,n\},\ a_{ii} \neq 0\right).$$

De plus, si $A \in \mathbf{GL}_n(K)$, alors les termes diagonaux de A^{-1} sont les inverses des termes diagonaux de A :

$$A^{-1} = \begin{pmatrix} a_{11}^{-1} & & \cdots \\ & \ddots & \\ 0 & & a_{nn}^{-1} \end{pmatrix}.$$

Preuve :

• Supposons $A \in \mathbf{GL}_n(K)$. D'après la Prop. précédente, $A^{-1} \in \mathbf{T}_{n,s}(K)$.

En notant $A^{-1} = \begin{pmatrix} b_{11} & & \cdots \\ & \ddots & \\ 0 & & b_{nn} \end{pmatrix}$, on a : $\mathrm{I}_n = AB = \begin{pmatrix} a_{11}b_{11} & & \cdots \\ & \ddots & \\ 0 & & a_{nn}b_{nn} \end{pmatrix}$ d'où :

$\forall i \in \{1,\ldots,n\},\ a_{ii}b_{ii} = 1$, et donc : $\forall i \in \{1,\ldots,n\},\ \left(a_{ii} \neq 0 \text{ et } b_{ii} = a_{ii}^{-1}\right)$.

• Réciproquement, si $\left(\forall i \in \{1,\ldots,n\},\ a_{ii} \neq 0\right)$, alors, d'après la méthode de Gauss (8.1.7 p. 281), $\mathrm{rg}(A) = n$, et donc A est inversible.

Exercices

◇ **8.3.1** Montrer : $\forall Q \in \mathbb{C}_n[X],\ \exists! P \in \mathbb{C}_n[X],\ Q(X) = P(X) + P'\left(\frac{X}{2}\right) + \ldots + P^{(n)}\left(\frac{X}{2^n}\right)$.

◇ **8.3.2** Soit $A = \begin{pmatrix} a_{11} & & \cdots \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix} \in \mathbf{T}_{n,s}(K)$. Montrer que A est nilpotente si et seulement si $(\forall i \in \{1,\ldots,n\},\ a_{ii} = 0)$ et que, si A est nilpotente, alors $A^n = 0$.

◇ **8.3.3** *a)* Montrer que $G = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} ;\ (x,y,z) \in K^3 \right\}$ est un groupe multiplicatif.

b) Trouver le centre de G, c'est-à-dire $\{A \in G;\ \forall M \in G,\quad AM = MA\}$.

◇ **8.3.4** Déterminer le commutant de $\mathbf{T}_{n,s}(K)$ dans $\mathbf{M}_n(K)$, c'est-à-dire :

$$\left\{A \in \mathbf{M}_n(K);\ \forall T \in \mathbf{T}_{n,s}(K),\quad AT = TA\right\}.$$

8.3.3 Matrices diagonales

Soit $n \in \mathbb{N}^*$.

◆ **Définition** Une matrice carrée $A = (a_{ij})_{1 \leqslant i,j \leqslant n}$ de $\mathbf{M}_n(K)$ est dite **diagonale** si et seulement si :

$$\forall (i,j) \in \{1,\ldots,n\}^2,\quad (i \neq j \Longrightarrow a_{ij} = 0).$$

On note $\mathbf{D}_n(K)$ l'ensemble des matrices diagonales d'ordre n à coefficients dans K.

Pour tout $(\lambda_1,\ldots,\lambda_n)$ de K^n, on note $\mathrm{diag}(\lambda_1,\ldots,\lambda_n)$ la matrice diagonale de $\mathbf{M}_n(K)$ dont les termes diagonaux sont $\lambda_1,\ldots,\lambda_n$:

$$\mathrm{diag}(\lambda_1,\ldots,\lambda_n) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

Remarque : $\mathbf{T}_{n,s}(K) \cap \mathbf{T}_{n,i}(K) = \mathbf{D}_n(K)$.

La Proposition suivante est immédiate.

♦ **Proposition 1**
$\mathbf{D}_n(K)$ est une sous-algèbre commutative et unitaire de $\mathbf{M}_n(K)$.

Remarques :

1) Il est clair que la famille $(E_{ii})_{1\leqslant i\leqslant n}$ est une base de $\mathbf{D}_n(K)$, et donc dim $\left(\mathbf{D}_n(K)\right) = n$.

2) Pour tous $\alpha \in K$, $(\lambda_1,\ldots,\lambda_n) \in K^n$, $(\mu_1,\ldots,\mu_n) \in K^n$, on a :

$$\begin{cases} \alpha\mathrm{diag}(\lambda_1,\ldots,\lambda_n) = \mathrm{diag}(\alpha\lambda_1,\ldots,\alpha\lambda_n) \\ \mathrm{diag}(\lambda_1,\ldots,\lambda_n) + \mathrm{diag}(\mu_1,\ldots,\mu_n) = \mathrm{diag}(\lambda_1+\mu_1,\ldots,\lambda_n+\mu_n) \\ \mathrm{diag}(\lambda_1,\ldots,\lambda_n)\mathrm{diag}(\mu_1,\ldots,\mu_n) = \mathrm{diag}(\lambda_1\mu_1,\ldots,\lambda_n\mu_n). \end{cases}$$

On en déduit, par récurrence sur k, que pour tous $k \in \mathbb{N}^*$, $(\lambda_1,\ldots,\lambda_n) \in K^n$:

$$\left(\mathrm{diag}(\lambda_1,\ldots,\lambda_n)\right)^k = \mathrm{diag}(\lambda_1^k,\ldots,\lambda_n^k). \qquad \blacksquare$$

La Proposition suivante est immédiate.

♦ **Proposition 2** Soit $D = \mathrm{diag}(\lambda_1,\ldots,\lambda_n) \in \mathbf{D}_n(K)$.
On a : $D \in \mathbf{GL}_n(K) \iff (\forall i \in \{1,\ldots,n\}, \lambda_i \neq 0)$.
De plus, si $D \in \mathbf{GL}_n(K)$, alors $D^{-1} = \mathrm{diag}(\lambda_1^{-1},\ldots,\lambda_n^{-1})$.

Exercices

◊ **8.3.5** Déterminer le commutant de $\mathbf{D}_n(K)$ dans $\mathbf{M}_n(K)$, c'est-à-dire :

$$\left\{A \in \mathbf{M}_n(K);\ \forall D \in \mathbf{D}_n(K),\ AD = DA\right\}.$$

◊ **8.3.6** Soient $\lambda_1,\ldots,\lambda_n \in K$ deux à deux distincts, $D = \mathrm{diag}(\lambda_1,\ldots,\lambda_n)$. Déterminer le commutant de D, c'est-à-dire : $\{A \in \mathbf{M}_n(K);\ AD = DA\}$.

Complément

◇ C 8.1 Une inégalité de dénombrement résolue par l'algèbre linéaire

I Soient $n \in \mathbb{N} - \{0,1\}, \alpha_1, \ldots, \alpha_n, \beta \in \mathbb{R}_+^*$ tels que : $\forall i \in \{1,\ldots,n\}, \alpha_i \geqslant \beta$.
On suppose qu'il n'existe qu'au plus un indice i de $\{1,\ldots,n\}$ tel que $\alpha_i = \beta$.
On note $A = (a_{ij})_{ij} \in \mathbf{M}_n(\mathbb{R})$ définie par :

$$a_{ij} = \begin{cases} \alpha_i & \text{si } i = j \\ \beta & \text{si } i \neq j. \end{cases}$$

Démontrer : $A \in \mathbf{GL}_n(\mathbb{R})$.

(Pour $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbf{M}_{n,1}(\mathbb{R})$ tel que $AX = 0$, on pourra étudier les signes de $x_1, \ldots, x_n$).

II Soient $\beta \in \mathbb{N}^*, (n,p) \in (\mathbb{N}^*)^2$, E un ensemble fini à p éléments notés $u_1, \ldots, u_p$, $(A_j)_{1 \leqslant j \leqslant n}$ une famille de n parties de E deux à deux distinctes et telles que :

$$\forall (i,j) \in \{1,\ldots,n\}^2, \left(i \neq j \Longrightarrow \text{Card}(A_i \cap A_j) = \beta\right).$$

On considère $B = (b_{ij})_{\substack{1 \leqslant i \leqslant p \\ 1 \leqslant j \leqslant n}} \in \mathbf{M}_{p,n}(\mathbb{R})$ définie par $b_{ij} = \begin{cases} 1 & \text{si } u_i \in A_j \\ 0 & \text{sinon} \end{cases}$,

et $A = {}^tBB \in \mathbf{M}_n(\mathbb{R})$.

1) Montrer (en utilisant I) : $A \in \mathbf{GL}_n(\mathbb{R})$.

2) En déduire : $n \leqslant p$.

Complément

◇ C 8.1 Une inégalité de dénombrement résolue par l'algèbre linéaire

I Soient $n \in \mathbb{N} - \{0,1\}, \alpha_1, \ldots, \alpha_n, \beta \in \mathbb{R}_+^*$ tels que : $\forall i \in \{1,\ldots,n\}, \alpha_i \geqslant \beta$.
On suppose qu'il n'existe qu'au plus un indice i de $\{1,\ldots,n\}$ tel que $\alpha_i = \beta$.
On note $A = (a_{ij})_{ij} \in \mathbf{M}_n(\mathbb{R})$ définie par :

$$a_{ij} = \begin{cases} \alpha_i & \text{si } i = j \\ \beta & \text{si } i \neq j. \end{cases}$$

Démontrer : $A \in \mathbf{GL}_n(\mathbb{R})$.

(Pour $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbf{M}_{n,1}(\mathbb{R})$ tel que $AX = 0$, on pourra étudier les signes de $x_1, \ldots, x_n$).

II Soient $\beta \in \mathbb{N}^*, (n,p) \in (\mathbb{N}^*)^2$, E un ensemble fini à p éléments notés $u_1, \ldots, u_p$, $(A_j)_{1 \leqslant j \leqslant n}$ une famille de n parties de E deux à deux distinctes et telles que :

$$\forall (i,j) \in \{1,\ldots,n\}^2, \left(i \neq j \Longrightarrow \text{Card}(A_i \cap A_j) = \beta\right).$$

On considère $B = (b_{ij})_{\substack{1 \leqslant i \leqslant p \\ 1 \leqslant j \leqslant n}} \in \mathbf{M}_{p,n}(\mathbb{R})$ définie par $b_{ij} = \begin{cases} 1 & \text{si } u_i \in A_j \\ 0 & \text{sinon} \end{cases}$,

et $A = {}^tBB \in \mathbf{M}_n(\mathbb{R})$.

1) Montrer (en utilisant I) : $A \in \mathbf{GL}_n(\mathbb{R})$.

2) En déduire : $n \leqslant p$.

Chapitre 9

Déterminants, systèmes linéaires

Dans ce ch. 9, K désigne un corps commutatif. On suppose $2 \cdot 1_K \neq 0$ (où 1_K désigne le neutre de K pour la multiplication); ainsi 2 (confondu avec $2 \cdot 1_K$) admet dans K un inverse, noté $\frac{1}{2}$.

On dit aussi que K est un corps de caractéristique $\neq 2$ (cf. exercice 2.3.4 p. 58). C'est le cas si $K = \mathbb{R}$ ou $K = \mathbb{C}$.

Tous les K-ev considérés sont supposés de dimension finie, et de dimension $\neq 0$.

9.1 Applications multilinéaires

9.1.1 Généralités

♦ **Définition** Soient $p \in \mathbb{N}^*$, $E_1, \ldots, E_p, F$ des K-ev.

Une application $\varphi : E_1 \times \ldots \times E_p \longrightarrow F$ est dite ***p*- linéaire** (ou : **multilinéaire**) si et seulement si φ est linéaire par rapport à chaque place (ou : variable), c'est-à-dire :

$$\forall i \in \{1, \ldots, p\},\ \forall \lambda \in K,\ \forall x_1 \in E_1, \ldots,\ \forall x_i \in E_i, \forall y_i \in E_i, \ldots,\ \forall x_p \in E_p,$$
$$\varphi(x_1, \ldots, x_{i-1}, \lambda x_i + y_i, x_{i+1}, \ldots, x_p) = \lambda \varphi(x_1, \ldots, x_i, \ldots, x_p) + \varphi(x_1, \ldots, y_i, \ldots, x_p).$$

Si de plus $F = K$, on dit que φ est une **forme *p*-linéaire**.

EXEMPLES :

1) Pour $p = 1$, la notion d'application 1-linéaire coïncide avec celle d'application linéaire.

2) L'application nulle est p-linéaire.

3) Le produit scalaire canonique sur $\mathbb{R}^2$, $\varphi : \begin{array}{c} \mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow \mathbb{R} \\ ((x_1, x_2), (y_1, y_2)) \longmapsto x_1 y_1 + x_2 y_2 \end{array}$ est une forme 2-linéaire (on dit plutôt : **bilinéaire**).

4) Le produit vectoriel dans $\mathbb{R}^3$: $\phi : \mathbb{R}^3 \times \mathbb{R}^3 \longrightarrow \mathbb{R}^3$, défini par :

$$\phi\big((x_1, x_2, x_3), (y_1, y_2, y_3)\big) = (x_2 y_3 - x_3 y_2,\ x_3 y_1 - x_1 y_3,\ x_1 y_2 - x_2 y_1)$$

(cf. plus loin 10.5.2 Prop. 5 p. 375) est une application bilinéaire.

◆ **Proposition** L'ensemble $\mathcal{L}_p(E_1,\ldots,E_p;\,F)$ des applications p-linéaires de $E_1 \times \ldots \times E_p$ dans F est un K-ev.

Preuve :
Il est clair que $\mathcal{L}_p(E_1,\ldots,E_p;\,F)$ est un sev de $F^{E_1\times\ldots\times E_p}$.

9.1.2 Applications multilinéaires alternées

Soient E un K-ev, et $p \in \mathbb{N}^*$.

◆ **Définition** Une application p-linéaire $\varphi : E^p \longrightarrow F$ est dite **alternée** si et seulement si, pour tout couple (i,j) de $\{1,\ldots,p\}^2$ tel que $i \neq j$, et pour tout $(x_1,\ldots,x_p)$ de E^p : $x_i = x_j \Longrightarrow \varphi(x_1,\ldots,x_p) = 0$.
Si de plus $F = K$, on dit que φ est une **forme p-linéaire alternée**.

Autrement dit, φ est alternée si et seulement si $\varphi(x_1,\ldots,x_p)$ est nul pour tout p-uplet $(x_1,\ldots,x_p)$ comportant au moins une *répétition*.

Remarque :
L'ensemble des applications p-linéaires alternées de E^p dans F est un sev de $\mathcal{L}_p(E,\ldots,E;\,F)$.

◆ **Proposition 1** Une application p-linéaire $\varphi : E^p \longrightarrow F$ est alternée si et seulement si :

$$\forall \sigma \in \mathfrak{S}_p,\ \forall (x_1,\ldots,x_p) \in E^p,\ \varphi\big(x_{\sigma(1)},\ldots,x_{\sigma(p)}\big) = \varepsilon(\sigma)\varphi(x_1,\ldots,x_p).$$

Rappelons (3.3.1 Not. p. 78) que $\mathfrak{S}_p$ est le groupe symétrique d'indice p, formé des permutations de $\{1,\ldots,p\}$, et que, pour toute σ de $\mathfrak{S}_p$, $\varepsilon(\sigma)$ désigne la signature de σ.

Preuve :
1) Cas d'une transposition

Soit $(i,j) \in \{1,\ldots,p\}^2$ tel que $i < j$; notons τ_{ij} la transposition qui échange i et j et laisse les autres éléments de $\{1,\ldots,p\}$ fixes (cf. 3.4.2 Déf. 1 p. 84).
Puisque φ est alternée, on a :

$$\varphi(x_1,\ldots,x_{i-1},x_i + x_j,x_{i+1},\ldots,x_{j-1},x_i + x_j,x_{j+1},\ldots,x_p) = 0,$$

d'où en développant par multilinéarité :

$$\varphi(x_1,\ldots,x_i,\ldots,x_i,\ldots x_p) + \varphi(x_1,\ldots,x_i,\ldots,x_j,\ldots,x_p) + \varphi(x_1,\ldots,x_j,\ldots,x_i,\ldots,x_p) + \varphi(x_1,\ldots,x_j,\ldots,x_j,\ldots,x_p) = 0,$$

et donc $\varphi(x_1,\ldots,x_j,\ldots,x_i,\ldots,x_p) = -\varphi(x_1,\ldots,x_i,\ldots,x_j,\ldots,x_p)$.
Ceci montre : $\varphi\left(x_{\tau_{ij}(1)},\ldots,x_{\tau_{ij}(p)}\right) = \varepsilon(\tau_{ij})\varphi(x_1,\ldots,x_p)$.

2) Cas général

Soit $\sigma \in \mathfrak{S}_p$. D'après 3.4.2 Th.1 p. 84, σ est décomposable en un produit de transpositions; il existe $N \in \mathbb{N}^*$ et des transpositions $\sigma_1,\ldots,\sigma_N$ telles que $\sigma = \sigma_1 \circ \ldots \circ \sigma_N$; de plus, $\varepsilon(\sigma) = (-1)^N$.

En appliquant de façon itérée le résultat de 1), on obtient :

$$\begin{aligned}\varphi(x_{\sigma(1)},\ldots,x_{\sigma(p)}) &= -\varphi(x_{\sigma_2\circ\ldots\circ\sigma_N(1)},\ldots,\varphi_{\sigma_2\circ\ldots\circ\sigma_N(p)}) \\ &= \ldots = (-1)^N\varphi(x_1,\ldots,x_p) = \varepsilon(\sigma)\varphi(x_1,\ldots,x_p).\end{aligned}$$

♦ **Proposition 2** Soient $\varphi : E^p \longrightarrow F$ une application p-linéaire et alternée, et $(x_1,\ldots,x_p) \in E^p$. Si $(x_1,\ldots,x_p)$ est liée, alors $\varphi(x_1,\ldots,x_p) = 0$.

Preuve :

Supposons $(x_1,\ldots,x_p)$ liée; l'un au moins des $x_1,\ldots,x_p$ s'exprime donc comme combinaison linéaire des autres. D'après la Prop. précédente, on peut se ramener au cas où il existe $(\alpha_1,\ldots,\alpha_{p-1}) \in K^{p-1}$ tel que $x_p = \sum_{i=1}^{p-1} \alpha_i x_i$. Alors :

$$\varphi(x_1,\ldots,x_p) = \sum_{i=1}^{p-1} \alpha_i \varphi(x_1,\ldots,x_{p-1},x_i) = 0,$$

puisque chaque p-uplet $(x_1,\ldots,x_{p-1},x_i)$ comporte une répétition.

♦ **Corollaire** Si $p > \dim(E)$, alors la seule application p-linéaire et alternée de E^p dans F est l'application nulle.

Preuve :

Toute famille de p éléments de E est liée.

9.2 Déterminant d'une famille de n vecteurs dans une base d'un ev de dimension n

Soient $n \in \mathbb{N}^*$, E un K-ev de dimension n.

9.2.1 Espace $\wedge_n(E)$

Soit $\mathcal{B} = (e_1,\dots,e_n)$ une base de E.

1) Soient $S = (V_1,\dots,V_n) \in E^n$ et, pour chaque j de $\{1,\dots,n\}$, $(a_{ij\,j})_{i_j\in\{1,\dots,n\}} \in K^n$ tel que : $V_j = \sum_{i_j=1}^{n} a_{i_j\,j}\, e_{i_j}$.

Soit $\varphi : E^n \longrightarrow K$ une forme n-linéaire alternée. Nous allons calculer $\varphi(S)$ en fonction des $a_{i_j\,j}$. On a :

$$\varphi(S) = \varphi\left(\sum_{i_1=1}^{n} a_{i_1 1} e_{i_1},\dots,\sum_{i_n=1}^{n} a_{i_n n} e_{i_n}\right) = \sum_{i_1=1}^{n} a_{i_1 1}\varphi\left(e_{i_1},\sum_{i_2=1}^{n} a_{i_2 2} e_{i_2},\dots,\sum_{i_n=1}^{n} a_{i_n n} e_{i_n}\right)$$

$$= \dots = \sum_{i_1=1}^{n}\cdots\sum_{i_n=1}^{n} a_{i_1 1}\dots a_{i_n n}\varphi\left(e_{i_1},\dots,e_{i_n}\right) = \sum_{(i_1,\dots,i_n)\in\{1,\dots,n\}^n} a_{i_1 1}\dots a_{i_n n}\varphi\left(e_{i_1},\dots,e_{i_n}\right).$$

Comme φ est alternée, $\varphi(e_{i_1},\dots,e_{i_n})$ est nul dès que $i_1,\dots,i_n$ ne sont pas deux à deux distincts. Il ne reste donc, dans la somme multiple précédente, que les termes correspondant aux cas où $(1,\dots,n) \longmapsto (i_1,\dots,i_n)$ est une permutation de $\{1,\dots,n\}$.

D'où :

$$\varphi(S) = \sum_{\sigma\in\mathfrak{S}_n} a_{\sigma(1)1}\dots a_{\sigma(n)n}\varphi(e_{\sigma(1)},\dots,e_{\sigma(n)})$$

$$= \left(\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1}\dots a_{\sigma(n)n}\right)\varphi(e_1,\dots,e_n).$$

2) Réciproquement, soient $\lambda \in K$ et $\psi : E^n \longrightarrow K$ l'application définie par, pour tout $S = (V_1,\dots,V_n)$ de E^n : $\psi(S) = \lambda \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1}\dots a_{\sigma(n)n}$,

où les $a_{i_j\,j}$ sont les composantes des V_j dans $\mathcal{B}$: $\forall\, j \in \{1,\dots,n\}$, $V_j = \sum_{i_j=1}^{n} a_{i_j\,j} e_{i_j}$.

• ψ est n-linéaire car, pour tous i de $\{1,\dots,n\}$, α de K, $V_1,\dots,V_{i-1},V_i,V_i',V_{i+1},\dots,V_n$ de E, on a, en notant $(a'_{ki})_{1\leqslant k\leqslant n}$ les composantes de V_i' dans $\mathcal{B}$:

$$\begin{aligned}\psi(V_1,\dots,\alpha V_i + V_i',\dots,V_n) &= \lambda \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1}\dots\left(\alpha a_{\sigma(i)i} + a'_{\sigma(i)i}\right)\dots a_{\sigma(n)n}\\ &= \alpha\lambda \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1}\dots a_{\sigma(n)n} + \lambda \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1}\dots a'_{\sigma(i)i}\dots a_{\sigma(n)n}\\ &= \alpha\psi(V_1,\dots,V_i,\dots,V_n) + \psi(V_1,\dots,V_i',\dots,V_n).\end{aligned}$$

• ψ est alternée car, pour tout (i,j) de $\{1,\dots,n\}^2$ tel que $i < j$ et tout $(V_1,\dots,V_n)$ de E^n tel que $V_i = V_j$, on a, en effectuant le changement d'indice $\sigma' = \sigma\circ\tau_{ij}$ dans la sommation :

$$\begin{aligned}\psi(V_1,\dots,V_n) &= \lambda \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1}\dots a_{\sigma(n)n}\\ &= \lambda \sum_{\sigma'\in\mathfrak{S}_n} -\varepsilon(\sigma') a_{\sigma'(1)1}\dots a_{\sigma'(j)i}\dots a_{\sigma'(i)j}\dots a_{\sigma'(n)n}\\ &= -\lambda \sum_{\sigma'\in\mathfrak{S}_n} \varepsilon(\sigma') a_{\sigma'(1)1}\dots a_{\sigma'(i)i}\dots a_{\sigma'(j)j}\dots a_{\sigma'(n)n},\end{aligned}$$

puisque $V_i = V_j$.

D'où $\psi(V_1,\dots,V_n) = -\psi(V_1,\dots,V_n)$, $2\psi(V_1,\dots,V_n) = 0$, $\psi(V_1,\dots,V_n) = 0$ (puisque K est de caractéristique $\neq 2$, cf. p. 302).

• Montrons $\psi \neq 0$.

Pour chaque j de $\{1,\dots,n\}$, la décomposition de e_j sur la base $\mathcal{B}$ est : $e_j = \sum_{i_j=1}^{n} \delta_{i_j\,j}\, e_{i_j}$,

où $\delta_{i_j\,j}$ est le symbole de Kronecker. D'où : $\psi(\mathcal{B}) = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma)\delta_{\sigma(1)1}\dots\delta_{\sigma(n)n} = 1$,

car, si $\sigma \neq \mathrm{Id}_{\{1,\dots,n\}}$, l'un des facteurs $\delta_{\sigma(j)j}$ $(1 \leqslant j \leqslant n)$ est nul.

Résumons l'étude :

♦ **Théorème - Définition** L'ensemble $\wedge_n(E)$ des formes n-linéaires alternées sur un K-ev de dimension n $(n \geqslant 1)$ est un K-ev de dimension 1.

Pour toute base $\mathcal{B} = (e_1,\dots,e_n)$ de E, on note $\det_{\mathcal{B}} : E^n \longrightarrow K$ l'application définie par, pour tout $(V_1,\dots,V_n)$ de E^n :

$$\det_{\mathcal{B}}(V_1,\dots,V_n) = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1}\dots a_{\sigma(n)n}\ ,$$

où, pour chaque j de $\{1,\dots,n\}$, $(a_{i_j\,j})_{1\leqslant i_j\leqslant n}$ sont les composantes de V_j dans $\mathcal{B}$:

$$V_j = \sum_{i_j=1}^{n} a_{i_j\,j}\, e_{ij}.$$

L'élément $\det_{\mathcal{B}}(V_1,\dots,V_n)$ (de K) est appelé le **déterminant de** $(V_1,\dots,V_n)$ **dans la base** $\mathcal{B}$.

Pour toute base $\mathcal{B}$ de E, $(\det_{\mathcal{B}})$ est une base de $\wedge_n(E)$.

Autrement dit, pour toute base $\mathcal{B}$ de E, les éléments de $\Lambda_n(E)$ sont *proportionnels* à $\det_{\mathcal{B}}$.

Remarque :
On a vu plus haut que, pour toute base $\mathcal{B}$ de E : $\det_{\mathcal{B}}(\mathcal{B}) = 1$.

9.2.2 Propriétés

On note ici $\beta(E)$ l'ensemble des bases de E.

◆ **Proposition 1**

$$\forall \varphi \in \Lambda_n(K),\ \forall S \in E^n,\ \forall \mathcal{B} \in \beta(E),\ \varphi(S) = \varphi(\mathcal{B})\det_{\mathcal{B}}(S).$$

Preuve :
Soient $\varphi \in \Lambda_n(E), \mathcal{B} \in \beta(E)$. Puisque $\det_{\mathcal{B}}$ engendre $\Lambda_n(E)$, il existe $\alpha \in K$ tel que $\varphi = \alpha\det_{\mathcal{B}}$. En particulier : $\varphi(\mathcal{B}) = \alpha\det_{\mathcal{B}}(\mathcal{B}) = \alpha$, d'où : $\varphi = \varphi(\mathcal{B})\det_{\mathcal{B}}$, c'est-à-dire :

$$\forall S \in E^n,\ \varphi(S) = \varphi(\mathcal{B})\det_{\mathcal{B}}(S).$$

◆ **Corollaire**

$$\forall \mathcal{B}, \mathcal{B}' \in \beta(E),\ \forall S \in E^n,\ \det_{\mathcal{B}'}(S) = \det_{\mathcal{B}'}(\mathcal{B})\det_{\mathcal{B}}(S).$$

Preuve :
Il suffit d'appliquer la Prop. précédente à $\varphi = \det_{\mathcal{B}'}$.

Remarques :

1) On retient la formule ci-dessus en remarquant l'analogie avec la *relation de Chasles* ($\overrightarrow{B'S} = \overrightarrow{B'B} + \overrightarrow{BS}$) ou le calcul sur fractions $\left(\dfrac{s}{b'} = \dfrac{b}{b'} \cdot \dfrac{s}{b}\right)$.

2) $\forall \mathcal{B}, \mathcal{B}', \mathcal{B}'' \in \beta(E),\quad \det_{\mathcal{B}''}(\mathcal{B}) = \det_{\mathcal{B}''}(\mathcal{B}')\det_{\mathcal{B}'}(\mathcal{B})$.

3) En particulier, en prenant $\mathcal{B}'' = \mathcal{B}$ dans le résultat précédent :

$$\forall \mathcal{B}, \mathcal{B}' \in \beta(E),\ \left(\det_{\mathcal{B}'}(\mathcal{B}) \neq 0 \quad \text{et} \quad \det_{\mathcal{B}}(\mathcal{B}') = (\det_{\mathcal{B}'}(\mathcal{B}))^{-1}\right).$$

◆ **Proposition 2** Soient $\mathcal{B} \in \beta(E)$, $S \in E^n$.
Alors S est liée si et seulement si $\det_{\mathcal{B}}(S) = 0$.

Preuve :

1) Si S est liée, alors $\det_{\mathcal{B}}(S) = 0$, puisque $\det_{\mathcal{B}}$ est n-linéaire et alternée (cf. 9.1.2 Prop. 2 p. 303).

2) Si S est libre, alors, comme, S a n éléments, S est une base de E, et donc (cf. Rem. *3)* ci-dessus) : $\det_{\mathcal{B}}(S) \neq 0$.

9.3 Déterminant d'un endomorphisme

Soient $n \in \mathbb{N}^*$, E un K-ev de dimension n. Soient $f \in \mathcal{L}(E)$, $\varphi \in \Lambda_n(E) - \{0\}$.
Il est clair que l'application $\varphi \circ (f \times \ldots \times f) : E^n \longrightarrow K$ définie par :

$$\forall (V_1,\ldots,V_n) \in E^n, \big(\varphi \circ (f \times \ldots \times f)\big)(V_1,\ldots,V_n) = \varphi\big(f(V_1),\ldots,f(V_n)\big)$$

est n-linéaire et alternée.
Puisque $\Lambda_n(E)$ est de dimension 1 et que $\varphi \neq 0$, φ engendre $\Lambda_n(E)$, et il existe donc $\alpha \in K$ tel que : $\varphi \circ (f \times \ldots \times f) = \alpha\varphi$. Montrons que α ne dépend pas de φ.
Soit $\psi \in \Lambda_n(E) - \{0\}$. Puisque φ engendre $\Lambda_n(E)$, il existe $\lambda \in K - \{0\}$ tel que $\psi = \lambda\varphi$.
On a alors :

$$\psi \circ (f \times \ldots \times f) = (\lambda\varphi) \circ (f \times \ldots \times f) = \lambda\big(\varphi \circ (f \times \ldots \times f)\big) = \lambda(\alpha\varphi) = \alpha(\lambda\varphi) = \alpha\psi.$$

Ceci montre que α ne dépend pas du choix de φ dans $\Lambda_n(E) - \{0\}$.
Résumons l'étude :

♦ **Proposition - Définition 1** Pour tout f de $\mathcal{L}(E)$, il existe un élément unique α de K tel que : $\forall \varphi \in \Lambda_n(E),\ \varphi \circ (f \times \ldots \times f) = \alpha\varphi$.
Cet élément α est appelé le **déterminant** de f, et noté $\det(f)$.

On a ainsi :

$$\forall f \in \mathcal{L}(E),\ \forall \varphi \in \Lambda_n(E),\ \varphi \circ (f \times \ldots \times f) = \big(\det(f)\big)\varphi.$$

La Prop. suivante est immédiate.

♦ **Proposition 2**

1) $\forall f \in \mathcal{L}(E), \forall \varphi \in \Lambda_n(E), \forall (V_1,\ldots,V_n) \in E^n$,
$\varphi\big(f(V_1),\ldots,f(V_n)\big) = \big(\det(f)\big)\varphi(V_1,\ldots,V_n)$.

2) $\forall f \in \mathcal{L}(E),\ \forall \mathcal{B} \in \beta(E),\ \forall (V_1,\ldots,V_n) \in E^n$,
$\det_{\mathcal{B}}\big(f(V_1),\ldots,f(V_n)\big) = \det(f)\det_{\mathcal{B}}(V_1,\ldots,V_n)$.

3) $\forall f \in \mathcal{L}(E),\ \forall \mathcal{B} = (e_1,\ldots,e_n) \in \beta(E)$,
$\det(f) = \det_{(e_1,\ldots,e_n)}\big(f(e_1),\ldots,f(e_n)\big)$. ■

♦ **Proposition 3**

1) $\det(\mathrm{Id}_E) = 1$.

2) $\forall \alpha \in K, \forall f \in \mathcal{L}(E), \det(\alpha f) = \alpha^n \det(f)$.

3) $\forall f,g \in \mathcal{L}(E), \det(g \circ f) = \det(g)\det(f)$.

4) $\forall f \in \mathcal{L}(E), \big(f \in \mathcal{GL}(E) \Longleftrightarrow \det(f) \neq 0\big)$.

5) $\forall f \in \mathcal{GL}(E), \det(f^{-1}) = \big(\det(f)\big)^{-1}$.

Preuve :

E admet au moins une base $\mathcal{B} = (e_1, \ldots, e_n)$.

1) $\det(\mathrm{Id}_E) = \det_{\mathcal{B}}(\mathcal{B}) = 1$.

2) $\det(\alpha f) = \det_{(e_1,\ldots,e_n)}\big(\alpha f(e_1), \ldots, \alpha f(e_n)\big) = \alpha^n \det_{(e_1,\ldots,e_n)}\big(f(e_1), \ldots, f(e_n)\big)$
$= \alpha^n \det(f)$.

3) $\det(g \circ f) = \det_{\mathcal{B}}\big(g(f(\mathcal{B}))\big) = \det(g)\det_{\mathcal{B}}\big(f(\mathcal{B})\big) = \det(g)\det(f)$.

4) $\big(f \in \mathcal{GL}(E)\big) \Longleftrightarrow \big(f(\mathcal{B}) \in \beta(E)\big) \Longleftrightarrow \det_{\mathcal{B}}\big(f(\mathcal{B})\big) \neq 0 \Longleftrightarrow \det(f) \neq 0$.

5) Soit $f \in \mathcal{GL}(E)$. On a : $\det(f)\det(f^{-1}) = \det(f \circ f^{-1}) = \det(\mathrm{Id}_E) = 1$,
donc $\det(f^{-1}) = \big(\det(f)\big)^{-1}$.

Remarque : Dans la preuve précédente, on a noté $f(\mathcal{B}) = \big(f(e_1), \ldots, f(e_n)\big)$, ce qui peut aussi se noter $(f \times \ldots \times f)(\mathcal{B})$.

9.4 Déterminant d'une matrice carrée

Soit $n \in \mathbb{N}^*$.

♦ **Définition** Soit $A = (a_{ij})_{1 \leqslant i,j \leqslant n} \in \mathbf{M}_n(K)$. On appelle **déterminant** de A, et on note $\det(A)$, ou $\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}$, l'élément de K défini par :

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n}.$$

Autrement dit, en notant $C_1 = \begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix}, \dots, C_n = \begin{pmatrix} a_{1n} \\ \vdots \\ a_{nn} \end{pmatrix}$ les colonnes de A, et $\mathcal{B}$ la base canonique de $\mathbf{M}_{n,1}(K)$, on a : $\det(A) = \det_{\mathcal{B}}(C_1, \dots, C_n)$. ■

On dit que $\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}$ est un déterminant **d'ordre** n.

Pour rappeler l'ordre n, on peut noter $[n]$ en bas à droite : $\det(A) = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}_{[n]}$.

EXEMPLES :

1) $\forall (a,b,c,d) \in K^4$, $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$, puisque $\mathfrak{S}_2 = \{\mathrm{Id}_{\{1,2\}}, \tau_{12}\}$.

2) Soit $A = (a_{ij})_{ij} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ & \ddots & \ddots & \vdots \\ & & \ddots & a_{n-1\,n} \\ 0 & & & a_{nn} \end{pmatrix} \in \mathbf{T}_{n,s}(K)$.

Pour $\sigma \in \mathfrak{S}_n$, s'il existe $j \in \{1,\dots,n\}$ tel que $\sigma(j) > j$, alors $a_{\sigma(j)j} = 0$, donc $\prod_{k=1}^{n} a_{\sigma(k)k} = 0$. Ceci montre que la somme $\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n}$ se réduit au(x) seul(s) termes (s) correspondant à σ telle(s) que : $\forall j \in \{1,\dots,n\}$, $\sigma(j) \leqslant j$.

Pour une telle σ, on a $\sigma(1) \leqslant 1$ donc $\sigma(1) = 1$, puis $\sigma(2) \leqslant 2$ et $\sigma(2) \neq \sigma(1) = 1$, donc $\sigma(2) = 2 \dots$ Il est clair que, pour tout j de $\{1,\dots,n-1\}$ si $(\sigma(1) = 1, \dots, \sigma(j) = j)$, alors $\sigma(j+1) = j+1$, puisque $\sigma(j+1) \leqslant j+1$ et $\sigma(j+1) \notin \{1,\dots,j\}$. Ainsi, la seule permutation σ pour laquelle $(\forall j \in \{1,\dots,n\}, \sigma(j) \leqslant j)$ est l'identité, d'où : $\det(A) = \prod_{j=1}^{n} a_{jj}$

(cf. aussi plus loin 9.6.1 Prop. p. 318).

La Proposition suivante est immédiate.

◆ **Proposition 1** Soient E un K-ev de dimension n, $f \in \mathcal{L}(E)$, $\mathcal{B}$ une base de E, $A = \mathrm{Mat}_{\mathcal{B}}(f)$. On a :

$$\det(f) = \det(A).$$

◆ **Proposition 2**

1) $\det(\mathrm{I}_n) = 1$.

2) $\forall \alpha \in K, \forall A \in \mathbf{M}_n(K), \quad \det(\alpha A) = \alpha^n \det(A)$.

3) $\forall (A,B) \in (\mathbf{M}_n(K))^2, \quad \det(AB) = \det(A)\det(B)$.

4) $\forall A \in \mathbf{M}_n(K), \quad (A \in \mathbf{GL}_n(K) \iff \det(A) \neq 0)$.

5) $\forall A \in \mathbf{GL}_n(K), \quad \det(A^{-1}) = \big(\det(A)\big)^{-1}$.

6) $\forall A \in \mathbf{M}_n(K), \quad \det({}^tA) = \det(A)$.

Preuve :

Les propriétés *1)* à *5)* se déduisent de la Prop. 1 précédente et des propriétés du déterminant d'un endomorphisme (9.3 Prop. 3 p. 307).

En notant $A = (a_{ij})_{ij} \in \mathbf{M}_n(K)$, on a :

$$\det({}^tA) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma^{-1}(\sigma(1))\,\sigma(1)} \cdots a_{\sigma^{-1}(\sigma(n))\,\sigma(n)}.$$

Comme la multiplication est commutative dans K, en réordonnant suivant le deuxième indice, on a, pour toute σ de $\mathfrak{S}_n$:

$$a_{\sigma^{-1}(\sigma(1))\,\sigma(1)} \cdots a_{\sigma^{-1}(\sigma(n))\,\sigma(n)} = a_{\sigma^{-1}(1)1} \cdots a_{\sigma^{-1}(n)n},$$

et donc : $\det({}^tA) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma^{-1}(1)1} \cdots a_{\sigma^{-1}(n)n}$.

Enfin, comme $\begin{array}{ccc} \mathfrak{S}_n & \longrightarrow & \mathfrak{S}_n \\ \sigma & \longmapsto & \sigma^{-1} \end{array}$ est une bijection conservant la signature (c'est-à-dire : $\forall \sigma \in \mathfrak{S}_n$, $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$), on obtient :

$$\det({}^tA) = \sum_{\tau \in \mathfrak{S}_n} \varepsilon(\tau) a_{\tau(1)1} \cdots a_{\tau(n)n} = \det(A).$$

Remarques :

1) De la propriété *3)* précédente, on déduit par une récurrence immédiate :

$$\forall A \in \mathbf{M}_n(K), \forall k \in \mathbb{N}^*, \quad \det(A^k) = \big(\det(A)\big)^k.$$

2) De la remarque précédente et la propriété *5)*, on déduit :

$$\forall A \in \mathbf{GL}_n(K), \forall k \in \mathbb{Z}, \quad \det(A^k) = \big(\det(A)\big)^k.$$

3) Si $A \in \mathbf{M}_n(K)$ est nilpotente, il existe $k \in \mathbb{N}^*$ tel que $A^k = 0$, d'où :

$$\big(\det(A)\big)^k = \det(A^k) = 0,$$

et donc : $\det(A) = 0$.

4) Si $A \in \mathbf{M}_n(K)$ est antisymétrique et si n est impair, alors :

$$\det(A) = \det({}^tA) = \det(-A) = (-1)^n \det(A) = -\det(A),$$

d'où : $\det(A) = 0$.

Exercices

◇ **9.4.1** Montrer, pour tout $A = (a_{ij})_{ij}$ de $\mathbf{M}_n(\mathbb{C})$: $|\det(A)| \leqslant \prod_{j=1}^{n} \left(\sum_{i=1}^{n} |a_{ij}| \right)$.

◇ **9.4.2** *a)* Soit $n \in \mathbb{N}^*$. On suppose qu'il existe $A, B \in \mathbf{GL}_n(\mathbb{R})$ telles que $AB + BA = 0$; montrer que n est pair.

b) Donner un exemple de $(A, B) \in (\mathbf{GL}_2(\mathbb{R}))^2$ tel que $AB + BA = 0$.

◇ **9.4.3** **Groupe spécial linéaire**

On note $\mathbf{SL}_n(K) = \{A \in \mathbf{M}_n(K);\ \det(A) = 1\}$.

a) Vérifier que $\mathbf{SL}_n(K)$ est un sous-groupe de $\mathbf{GL}_n(K)$ pour la multiplication, appelé **groupe spécial linéaire**.

b) Montrer : $\forall\, A \in \mathbf{GL}_n(\mathbb{C}), \exists (\alpha, B) \in \mathbb{C}^* \times \mathbf{SL}_n(\mathbb{C}),\ A = \alpha B$.

◇ **9.4.4** Soit $n \in \mathbb{N} - \{0, 1\}$. Trouver toutes les A de $\mathbf{M}_n(\mathbb{C})$ telles que :

$$\forall\, M \in \mathbf{M}_n(\mathbb{C}),\ \det(A + M) = \det(A) + \det(M).$$

◇ **9.4.5** Soit $n \in \mathbb{N}^*$.

a) Montrer : $\forall\, A, B \in \mathbf{M}_n(\mathbb{R}),\quad \big(AB = BA \Longrightarrow \det(A^2 + B^2) \geqslant 0\big)$.

b) A-t-on : $\forall\, A, B \in \mathbf{M}_2(\mathbb{R}),\quad \det(A^2 + B^2) \geqslant 0$?

◇ **9.4.6** Soient $n \in \mathbb{N}^*$, $A \in \mathbf{GL}_n(\mathbb{R})$, $B \in \mathbf{M}_n(\mathbb{R})$.

Montrer qu'il existe $\varepsilon \in \mathbb{R}_+^*$ tel que : $\forall\, x \in \mathbb{R},\ \big(|x| < \varepsilon \Longrightarrow A + x\,B \in \mathbf{GL}_n(\mathbb{R})\big)$.

◇ **9.4.7** Soient $n \in \mathbb{N}^*$, $A, B \in \mathbf{M}_n(\mathbb{R})$ telles que $AB - BA = B$.

a) Montrer : $\forall\, k \in \mathbb{N},\ AB^k = B^k(A + kI_n)$.

b) En déduire : $\det(B) = 0$.

9.5 Développement par rapport à une rangée

9.5.1 Cofacteurs et mineurs

1) Examen du cas $n = 3$

Soit $A = (a_{ij})_{ij} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \in \mathbf{M}_3(K)$.

Par définition (cf. 9.4 Déf. p. 309) :

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_3} \varepsilon(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} a_{\sigma(3)3}.$$

Comme $\mathfrak{S}_3 = \{\mathrm{Id}, \tau_{12}, \tau_{13}, \tau_{23}, c, c'\}$, où $c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ et $c' = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, on obtient :

$$\det(A) = a_{11}a_{22}a_{33} - a_{21}a_{12}a_{33} - a_{31}a_{22}a_{13} - a_{11}a_{32}a_{23} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23}.$$

On peut grouper, par exemple, ainsi :

$$\begin{aligned} \det(A) &= a_{11}(a_{22}a_{33} - a_{32}a_{23}) + a_{21}(-a_{12}a_{33} + a_{32}a_{13}) + a_{31}(a_{12}a_{23} - a_{22}a_{13}) \\ &= a_{11}\begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{21}\begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} + a_{31}\begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix}, \end{aligned}$$

et on obtient le *développement de* $\det(A)$ *par rapport à la* $1^{ère}$ *colonne.*

2) Etude du cas général

- Soit $A = (a_{ij})_{ij} \in \mathbf{M}_n(K)$.

Notons $\mathcal{B} = (e_1, \ldots, e_n)$ la base canonique de $\mathbf{M}_{n,1}(K)$:

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, e_n \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix},$$

et $C_1 = \begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix}, \ldots, C_n = \begin{pmatrix} a_{1n} \\ \vdots \\ a_{nn} \end{pmatrix}$ les colonnes de A.

Soit $j \in \{1, \ldots, n\}$.

En développant par linéarité par rapport à la $j^{ème}$ colonne, on a :

$$\det(A) = \det_{\mathcal{B}}\left(C_1, \ldots, C_{j-1}, \sum_{i=1}^{n} a_{ij} e_i, C_{j+1}, \ldots, C_n\right) = \sum_{i=1}^{n} a_{ij} A_{ij},$$

en notant

$$A_{ij} = \det_{\mathcal{B}}(C_1,\ldots,C_{j-1},e_i,C_{j+1},\ldots,C_n) = \begin{vmatrix} a_{11} & \ldots & a_{1\,j-1} & 0 & a_{1\,j+1} & \ldots & a_{1n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \vdots & & \vdots & 0 & \vdots & & \vdots \\ \vdots & & \vdots & 1 & \vdots & & \vdots \\ \vdots & & \vdots & 0 & \vdots & & \vdots \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & \ldots & a_{n\,j-1} & 0 & a_{n\,j+1} & \ldots & a_{nn} \end{vmatrix},$$

le «1» étant situé à la ligne n°i.

Faisons passer, dans le déterminant ci-dessus, la $j^{\text{ème}}$ colonne en dernier, c'est-à-dire permutons les colonnes suivant la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & j-1 & j & j+1 & \ldots & n \\ 1 & 2 & \ldots & j-1 & n & j & \ldots & n-1 \end{pmatrix},$$

qui admet exactement $(n-1)-j+1$ inversions (et qui est aussi le produit de $n-j$ transpositions du type $\tau_{k\,k+1}$) :

$$A_{ij} = (-1)^{n-j} \begin{vmatrix} a_{11} & \ldots & a_{1j-1} & a_{1j+1} & \ldots & a_{1n} & 0 \\ \vdots & & \vdots & \vdots & & \vdots & \vdots \\ \vdots & & \vdots & \vdots & & \vdots & 1 \\ \vdots & & \vdots & \vdots & & \vdots & \vdots \\ a_{n1} & \ldots & a_{n\,j-1} & a_{n\,j+1} & \ldots & a_{nn} & 0 \end{vmatrix}.$$

De même faisons maintenant passer la $i^{\text{ème}}$ ligne en dernier :

$$A_{ij} = (-1)^{n-j}(-1)^{n-i} \begin{vmatrix} a_{11} & \ldots & a_{1j-1} & a_{1j+1} & \ldots & a_{1n} & 0 \\ \vdots & & \vdots & \vdots & & \vdots & \vdots \\ a_{i-1\,1} & \ldots & a_{i-1\,j-1} & a_{i-1\,j+1} & \ldots & a_{i-1\,n} & 0 \\ a_{i+1\,1} & \ldots & a_{i+1\,j-1} & a_{i+1\,j+1} & \ldots & a_{i+1\,n} & 0 \\ \vdots & & \vdots & \vdots & & \vdots & \vdots \\ a_{n1} & \ldots & a_{n\,j-1} & a_{n\,j+1} & \ldots & a_{nn} & 0 \\ a_{i1} & \ldots & a_{i\,j-1} & a_{i\,j+1} & \ldots & a_{in} & 1 \end{vmatrix}.$$

• Considérons une matrice quelconque $B = (b_{uv})_{uv}$ de $\mathbf{M}_{n,n-1}(K)$, et

$$B' = \begin{pmatrix} b_{11} & \ldots & b_{1n-1} & 0 \\ \vdots & & \vdots & \vdots \\ b_{n-1\,1} & \ldots & b_{n-1\,n-1} & 0 \\ b_{n1} & \ldots & b_{n\,n-1} & 1 \end{pmatrix} \in \mathbf{M}_n(K).$$

En notant $B' = (b'_{uv})_{uv}$, on a donc :

$$b'_{uv} = \begin{cases} b_{uv} & \text{si } v \leqslant n-1 \\ 1 & \text{si } u = v = n \\ 0 & \text{sinon.} \end{cases}$$

Par définition : $\det(B') = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) b'_{\sigma(1)1} \dots b'_{\sigma(n)n}$.

Pour tout σ de $\mathfrak{S}_n$ telle que $\sigma(n) \neq n$, on a $b'_{\sigma(n)n} = 0$. Comme $b'_{nn} = 1$, on a donc :

$$\det(B') = \sum_{\substack{\sigma \in \mathfrak{S}_n \\ \sigma(n)=n}} \varepsilon(\sigma) b'_{\sigma(1)1} \dots b'_{\sigma(n-1)n-1}.$$

Il est clair que l'application $\{\sigma \in \mathfrak{S}_n ; \sigma(n) = n\} \longrightarrow \mathfrak{S}_{n-1}$, où ρ est définie par :
$\sigma \longmapsto \rho$

$\forall k \in \{1, \dots, n-1\}$, $\rho(k) = \sigma(k)$, est une bijection et qu'elle conserve la signature.
D'où :

$$\det(B') = \sum_{\rho \in \mathfrak{S}_{n-1}} \varepsilon(\rho) b'_{\rho(1)1} \dots b'_{\rho(n-1)n-1} = \sum_{\rho \in \mathfrak{S}_{n-1}} \varepsilon(\rho) b_{\rho(1)1} \dots b_{\rho(n-1)n-1}.$$

- En appliquant ce résultat au déterminant obtenu pour A_{ij}, on arrive à

$$A_{ij} = (-1)^{i+j} \begin{vmatrix} a_{11} & \dots & a_{1j-1} & a_{1j+1} & \dots & a_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{i-11} & & a_{i-1j-1} & a_{i-1j+1} & & a_{i-1n} \\ a_{i+11} & & a_{i+1j-1} & a_{i+1j+1} & & a_{i+1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \dots & a_{nj-1} & a_{nj+1} & \dots & a_{nn} \end{vmatrix}.$$

3) Enoncé des résultats

Soit $n \in \mathbb{N}^*$.

◆ **Définition** Soit $A = (a_{ij})_{ij} \in \mathbf{M}_n(K)$.

1) Pour chaque (i,j) de $\{1, \dots, n\}^2$, on appelle **mineur de la place** (i,j) **dans** A (ou, par abus : mineur de a_{ij} dans A) le déterminant Δ_{ij} d'ordre $n-1$ obtenu en supprimant dans A la $i^{\text{ème}}$ ligne et la $j^{\text{ème}}$ colonne :

$$\Delta_{ij} = \begin{vmatrix} a_{11} & \dots & a_{1j-1} & a_{1j+1} & \dots & a_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{i-11} & \dots & a_{i-1j-1} & a_{i-1j+1} & \dots & a_{i-1n} \\ a_{i+11} & \dots & a_{i+1j-1} & a_{i+1j+1} & \dots & a_{i+1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \dots & a_{nj-1} & a_{nj+1} & \dots & a_{nn} \end{vmatrix}$$

2) Pour chaque (i,j) de $\{1,\ldots,n\}^2$, on appelle **cofacteur de la place** (i,j) **dans** A (ou, par abus : cofacteur de a_{ij} dans A), et on note A_{ij} le produit de $(-1)^{i+j}$ par le mineur de la place (i,j) dans A :

$$A_{ij} = (-1)^{i+j}\Delta_{ij}.$$

Remarque :

Le calcul de Δ_{ij} et de A_{ij} ne fait pas intervenir les éléments de A situés dans la $i^{\text{ème}}$ ligne ni ceux situés dans la $j^{\text{ème}}$ colonne de A. ■

On appelle **rangée** d'une matrice ou d'un déterminant toute ligne ou colonne de cette matrice ou de ce déterminant.

♦ **Proposition (Développement d'un déterminant par rapport à une rangée)**

Soit $A = (a_{ij})_{ij} \in \mathbf{M}_n(K)$. On a :

1) $\forall\, j \in \{1,\ldots,n\}$, $\det(A) = \sum_{i=1}^{n} a_{ij}A_{ij}$ (développement de $\det(A)$ par rapport à la $j^{\text{ème}}$ colonne)

2) $\forall\, i \in \{1,\ldots,n\}$, $\det(A) = \sum_{j=1}^{n} a_{ij}A_{ij}$ (développement de $\det(A)$ par rapport à la $i^{\text{ème}}$ ligne).

Preuve :

1) Cf. plus haut, pp. 314-315.

2) Se déduit de *1)* appliqué à ${}^tA$ au lieu de A.

EXEMPLE :

En développant par rapport à la $4^{\text{ème}}$ colonne :

$$\begin{vmatrix} 2 & 6 & -3 & 4 \\ 1 & 3 & 4 & -5 \\ 4 & 1 & 2 & 0 \\ -3 & 0 & 3 & 6 \end{vmatrix} = -4\begin{vmatrix} 1 & 3 & 4 \\ 4 & 1 & 2 \\ -3 & 0 & 3 \end{vmatrix} - 5\begin{vmatrix} 2 & 6 & -3 \\ 4 & 1 & 2 \\ -3 & 0 & 3 \end{vmatrix} + 6\begin{vmatrix} 2 & 6 & -3 \\ 1 & 3 & 4 \\ 4 & 1 & 2 \end{vmatrix}$$

$$= -4\left(-3\begin{vmatrix} 3 & 4 \\ 1 & 2 \end{vmatrix} + 3\begin{vmatrix} 1 & 3 \\ 4 & 1 \end{vmatrix}\right) - 5\left(-3\begin{vmatrix} 6 & -3 \\ 1 & 2 \end{vmatrix} + 3\begin{vmatrix} 2 & 6 \\ 4 & 1 \end{vmatrix}\right)$$

$$+ 6\left(2\begin{vmatrix} 3 & 4 \\ 1 & 2 \end{vmatrix} - \begin{vmatrix} 6 & -3 \\ 1 & 2 \end{vmatrix} + 4\begin{vmatrix} 6 & -3 \\ 3 & 4 \end{vmatrix}\right)$$

$$= 1437.$$

Remarques :

1) Il est souvent utile de développer un déterminant par rapport à une rangée lorsque cette rangée comporte peu de termes non nuls (plusieurs termes nuls).

2) Pour le calcul numérique des déterminants, il existe des méthodes nettement plus rapides que celle consistant à développer par rapport à des rangées.

9.5.2 Comatrice

Soit $n \in \mathbb{N}^*$.

◆ **Définition** Soit $A = (a_{ij})_{ij} \in \mathbf{M}_n(K)$. On appelle **comatrice** de A la matrice carrée d'ordre n, notée com (A), définie par :

$$\text{com}\,(A) = (A_{ij})_{ij} = \begin{pmatrix} A_{11} & \dots & A_{1n} \\ \vdots & & \vdots \\ A_{n1} & \dots & A_{nn} \end{pmatrix},$$

où A_{ij} est le cofacteur de la place (i,j) dans A.

On a vu (9.5.1 Prop. *1)* p. 315) :

$$\forall\, j \in \{1,\dots,n\}, \quad \sum_{i=1}^{n} a_{ij} A_{ij} = \det(A).$$

Intéressons-nous à $\displaystyle\sum_{i=1}^{n} a_{ij} A_{ik}$, pour $(j,k) \in \{1,\dots,n\}^2$ fixé tel que $j \neq k$.

Considérons la matrice $B = (b_{ip})_{ip}$ obtenue à partir de A en remplaçant, dans A, la $k^{\text{ème}}$ colonne par la $j^{\text{ème}}$ colonne de A :

$$B = \begin{pmatrix} a_{11} & \dots & a_{1j} & \dots & a_{1k-1} & a_{1j} & a_{1k+1} & \dots & a_{1n} \\ \vdots & & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & \dots & a_{nj} & \dots & a_{nk-1} & a_{nj} & a_{nk+1} & \dots & a_{nn} \end{pmatrix}.$$

$k^{\text{ème}}$ colonne

D'une part, $\det(B) = 0$, puisque B a deux colonnes égales.

D'autre part, en développant $\det(B)$ par rapport à la $k^{\text{ème}}$ colonne, on a :

$$\det(B) = \sum_{i=1}^{n} b_{ik} B_{ik} = \sum_{i=1}^{n} a_{ij} A_{ik},$$

puisque les cofacteurs des éléments de la $k^{\text{ème}}$ colonne sont les mêmes dans B que dans A.

Ainsi : $\displaystyle\sum_{i=1}^{n} a_{ij} A_{ik} = 0.$

On a donc prouvé :

$$\forall\,(j,k) \in \{1,\dots,n\}^2, \quad \sum_{i=1}^{n} a_{ij} A_{ik} = \begin{cases} \det(A) & \text{si } j = k \\ 0 & \text{si } j \neq k \end{cases}.$$

Mais, pour $(j,k) \in \{1,\dots,n\}^2$, $\displaystyle\sum_{i=1}^{n} a_{ij} A_{ik}$ est le $(j,k)^{\text{ème}}$ terme du produit de ${}^tA$ par com (A), d'où :

$${}^tA \cdot \text{com}\,(A) = \begin{pmatrix} \det(A) & & 0 \\ & \ddots & \\ 0 & & \det(A) \end{pmatrix} = \det(A)\, \mathrm{I}_n.$$

En appliquant ce résultat à ${}^tA$ au lieu de A, et en remarquant $\text{com}({}^tA) = {}^t\text{com}(A)$ et $\det({}^tA) = \det(A)$ (cf. 9.4 Prop. 2 *6)* p. 310), on obtient :

$$A \cdot {}^t\text{com}(A) = \det(A)\mathrm{I}_n,$$

et, en transposant le résultat de la page précédente : ${}^t\text{com}(A) \cdot A = \det(A)\,\mathrm{I}_n$.

Enonçons le résultat obtenu :

♦ **Théorème**

$$\forall A \in \mathbf{M}_n(K), \quad A \cdot {}^t\text{com}(A) = {}^t\text{com}(A) \cdot A = \det(A)\mathrm{I}_n.$$

♦ **Corollaire**

$$\forall A \in \mathbf{GL}_n(K), \quad A^{-1} = \frac{1}{\det(A)}\,{}^t\text{com}(A).$$

EXEMPLE :

Pour $n = 2$, si $ad - bc \neq 0$, alors $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est inversible, et

$$A^{-1} = \frac{1}{ad - bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Remarque :

La formule précédente, donnant A^{-1} à l'aide de com (A), et en pratique quasiment inutilisable dès que $n \geqslant 3$. En effet, l'application de cette formule nécessite apparemment le calcul d'un déterminant d'ordre n $\big(\det(A)\big)$ et de n^2 déterminants d'ordre $n - 1$ (les cofacteurs dans A).

Exercices

◊ **9.5.1** Soient $n \in \mathbb{N}^*$, $M \in \mathbf{M}_n(K)$, $A = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & M & \\ 0 & & \end{pmatrix} \in \mathbf{M}_{n+1}(K)$. Calculer com (A).

◊ **9.5.2** Soient $n, p \in \mathbb{N}^*$, $A \in \mathbf{M}_n(K)$. Montrer :

$$A^p = \mathrm{I}_n \Longrightarrow \big(\text{com}(A)\big)^p = \mathrm{I}_n.$$

◊ **9.5.3** Soit $n \in \mathbb{N}^*$. Montrer : $\forall A \in \mathbf{GL}_n(K)$, $\begin{cases} \text{com}(A) \in \mathbf{GL}_n(K) \\ \big(\text{com}(A)\big)^{-1} = \text{com}(A^{-1}). \end{cases}$

9.6 Calcul des déterminants

9.6.1 Déterminant d'une matrice triangulaire

(Cf. aussi 9.4 Exemple *2)* p. 309).

◆ **Proposition** Le déterminant d'une matrice triangulaire est égal au produit des éléments diagonaux :

$$\begin{vmatrix} a_{11} & & \cdots \\ & \ddots & \\ 0 & & a_{nn} \end{vmatrix} = \prod_{i=1}^{n} a_{ii}.$$

Preuve :

Récurrence sur n. La propriété est évidente pour $n = 1$.

Supposons-la vraie pour un n de $\mathbb{N}^*$, et soit $A = \begin{pmatrix} a_{11} & & \cdots \\ & \ddots & \\ 0 & & a_{n+1\,n+1} \end{pmatrix} \in \mathbf{T}_{n+1,s}(K)$.

En développant $\det(A)$ par rapport à la $(n+1)^{\text{ème}}$ ligne, on obtient :

$$\det(A) = \begin{vmatrix} a_{11} & \cdots & \\ & \ddots & \\ 0 & & a_{nn} \end{vmatrix} a_{n+1\,n+1} = (a_{11} \ldots a_{nn}) a_{n+1\,n+1} = \prod_{i=1}^{n+1} a_{ii}.$$

Remarque :

En particulier, le déterminant d'une matrice diagonale est égal au produit des éléments diagonaux.

9.6.2 Manipulation de lignes et de colonnes

1) Utilisation de la multilinéarité

La multilinéarité du déterminant se traduit schématiquement par :

$$\begin{vmatrix} \boxed{\text{I}} & \begin{matrix} \lambda a_{1j} + b_{1j} \\ \vdots \\ \lambda a_{nj} + b_{nj} \end{matrix} & \boxed{\text{II}} \end{vmatrix} = \lambda \begin{vmatrix} \boxed{\text{I}} & \begin{matrix} a_{1j} \\ \vdots \\ a_{nj} \end{matrix} & \boxed{\text{II}} \end{vmatrix} + \begin{vmatrix} \boxed{\text{I}} & \begin{matrix} b_{1j} \\ \vdots \\ b_{nj} \end{matrix} & \boxed{\text{II}} \end{vmatrix}.$$

2) Pour que le déterminant d'une matrice soit nul, il faut et il suffit que la famille des colonnes de cette matrice soit liée (cf. 9.4 Prop. 2 *4)* p. 000). En particulier, si un déterminant a une colonne nulle, ou deux colonnes colinéaires, ce déterminant est nul.

Résultat analogue pour les lignes.

3) Remplacement d'une colonne par la somme de celle-ci et d'une combinaison linéaire des autres

Soient $A = (a_{ij})_{ij} \in \mathbf{M}_n(K)$, $C_1,\ldots,C_n$ les colonnes de A, $j \in \{1,\ldots,n\}$, $(\alpha_k)_{k\neq j} \in K^{n-1}$.
Considérons la matrice B obtenue à partir de A en remplaçant C_j par $C_j + \sum_{k\neq j} \alpha_k C_k$.

En notant $\mathcal{B} = (e_1,\ldots,e_n)$ la base canonique de $\mathbf{M}_{n,1}(K)$, on a :

$$\begin{aligned}\det(B) &= \det_{\mathcal{B}}\left(C_1,\ldots,C_j + \sum_{k\neq j}\alpha_k C_k,\ldots,C_n\right)\\ &= \det_{\mathcal{B}}(C_1,\ldots,C_j,\ldots,C_n) + \sum_{k\neq j}\alpha_k \det_{\mathcal{B}}(C_1,\ldots,C_{j-1},C_k,C_{j+1},\ldots,C_n)\\ &= \det(A),\end{aligned}$$

puisque chaque $\det_{\mathcal{B}}(C_1,\ldots,C_{j-1},C_k,C_{j+1},\ldots,C_n)$ $(k \neq j)$ contient deux fois la colonne C_k.

Ainsi :

On ne change pas la valeur d'un déterminant en remplaçant une colonne par la somme de celle-ci et d'une combinaison linéaire des autres colonnes.

Résultat analogue sur les lignes.

Remarque :

On peut aussi montrer le résultat précédent en remarquant $B = AF$, où

$$F = \begin{pmatrix} 1 & & 0 & \alpha_1 & & \\ & \ddots & & \vdots & & 0 \\ & & 1 & \alpha_{j-1} & & \\ & & & 1 & & \\ & 0 & & \alpha_{j+1} & \ddots & \\ & & & \vdots & 0 & \\ & & & \alpha_n & & 1 \end{pmatrix},$$

et en développant $\det(F)$ par rapport à la $1^{\text{ère}}$ colonne, $j-1$ fois :

$$\det(F) = \begin{pmatrix} 1 & & 0 \\ \alpha_{j+1} & \ddots & \\ \vdots & 0 & \\ \alpha_n & & 1 \end{pmatrix},$$

puis (matrice triangulaire) : $\det(F) = 1$.

4) Remplacement simultané de colonnes

Soient $A = (a_{ij})_{ij} \in \mathbf{M}_n(K)$, $C_1, \ldots, C_n$ les colonnes de A. Nous allons montrer qu'on peut, sans changer $\det(A)$, remplacer dans A chaque colonne par la somme de celle-ci et d'une combinaison linéaire des colonnes *suivantes*.

Pour chaque k de $\{2, \ldots, n\}$, soient $\alpha_{k\,k-1}, \ldots, \alpha_{n\,k-1} \in K$.

Considérons la matrice B obtenue à partir de A en remplaçant :

C_1 par $C_1 + \alpha_{21}C_2 + \ldots + \alpha_{n1}C_n$

C_2 par $C_2 + \alpha_{32}C_3 + \ldots + \alpha_{n2}C_n$

$\vdots$

C_{n-1} par $C_{n-1} + \alpha_{n\,n-1}C_n$

C_n par C_n.

En notant $T = \begin{pmatrix} 1 & & & 0 \\ \alpha_{21} & 1 & & \\ \alpha_{31} & \alpha_{32} & 1 & \\ \vdots & \vdots & \ddots & \\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{n\,n-1} \quad 1 \end{pmatrix}$, on a : $B = AT$, d'où :

$\det(B) = \det(A)\det(T) = \det(A) \cdot 1 = \det(A)$ (cf. 9.6.1 Prop. p. 318).

Ainsi :

On ne change pas la valeur d'un déterminant en remplaçant (simultanément) chaque colonne par la somme de celle-ci et d'une combinaison linéaire des colonnes suivantes.

De même, en utilisant la postmultiplication de A par une matrice triangulaire supérieure :

On ne change pas la valeur d'un déterminant en remplaçant (simultanément) chaque colonne par la somme de celle-ci et d'une combinaison linéaire des colonnes précédentes.

Résultats analogues sur les lignes.

EXEMPLE :

Pour $(a,b) \in K^2$ et $n \geqslant 2$, calculer $\begin{vmatrix} a & & b \\ & \ddots & \\ b & & a \end{vmatrix}_{|n|}$.

$$\begin{vmatrix} a & b & \cdots & b \\ b & a & \ddots & \vdots \\ \vdots & \ddots & \ddots & b \\ b & \cdots & b & a \end{vmatrix}_{[n]} = \begin{vmatrix} a+(n-1)b & b & \cdots & b \\ \vdots & a & \ddots & \vdots \\ a+(n-1)b & b & \cdots & a \end{vmatrix}_{[n]} \quad C_1 \leftarrow C_1 + \sum_{j=2}^{n} C_j$$

$$= \big(a+(n-1)b\big) \begin{vmatrix} 1 & b & \cdots & b \\ \vdots & a & \ddots & \vdots \\ 1 & b & \cdots & a \end{vmatrix}_{[n]}$$

$$= \big(a+(n-1)b\big) \begin{vmatrix} 1 & b & \cdots & b \\ 0 & a-b & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & a-b \end{vmatrix}_{[n]} \begin{matrix} \\ L_2 \leftarrow L_2 - L_1 \\ \vdots \\ L_n \leftarrow L_n - L_1 \end{matrix}$$

$$= \big(a+(n-1)b\big)(a-b)^{n-1}.$$

9.6.3 Cas $n = 2$, $n = 3$

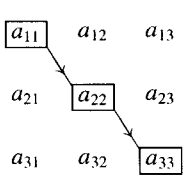
1) $n = 2$: $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{21}a_{12}.$

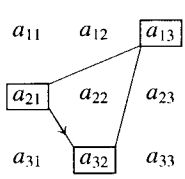
2) $n = 3$: $\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} - a_{21}a_{12}a_{33} - a_{31}a_{22}a_{13}$
$$- a_{11}a_{32}a_{23} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23}$$

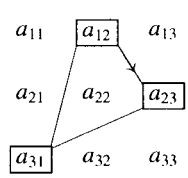
(cf. 9.5.1 1) p. 312).

On peut retrouver ce résultat par la **règle de Sarrus** : le déterminant d'ordre 3 contient six termes (cf. 9.4 Déf. p. 309) :

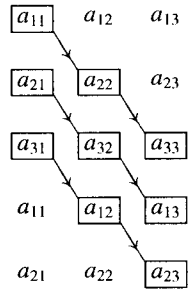
- $a_{11}a_{22}a_{33}$, $a_{21}a_{32}a_{13}$, $a_{31}a_{12}a_{23}$ correspondant à des «diagonales descendantes» :



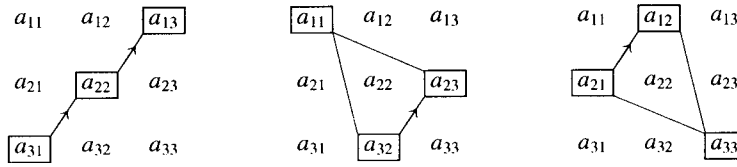




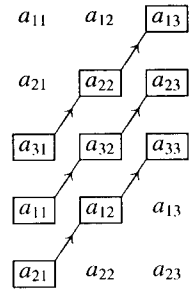
ou encore, en reportant des lignes en dessous :



- $-a_{31}a_{22}a_{13}$, $-a_{11}a_{32}a_{23}$, $-a_{21}a_{12}a_{33}$ correspondant à des «diagonales montantes » :



ou encore :



Mais attention : la règle de Sarrus n'est applicable que pour $n = 3$ (et $n = 2$).

EXEMPLE :

$$\begin{vmatrix} a & p & q \\ -p & a & r \\ -q & -r & a \end{vmatrix} = a^3 + pqr - pqr + aq^2 + ar^2 + ap^2 = a(a^2 + p^2 + q^2 + r^2).$$

9.6.4 Déterminant de Vandermonde

Soit $n \in \mathbb{N}^*$.

◆ **Définition** Soit $(x_1, \ldots, x_n) \in K^n$. On appelle **déterminant de Vandermonde**, et on note $V(x_1, \ldots, x_n)$ l'élément de K défini par :

$$V(x_1, \ldots, x_n) = \begin{vmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{vmatrix} = \det\left((x_i^{j-1})_{1 \leqslant i,j \leqslant n}\right).$$

Nous allons calculer $V(x_1,\dots,x_n)$.

Si $n=1$: $V(x_1)=1$

Si $n=2$: $V(x_1,x_2)=\begin{vmatrix}1 & x_1\\ 1 & x_2\end{vmatrix}=x_2-x_1$.

Si $n=3$: $V(x_1,x_2,x_3)=\begin{vmatrix}1 & x_1 & x_1^2\\ 1 & x_2 & x_2^2\\ 1 & x_3 & x_3^2\end{vmatrix}=\begin{vmatrix}1 & 0 & 0\\ 1 & x_2-x_1 & x_2^2-x_1x_2\\ 1 & x_3-x_1 & x_3^2-x_1x_3\end{vmatrix}$

$$C_2\leftarrow C_2-x_1C_1,\quad C_3\leftarrow C_3-x_1C_2$$

$$=(x_2-x_1)(x_3-x_1)\begin{vmatrix}1 & x_2\\ 1 & x_3\end{vmatrix}=(x_2-x_1)(x_3-x_1)(x_3-x_2)$$

Pour tout n de $\mathbb{N}$ tel que $n\geqslant 3$:

$$V(x_1,\dots,x_n)=\begin{vmatrix}1 & x_1 & x_1^2 & \dots & x_1^{n-1}\\ & x_2 & x_2^2 & \dots & x_2^{n-1}\\ & \vdots & \vdots & & \vdots\\ 1 & x_n & x_n^2 & \dots & x_n^{n-1}\end{vmatrix}$$

$$=\begin{vmatrix}1 & 0 & 0 & \dots & 0\\ & x_2-x_1 & x_2^2-x_1x_2 & \dots & x_2^{n-1}-x_1x_2^{n-2}\\ & \vdots & \vdots & & \vdots\\ 1 & x_n-x_1 & x_n^2-x_1x_n & \dots & x_n^{n-1}-x_1x_n^{n-2}\end{vmatrix}$$

$$C_2\leftarrow C_2-x_1C_1,\quad C_3\leftarrow C_3-x_1C_2,\dots\ C_n\leftarrow C_n-x_1C_{n-1}$$

$$=\begin{vmatrix}1 & 0 & 0 & \dots & 0\\ & x_2-x_1 & (x_2-x_1)x_2 & \dots & (x_2-x_1)x_2^{n-2}\\ & \vdots & \vdots & & \vdots\\ 1 & x_n-x_1 & (x_n-x_1)x_n & \dots & (x_n-x_1)x_n^{n-2}\end{vmatrix}$$

$$=(x_2-x_1)\dots(x_n-x_1)\begin{vmatrix}1 & x_2 & \dots & x_2^{n-2}\\ & \vdots & & \vdots\\ 1 & x_n & \dots & x_n^{n-2}\end{vmatrix},$$

en développant par rapport à la 1ère colonne, puis en factorisant dans chaque ligne.

On obtient ainsi : $V(x_1,\dots,x_n)=\left(\prod_{n\geqslant i>1}(x_i-x_1)\right)V(x_2,\dots,x_n)$.

On conclut, par récurrence :

♦ **Proposition**

$$\forall n\in\mathbb{N}^*,\ \forall (x_1,\dots,x_n)\in K^n,\ V(x_1,\dots,x_n)=\prod_{n\geqslant i>j\geqslant 1}(x_i-x_j).$$

◆ **Corollaire** Pour tout $(x_1,\ldots,x_n)$ de K^n, $V(x_1,\ldots,x_n)$ est non nul si et seulement si $x_1,\ldots,x_n$ sont deux à deux distincts.

Exercices

◇ **9.6.1** Calculer les déterminants suivants :

a) $\begin{vmatrix} 1^2 & 2^2 & 3^2 & \ldots & n^2 \\ 2^2 & 3^2 & 4^2 & \ldots & (n+1)^2 \\ 3^2 & 4^2 & 5^2 & \ldots & (n+2)^2 \\ \vdots & \vdots & \vdots & & \vdots \\ n^2 & (n+1)^2 & (n+2)^2 & \ldots & (2n-1)^2 \end{vmatrix}$, $n \in \mathbb{N}^*$

b) $\begin{vmatrix} S_1 & S_1 & S_1 & \cdots & S_1 \\ S_1 & S_2 & S_2 & \cdots & S_2 \\ S_1 & S_2 & S_3 & \cdots & S_3 \\ \vdots & \vdots & \vdots & & \vdots \\ S_1 & S_2 & S_3 & \cdots & S_n \end{vmatrix}$, $n \in \mathbb{N}^*$, $S_k = \sum_{i=1}^{k} i$

c) $\begin{vmatrix} a_1 & a_2 & \ldots & a_n \\ & & & \vdots \\ & & & a_2 \\ a_1 & & & \\ & & & a_1 \end{vmatrix}$, $n \in \mathbb{N}^*$, $a_1,\ldots,a_n \in K$

d) $\begin{vmatrix} a_1+b_1 & a_1 & a_1 & \cdots & a_1 \\ a_2 & a_2+b_2 & a_2 & \cdots & a_2 \\ a_3 & a_3 & a_3+b_3 & \ldots & a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & a_n & a_n & \ldots & a_n+b_n \end{vmatrix}$, $n \in \mathbb{N}^*$, $a_1,\ldots,a_n,b_1,\ldots,b_n \in K$

e) $\begin{vmatrix} a_1 & -a_1 & 0 & \cdots & 0 \\ -a_1 & a_1+a_2 & -a_2 & \ddots & \vdots \\ 0 & -a_2 & a_2+a_3 & \ddots & \\ \vdots & \ddots & \ddots & \ddots & -a_{n-1} \\ 0 & \cdots & -a_{n-1} & a_{n-1}+a_n & \end{vmatrix}$,

$n \in \mathbb{N}^*$, $a_1,\ldots,a_n \in K$

f) $\begin{vmatrix} a & b & & 0 \\ c & & \ddots & \\ & \ddots & & b \\ 0 & & c & a \end{vmatrix}_{[n]}$, $n \in \mathbb{N}^*$, $(a,b,c) \in \mathbb{C}^3$

(on exprimera la réponse à l'aide des zéros complexes de $X^2 - aX + bc$)

g) $\det\left(\left(C_{i+j}^{j}\right)_{0\leqslant i,j\leqslant n}\right) = \begin{vmatrix} C_0^0 & C_1^1 & \dots & C_n^n \\ C_1^0 & C_2^1 & \dots & C_{n+1}^n \\ \vdots & \vdots & & \vdots \\ C_n^0 & C_{n+1}^1 & \dots & C_{2n}^n \end{vmatrix}_{[n+1]}$, $n \in \mathbb{N}$

h) $\begin{vmatrix} \alpha + a_1 & -1 & 0 & \cdots & 0 \\ a_2 & \alpha & -1 & \ddots & \vdots \\ a_3 & 0 & \alpha & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & -1 \\ a_n & 0 & \cdots & 0 & \alpha \end{vmatrix}$, $n \in \mathbb{N}^*$, $\alpha, a_1, \dots, a_n \in K$

i) $\begin{vmatrix} 1 & -a_1 & -a_2 & \dots & -a_n \\ a_1 & b_1 & 0 & & \\ a_2 & 0 & b_2 & \ddots & \\ \vdots & \vdots & \ddots & \ddots & 0 \\ a_n & & & & b_n \end{vmatrix}_{[n+1]}$, $n \in \mathbb{N}^*$, $a_1, \dots, a_n, b_1, \dots, b_n \in K$

j) $\begin{vmatrix} a & x & \cdots & x \\ y & z & \ddots & \\ \vdots & \ddots & \ddots & 0 \\ y & 0 & & z \end{vmatrix}_{[n]}$, $n \in \mathbb{N}^*$, $a,x,y,z \in K$

k) $\begin{vmatrix} -(a+1) & 1 & 0 & \cdots & 0 \\ a & -(a+2) & 2 & \ddots & \vdots \\ 0 & a & -(a+3) & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & n-1 \\ 0 & \cdots & 0 & a & -(a+n) \end{vmatrix}$, $n \in \mathbb{N}^*$, $a \in K$.

◊ **9.6.2** Montrer que $E = \left\{ \begin{pmatrix} x & y & z \\ 2z & x & y \\ 2y & 2z & x \end{pmatrix} ; (x,y,z) \in \mathbb{Q}^3 \right\}$ est un sous-corps de l'anneau $\mathbf{M}_3(\mathbb{Q})$.

◇ **9.6.3** Soit $A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & k \end{pmatrix} \in \mathbf{M}_3(\mathbb{R})$.

a) Montrer qu'il est impossible que : le produit des éléments dans chaque ligne (de A) soit < 0 et le produit dans chaque colonne soit > 0.

b) Montrer qu'il est impossible que les six termes de $\det(A) = aek + bfg + cdh + (-ceg) + (-afh) + (-bdk)$ soient tous > 0.

◇ **9.6.4** Calculer $\det(f)$, où $f : \begin{array}{ccc} \mathbf{M}_n(\mathbb{R}) & \longrightarrow & \mathbf{M}_n(\mathbb{R}) \\ X & \longmapsto & {}^tX \end{array}$.

◇ **9.6.5** Pour $(p,x) \in \mathbb{N} \times \mathbb{R}$, on note :

$$\varphi_p(x) = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 & x \\ & 2 & 0 & \cdots & 0 & x^2 \\ & & 3 & \ddots & \vdots & \vdots \\ & & & \ddots & 0 & \\ & & & & C_p^{p-1} & x^p \\ 1 & C_{p+1}^1 & C_{p+1}^2 & \cdots & C_{p+1}^{p-1} & x^{p+1} \end{vmatrix}_{[p+1]}$$

a) Pour $(p,x) \in \mathbb{N} \times \mathbb{R}$, calculer $\varphi_p(x+1) - \varphi_p(x)$.

b) Montrer : $\forall n \in \mathbb{N}^*,\ \varphi_p(n+1) = (p+1)! \sum_{k=1}^{n} k^p$.

c) En déduire les valeurs de $\sum_{k=1}^{n} k$, $\sum_{k=1}^{n} k^2$, $\sum_{k=1}^{n} k^3$, pour $n \in \mathbb{N}^*$.

◇ **9.6.6** Soient $n \in \mathbb{N} - \{0,1\}$, $P_n = X^n - X + 1$. On note $x_1, \ldots, x_n$ les zéros de P_n dans $\mathbb{C}$.

Soit $A = (a_{ij})_{ij} \in \mathbf{M}_n(\mathbb{C})$ où : $a_{ij} = \begin{cases} 1 + x_i & \text{si } i = j \\ 1 & \text{si } i \neq j \end{cases}$. Calculer $\det(A)$.

◇ **9.6.7** Soient $n \in \mathbb{N}^*$, E un K-ev de dimension n, $V_1, \ldots, V_n \in E$, $f \in \mathcal{L}(E)$, $\mathcal{B}$ une base de E.

Démontrer : $\sum_{j=1}^{n} \det_{\mathcal{B}}(V_1, \ldots, f(V_j), \ldots, V_n) = \mathrm{tr}(f) \det_{\mathcal{B}}(V_1, \ldots, V_n)$.

◇ **9.6.8** Soit $A = (a_{ij})_{ij} \in \mathbf{M}_n(\mathbb{R})$ telle que, pour tout (i,j) de $\{1,\ldots,n\}^2$: $\begin{cases} a_{ij} \in \mathbb{Z} \\ i \neq j \Longrightarrow a_{ij} \text{ pair} \\ a_{ii} \text{ impair.} \end{cases}$

Montrer : $\det(A) \neq 0$.

◇ **9.6.9** Soit $A = (a_{ij})_{ij} \in \mathbf{M}_n(\mathbb{R})$ telle que, pour tout (i,j) de $\{1,\ldots,n\}^2$:

$\begin{cases} a_{ij} \in \mathbb{Z} \\ i \neq j \Longrightarrow a_{ij} \text{ impair} \\ a_{ii} \text{ pair} \end{cases}$. Montrer que, si n est pair, alors $\det(A) \neq 0$.

9.7 Orientation d'un espace vectoriel réel de dimension finie

Soient $n \in \mathbb{N}^*$ et E un $\mathbb{R}$-ev de dimension n. On note $\beta(E)$ l'ensemble des bases de E.

♦ **Définition 1** On dit que deux bases $\mathcal{B},\mathcal{B}'$ de E sont :

- **de même sens** si et seulement si : $\det_{\mathcal{B}}(\mathcal{B}') > 0$.
- **de sens contraires** si et seulement si : $\det_{\mathcal{B}}(\mathcal{B}') < 0$.

Puisque $\mathbb{R}$ est totalement ordonné et que, pour toutes bases $\mathcal{B},\mathcal{B}'$ de E, $\det_{\mathcal{B}}(\mathcal{B}') \neq 0$, deux bases données sont de même sens ou de sens contraires.

Notons $\mathcal{R}$ la relation définie dans $\beta(E)$ par :

$$\forall \mathcal{B},\mathcal{B}' \in \beta(E),\ (\mathcal{B}\ \mathcal{R}\ \mathcal{B}' \iff \det_{\mathcal{B}'}(\mathcal{B}) > 0).$$

La relation $\mathcal{R}$ est une relation d'équivalence dans $\beta(E)$ car, pour toutes $\mathcal{B},\mathcal{B}',\mathcal{B}''$ de $\beta(E)$:

- $\det_{\mathcal{B}}(\mathcal{B}) = 1 > 0$
- $\mathcal{B}\ \mathcal{R}\ \mathcal{B}' \iff \det_{\mathcal{B}}(\mathcal{B}') > 0 \Longrightarrow \det_{\mathcal{B}'}(\mathcal{B}) = \left(\det_{\mathcal{B}}(\mathcal{B}')\right)^{-1} > 0 \Longrightarrow \mathcal{B}'\ \mathcal{R}\ \mathcal{B}$
- $\begin{cases} \mathcal{B}\ \mathcal{R}\ \mathcal{B}' \\ \mathcal{B}'\ \mathcal{R}\ \mathcal{B}'' \end{cases} \iff \begin{cases} \det_{\mathcal{B}'}(\mathcal{B}) > 0 \\ \det_{\mathcal{B}''}(\mathcal{B}') > 0 \end{cases} \Longrightarrow \det_{\mathcal{B}''}(\mathcal{B}) = \det_{\mathcal{B}''}(\mathcal{B}')\det_{\mathcal{B}'}(\mathcal{B}) > 0 \Longrightarrow \mathcal{B}\ \mathcal{R}\ \mathcal{B}''.$

Le $\mathbb{R}$-ev E, étant de dimension finie, admet au moins une base $\mathcal{B}_1 = (e_1,\ldots,e_n)$; considérons $\mathcal{B}_2 = (-e_1,e_2,\ldots,e_n)$, qui est une base de E. Comme $\det_{\mathcal{B}_1}(\mathcal{B}_2) = -1 < 0$, $\mathcal{B}_1$ et $\mathcal{B}_2$ sont de sens contraires.

Soit $\mathcal{B} \in \beta(E)$.

- Si $\det_{\mathcal{B}_1}(\mathcal{B}) > 0$, alors $\mathcal{B}_1\ \mathcal{R}\ \mathcal{B}$
- Si $\det_{\mathcal{B}_1}(\mathcal{B}) < 0$, alors $\det_{\mathcal{B}_2}(\mathcal{B}) = \det_{\mathcal{B}_2}(\mathcal{B}_1)\det_{\mathcal{B}_1}(\mathcal{B}) = -\det_{\mathcal{B}_1}(\mathcal{B}) > 0$, donc $\mathcal{B}_2\ \mathcal{R}\ \mathcal{B}$.

Ceci montre que $\beta(E)$ admet exactement deux classes d'équivalence modulo $\mathcal{R}$, qui sont la classe de $\mathcal{B}_1$ et la classe de $\mathcal{B}_2$. D'où la définition suivante.

♦ **Définition 2** On appelle **orientation** de E le choix, dans l'ensemble $\beta(E)$ des bases de E, de l'une des deux classes d'équivalence modulo la relation «est de même sens que ». Les bases de cette classe sont alors dites **directes**, les autres bases (celles de l'autre classe) sont dites **indirectes**. On dit alors que E est un $\mathbb{R}$-ev **orienté**.

On convient que la base canonique de $\mathbb{R}^n$ est directe (ce qui revient à choisir une orientation dans $\mathbb{R}^n$).

On appelle **axe** toute droite vectorielle orientée. ■

Soit $f \in \mathcal{GL}(E)$. Comme $\det(f) \neq 0$, on a : $\det(f) > 0$ ou $\det(f) < 0$.
Soit $\mathcal{B} \in \beta(E)$.

- Si $\det(f) > 0$, alors $\det_{\mathcal{B}}\big(f(\mathcal{B})\big) = \det(f) > 0$, et donc $\mathcal{B}$ et $f(\mathcal{B})$ sont de même sens
- Si $\det(f) < 0$, alors $\det_{\mathcal{B}}\big(f(\mathcal{B})\big) = \det(f) < 0$, et donc $\mathcal{B}$ et $f(\mathcal{B})$ sont de sens contraires.

D'où la Définition et la Proposition suivantes.

◆ **Définition 3** Soit $f \in \mathcal{GL}(E)$. On dit que :

- f **conserve l'orientation** (ou : **est direct**) si et seulement si : $\det(f) > 0$.
- f **change l'orientation** (ou : **est indirect**) si et seulement si : $\det(f) < 0$.

◆ **Proposition** Soit $f \in \mathcal{GL}(E)$.

1) Si f conserve l'orientation, alors, pour toute base $\mathcal{B}$ de E, $f(\mathcal{B})$ est une base de même sens que $\mathcal{B}$.

2) Si f change l'orientation, alors, pour toute base $\mathcal{B}$ de E, $f(\mathcal{B})$ est une base de sens contraire de $\mathcal{B}$.

9.8 Rang et sous-matrices

Rappels sur le rang

Nous avons défini :

• le rang d'une famille finie $\mathcal{F}$ d'éléments d'un K-ev E :

$$\mathrm{rg}(\mathcal{F}) = \dim\big(\mathrm{Vect}\,(\mathcal{F})\big),\quad \text{6.4 Déf. 3 p. 234}$$

• le rang d'une application linéaire $f \in \mathcal{L}(E,F)$:

$$\mathrm{rg}(f) = \dim\big(\mathrm{Im}(f)\big),\quad \text{7.3.1 Déf. p. 254}$$

• le rang d'une matrice A de $\mathbf{M}_{n,p}(K)$:

$$\mathrm{rg}(A) = \mathrm{rg}(C_1,\ldots,C_p),\quad \text{8.1.6 Déf. p. 276,}$$

où $C_1,\ldots,C_p$ sont les colonnes de A.

Ces notions sont reliées entre elles :

• le rang d'une famille finie $\mathcal{F}$ d'éléments de E est aussi le rang de la matrice dont les colonnes sont formées par les composantes des éléments de $\mathcal{F}$ dans une base de E

• le rang de $f \in \mathcal{L}(E,F)$ est, pour toute base $\mathcal{B} = (e_1,\ldots,e_p)$ de E, le rang de la famille $\big(f(e_i)\big)_{1\leqslant i\leqslant n}$, et est aussi le rang de n'importe quelle matrice représentant f.

• le rang de $A \in \mathbf{M}_{n,p}(K)$ est le rang de n'importe quelle application linéaire représentée par A.

Rappelons enfin le théorème du rang (7.3.1 Th. 1 p. 254) :

$$\forall f \in \mathcal{L}(E,F),\quad \mathrm{rg}(f) = \dim(E) - \dim\big(\mathrm{Ker}(f)\big).$$ ■

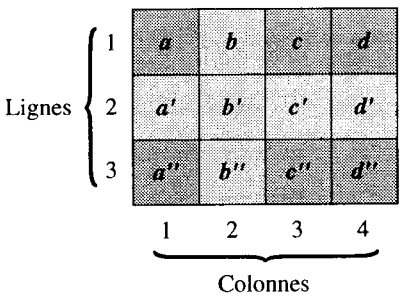
♦ **Définition** Soient $(n,p) \in (\mathbb{N}^*)^2$, $A = (a_{ij})_{ij} \in \mathbf{M}_{n,p}(K)$, $(u,v) \in (\mathbb{N}^*)^2$,

$$\begin{cases} (i_1,\ldots,i_u) \in \{1,\ldots,n\}^u \text{ tel que } i_1 < \ldots < i_u \\ (j_1,\ldots,j_v) \in \{1,\ldots,p\}^v \text{ tel que } j_1 < \ldots < j_v \end{cases}.$$

On appelle **sous-matrice** (ou : **matrice extraite**) de A, par utilisation des lignes $i_1,\ldots,i_u$ et des colonnes $j_1,\ldots,j_v$, la matrice $\big(a_{i_k j_l}\big)_{\substack{1\leqslant k\leqslant u\\ 1\leqslant l\leqslant v}}$ de $\mathbf{M}_{u,v}(K)$.

EXEMPLE :

La matrice $\begin{pmatrix} a & c & d \\ a'' & c'' & d'' \end{pmatrix}$ est une sous-matrice de $\begin{pmatrix} a & b & c & d \\ a' & b' & c' & d' \\ a'' & b'' & c'' & d'' \end{pmatrix}$, par utilisation des lignes 1, 3 et des colonnes 1,3,4 :



◆ **Théorème** Pour toute A de $\mathbf{M}_{n,p}(K)$, le rang de A est égal à l'ordre maximum des sous-matrices carrées inversibles extraites de A.

Preuve :

Notons $r = \text{rg}(A)$, et s l'ordre maximum des sous-matrices carrées inversibles extraites de A.

1) $r \geqslant s$

Soit B une sous-matrice carrée de A, α l'ordre de B, et supposons $\alpha > r$. Notons $i_1,\ldots,i_\alpha$ $(i_1 < \ldots < i_\alpha)$ les numéros des lignes de A utilisées pour extraire $B, v_1,\ldots,v_\alpha$ les colonnes de B (dans $\mathbf{M}_{\alpha,1}(K)$), $V_1,\ldots,V_\alpha$ les colonnes de A utilisées pour extraire B (dans $\mathbf{M}_{n,1}(K)$). Puisque $\alpha > r$, la famille $(V_1,\ldots,V_\alpha)$ est liée. Il existe $(\lambda_1,\ldots,\lambda_\alpha) \in K^\alpha - \{(0,\ldots,0)\}$ tel que $\sum_{i=1}^{\alpha} \lambda_i V_i = 0$. Il en résulte, en ne prenant que les lignes numéros $i_1,\ldots,i_\alpha$: $\sum_{i=1}^{\alpha} \lambda_i v_i = 0$, et donc B n'est pas inversible. Ceci montre : $r \geqslant s$.

2) $r \leqslant s$

Soient $\mathcal{B} = (e_1,\ldots,e_p)$ la base canonique de K^p, $\mathcal{B}' = (f_1,\ldots,f_n)$ la base canonique de K^n, $f : K^p \longrightarrow K^n$ l'application linéaire représentée par A dans les bases $\mathcal{B}$ et $\mathcal{B}'$.

Puisque $\text{rg}(f) = \text{rg}(A) = r$, il existe $i_1,\ldots,i_r \in \{1,\ldots,p\}$ tels que :

$$i_1 < \ldots < i_r \text{ et } \big(f(e_{i_1}),\ldots,f(e_{i_r})\big) \text{ est une base de } \text{Im}(f).$$

En permutant les colonnes de A (ce qui ne change ni r ni s), on peut se ramener à supposer : $i_1 = 1,\ldots,i_r = r$.

D'après le théorème de la base incomplète, forme faible (6.4 Th. 2 p. 229), il existe $j_{r+1},\ldots,j_n \in \{1,\ldots,n\}$ tels que la famille $\mathcal{F} = \left(f(e_1),\ldots,f(e_r),f_{j_{r+1}},\ldots,f_{j_n}\right)$ soit une base de K^n. Ainsi $\det_{\mathcal{B}'}(\mathcal{F}) \neq 0$, et :

$$\det_{\mathcal{B}'}(\mathcal{F}) = \begin{pmatrix} a_{11} & \ldots & a_{1r} & 0 & 0 & 0 \\ \vdots & & \vdots & \vdots & \vdots & \vdots \\ \vdots & & \vdots & 0 & 1 & \vdots \\ \vdots & & \vdots & 1 & 0 & \vdots \\ \vdots & & \vdots & 0 & \vdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & 1 \\ \vdots & & \vdots & \vdots & \vdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \ldots & a_{nr} & 0 & 0 & 0 \end{pmatrix},$$

où, pour tout k de $\{1,\ldots,n-r\}$, la colonne numéro $r+k$ est formée de zéros, sauf un terme égal à 1, situé à la ligne j_{r+k}.

En développant ce déterminant par rapport à la dernière colonne, de façon itérée, on obtient, en notant $j_1,\ldots,j_r \in \{1,\ldots,n\}$ tels que $j_1 < \ldots < j_r$ et $\{j_1,\ldots,j_r\} = \complement_{\{1,\ldots,n\}}\{j_{r+1},\ldots,j_n\}$:

$$\det_{\mathcal{B}'}(\mathcal{F}) = \pm \begin{pmatrix} a_{j_1 1} & \ldots & a_{j_1 r} \\ \vdots & & \vdots \\ a_{j_r 1} & \ldots & a_{j_r r} \end{pmatrix}.$$

On fait ainsi apparaître une matrice carrée d'ordre r, inversible, extraite de A.

Ceci montre : $r \leqslant s$ ■

EXEMPLE :

Quel est le rang de $A = \begin{pmatrix} 2 & 1 & 4 & -3 \\ 4 & 0 & 6 & 1 \end{pmatrix} \in \mathbf{M}_{2,4}(\mathbb{R})$?

D'une part, $\operatorname{rg}(A) \leqslant 2$ car $A \in \mathbf{M}_{2,4}(\mathbb{R})$.

D'autre part, la matrice $\begin{pmatrix} 2 & 1 \\ 4 & 0 \end{pmatrix}$, d'ordre 2, extraite de A , est inversible (car de déterminant -4, non nul).

On conclut : $\operatorname{rg}(A) = 2$. ■

Le Corollaire suivant se déduit clairement du théorème précédent.

♦ **Corollaire**

$$\forall A \in \mathbf{M}_{n,p}(K), \quad \operatorname{rg}({}^tA) = \operatorname{rg}(A).$$

Cf. aussi 8.2.3 Cor. 2 p. 289.

Exercices

◇ **9.8.1** Soient $n \in \mathbb{N} - \{0,1\}$, $A \in \mathbf{M}_n(K)$. Démontrer :

$$\begin{cases} \text{rg}(A) \leqslant n-2 & \Longrightarrow \quad \text{rg}(\text{com}\,(A)) = 0 \\ \text{rg}(A) = n-1 & \Longrightarrow \quad \text{rg}(\text{com}\,(A)) = 1 \\ \text{rg}(A) = n & \Longrightarrow \quad \text{rg}(\text{com}\,(A)) = n. \end{cases}$$

◇ **9.8.2** Soient $n \in \mathbb{N} - \{0,1\}$, $A \in \mathbf{M}_n(K)$, $p \in \mathbb{N}^*$. Calculer com (com (... (com (A)) ...)), où com est itéré p fois. (On pourra utiliser l'exercice 9.8.1).

◇ **9.8.3** Soient $n \in \mathbb{N} - \{0,1\}$, $A \in \mathbf{M}_n(K)$ telle que $\text{rg}(A) = n-1$, $B \in \mathbf{M}_n(K)$ telle que $AB = BA = 0$.

Démontrer : $\exists \gamma \in K, B = \gamma\, {}^t\text{com}\,(A)$.

◇ **9.8.4** Soient $n \in \mathbb{N} - \{0,1\}$, $A = \begin{pmatrix} 1-n & & 1 \\ & \diagdown & \\ 1 & & 1-n \end{pmatrix} \in \mathbf{M}_n(K)$.

Calculer com (A). (On pourra utiliser les exercices 9.8.1 et 9.8.3).

◇ **9.8.5*** Soient $n \in \mathbb{N}$ tel que $n \geqslant 3$, $A = (a_{ij})_{ij} \in \mathbf{M}_n(K)$.

Pour $(i,j) \in \{1,\ldots,n\}^2$, on note A_{ij} le cofacteur de a_{ij} dans A. On note B la matrice carrée d'ordre $n-2$ obtenue à partir de A en supprimant les lignes n^{os} 1 et n et les colonnes n^{os} 1 et n.

Démontrer : $\det(A)\det(B) = \begin{vmatrix} A_{11} & A_{1n} \\ A_{n1} & A_{nn} \end{vmatrix}$.

(On pourra considérer le déterminant d'ordre n suivant : $\begin{vmatrix} A_{11} & 0 & \cdots & 0 & A_{1n} \\ A_{21} & 1 & \diagdown & & A_{2n} \\ \vdots & & 0 & & \vdots \\ A_{n-11} & & \diagdown & 1 & A_{n-1n} \\ A_{n1} & 0 & \cdots & 0 & A_{nn} \end{vmatrix}$).

9.9 Systèmes affines

9.9.1 Position du problème

Soient $A = \begin{pmatrix} a_{11} & \dots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{np} \end{pmatrix} \in \mathbf{M}_{n,p}(K)$, $B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in \mathbf{M}_{n,1}(K)$.

On s'intéresse au **système** d'équations :

$$(S) \begin{cases} a_{11}x_1 & +\ldots+ & a_{1p}x_p = b_1 \\ \vdots & & \vdots \quad \vdots \\ a_{n1}x_1 & +\ldots+ & a_{np}x_p = b_n \end{cases},$$

d'inconnue $(x_1,\ldots,x_p) \in K^p$, appelé **système affine**.

En notant $\mathcal{S}$ l'ensemble des solutions de (S) dans K^p, il s'agit de savoir si $\mathcal{S}$ est vide ou non, et, lorsque $\mathcal{S} \neq \varnothing$, d'expliciter les éléments de $\mathcal{S}$.

1) Interprétation matricielle

En notant $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \in \mathbf{M}_{p,1}(K)$, $(x_1,\ldots,x_p)$ est solution de (S) dans K^p si et seulement si : $AX = B$. Ainsi, la résolution de (S) se ramène à celle de l'équation matricielle $AX = B$, d'inconnue $X \in \mathbf{M}_{p,1}(K)$.

2) Interprétation vectorielle

Soient :
- E un K-ev de dimension p
- F un K-ev de dimension n
- $\mathcal{B}$ une base de E, $\mathcal{C}$ une base de F
- $f \in \mathcal{L}(E,F)$ telle que $\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f) = A$
- $b \in F$ tel que $\mathrm{Mat}_{\mathcal{C}}(b) = B$
- $x \in E$ tel que $\mathrm{Mat}_{\mathcal{B}}(x) = X$.

On a : $AX = B \iff f(x) = b \iff x \in f^{-1}(\{b\})$.

Ainsi, la résolution de (S) revient à la détermination de l'image réciproque du singleton $\{b\}$ par f.

3) Interprétation affine

Notons, pour $i \in \{1,\dots,n\}$, $\varphi_i : K^p \longrightarrow K$ l'application définie par :

$$\forall (x_1,\dots,x_p) \in K^p,\ \varphi_i(x_1,\dots,x_p) = \sum_{j=1}^{p} a_{ij}x_j.$$

Il est clair que $\varphi_1,\dots,\varphi_n$ sont des formes linéaires sur K^p.
On a, pour tout $(x_1,\dots,x_p)$ de K^p :

$$(S) \iff (\forall i \in \{1,\dots,n\},\ \varphi_i(x) = b_i) \iff x \in \bigcap_{i=1}^{n} \varphi_i^{-1}(\{b_i\}).$$

Pour $i \in \{1,\dots,n\}$, si $(a_{i1},\dots,a_{ip}) \neq (0,\dots,0)$, $\varphi_i^{-1}(\{b_i\})$ est un hyperplan affine de K^p (voir le Tome de Géométrie).
Résoudre (S) revient donc à déterminer l'intersection d'une famille finie d'hyperplans affines.

9.9.2 Résolution

Gardons les notations de 9.9.1 p. 333, et notons $r = \mathrm{rg}(A)$.

1) Systèmes de Cramer

Le système (S) est dit **de Cramer** si et seulement si A est carrée et inversible, c'est-à-dire : $n = p = r$.

Nous supposons ici cette condition réalisée. On a alors : $AX = B \iff X = A^{-1}B$. Ainsi, (S) admet une solution et une seule, dont la détermination se déduit théoriquement du calcul de A^{-1} (puis de $A^{-1}B$).

Notons, pour $1 \leqslant j \leqslant n$, $C_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix}$ la $j^{\text{ème}}$ colonne de A. Puisque A est inversible, la famille $\mathcal{F} = (C_1,\dots,C_n)$ est une base de $\mathbf{M}_{n,1}(K)$. Il existe donc $(x_1,\dots,x_p) \in K^p$ unique tel que $B = \sum_{j=1}^{n} x_j C_j$, et (S) admet donc une solution et une seule, qui est $(x_1,\dots,x_p)$.
Soit $k \in \{1,\dots,n\}$. On a :

$$\begin{aligned}\det_{\mathcal{F}}(C_1,\dots,C_{k-1},B,C_{k+1},\dots,C_n) &= \det_{\mathcal{F}}\left(C_1,\dots,\sum_{j=1}^{n} x_j C_j,\dots,C_n\right) \\ &= \sum_{j=1}^{n} x_j \det_{\mathcal{F}}(C_1,\dots,C_j,\dots,C_n) = x_k \det_{\mathcal{F}}(\mathcal{F}) = x_k,\end{aligned}$$

puisque, pour tout j de $\{1,\dots,n\}$ tel que $j \neq k$, $\det_{\mathcal{F}}(C_1,\dots,C_j,\dots,C_n) = 0$ par répétition d'une colonne.

En notant $\mathcal{B}$ la base canonique de $\mathbf{M}_{n,1}(K)$, on a donc :

$$x_k = \det_{\mathcal{F}}(C_1,\ldots,C_{k-1},B,C_{k+1},\ldots C_n) = \det_{\mathcal{F}}(\mathcal{B})\,\det_{\mathcal{B}}(C_1,\ldots,B,\ldots,C_n)$$
$$= \left(\det_{\mathcal{B}}(C_1,\ldots,C_n)\right)^{-1}\det_{\mathcal{B}}(C_1,\ldots,B,\ldots,C_n).$$

On a prouvé :

♦ **Proposition** Si $A = (a_{ij})_{ij} \in \mathbf{GL}_n(K)$ et $(b_1,\ldots,b_n) \in K^n$, le système

$$(S)\quad \begin{cases} a_{11}x_1 & +\ldots+ & a_{1n}x_n = b_1 \\ \vdots & & \vdots \quad \vdots \\ a_{n1}x_1 & +\ldots+ & a_{nn}x_n = b_n \end{cases}$$

d'inconnue $(x_1,\ldots,x_n) \in K^n$ admet une solution et une seule, et, pour tout k de $\{1,\ldots,n\}$:

$$x_k = \frac{1}{\det(A)}\begin{vmatrix} a_{11} & \ldots & a_{1\,k-1} & b_1 & a_{1\,k+1} & \ldots & a_{1n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & \ldots & a_{n\,k-1} & b_n & a_{n\,k+1} & \ldots & a_{nn} \end{vmatrix}.$$

Les formules ci-dessus, donnant $x_k (1 \leqslant k \leqslant n)$ s'appellent les **formules de Cramer**.

Remarque :

Dès que $n \geqslant 3$, les formules de Cramer sont quasiment impraticables dans les exemples numériques. On préfèrera souvent une méthode de combinaisons des équations et d'élimination d'inconnues.

2) Cas $r = n < p$

En permutant les inconnues, d'après 9.8 Th. p. 330, on peut supposer que la matrice carrée d'ordre n, $A_1 = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}$, extraite de A, est inversible.

Pour tout $(x_{n+1},\ldots,x_p)$ de K^{p-n}, le système

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1 - (a_{1\,n+1}x_{n+1} + \ldots + a_{1p}x_p) \\ \qquad\qquad \vdots \\ a_{n1}x_1 + \ldots + a_{nn}x_n = b_n - (a_{n\,n+1}x_{n+1} + \ldots + a_{np}x_p) \end{cases},$$

d'inconnue $(x_1,\ldots,x_n) \in K^n$, est de Cramer, donc admet une solution et une seule $(x_1,\ldots,x_n)$ qu'on peut exprimer linéairement en fonction de $x_{n+1},\ldots,x_p$.

Nous verrons (Tome de Géométrie) que l'ensemble $\mathcal{S}$ des solutions (S) est un sous-espace affine de K^p de dimension $p - r$ $(= p - n)$.

EXEMPLE :

Résoudre dans $\mathbb{R}^4$: $(S)\begin{cases} x+y-z+t=2 & (1) \\ 2x-2y+z-3t=1 & (2). \\ -x+y+z-2t=-2 & (3) \end{cases}$

En effectuant $(2)-2\cdot(1)$ et $(3)+(1)$, on a :

$$(S) \iff \begin{cases} x+y-z+t=2 & (1') \\ -4y+3z-5t=-3 & (2'). \\ 2y-t=0 & (3') \end{cases}$$

$(3')$ fournit y en fonction de t, puis, en reportant dans $(2')$, on obtient z en fonction de t, et enfin, en reportant dans $(1')$, x en fonction de t :

$$(S) \iff \begin{cases} y=\dfrac{1}{2}t \\ z=\dfrac{1}{3}(7t-3)=\dfrac{7}{3}t-1. \\ x=\dfrac{5}{6}t+1 \end{cases}$$

Donc : $\mathcal{S}=\left\{\left(\frac{5}{6}t+1,\ \frac{1}{2}t,\ \frac{7}{3}t-1,\ t\right);\ t\in\mathbb{R}\right\}$.

Dans cet exemple, $\mathcal{S}$ est la droite affine de $\mathbb{R}^4$ passant par le point $(1,0,-1,0)$, et dirigée par le vecteur $(5, 3, 14, 6)$ par exemple.

3) Cas général : $r < n$

On procèdera le plus souvent par combinaison linéaire d'équations pour ramener le système à un système relevant du cas 2) ci-dessus, ou à un système n'ayant pas de solution.

EXEMPLE :

Discuter et résoudre, suivant $a\in\mathbb{R}$, le système d'équations, d'inconnue $(x,y,z)\in\mathbb{R}^3$:

$$(S)\begin{cases} 2x+y-3z=a \\ 3x+2y+z=a+3 \\ 7x+4y-5z=2a+5. \end{cases}$$

En tirant y dans la 1ère équation et en reportant dans les deux autres :

$$(S) \iff \begin{cases} y=-2x+3z+a \\ -x+7z=-a+3 \\ -x+7z=-2a+5. \end{cases}$$

Si $-a+3 \neq -2a+5$ (c'est-à-dire : $a \neq 2$), les deux dernières équations sont incompatibles.
Si $a = 2$, alors :

$$(S) \iff \begin{cases} y = -2x + 3z + 2 \\ x = 7z - 1 \end{cases} \iff \begin{cases} x = 7z - 1 \\ y = -11z + 4 \end{cases}.$$

Conclusion : $\mathcal{S} = \begin{cases} \{(7z-1, -11z+4, z);\ z \in \mathbb{R}\} & \text{si } a = 2 \\ \varnothing & \text{si } a \neq 2 \end{cases}$.

4) Cas des systèmes linéaires-homogènes

Le système affine (S) $\left\{ \begin{array}{l} a_{11}x_1 + \ldots + a_{1p}x_p = b_1 \\ \qquad\qquad\qquad\quad \vdots \\ a_{n1}x_1 + \ldots + a_{np}x_p = b_n \end{array} \right.$ est dit **linéaire-homogène** (ou : **linéaire**; ou : **homogène**) si et seulement si : $b_1 = \ldots = b_n = 0$.

Dans ce cas $(0,\ldots,0)$ est solution de (S), appelée solution triviale (ou : banale). Avec les notations de 9.9.1 2) p. 333, l'ensemble $f^{-1}(\{0\})$ étant le noyau de f, on déduit du théorème du rang le résultat suivant.

♦ **Proposition** L'ensemble des solutions du système linéaire-homogène

(S_0) $\left\{ \begin{array}{l} a_{11}x_1 + \ldots + a_{1p}x_p = 0 \\ \qquad\qquad\qquad\quad \vdots \\ a_{n1}x_1 + \ldots + a_{np}x_p = 0 \end{array} \right.$ est un sev de K^p, de dimension $p - r$,

où $r = \operatorname{rg} \begin{pmatrix} a_{11} & \ldots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{np} \end{pmatrix}$.

En particulier, (S_0) admet une solution autre que $(0,\ldots,0)$ si et seulement si :

$$r < p.$$

Exercices

◇ **9.9.1** Résoudre les systèmes d'équations suivants (inconnues $(x,y,z) \in \mathbb{C}^3$, paramètres $a,b,m \in \mathbb{C}$) :

a) $\begin{cases} 2x+3y-z=-1 \\ x+2y+3z=2 \\ 3x+4y-5z=-4 \end{cases}$ *b)* $\begin{cases} x+y+(2m-1)z=1 \\ mx+y+z=1 \\ x+my+z=3(m+1) \end{cases}$

c) $\begin{cases} 3mx+(3m-7)y+(m-5)z=m-1 \\ (2m-1)x+(4m-1)y+2mz=m+1 \\ 4mx+(5m-7)y+(2m-5)z=m-1 \end{cases}$

d) $\begin{cases} x-my+m^2z=m \\ mx-m^2y+mz=1 \\ mx+y-m^3z=1 \end{cases}$ *e)* $\begin{cases} 3x+y-z=1 \\ 5x+2y-2z=a \\ 4x+y-z=b \end{cases}$

f) $\begin{cases} ax+(b-1)y+2z=1 \\ ax+(2b-3)y+3z=1 \\ ax+(b-1)y+(b+2)z=2b-3 \end{cases}$ *g)* $\begin{cases} 2x+y-z=2 \\ x-y+z=4 \\ 3x+3y-z=4a \\ (2-a)x+2y-2z=-2b. \end{cases}$

◇ **9.9.2** CNS sur $m \in \mathbb{C}$ pour que les trois plans vectoriels de $\mathbb{C}^3$ d'équations :

$$x-2y+z=mx, \quad 3x-y-2z=my, \quad 3x-2y-z=mz$$

contiennent une même droite vectorielle.

◇ **9.9.3** Résoudre les systèmes d'équations suivants (inconnue $(x,y,z,t) \in \mathbb{C}^4$, paramètres $a,b,m \in \mathbb{C}$) :

a) $\begin{cases} 3x+4y+z+2t=3 \\ 6x+8y+2z+6t=7 \\ 9x+12y+3z+10t=0 \end{cases}$ *b)* $\begin{cases} 2x-y+z+t=1 \\ x+2y-z+4t=2 \\ x+7y-4z+11t=m \end{cases}$

c) $\begin{cases} mx+y+z+t=1 \\ x+my+z+t=m \\ x+y+mz+t=m+1 \end{cases}$ *d)* $\begin{cases} 2x+y+z+t=3 \\ x+2y+z+t=1 \\ x+y+2z+t=2 \\ x+y+z+2t=4 \\ 4x-3y+3z-4t=a \\ 2x+7y+7z+2t=b \end{cases}$

e) $\begin{cases} ax+y+z+t=1 \\ x+ay+z+t=b \\ x+y+az+t=b^2 \\ x+y+z+at=b^3. \end{cases}$

◇ **9.9.4** Résoudre (inconnue $(x_1,\ldots,x_n) \in \mathbb{C}^n$, paramètre $(a_1,\ldots,a_n) \in \mathbb{C}^n$) :

$$\begin{cases} x_1+x_2=2a_1 \\ x_2+x_3=2a_2 \\ \quad\vdots \\ x_{n-1}+x_n=2a_{n-1} \\ x_n+x_1=2a_n. \end{cases}$$

Chapitre 10

Espaces vectoriels euclidiens

(1ère étude)

Le corps utilisé est celui des réels; les ev considérés sont des $\mathbb{R}$-ev.

10.1 Produit scalaire

Cette étude figure de façon plus approfondie et dans un cadre plus général ($K = \mathbb{R}$ ou $\mathbb{C}$) dans le Tome 3, 1.6.

10.1.1 Généralités

◆ **Définition** Soit E un $\mathbb{R}$-ev; on appelle **produit scalaire** sur E toute application $\varphi : E^2 \longrightarrow \mathbb{R}$ telle que :

(i) $\forall (x,y) \in E^2,\ \varphi(y,x) = \varphi(x,y)$ (φ est **symétrique**)

(ii) $\forall \lambda \in \mathbb{R},\ \forall (x,y,y') \in E^3,\ \varphi(x,\lambda y + y') = \lambda\varphi(x,y) + \varphi(x,y')$
(φ est **linéaire par rapport à la 2ème place**)

(iii) $\forall x \in E,\ \varphi(x,x) \geqslant 0$

(iv) $\forall x \in E,\ (\varphi(x,x) = 0 \Longleftrightarrow x = 0)$.

Remarque :
Si φ est un produit scalaire sur le $\mathbb{R}$-ev E, alors :

$$\forall \lambda \in \mathbb{R},\ \forall (x,x',y) \in E^3,\ \varphi(\lambda x + x', y) = \lambda\varphi(x,y) + \varphi(x',y).$$

On dit que φ est **linéaire par rapport à la 1ère place**.
On peut donc remplacer (i) et (ii) par : «φ est une forme bilinéaire symétrique ».
Lorsque φ est un produit scalaire, on note souvent $(x|y)$ ou $< x,y >$ ou $x \cdot y$ à la place de $\varphi(x,y)$.

EXEMPLES :

1) Produit scalaire usuel sur $\mathbb{R}^n$, $n \in \mathbb{N}^*$

L'application $\varphi : (\mathbb{R}^n)^2 \longrightarrow \mathbb{R}$ définie par :

$$\varphi\big((x_1,\ldots,x_n),(y_1,\ldots,y_n)\big) = \sum_{k=1}^{n} x_k y_k$$

est un produit scalaire sur $\mathbb{R}^n$, appelé **produit scalaire usuel** (ou : **canonique**) **sur** $\mathbb{R}^n$.

2) Produit scalaire canonique sur $\mathbf{M}_{n,p}(\mathbb{R})$, $(n,p) \in (\mathbb{N}^*)^2$

Considérons l'application : $\varphi : \big(\mathbf{M}_{n,p}(\mathbb{R})\big)^2 \longrightarrow \mathbb{R}$.
$(A,B) \longmapsto \mathrm{tr}\,({}^tAB)$

(i) $\varphi(B,A) = \mathrm{tr}\,({}^tBA) = \mathrm{tr}\,\big({}^t({}^tAB)\big) = \mathrm{tr}\,({}^tAB) = \varphi(A,B)$

(ii) $\varphi(A,\lambda B + B') = \mathrm{tr}\,\big({}^tA(\lambda B + B')\big) = \mathrm{tr}\,(\lambda\,{}^tAB + {}^tAB') = \lambda\,\mathrm{tr}\,({}^tAB) + \mathrm{tr}\,({}^tAB')$
$= \lambda\varphi(A,B) + \varphi(A,B')$

(iii) En notant $A = (a_{ij})_{ij}$, on a :

$$\varphi(A,A) = \mathrm{tr}({}^tAA) = \sum_{i=1}^{n}\sum_{j=1}^{p} a_{ij}^2 = \sum_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant p}} a_{ij}^2 \geqslant 0$$

(iv) De même : $\varphi(A,A) = 0 \Longleftrightarrow \sum_{i,j} a_{ij}^2 = 0$

$$\Longleftrightarrow \big(\forall\,(i,j) \in \{1,\ldots,n\}\times\{1,\ldots,p\},\ a_{ij} = 0\big) \Longleftrightarrow A = 0.$$

Ainsi, φ est un produit scalaire sur $\mathbf{M}_{n,p}(\mathbb{R})$, appelé **produit scalaire canonique sur** $\mathbf{M}_{n,p}(\mathbb{R})$. En particulier pour $p = 1$ et en identifiant $\mathbf{M}_{n,1}(\mathbb{R})$ et $\mathbb{R}^n$, on retrouve le produit scalaire usuel sur $\mathbb{R}^n$ (exemple 1) ci-dessus).

3) Soient $(a,b) \in \mathbb{R}^2$ tel que $a < b$, et $E = C^0([a;b],\mathbb{R})$ le $\mathbb{R}$-ev des applications continues de $[a;b]$ dans $\mathbb{R}$.

Considérons l'application $\varphi : E^2 \longrightarrow \mathbb{R}$.
$(f,g) \longmapsto \int_a^b fg$

(i) $\varphi(g,f) = \displaystyle\int_a^b gf = \int_a^b fg = \varphi(f,g)$

(ii) $\varphi(f,\lambda g_1 + g_2) = \displaystyle\int_a^b f(\lambda g_1 + g_2) = \lambda\int_a^b fg_1 + \int_a^b fg_2 = \lambda\varphi(f,g_1) + \varphi(f,g_2)$

(iii) $\varphi(f,f) = \displaystyle\int_a^b f^2 \geqslant 0$

(iv) $\varphi(f,f) = 0 \Longleftrightarrow \displaystyle\int_a^b f^2 = 0 \Longleftrightarrow f = 0,$

car f est continue (cf. Tome 1, 6.2.5 Cor. 4).

Ainsi, φ est un produit scalaire sur E.

♦ **Proposition** Soient E un $\mathbb{R}$-ev, φ un produit scalaire sur E.

Notons $\phi : \begin{array}{ccc} E & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \varphi(x,x) \end{array}$. On a :

1) $\forall (n,p) \in (\mathbb{N}^*)^2$, $\forall (\lambda_1,\ldots,\lambda_n) \in \mathbb{R}^n$, $\forall (\mu_1,\ldots,\mu_p) \in \mathbb{R}^p$
$\forall (x_1,\ldots,x_n) \in E^n$, $\forall (y_1,\ldots,y_p) \in E^p$,

$$\varphi\Big(\sum_{i=1}^{n} \lambda_i x_i, \sum_{j=1}^{p} \mu_j y_j\Big) = \sum_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant p}} \lambda_i \mu_j \varphi(x_i,y_j)$$

2) $\forall (\lambda,\mu) \in \mathbb{R}^2$, $\forall (x,y) \in E^2$,

$$\phi(\lambda x + \mu y) = \lambda^2 \phi(x) + 2\lambda\mu\varphi(x,y) + \mu^2 \phi(y)$$

3) $\forall \lambda \in \mathbb{R}$, $\forall x \in E$, $\quad \phi(\lambda x) = \lambda^2 \phi(x)$

4) $\forall (x,y) \in E^2$, $\quad \phi(x+y) = \phi(x) + 2\varphi(x,y) + \phi(y)$

5) $\forall (x,y) \in E^2$, $\quad \phi(x+y) + \phi(x-y) = 2\big(\phi(x) + \phi(y)\big)$.

Preuve :

1) On voit, par récurrence sur n :

$$\forall Y \in E, \varphi\left(\sum_{i=1}^{n} \lambda_i x_i, Y\right) = \sum_{i=1}^{n} \lambda_i \varphi(x_i, Y),$$

d'où : $\varphi\Big(\sum_{i=1}^{n} \lambda_i x_i, \sum_{j=1}^{p} \mu_j y_j\Big) = \sum_{i=1}^{n} \lambda_i \varphi\Big(x_i, \sum_{j=1}^{p} \mu_j y_j\Big)$

$$= \sum_{i=1}^{n} \lambda_i \Big(\sum_{j=1}^{p} \mu_j \varphi(x_i,y_j)\Big) = \sum_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant p}} \lambda_i \mu_j \varphi(x_i,y_j).$$

2) Cas particulier de *1)* .

3) et *4)* Cas particuliers de *2)*.

5) $\begin{cases} \phi(x+y) = \phi(x) + 2\varphi(x,y) + \phi(y) \\ \phi(x-y) = \phi(x) - 2\varphi(x,y) + \phi(y) \end{cases}$, puis additionner.

10.1.2 Inégalités, normes euclidiennes

Soient E un $\mathbb{R}$-ev, φ un produit scalaire sur E, $\phi : \begin{array}{ccc} E & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \varphi(x,x) \end{array}$.

◆ **Théorème 1** **(Inégalité de Cauchy-Schwarz)**

$$\forall (x,y) \in E^2,\ \big(\varphi(x,y)\big)^2 \leqslant \phi(x)\phi(y).$$

Preuve :

On a : $\forall \lambda \in \mathbb{R},\ \phi(x+\lambda y) \geqslant 0$, d'où : $\forall \lambda \in \mathbb{R},\ \phi(y)\lambda^2 + 2\varphi(x,y)\lambda + \phi(x) \geqslant 0$.

• Si $\phi(y) \neq 0$, le trinôme $\lambda \longmapsto \phi(y)\lambda^2 + 2\varphi(x,y)\lambda + \phi(x)$ est $\geqslant 0$ sur $\mathbb{R}$, donc de discriminant $\leqslant 0$:

$$\big(\varphi(x,y)\big)^2 - \phi(x)\phi(y) \leqslant 0.$$

• Si $\phi(y) = 0$, alors $y = 0$, et l'inégalité voulue est évidente.

◆ **Proposition 1** **(Etude du cas d'égalité dans l'inégalité de Cauchy-Schwarz)**

$$\forall (x,y) \in E^2,\ \big((\varphi(x,y))^2 = \phi(x)\phi(y) \Longleftrightarrow (x,y) \text{ lié}\big).$$

Preuve :

1) Supposons (x,y) lié; par exemple, il existe $\alpha \in \mathbb{R}$ tel que $y = \alpha x$. On a alors :

$$\begin{cases} \big(\varphi(x,y)\big)^2 = \big(\varphi(x,\alpha x)\big)^2 = \alpha^2\big(\varphi(x,x)\big)^2 = \alpha^2\big(\phi(x)\big)^2 \\ \phi(x)\phi(y) = \phi(x)\alpha^2\phi(x) = \alpha^2\big(\phi(x)\big)^2, \end{cases}$$

d'où l'égalité voulue.

2) Réciproquement supposons : $(\varphi(x,y))^2 = \phi(x)\phi(y)$.

Si $y = 0$, alors (x,y) est lié.

Supposons $y \neq 0$ (donc $\phi(y) > 0$). En notant $\lambda_0 = -\dfrac{\varphi(x,y)}{\phi(y)}$, on a :

$$\begin{aligned} \phi(x+\lambda_0 y) &= \left(\frac{\varphi(x,y)}{\phi(y)}\right)^2 \phi(y) - 2\frac{\varphi(x,y)}{\phi(y)}\varphi(x,y) + \phi(x) \\ &= \frac{1}{\phi(y)}\big(-(\varphi(x,y))^2 + \phi(x)\phi(y)\big) = 0 \end{aligned}$$

d'où $x + \lambda_0 y = 0$, (x,y) est lié.

Le choix de λ_0 correspond à celui de l'unique zéro de la dérivée du trinôme $\lambda \longmapsto \phi(x+\lambda y)$, qui permet d'obtenir la valeur minimale de ce trinôme.

On peut aussi remarquer que, dans *1)*, α vaut $\dfrac{\varphi(x,y)}{\phi(x)}$ (si $x \neq 0$).

♦ **Théorème 2** (Inégalité de Minkowski)

$$\forall (x,y) \in E^2, \quad (\phi(x+y))^{\frac{1}{2}} \leqslant (\phi(x))^{\frac{1}{2}} + (\phi(y))^{\frac{1}{2}}.$$

Preuve :

$$(\phi(x+y))^{\frac{1}{2}} \leqslant (\phi(x))^{\frac{1}{2}} + (\phi(y))^{\frac{1}{2}} \iff \phi(x+y) \leqslant \phi(x) + 2(\phi(x)\phi(y))^{\frac{1}{2}} + \phi(y)$$
$$\iff \varphi(x,y) \leqslant (\phi(x)\phi(y))^{\frac{1}{2}},$$

et cette dernière inégalité est conséquence de l'inégalité de Cauchy-Schwarz.

♦ **Proposition 2** (Etude du cas d'égalité dans l'inégalité de Minkowski)
Pour tout (x,y) de E^2.

$$\left((\phi(x+y))^{\frac{1}{2}} = (\phi(x))^{\frac{1}{2}} + (\phi(y))^{\frac{1}{2}} \iff \begin{vmatrix} x = 0 \\ \text{ou} \\ (\exists \alpha \in \mathbb{R}_+,\ y = \alpha x) \end{vmatrix}\right.$$

On traduit cette dernière condition par : (x,y) est *positivement lié.*

Preuve :

1) L'étude du cas $x = 0$ est immédiate.

S'il existe $\alpha \in \mathbb{R}_+$ tel que $y = \alpha x$, alors (cf. 10.1.1 Prop. *3)* p. 341) :

$$\begin{cases} (\phi(x+y))^{\frac{1}{2}} = (\phi((1+\alpha)x))^{\frac{1}{2}} = (1+\alpha)(\phi(x))^{\frac{1}{2}} \\ (\phi(x))^{\frac{1}{2}} + (\phi(y))^{\frac{1}{2}} = (\phi(x))^{\frac{1}{2}} + \alpha(\phi(x))^{\frac{1}{2}}. \end{cases}$$

2) Réciproquement, supposons $(\phi(x+y))^{\frac{1}{2}} = (\phi(x))^{\frac{1}{2}} + (\phi(y))^{\frac{1}{2}}$.

En reprenant le schéma de calcul dans la preuve de l'inégalité de Minkowski, on obtient :

$$\varphi(x,y) = (\phi(x))^{\frac{1}{2}}(\phi(y))^{\frac{1}{2}}.$$

Il y a alors égalité dans l'inégalité de Cauchy-Schwarz, donc (cf. Prop. 1 p. 342), (x,y) est lié.

Le cas $x = 0$ étant d'étude immédiate, supposons $x \neq 0$. Il existe $\alpha \in \mathbb{R}$ tel que $y = \alpha x$.

On a alors $|1 + \alpha|\phi(x) = (1 + |\alpha|)\phi(x)$, d'où $(1+\alpha)^2 = (1+|\alpha|)^2$, $2\alpha = 2|\alpha|$, et finalement $\alpha \in \mathbb{R}_+$.

♦ **Proposition - Définition 3** Soient E un $\mathbb{R}$-ev, φ un produit scalaire sur E. L'application $||.|| : E \longrightarrow \mathbb{R}$, $x \longmapsto (\varphi(x,x))^{\frac{1}{2}}$ est une norme sur E, appelée **norme euclidienne associée à** φ. L'application $d : E \times E \longrightarrow \mathbb{R}$, $(x,y) \longmapsto ||x-y||$ est appelée **distance euclidienne associée à** φ.

Preuve :
Les conditions $||\lambda x|| = |\lambda|\,||x||$ et ($||x|| = 0 \Longleftrightarrow x = 0$) sont immédiates.
L'inégalité triangulaire $||x + y|| \leqslant ||x|| + ||y||$ est l'inégalité de Minkowski.

Remarque :
D'après 10.1.1 Prop. *4), 5)* p. 341, on a :

$$\forall (x,y) \in E^2, \quad \begin{cases} \varphi(x,y) = \dfrac{1}{2}(||x+y||^2 - ||x||^2 - ||y||^2) \\ ||x+y||^2 + ||x-y||^2 = 2(||x||^2 + ||y||^2). \end{cases}$$

La dernière égalité est appelée **égalité du parallélogramme** (ou : **égalité de la médiane**).

Exercices

◇ **10.1.1** Soient E un ev, $||\cdot||$ une norme euclidienne sur E, $a,b,c,d \in E$. Montrer :

$$||b-a||^2 + ||c-b||^2 + ||d-c||^2 + ||a-d||^2 = ||c-a||^2 + ||d-b||^2 + ||a-b+c-d||^2.$$

◇ **10.1.2** Soient $n \in \mathbb{N}^*$, $A \in \mathbf{M}_n(\mathbb{R})$ antisymétrique.
Montrer que $I_n + A$ est inversible.

◇ **10.1.3** Soient E un ev $< \cdot,\cdot >$ un produit scalaire sur E, $||.||$ la norme associée, $n \in \mathbb{N}^*$, $x_1,\ldots,x_n \in E$. Montrer :

$$\left|\left|\sum_{k=1}^{n} x_k\right|\right|^2 \leqslant n \sum_{k=1}^{n} ||x_k||^2.$$

◇ **10.1.4** Soient E un ev, $< \cdot,\cdot >$ un produit scalaire sur E, $||\cdot||$ la norme associée, $x,y,z \in E$.
Montrer : $||x-z||^2 \leqslant 2(||x-y||^2 + ||y-z||^2)$.

◇ **10.1.5** Résoudre l'équation $(1-x)^2 + (x-y)^2 + (y-z)^2 + z^2 = \dfrac{1}{4}$, d'inconnue $(x,y,z) \in \mathbb{R}^3$.

◇ **10.1.6** Soient $n \in \mathbb{N}^*$, $x_1,\ldots,x_n \in \mathbb{R}_+^*$ tels que $\displaystyle\sum_{i=1}^{n} x_i = 1$.

Montrer : $\displaystyle\sum_{i=1}^{n} \frac{1}{x_i} \geqslant n^2$, et étudier le cas d'égalité .

◇ **10.1.7*** Soient $n \in \mathbb{N} - \{0,1\}$, $(a_1,\ldots,a_n) \in (\mathbb{R}_+^*)^n$, $(b_1,\ldots,b_n) \in \mathbb{R}^n$. Montrer :

$$\sum_{i \neq j} a_i b_j = 0 \Longrightarrow \sum_{i \neq j} b_i b_j \leqslant 0.$$

10.1.3 Orthogonalité

Soient E un $\mathbb{R}$-ev, $< \cdot,\cdot >$ un produit scalaire sur E, $|| \cdot ||$ la norme euclidienne associée à $< \cdot,\cdot >$.

♦ **Définition**

1) Soit $(x,y) \in E^2$; on dit que x est **orthogonal à** y, et on note $x \perp y$, si et seulement si : $< x,y >= 0$.

2) Soient $x \in E$, $A \in \mathfrak{P}(E)$; on dit que x est **orthogonal à** A, et on note $x \perp A$, si et seulement si :

$$\forall a \in A,\ < x,a > = 0.$$

3) Pour toute partie A de E, on définit l'**orthogonal** de A, noté $A^\perp$:

$$A^\perp = \{x \in E;\ \forall a \in A,\ < x,a >= 0\}.$$

4) Une famille $(x_i)_{i \in I}$ d'éléments de E est dite **orthogonale** si et seulement si :

$$\forall (i,j) \in I^2,\ (i \neq j \Longrightarrow\ < x_i,x_j >= 0).$$

5) Une famille $(x_i)_{i \in I}$ d'éléments de E est dite **orthonormale** si et seulement si :

$$\begin{cases} (x_i)_{i \in I} \text{ est orthogonale} \\ \forall i \in I,\ ||x_i|| = 1 \end{cases}.$$

♦ **Proposition 1**

1) Pour toute partie A de E, $A^\perp$ est un sev de E.

2) $\forall (A,B) \in (\mathfrak{P}(E))^2,\ (A \subset B \Longrightarrow A^\perp \supset B^\perp)$.

3) $\forall A \in \mathfrak{P}(E),\ A^\perp = (\text{Vect}\,(A))^\perp$.

4) $\forall A \in \mathfrak{P}(E),\ A \subset A^{\perp\perp}$.

5) $E^\perp = \{0\},\ \{0\}^\perp = E$.

6) $\forall A \in \mathfrak{P}(E),\ A \cap A^\perp \subset \{0\}$.

7) Pour tous sev F,G de E :

$$(F+G)^\perp = F^\perp \cap G^\perp,\quad (F \cap G)^\perp \supset F^\perp + G^\perp.$$

Preuve :

1) • $(\forall a \in A,\ < 0,a >= 0)$, donc $0 \in A^\perp$.

• Si $\lambda \in \mathbb{R}$ et $(x,y) \in (A^\perp)^2$, alors :

$$\forall a \in A,\ < \lambda x + y,a >= \lambda < x,a > + < y,a >= 0,$$

donc $\lambda x + y \in A^\perp$.

2) Supposons $A \subset B$, et soit $y \in B^\perp$. On a : $\forall b \in B, < y,b >= 0$,
donc a fortiori : $\forall a \in A, < y,a >= 0$, d'où $y \in A^\perp$.

3) • $A \subset \text{Vect}(A)$, donc $A^\perp \supset (\text{Vect}(A))^\perp$, cf. *2)*.

• La propriété est évidente si $A = \varnothing$. Supposons $A \neq \varnothing$. Soit $x \in A^\perp$; pour tout y de Vect (A), il existe $n \in \mathbb{N}^*$, $\lambda_1,\ldots,\lambda_n \in \mathbb{R}$, $a_1,\ldots,a_n \in A$ tels que $y = \sum_{i=1}^{n} \lambda_i a_i$, d'où :

$$< x,y >=< x,\sum_{i=1}^{n} \lambda_i a_i >= \sum_{i=1}^{n} \lambda_i < x,a_i >= 0,$$

et donc $x \in (\text{Vect}(A))^\perp$. On a ainsi montré : $A^\perp \subset (\text{Vect}(A))^\perp$.

4) Soit $a \in A$. Comme : $\forall x \in A^\perp, < a,x >=< x,a >= 0$, on a : $a \in (A^\perp)^\perp$.

5) Evident.

6) Si $x \in A \cap A^\perp$, alors, en particulier, $< x,x >= 0$, d'où $x = 0$.

7) a) • $\left\{\begin{array}{l} F \subset F+G \\ G \subset F+G \end{array}\right. \Longrightarrow \left\{\begin{array}{l} F^\perp \supset (F+G)^\perp \\ G^\perp \supset (F+G)^\perp \end{array}\right. \Longrightarrow F^\perp \cap G^\perp \subset (F+G)^\perp$.

• Réciproquement, soit $x \in F^\perp \cap G^\perp$. On a :

$$\left\{\begin{array}{l} \forall f \in F, \ < x,f >= 0 \\ \forall g \in G, \ < x,g >= 0 \end{array}\right.$$

Pour tout h de $F+G$, il existe $(f,g) \in F \times G$ tel que $h = f+g$, et donc :

$$< x,h >=< x,f > + < x,g >= 0, \text{ d'où } x \in (F+G)^\perp.$$

b) $\left\{\begin{array}{l} F \cap G \subset F \\ F \cap G \subset G \end{array}\right. \Longrightarrow \left\{\begin{array}{l} (F \cap G)^\perp \supset F^\perp \\ (F \cap G)^\perp \supset G^\perp \end{array}\right. \Longrightarrow (F \cap G)^\perp \supset F^\perp + G^\perp$.

Remarque :
Nous verrons plus loin (10.2.1 Cor.3 p. 351) que, si E est de dimension finie, alors il y a égalité dans la 2ème formule *7)*.

◆ **Proposition 2** Soit $(x_i)_{i\in I}$ une famille d'éléments de E.
Si $\left\{\begin{array}{l} (x_i)_{i\in I} \text{ est orthogonale} \\ \forall i \in I, \ x_i \neq 0 \end{array}\right.$, alors $(x_i)_{i\in I}$ est libre.

Preuve :

Soient $N \in \mathbb{N}^*$, $\lambda_1,\ldots,\lambda_N \in \mathbb{R}$, $i_1,\ldots,i_N \in I$ deux à deux distincts, tels que $\sum_{k=1}^{N} \lambda_k x_{i_k} = 0$.

Pour tout j de $\{1,\ldots,N\}$, on a : $0 =< x_{i_j},\sum_{k=1}^{N} \lambda_k x_{i_k} >= \sum_{k=1}^{N} \lambda_k < x_{i_j},x_{i_k} > = \lambda_j ||x_{i_j}||^2$,

d'où $\lambda_j = 0$.

◆ **Proposition 3** **(Théorème de Pythagore)**

On a, pour tout (x,y) de E^2 :

$$x \perp y \iff ||x+y||^2 = ||x||^2 + ||y||^2 \iff ||x-y||^2 = ||x||^2 + ||y||^2.$$

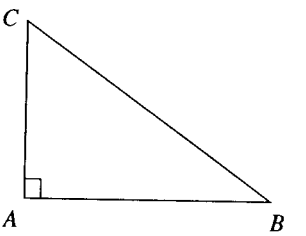
Preuve :

Immédiat en développant : $||x+y||^2 = ||x||^2 + 2 < x,y > + ||y||^2$.

Remarques :

1) Avec le vocabulaire de la géométrie affine, le théorème de Pythagore devient : pour qu'un triangle ABC soit rectangle en A, il faut et il suffit que

$$BC^2 = AB^2 + AC^2.$$



2) Pour toute famille finie orthogonale $(x_i)_{1 \leqslant i \leqslant n}$ de E, on a $\left|\left|\sum_{i=1}^{n} x_i\right|\right|^2 = \sum_{i=1}^{n} ||x_i||^2$

(cf. 10.1.1 Prop. *1)* p. 341).

Mais la réciproque est fausse (si $n \geqslant 3$); par exemple, dans $\mathbb{R}^2$ usuel, la famille (x_1,x_2,x_3), définie par $x_1 = (1,2)$, $x_2 = (0,2)$, $x_3 = (0,-1)$, vérifie

$$||x_1 + x_2 + x_3||^2 = ||x_1||^2 + ||x_2||^2 + ||x_3||^2$$

et n'est pas orthogonale.

10.2 Espaces vectoriels euclidiens

◆ **Définition** On appelle **espace vectoriel euclidien** tout ev réel E de dimension finie muni d'un produit scalaire.

Par exemple, $\mathbb{R}^n$ muni du produit scalaire usuel est un espace vectoriel euclidien.

10.2.1 Procédé d'orthogonalisation de Schmidt

Soient E un espace vectoriel euclidien, $< \cdot,\cdot >$ le produit scalaire, $n = \dim(E)$, $p \in \mathbb{N}$ tel que $p \leqslant n$, $(e_1,\ldots,e_p)$ une famille libre dans E.

Nous allons construire une famille orthogonale $(V_1,\ldots,V_p)$ de vecteurs de E tous $\neq 0$, telle que :

$$\forall k \in \{1,\ldots,p\},\ \text{Vect}\,(e_1,\ldots,e_k) = \text{Vect}\,(V_1,\ldots,V_k).$$

- Notons $V_1 = e_1 \neq 0$.
- Cherchons V_2 de la forme $V_2 = e_2 + \lambda_{2,1} V_1$, $\lambda_{2,1} \in \mathbb{R}$ à trouver.

On a : $V_2 \perp V_1 \iff < V_1, e_2 + \lambda_{2,1} V_1 >= 0 \iff < V_1, e_2 > + \lambda_{2,1} \|V_1\|^2 = 0$.

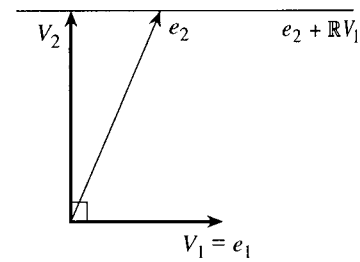
Puisque $V_1 \neq 0$, il existe $\lambda_{2,1}$ convenant.

Si $V_2 = 0$, alors $e_2 \in \mathbb{R}V_1 = \mathbb{R}e_1$, contradiction avec (e_1,e_2) libre.

Donc $V_2 \neq 0$.

Enfin, il est clair que :

$$\text{Vect}\,(e_1,e_2) = \text{Vect}\,(V_1,V_2).$$



- Supposons construits $V_1,\ldots,V_k$ (avec $k \leqslant p-1$) tels que :

$$\begin{cases} (V_1,\ldots,V_k) \text{ est orthogonale et à vecteurs tous } \neq 0 \\ \text{Vect}\,(e_1,\ldots,e_k) = \text{Vect}\,(V_1,\ldots,V_k). \end{cases}$$

Cherchons V_{k+1} de la forme. :

$$V_{k+1} = e_{k+1} + \sum_{i=1}^{k} \lambda_{k+1,i} V_i,$$

où $(\lambda_{k+1,1},\ldots,\lambda_{k+1,k}) \in \mathbb{R}^k$ est à trouver.

On a :

$$\begin{aligned} (\forall j \in \{1,\ldots,k\}, V_{k+1} \perp V_j) &\iff (\forall j \in \{1,\ldots,k\},\ < V_j, e_{k+1} + \sum_{i=1}^{k} \lambda_{k+1,i} V_i >= 0) \\ &\iff (\forall j \in \{1,\ldots,k\},\ < V_j, e_{k+1} > + \sum_{i=1}^{k} \lambda_{k+1,i} < V_j, V_i >= 0) \\ &\iff (\forall j \in \{1,\ldots,k\},\ < V_j, e_{k+1} > + \lambda_{k+1,j} \|V_j\|^2 = 0). \end{aligned}$$

Puisque $V_1,\ldots,V_k$ sont tous $\neq 0$, le système d'équations précédents admet une solution unique :

$$\forall\, j \in \{1,\ldots,k\},\quad \lambda_{k+1,j} = -\frac{< V_j, e_{k+1} >}{||V_j||^2}.$$

Considérons le vecteur V_{k+1} ainsi défini.

Par construction, $(V_1,\ldots,V_{k+1})$ est une famille orthogonale.

Si $V_{k+1} = 0$, alors :

$$e_{k+1} = -\sum_{i=1}^{k} \lambda_{k+1,i} V_i \in \text{Vect}\,(V_1,\ldots,V_k) = \text{Vect}\,(e_1,\ldots,e_k),$$

contradiction avec $(e_1,\ldots,e_{k+1})$ libre.

Donc : $V_{k+1} \neq 0$.

Comme $V_{k+1} \in \text{Vect}\,(e_{k+1}, V_1,\ldots,V_k)$ et que $\text{Vect}\,(V_1,\ldots,V_k) = \text{Vect}\,(e_1,\ldots,e_k)$, on a :

$$V_{k+1} \in \text{Vect}\,(e_1,\ldots,e_{k+1}),$$

et donc : $\text{Vect}\,(V_1,\ldots,V_{k+1}) \subset \text{Vect}\,(e_1,\ldots,e_{k+1})$.

De même, $e_{k+1} \in \text{Vect}\,(V_1,\ldots,V_k,V_{k+1})$ et $\text{Vect}\,(e_1,\ldots,e_k) = \text{Vect}\,(V_1,\ldots,V_k)$, d'où :

$$\text{Vect}\,(e_1,\ldots,e_{k+1}) \subset \text{Vect}\,(V_1,\ldots,V_{k+1}).$$

Finalement : $\text{Vect}\,(e_1,\ldots,e_{k+1}) = \text{Vect}\,(V_1,\ldots,V_{k+1})$.

Résumons l'étude :

♦ **Théorème (Orthogonalisation de Schmidt)**

Pour toute famille libre $(e_1,\ldots,e_p)$ d'un espace vectoriel euclidien E, il existe une famille $(V_1,\ldots,V_p)$ dans E telle que :

$$\begin{cases} (V_1,\ldots,V_p) \text{ est orthogonale} \\ \forall\, k \in \{1,\ldots,p\},\ \text{Vect}\,(V_1,\ldots,V_k) = \text{Vect}\,(e_1,\ldots,e_k). \end{cases}$$

Remarques :

1) Dans le théorème précédent, il y a unicité de $(V_1,\ldots,V_p)$ si on rajoute la condition :

$$\forall\, k \in \{1,\ldots,p\},\ < V_k, e_k >= 1.$$

2) Comme, dans la construction, V_k se décompose sur $e_k, V_1,\ldots,V_{k-1}$, la matrice de passage de $(e_1,\ldots,e_k)$ à $(V_1,\ldots,V_k)$ est triangulaire supérieure à termes diagonaux égaux à 1. ■

On abrège base orthonormée en b.o.n.

◆ **Corollaire 1** **(Théorème de la b.o.n. incomplète)**

Pour toute famille orthonormale $(e_1,\ldots,e_p)$ d'un espace vectoriel euclidien E, il existe $e_{p+1},\ldots,e_n \in E$ (où $n = \dim(E)$) tels que $(e_1,\ldots,e_n)$ soit une b.o.n. de E.

Preuve :

D'après le théorème de la base incomplète, forme faible (6.4 Th.2 p. 229), il existe $x_{p+1},\ldots,x_n \in E$ tels que $(e_1,\ldots,e_p,x_{p+1},\ldots,x_n)$ soit une base de E. L'application du procédé d'orthogonalisation de Schmidt conserve $e_1,\ldots,e_p$ et donne une famille orthogonale $(e_1,\ldots,e_p,V_{p+1},\ldots,V_n)$ à termes tous $\neq 0$. En notant $e_k = \dfrac{1}{||V_k||} V_k$ pour $k \in \{p+1,\ldots,n\}$, on obtient une famille orthonormale $(e_1,\ldots,e_n)$, et donc une b.o.n. de E.

◆ **Corollaire 2**

Tout espace vectoriel euclidien admet au moins une b.o.n.

Preuve :

Il suffit d'appliquer le Cor. 1 à la famille vide.

Remarque :

Si $\mathcal{B} = (e_1,\ldots,e_n)$ est une b.o.n. de E, alors :

$$\forall x \in E,\ x = \sum_{i=1}^{n} < e_i,x > e_i.$$

En effet, pour $x \in E$, il existe $(x_1,\ldots,x_n) \in \mathbb{R}^n$ tel que $x = \sum_{i=1}^{n} x_i e_i$, et, pour tout i de $\{1,\ldots,n\}$:

$$< e_i,x > = < e_i, \sum_{j=1}^{n} x_j e_j > = \sum_{j=1}^{n} x_j < e_i,e_j > = x_i.$$

◆ **Proposition 1** Soient E un espace vectoriel euclidien, $\mathcal{B}$ une b.o.n. de E,

$$x,y \in E,\quad X = \mathrm{Mat}_{\mathcal{B}}(x) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},\ Y = \mathrm{Mat}_{\mathcal{B}}(y) = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

On alors : $< x,y > = {}^tXY = \sum_{i=1}^{n} x_i y_i.$

Preuve :

En notant $\mathcal{B} = (e_1,\ldots,e_n)$, on a :

$$< x,y > = < \sum_{i=1}^{n} x_i e_i, \sum_{j=1}^{n} y_j e_j > = \sum_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant n}} x_i y_j < e_i,e_j > = \sum_{i=1}^{n} x_i y_i,$$

car $< e_i,e_j > = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$.

♦ **Proposition - Définition 2** Soit E un espace vectoriel euclidien.
Pour tout sev F de E, $F^{\perp}$ est un supplémentaire de F dans E, appelé **supplémentaire orthogonal de F dans E**.
En particulier : $\dim(F^{\perp}) = \dim(E) - \dim(F)$.

Preuve :
D'après le Cor. 2, F admet au moins une b.o.n. $(e_1,\ldots,e_p)$, puis , d'après le Cor. 1, il existe $e_{p+1},\ldots,e_n \in E$ tels que $(e_1,\ldots,e_n)$ soit un b.o.n. de E.

Montrons : $F^{\perp} = \text{Vect}\,(e_{p+1},\ldots,e_n)$.

Soient $x \in E$, $x = \sum_{i=1}^{n} x_i e_i$ sa décomposition sur la base $(e_1,\ldots,e_n)$ de E. On a :

$$\begin{aligned} x \in F^{\perp} &\iff (\forall\, j \in \{1,\ldots,p\}, \quad < e_j, x >= 0) \\ &\iff (\forall\, j \in \{1,\ldots,p\}, \quad \sum_{i=1}^{n} x_i < e_j, e_i >= 0) \\ &\iff (\forall\, j \in \{1,\ldots,p\}, \quad x_j = 0) \\ &\iff x \in \text{Vect}\,(e_{p+1},\ldots,e_n). \end{aligned}$$

Ainsi, $F = \text{Vect}\,(e_1,\ldots,e_p)$ et $F^{\perp} = \text{Vect}\,(e_{p+1},\ldots,e_n)$ sont supplémentaires dans E.

♦ **Corollaire 3** Soit E un espace vectoriel euclidien.
1) Pour tout sev F de E : $F^{\perp\perp} = F$
2) Pour tous sev F, G de E : $(F \cap G)^{\perp} = F^{\perp} + G^{\perp}$.

Preuve :
1) On a vu : $F \subset F^{\perp\perp}$ (cf. 10.1.3 Prop. 1 *4)* p. 345).
De plus : $\dim(F^{\perp\perp}) = \dim(E) - \big(\dim(E) - \dim(F)\big) = \dim(F)$.

2) On a vu : $(F \cap G)^{\perp} \subset F^{\perp} + G^{\perp}$ (cf. 10.1.3 Prop. 1 *7)* p. 345). De plus :

$$\begin{aligned} \dim\Big((F \cap G)^{\perp}\Big) &= \dim(E) - \dim(F \cap G) \\ &= \dim(E) - \big(\dim(F) + \dim(G) - \dim(F+G)\big) \\ &= \big(\dim(E) - \dim(F)\big) + \big(\dim(E) - \dim(G)\big) - \big(\dim(E) - \dim(F+G)\big) \\ &= \dim(F^{\perp}) + \dim(G^{\perp}) - \dim\Big((F+G)^{\perp}\Big) \\ &= \dim(F^{\perp}) + \dim(G^{\perp}) - \dim(F^{\perp} \cap G^{\perp}), \text{ cf. 10.1.3 Prop. 1. } \textit{7)} \text{ p. 345} \\ &= \dim(F^{\perp} + G^{\perp}). \end{aligned}$$

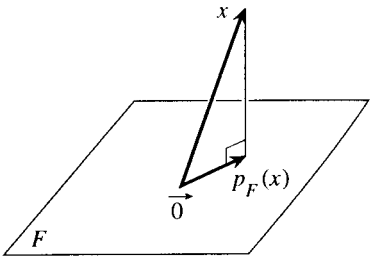
10.2.2 Projecteurs orthogonaux, symétries orthogonales

Soient E un espace vectoriel euclidien, $< \cdot,\cdot >$ le produit scalaire, $n = \dim(E)$.

◆ **Définition 1** Pour tout sev F de E, on appelle **projecteur orthogonal sur** F le projecteur sur F parallèlement à $F^\perp$.

En notant p_F le projecteur orthogonal sur F, on a donc (cf. 7.2.2 Prop.7 p. 249) :

$$\begin{cases} p_F \circ p_F = p_F, \quad \mathrm{Im}(p_F) = F, \quad \mathrm{Ker}(p_F) = F^\perp \\ \forall x \in E, \quad \big(p_F(x) \in F,\ x - p_F(x) \in F^\perp\big). \end{cases}$$



◆ **Proposition 1** Soit p un projecteur de E (c'est-à-dire : $p \in \mathcal{L}(E)$ et $p \circ p = p$).
Les propriétés suivantes sont équivalentes :

(i) p est un projecteur orthogonal

(ii) $\forall (x,y) \in E^2, < p(x), y > = < x, p(y) >$.

Preuve :

(i) $\Longrightarrow$ (ii) :

On suppose que p est un projecteur orthogonal, c'est-à-dire $p \circ p = p$ et $\mathrm{Ker}(p) = \big(\mathrm{Im}(p)\big)^\perp$.
Soit $(x,y) \in E^2$. On a :

$$< p(x), y > = < p(x),\ y - p(y) > \ + \ < p(x), p(y) > = < p(x), p(y) >,$$

puisque $p(x) \in \mathrm{Im}(p)$ et $y - p(y) \in \mathrm{Ker}(p)$.
De même : $< x, p(y) > = < x - p(x),\ p(y) > \ + \ < p(x), p(y) > = < p(x), p(y) >$,
d'où : $< x, p(y) > = < p(x), y >$.

(ii) $\Longrightarrow$ (i) :

On suppose : $\forall (x,y) \in E^2, < x, p(y) > = < p(x), y >$.
On a, pour tout (x,y) de $\mathrm{Ker}(p) \times \mathrm{Im}(p)$:

$$< x, y > = < x, p(y) > = < p(x), y > = < 0, y > = 0,$$

et donc p est un projecteur orthogonal.

◆ **Définition 2** Soient F un sev de E, $x \in E$. On appelle **distance de** x **à** F, et on note $d(x,F)$, le réel défini par : $d(x,F) = \inf\limits_{y \in F} ||x - y||$.

Il s'agit d'un cas particulier de la distance d'un point à une partie non vide dans un evn (cf. Tome 3, 1.1.8 Déf. 1).

♦ **Proposition 2** Soient F un sev de E, $x \in E$. On a :

$$\begin{cases} \forall y \in F,\ \|x-y\| \geqslant \|x-p_F(x)\| \\ \forall y \in F,\ \big(\|x-y\| = \|x-p_F(x)\| \Longleftrightarrow y = p_F(x)\big). \end{cases}$$

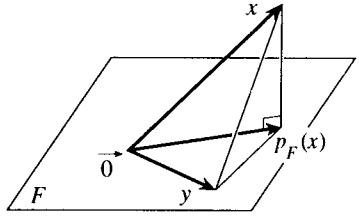
Autrement dit, l'application $F \underset{y \longmapsto \|x-y\|}{\longrightarrow} \mathbb{R}$ admet une borne inférieure et celle-ci est atteinte en $p_F(x)$ seulement.

Preuve :

Il suffit de remarquer que, pour tout y de F :

$$\begin{aligned} \|x-y\|^2 &= \big\|\big(x-p_F(x)\big)+\big(p_F(x)-y\big)\big\|^2 \\ &= \|x-p_F(x)\|^2 + \|p_F(x)-y\|^2, \end{aligned}$$

puisque $x - p_F(x) \in F^\perp$ et $p_F(x) - y \in F$.



♦ **Proposition 3** Soient F un sev de E, $(e_1,\ldots,e_p)$ une b.o.n. de F. On a alors :

$$\forall x \in E, \quad p_F(x) = \sum_{i=1}^{p} < e_i, x > e_i.$$

Preuve :

D'après 10.2.1 Rem. p. 350 appliquée à $p_F(x)$ comme élément de F, on a :

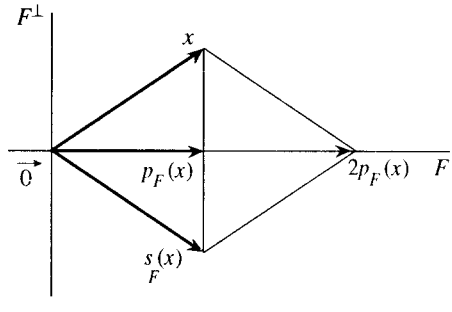
$$p_F(x) = \sum_{i=1}^{p} < e_i, p_F(x) > e_i = \sum_{i=1}^{p} < e_i, p_F(x) - x > e_i + \sum_{i=1}^{p} < e_i, x > e_i.$$

D'autre part : $\forall i \in \{1,\ldots,p\}$, $< e_i, p_F(x) - x >= 0$, puisque $p_F(x) - x \in F^\perp$.

♦ **Définition 3** Pour tout sev F de E, on appelle **symétrie orthogonale par rapport à** F l'endomorphisme s_F de E défini par : $s_F = 2p_F - e$, où p_F est le projecteur orthogonal sur F, et $e = \mathrm{Id}_E$.

Il est clair que :

$$\begin{cases} s_F \circ s_F = e \\ \mathrm{Ker}(s_F - e) = F,\ \mathrm{Ker}(s_F + e) = F^\perp \\ p_F = \dfrac{1}{2}(e + s_F). \end{cases}$$



Remarque : Soient F un sev de E, $(e_1,\dots,e_p)$ une b.o.n. de F, qu'on complète en une b.o.n. $\mathcal{B}=(e_1,\dots,e_n)$ de E (cf. 10.2.1 Cor.1 p. 350). Alors :

$$\mathrm{Mat}_{\mathcal{B}}(p_F)=\begin{pmatrix} 1 & & & & & \\ & \ddots & & & 0 & \\ & & 1 & & & \\ & & & 0 & & \\ & 0 & & & \ddots & \\ & & & & & 0 \end{pmatrix},\quad \mathrm{Mat}_{\mathcal{B}}(s_F)=\begin{pmatrix} 1 & & & & & \\ & \ddots & & & 0 & \\ & & 1 & & & \\ & & & -1 & & \\ & 0 & & & \ddots & \\ & & & & & -1 \end{pmatrix}.$$

(les p premières colonnes, puis les $n-p$ dernières)

10.2.3 Hyperplans

Rappelons que, dans un ev E de dimension finie n, on appelle hyperplans les sev de E de dimension $n-1$ (cf. 6.4 Déf. 2 p. 231).

Soient E un espace vectoriel euclidien, $<\cdot,\cdot>$ le produit scalaire, $n=\dim(E)\geqslant 1$.

◆ **Proposition 1** Pour tout u de E, l'application $\varphi_u:\begin{array}{ccc}E & \longrightarrow & \mathbb{R}\\ x & \longmapsto & <u,x>\end{array}$ est une forme linéaire sur E.

Preuve :

$\forall \alpha\in\mathbb{R},\ \forall x,y\in E,$

$$\varphi_u(\alpha x+y)=<u,\alpha x+y>=\alpha<u,x>+<u,y>=\alpha\varphi_u(x)+\varphi_u(y).$$

◆ **Proposition 2**

L'application $\delta:\begin{array}{ccc}E & \longrightarrow & E^*\\ u & \longmapsto & \varphi_u\end{array}$ est un isomorphisme d'ev.

Rappelons que $E^*=\mathcal{L}(E,\mathbb{R})$ est le dual de E (cf. 7.1.1 Déf. 3 p. 238).

Preuve :

1) δ est linéaire car : $\forall\alpha\in\mathbb{R},\ \forall u,v\in E,\ \forall x\in E,$

$$\begin{aligned}\big(\delta(\alpha u+v)\big)(x)&=\varphi_{\alpha u+v}(x)=<\alpha u+v,x>\\&=\alpha<u,x>+<v,x>=\alpha\varphi_u(x)+\varphi_v(x)\\&=(\alpha\varphi_u+\varphi_v)(x)=\big(\alpha\delta(u)+\delta(v)\big)(x).\end{aligned}$$

2) Soit $u\in\mathrm{Ker}(\delta)$. On a $\delta(u)=0$, donc : $\forall x\in E,\ <u,x>=0$.

En particulier : $||u||^2=<u,u>=0$, donc $u=0$.

Ainsi, $\mathrm{Ker}(\delta)=\{0\}$, d'où l'injectivité de δ.

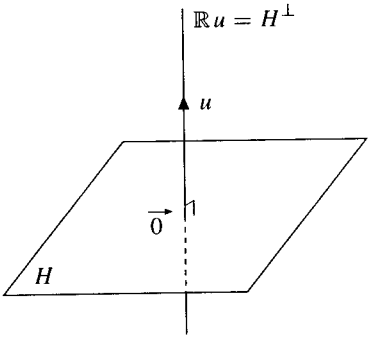
3) D'après 7.3.2 Prop. p. 258, $\dim(E^*)=\dim\big(\mathcal{L}(E,\mathbb{R})\big)=\dim(E)\cdot\dim(\mathbb{R})=\dim(E)$.

Il en résulte (cf. 7.3.1 Th. 1 p. 254) que δ est un isomorphisme d'ev. ∎

Soit H un hyperplan de E.
Comme $\dim(H^\perp) = \dim(E) - \dim(H)$
$= n - (n-1) = 1$,
$H^\perp$ est une droite vectorielle.
Il existe donc $u \in E$ tel que $H^\perp = \mathbb{R}u$.
Il est clair qu'alors :

$$H = H^{\perp\perp} = (\mathbb{R}u)^\perp = \{u\}^\perp.$$

La droite vectorielle $\mathbb{R}u$ est appelée
la normale à l'hyperplan H.



Avec les notations des deux Prop. précédentes :

$$H = \mathrm{Ker}(\varphi_u) = \mathrm{Ker}\big(\delta(u)\big).$$ ■

♦ **Définition** On appelle **reflexion** (de E) toute symétrie orthogonale par rapport à un hyperplan de E.

Exercice

◊ **10.2.1** Soient E un ev euclidien, $< \cdot,\cdot >$ le produit scalaire, $x, y \in E$. On suppose $\dim(E) \geqslant 2$.

a) Montrer que, si $||x|| = ||y||$, alors il existe un hyperplan H de E tel que $y = s_H(x)$.

b) Montrer que, si $< x, y >= ||y||^2$, alors il existe un hyperplan H de E tel que $y = p_H(x)$.

10.3 Groupe orthogonal

10.3.1 Endomorphismes orthogonaux

Soient $n \in \mathbb{N}^*$, E un espace vectoriel euclidien de dimension n, $< \cdot,\cdot >$ le produit scalaire.

◆ **Définition** Un endomorphisme f de E est dit **orthogonal** si et seulement si f conserve le produit scalaire, c'est-à-dire :

$$\forall (x,y) \in E^2, \quad < f(x), f(y) > = < x, y > .$$

On note $\mathcal{O}(E, < \cdot,\cdot >)$ (ou : $\mathcal{O}(E)$) l'ensemble des endomorphismes orthogonaux de E.

Remarque :

Comme inconséquence du vocabulaire, un projecteur orthogonal de E (autre que Id_E) n'est pas un endomorphisme orthogonal. En revanche, toute symétrie orthogonale de E est un endomorphisme orthogonal de E.

◆ **Proposition 1** Soit $f \in \mathcal{L}(E)$. Les deux propriétés suivantes sont équivalentes :

(i) $f \in \mathcal{O}(E)$

(ii) $\forall x \in E, \ ||f(x)|| = ||x||$.

Preuve :

(i) $\Longrightarrow$ (ii) :

Evident en remplaçant y par x dans la définition.

(ii) $\Longrightarrow$ (i) :

Supposons : $\forall x \in E, \ ||f(x)|| = ||x||$. On a, pour tout (x,y) de E^2 :

$$\begin{aligned} 2 < f(x), f(y) > &= ||f(x) + f(y)||^2 - ||f(x)||^2 - ||f(y)||^2 \\ &= ||f(x+y)||^2 - ||f(x)||^2 - ||f(y)||^2 \\ &= ||x+y||^2 - ||x||^2 - ||y||^2 = 2 < x, y > , \end{aligned}$$

et donc $f \in \mathcal{O}(E)$. ∎

Les éléments de $\mathcal{O}(E)$ sont aussi appelés **isométries vectorielles**.

◆ **Proposition 2** Soit $f \in \mathcal{L}(E)$. Les propriétés suivantes sont deux à deux équivalentes :

(i) $f \in \mathcal{O}(E)$

(ii) Pour toute b.o.n. $\mathcal{B}$ de E, $f(\mathcal{B})$ est une b.o.n. de E

(iii) Il existe une b.o.n. $\mathcal{B}$ de E telle que $f(\mathcal{B})$ soit une b.o.n. de E.

Preuve :

(i) $\Longrightarrow$ (ii) :

Supposons $f \in \mathcal{O}(E)$ et soit $\mathcal{B} = (e_1,\ldots,e_n)$ une b.o.n. de E. On a alors :

$$\forall (i,j) \in \{1,\ldots,n\}^2,\ < f(e_i)), f(e_j) >=< e_i, e_j >= \delta_{ij},$$

donc $f(\mathcal{B})$ est une b.o.n. de E.

(ii) $\Longrightarrow$ (iii) :

Résulte trivialement de l'existence d'une b.o.n. dans E (cf. 10.2.1 Cor. 2 p. 350).

(iii) $\Longrightarrow$ (i) :

Supposons qu'il existe une b.o.n. $\mathcal{B} = (e_1,\ldots,e_n)$ de E telle que $f(\mathcal{B}) = \big(f(e_1),\ldots,f(e_n)\big)$ soit une b.o.n. de E.

Soient $(x,y) \in E^2$, $(x_1,\ldots,x_n)$ (resp. $(y_1,\ldots,y_n)$) les composantes de x (resp. y) dans $\mathcal{B}$:

$$x = \sum_{i=1}^{n} x_i e_i,\ \ y = \sum_{j=1}^{n} y_j e_j.$$

Alors : $< f(x), f(y) > = < \sum_{i=1}^{n} x_i f(e_i), \sum_{j=1}^{n} y_j f(e_j) >$

$$= \sum_{1 \leqslant i,j \leqslant n} x_i y_j < f(e_i), f(e_j) > = \sum_{i=1}^{n} x_i y_i = < x, y >,$$

et donc : $f \in \mathcal{O}(E)$.

♦ **Proposition - Définition 3** L'ensemble $\mathcal{O}(E)$ des endomorphismes orthogonaux de E est un groupe pour la loi $\circ$, appelé **groupe orthogonal de** E.

Preuve :

Nous allons montrer que $\mathcal{O}(E)$ est un sous-groupe de $\mathcal{GL}(E)$ (cf. 7.2.3 Prop.-Déf. p. 250).

1) Soit $f \in \mathcal{O}(E)$.

Soit $x \in E$ tel que $f(x) = 0$; on a alors : $||x|| = ||f(x)|| = 0$, donc $x = 0$. Ainsi, $\mathrm{Ker}(f) = \{0\}$, donc f est injective. Puisque $f \in \mathcal{L}(E)$ est injective et que E est de dimension finie, f est un automorphisme de E (cf. 7.3.1 Th. 2 p. 256).

Ceci montre : $\mathcal{O}(E) \subset \mathcal{GL}(E)$.

2) $\mathrm{Id}_E \in \mathcal{O}(E)$ à l'évidence.

3) Si $f,g \in \mathcal{O}(E)$, alors :

$$\forall (x,y) \in E^2,\quad < (g \circ f)(x), (g \circ f)(y) >=< f(x), f(y) >=< x, y >,$$

donc : $g \circ f \in \mathcal{O}(E)$.

4) Soit $f \in \mathcal{O}(E)$. On a :

$$\forall (x,y) \in E^2,\ < f^{-1}(x),\ f^{-1}(y) >=< f\left(f^{-1}(x)\right),\ f\left(f^{-1}(y)\right) >=< x, y >,$$

et donc $f^{-1} \in \mathcal{O}(E)$.

10.3.2 Matrices orthogonales

Soit $n \in \mathbb{N}^*$.

◆ **Définition 1** Une matrice Ω de $\mathbf{M}_n(\mathbb{R})$ est dite **orthogonale** si et seulement si l'endomorphisme de $\mathbb{R}^n$ représenté par Ω dans la base canonique de $\mathbb{R}^n$ est un endomorphisme orthogonal de $\mathbb{R}^n$ muni du produit scalaire usuel.

On note $\mathbf{O}_n(\mathbb{R})$ l'ensemble des matrices orthogonales de $\mathbf{M}_n(\mathbb{R})$.

◆ **Proposition 1** Soient $\Omega \in \mathbf{M}_n(\mathbb{R})$, E un $\mathbb{R}$-ev de dimension n, $< \cdot,\cdot >$ un produit scalaire sur E. Les propriétés suivantes sont deux à deux équivalentes :

1) $\Omega \in \mathbf{O}_n(\mathbb{R})$

2) ${}^t\Omega\Omega = \mathrm{I}_n$

3) $\Omega\,{}^t\Omega = \mathrm{I}_n$

4) Pour toute b.o.n. $\mathcal{B}$ de E, l'endomorphisme de E représenté par Ω dans $\mathcal{B}$ est orthogonal

5) Il existe une b.o.n. de E dans laquelle l'endomorphisme représenté par Ω est orthogonal

6) Les colonnes de Ω forment une b.o.n. de $\mathbf{M}_{n,1}(\mathbb{R})$ pour le produit scalaire usuel

7) Les lignes de Ω forment une b.o.n. de $\mathbf{M}_{1,n}(\mathbb{R})$ pour le produit scalaire usuel.

Preuve :

Notons g l'endomorphisme de $\mathbb{R}^n$ représenté par Ω dans la base canonique $\mathcal{B}_0$ de $\mathbb{R}^n$.

1) $\iff$ *2)* :

1) $\iff \forall (x,y) \in (\mathbb{R}^n)^2,\ < g(x),g(y) >=< x,y >$

$\iff \forall (X,Y) \in (\mathbf{M}_{n,1}(\mathbb{R}))^2,\ {}^t(\Omega X)\Omega Y = {}^tXY$

$\iff \forall (X,Y) \in (\mathbf{M}_{n,1}(\mathbb{R}))^2,\ {}^tX({}^t\Omega\Omega)Y = {}^tXY.$

• En appliquant cette dernière égalité à $X = \mathrm{E}_i$ et $Y = \mathrm{E}_j$, où $(\mathrm{E}_1,\ldots,\mathrm{E}_n)$ est la base canonique de $\mathbf{M}_{n,1}(\mathbb{R})$, comme ${}^t\mathrm{E}_i({}^t\Omega\Omega)\mathrm{E}_j$ est le $(i,j)^{\text{ème}}$ terme de ${}^t\Omega\Omega$, on déduit ${}^t\Omega\Omega = \mathrm{I}_n$.

• Réciproque évidente.

2) $\iff$ *3)* : d'après 8.1.5 Th. p. 273.

2) $\iff$ *4)* :

Soient $\mathcal{B}$ une b.o.n. de E, f l'endomorphisme de E représenté par Ω dans $\mathcal{B}$. On a :

$$\begin{aligned} &\forall (x,y) \in E^2,\ < f(x),f(y) >=< x,y > \\ \iff &\forall (X,Y) \in (\mathbf{M}_{n,1}(\mathbb{R}))^2,\ {}^t(\Omega X)\Omega Y = {}^tXY \\ \iff &{}^t\Omega\Omega = \mathrm{I}_n, \end{aligned}$$

comme ci-dessus pour l'équivalence *1)* $\iff$ *2)*.

2) $\Longleftrightarrow$ *5)* :

Comme *2)* $\Longleftrightarrow$ *4)*, l'existence d'une b.o.n. étant assurée par 10.2.1 Cor.2 p. 350.

1) $\Longleftrightarrow$ *6)* :

En effet, les colonnes de Ω représentent les composantes des images par g des vecteurs de $\mathcal{B}_0$.

1) $\Longleftrightarrow$ *7)* :

Résulte de *2)* $\Longleftrightarrow$ *3)*, et *1)* $\Longleftrightarrow$ *6)* appliqué à ${}^t\Omega$. ■

♦ **Proposition 2** $\mathbf{O}_n(\mathbb{R})$ est un groupe pour la multiplication, appelé **groupe orthogonal (d'ordre n)**.

Preuve :

Nous allons montrer que $\mathbf{O}_n(\mathbb{R})$ est un sous-groupe de $\mathbf{GL}_n(\mathbb{R})$.

• $\mathbf{O}_n(\mathbb{R}) \subset \mathbf{GL}_n(\mathbb{R})$ car toute matrice orthogonale Ω est inversible (elle a pour inverse ${}^t\Omega$).

• $\mathrm{I}_n \in \mathbf{O}_n(\mathbb{R})$.

• Pour toutes Ω_1, Ω_2 de $\mathbf{O}_n(\mathbb{R})$:

$$ {}^t(\Omega_1\Omega_2)\Omega_1\Omega_2 = {}^t\Omega_2({}^t\Omega_1\Omega_1)\Omega_2 = {}^t\Omega_2\Omega_2 = \mathrm{I}_n, $$

donc $\Omega_1\Omega_2 \in \mathbf{O}_n(\mathbb{R})$.

Pour toute Ω de $\mathbf{O}_n(\mathbb{R})$, $\Omega^{-1} = {}^t\Omega \in \mathbf{O}_n(\mathbb{R})$ car $\Omega\,{}^t\Omega = \mathrm{I}_n$.

Remarque :

Soient $\mathcal{B}$ une b.o.n. de E, $f \in \mathcal{L}(E)$, $\Omega = \mathrm{Mat}_{\mathcal{B}}(f)$.

Alors : $f \in \mathcal{O}(E) \Longleftrightarrow \Omega \in \mathbf{O}_n(\mathbb{R})$.

L'application $\begin{array}{ccc} \mathcal{O}(E) & \longrightarrow & \mathbf{O}_n(\mathbb{R}) \\ f & \longmapsto & \mathrm{Mat}_{\mathcal{B}}(f) \end{array}$ est un isomorphisme de groupes.

♦ **Proposition 3** Soient $\mathcal{B}$ une b.o.n. de E, $\mathcal{B}'$ une base de E, P la matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$. Alors : $\mathcal{B}'$ est une b.o.n. si et seulement si P est orthogonale.

Preuve :

Soit $f \in \mathcal{L}(E)$ défini par $\mathrm{Mat}_{\mathcal{B}}(f) = P$. D'après Prop. 1 p. 358, $\mathcal{B}'$ est une b.o.n. si et seulement si $f \in \mathcal{O}(E)$. Et d'après la Prop. précédente : $f \in \mathcal{O}(E) \Longleftrightarrow P \in \mathbf{O}_n(\mathbb{R})$. ■

♦ **Proposition 4**

1) $\forall \Omega \in \mathbf{O}_n(\mathbb{R}),\ \det(\Omega) \in \{-1, 1\}$

2) $\forall f \in \mathcal{O}(E),\ \det(f) \in \{-1, 1\}$.

Preuve :

1) $\Omega \in \mathbf{O}_n(\mathbb{R}) \Longleftrightarrow {}^t\Omega\Omega = \mathrm{I}_n \Longrightarrow \big(\det(\Omega)\big)^2 = \det\big({}^t\Omega\Omega\big) = 1$.

2) Se déduit de *1)*.

◆ **Définition 2** Soit $f \in \mathcal{O}(E)$; on dit que f est un endomorphisme orthogonal **direct** (resp. **indirect**) si et seulement si $\det(f) = 1$ (resp. -1).

On dit aussi : **droit** au lieu de direct
gauche au lieu d'indirect.

Remarque :

Pour $f \in \mathcal{GL}(E)$, f est un endomorphisme orthogonal direct si et seulement si f est un endomorphisme orthogonal et un endomorphisme direct (cf. 9.7 Déf. 3 p. 328).

◆ **Proposition - Définition 5** L'ensemble des endomorphismes orthogonaux directs de E est un sous-groupe de $\mathcal{O}(E)$, appelé **groupe spécial orthogonal de** E, noté $\mathcal{SO}(E)$.

Preuve :

- $\mathcal{SO}(E) \subset \mathcal{O}(E)$
- $\det(\mathrm{Id}_E) = 1$
- $\forall f,g \in \mathcal{SO}(E)$, $\det(g \circ f) = \det(g)\det(f) = 1 \cdot 1 = 1$
- $\forall f \in \mathcal{SO}(E)$, $\det(f^{-1}) = (\det(f))^{-1} = 1^{-1} = 1$. ∎

On en déduit la Prop. suivante.

◆ **Proposition - Définition 6** Soit $\Omega \in \mathbf{O}_n(\mathbb{R})$.

On dit que Ω est orthogonale **droite** (resp. **gauche**) si et seulement si $\det(\Omega) = 1$ (resp. -1). L'ensemble des matrices orthogonales droites d'ordre n est un sous-groupe de $\mathbf{O}_n(\mathbb{R})$, appelé **groupe spécial orthogonal**, noté $\mathbf{SO}_n(\mathbb{R})$.

Remarque :

Soient $\mathcal{B}$ une b.o.n. de E, $f \in \mathcal{L}(E)$, $\Omega = \mathrm{Mat}_{\mathcal{B}}(f)$.

Alors : $f \in \mathcal{SO}(E) \iff \Omega \in \mathbf{SO}_n(\mathbb{R})$.

L'application $\mathcal{SO}(E) \longrightarrow \mathbf{SO}_n(\mathbb{R})$ est un isomorphisme de groupes.
$f \longmapsto \mathrm{Mat}_{\mathcal{B}}(f)$

◆ **Définition 3** Un espace vectoriel euclidien E est dit **orienté** si et seulement si l'ev E est orienté.

Autrement dit, un espace vectoriel euclidien orienté est un espace vectoriel euclidien dans lequel on a fait choix d'une base (orthogonale ou non) qualifiée de directe.

On abrège base orthonormale directe en b.o.n.d.

◆ **Proposition - Définition 7** Soit E un espace vectoriel euclidien orienté, $(V_1,\ldots,V_n) \in E^n$. Le déterminant $\det_{\mathcal{B}}(V_1,\ldots,V_n)$ ne dépend pas du choix de la b.o.n.d. $\mathcal{B}$, est appelé **produit mixte** de $(V_1,\ldots,V_n)$ et noté $[V_1,\ldots,V_n]$.

Ainsi, pour toute b.o.n.d. $\mathcal{B}$ de E : $[V_1,\ldots,V_n] = \det_{\mathcal{B}}(V_1,\ldots,V_n)$.

Exercices

◊ **10.3.1** Soient $A \in \mathbf{M}_n(\mathbb{R})$, $C_1, \ldots, C_n$ les colonnes de A.

Montrer : $A \in \mathbf{O}_n(\mathbb{R}) \iff \sum_{j=1}^{n} C_j \, {}^tC_j = \mathrm{I}_n$.

◊ **10.3.2** **Matrices de Householder**

Soient $V \in \mathbf{M}_{n,1}(\mathbb{R}) - \{0\}$, $S = \mathrm{I}_n - \dfrac{2}{{}^tVV} V \, {}^tV$ (appelée *matrice de Householder*). Vérifier que S est la matrice (dans la base canonique) de la réflexion par rapport à l'hyperplan orthogonal à V.

◊ **10.3.3** Montrer : $\forall A = (a_{ij})_{ij} \in \mathbf{O}_n(\mathbb{R}), \left| \sum_{1 \leqslant i,j \leqslant n} a_{ij} \right| \leqslant n$, et étudier le cas d'égalité.

◊ **10.3.4*** Soient E un ev euclidien de dimension n, $\mathcal{B}$ une b.o.n. de E, $V_1, \ldots, V_n \in E$.

a) Démontrer : $|\det_{\mathcal{B}}(V_1, \ldots, V_n)| \leqslant \prod_{i=1}^{n} \|V_i\|$.

b) Etudier le cas d'égalité.

◊ **10.3.5** **Endomorphisme orthogonal induit**

Soient E un ev euclidien, F un sev de E, $f \in \mathcal{O}(E)$. On suppose $f(F) \subset F$. Montrer :

$$\begin{cases} f(F) = F \\ f(F^\perp) = F^\perp \end{cases} \quad \text{et} \quad \begin{cases} f|_F \in \mathcal{O}(F) \\ f|_{F^\perp} \in \mathcal{O}(F^\perp) \end{cases}.$$

◊ **10.3.6** **Recollement d'endomorphismes orthogonaux**

Soient E un ev euclidien, F un sev de E, $u \in \mathcal{O}(F)$, $v \in \mathcal{O}(F^\perp)$, f l'application de E dans E définie par :

$$\forall x \in E, \quad f(x) = u\left(p_F(x)\right) + v\left(p_{F^\perp}(x)\right).$$

Montrer : $f \in \mathcal{O}(E)$.

◊ **10.3.7** **Décomposition d'un endomorphisme orthogonal en un produit de réflexions**

Soient E un ev euclidien, $n = \dim(E)$, $f \in \mathcal{O}(E)$. Montrer qu'il existe $s_1, \ldots, s_n \in \mathcal{L}(E)$ tels que $f = s_1 \circ \ldots \circ s_n$ et que chaque s_i $(1 \leqslant i \leqslant n)$ soit une réflexion ou l'identité. (Utiliser les exercices 10.2.1 p. 355 et 10.3.5, 10.3.6).

10.4 Géométrie vectorielle euclidienne plane

On note E_2 un espace vectoriel euclidien de dimension 2, $\cdot$ le produit scalaire sur E_2. Nous allons expliciter les éléments de $\mathbf{O}_2(\mathbb{R})$ et donc ceux de $\mathcal{O}(E_2)$.

Soit $\Omega = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{M}_2(\mathbb{R})$. On a (cf. 10.3.2 Prop. 1 p. 358) :

$$\Omega \in \mathbf{O}_2(\mathbb{R}) \iff \begin{cases} a^2+c^2=1 \\ ab+cd=0 \\ b^2+d^2=1 \end{cases} \iff \left(\begin{cases} c=0 \\ a^2=1 \\ b=0 \\ d^2=1 \end{cases} \text{ ou } \begin{cases} c\neq 0 \\ d=-\dfrac{ab}{c} \\ a^2+c^2=1 \\ b^2=c^2 \end{cases} \right)$$

$$\iff \left(\begin{cases} c=0 \\ a^2=1 \\ b=0 \\ d^2=1 \end{cases} \text{ ou } \begin{cases} c\neq 0 \\ b=c \\ d=-a \\ a^2+c^2=1 \end{cases} \text{ ou } \begin{cases} c\neq 0 \\ b=-c \\ d=a \\ a^2+c^2=1 \end{cases} \right).$$

Ainsi :

$$\mathbf{O}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & -c \\ c & a \end{pmatrix};\ (a,c) \in \mathbb{R}^2,\ a^2+c^2=1 \right\} \cup \left\{ \begin{pmatrix} a & c \\ c & -a \end{pmatrix};\ (a,c) \in \mathbb{R}^2,\ a^2+c^2=1 \right\}$$
$$= \left\{ \begin{pmatrix} a & -\varepsilon c \\ c & \varepsilon a \end{pmatrix};\ (a,c,\varepsilon) \in \mathbb{R}\times\mathbb{R}\times\{-1,1\},\ a^2+c^2=1 \right\}.$$

Résumons l'étude :

◆ **Proposition 1**

- $\mathbf{O}_2(R) = \{R_\theta;\ \theta \in \mathbb{R}\} \cup \{S_\varphi;\ \varphi \in \mathbb{R}\}$, où

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},\ S_\varphi = \begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix}.$$

- $\mathbf{SO}_2(\mathbb{R}) = \{R_\theta;\ \theta \in \mathbb{R}\}$.

Nous supposons dorénavant que E_2 est orienté.

Etude des rotations

◆ **Définition 1** Soient $\mathcal{B}$ une b.o.n.d. de E_2 et $\theta \in \mathbb{R}$.

L'endomorphisme de E_2 dont la matrice dans $\mathcal{B}$ est $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ est appelé la **rotation d'angle** θ, et noté Rot_θ.

La notion de rotation permet de donner une définition rigoureuse de la notion d'angle de deux vecteurs $\neq 0$ de E_2, qui correspond bien sûr à la notion intuitive déjà connue. Nous allons développer ce point de vue en utilisant les propriétés élémentaires des fonctions cos et sin (cf. Tome 2, 7.8).

Soient $u, v \in E_2 - \{0\}$, $U = \dfrac{1}{\|u\|}u$, $V = \dfrac{1}{\|v\|}v$.

Montrons qu'il existe $\theta \in \mathbb{R}$, unique modulo 2π, tel que $\text{Rot}_\theta(U) = V$.

Notons (u_1,u_2) (resp. (v_1,v_2)) les composantes de U (resp. V) dans une b.o.n.d. $\mathcal{B}$ de E_2. Puisque $u_1^2 + u_2^2 = 1$ et $v_1^2 + v_2^2 = 1$, il existe $(\alpha,\beta) \in \mathbb{R}^2$ tel que :

$$\begin{cases} u_1 = \cos\alpha \\ u_2 = \sin\alpha \end{cases} \text{ et } \begin{cases} v_1 = \cos\beta \\ v_2 = \sin\beta \end{cases}.$$

On a, pour tout θ de $\mathbb{R}$: $\text{Rot}_\theta(U) = V \iff \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix} = \begin{pmatrix} \cos\beta \\ \sin\beta \end{pmatrix}$

$$\iff \begin{cases} \cos\theta\cos\alpha - \sin\theta\sin\alpha = \cos\beta \\ \sin\theta\cos\alpha + \cos\theta\sin\alpha = \sin\beta \end{cases}$$

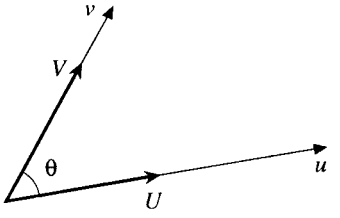
$$\iff \begin{cases} \cos(\theta+\alpha) = \cos\beta \\ \sin(\theta+\alpha) = \sin\beta \end{cases} \iff \theta \equiv \beta - \alpha\ [2\pi].$$

On déduit la Proposition suivante.

♦ **Proposition - Définition 2** Soient $u,v \in E_2 - \{0\}$, $U = \dfrac{1}{||u||}u$, $V = \dfrac{1}{||v||}v$.

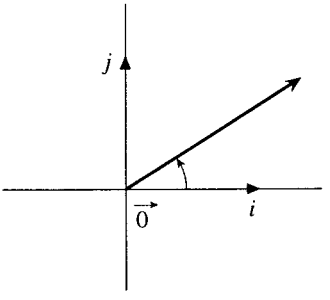
Il existe $\theta \in \mathbb{R}$, unique modulo 2π, tel que $\text{Rot}_\theta(U) = V$; ce réel θ (ou sa classe modulo 2π) est appelé l'**angle** de u et v, et noté $\widehat{(u,v)}$.

On a ainsi : $V = \text{Rot}_{\widehat{(u,v)}}(U)$

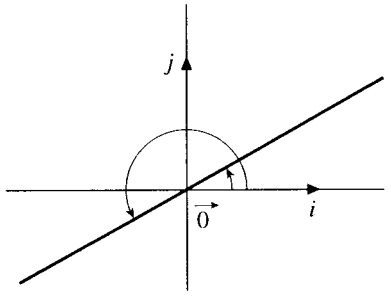


♦ **Définition 2** Soit $\mathcal{B} = (i,j)$ une b.o.n.d. de E_2.

- Pour $u \in E_2 - \{0\}$, on appelle **angle polaire** de u (dans $\mathcal{B}$), l'angle $\widehat{(i,u)}$, défini modulo 2π.
- On appelle **angle polaire** d'une droite vectorielle l'angle polaire d'un vecteur directeur de cette droite vectorielle, défini modulo π.



Angle polaire d'un vecteur



Angle polaire d'une droite

■

◆ **Proposition 3**

$$\forall (u,v) \in (E_2 - \{0\})^2, \quad u \cdot v = ||u||\,||v|| \cos \widehat{(u,v)}.$$

Preuve :
Avec les notations de l'étude précédente :

$$\begin{aligned} u \cdot v &= ||u||\,||v|| U \cdot V = ||u||\,||v|| (\cos\alpha \cos\beta + \sin\alpha \sin\beta) \\ &= ||u||\,||v|| \cos(\beta - \alpha) = ||u||\,||v|| \cos \widehat{(u,v)}. \end{aligned}$$

Rappelons (cf. 10.2.1 Rem. p. 000) que, si $\mathcal{B} = (i,j)$ est une b.o.n. de E_2, alors :

$$\forall u \in E_2, \quad u = (i \cdot u) i + (j \cdot u) j.$$

◆ **Proposition 4**

$$\forall (\theta,\theta') \in \mathbb{R}^2, \ \mathrm{Rot}_\theta \circ \mathrm{Rot}_{\theta'} = \mathrm{Rot}_{\theta+\theta'}.$$

Preuve :
$$\begin{aligned} R_\theta R_{\theta'} &= \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \cos\theta' & -\sin\theta' \\ \sin\theta' & \cos\theta' \end{pmatrix} \\ &= \begin{pmatrix} \cos\theta\cos\theta' - \sin\theta\sin\theta' & -\cos\theta\cos\theta' - \sin\theta\cos\theta' \\ \sin\theta\cos\theta' + \cos\theta\sin\theta' & -\sin\theta\sin\theta' + \cos\theta\cos\theta' \end{pmatrix} \\ &= \begin{pmatrix} \cos(\theta+\theta') & -\sin(\theta+\theta') \\ \sin(\theta+\theta') & \cos(\theta+\theta') \end{pmatrix} = R_{\theta+\theta'}. \end{aligned}$$

◆ **Corollaire** **(Relation de Chasles pour les angles)**

$$\forall u,v,w \in E_2 - \{0\}, \ \widehat{(u,w)} \equiv \widehat{(u,v)} + \widehat{(v,w)} \quad [2\pi].$$

Preuve :
Notons : $U = \dfrac{1}{||u||} u$, $V = \dfrac{1}{||v||} v$, $W = \dfrac{1}{||w||} w$.
On a : $W = \mathrm{Rot}_{\widehat{(v,w)}}(V)$ et $V = \mathrm{Rot}_{\widehat{(u,v)}}(U)$, d'où :

$$W = \mathrm{Rot}_{\widehat{(v,w)}} \circ \mathrm{Rot}_{\widehat{(u,v)}}(U) = \mathrm{Rot}_{\widehat{(v,w)}+\widehat{(u,v)}}(U).$$

D'autre part : $W = \mathrm{Rot}_{\widehat{(u,w)}}(U)$.
D'où : $\widehat{(u,v)} + \widehat{(v,w)} \equiv \widehat{(u,w)}$ $[2\pi]$.

Remarque : Comme $\widehat{(u,u)} \equiv 0$ $[2\pi]$, on déduit :

$$\forall u,v \in E_2 - \{0\}, \quad \widehat{(v,u)} \equiv -\widehat{(u,v)} \quad [2\pi].$$

Etude des réflexions

Soient $\varphi \in \mathbb{R}$, $S_\varphi = \begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix}$ (cf. Prop. 1 p. 362), $\mathcal{B} = (i, j)$ une b.o.n.d. de E_2, s_φ l'endomorphisme de E_2 de matrice S_φ dans la base $\mathcal{B}$.

Il est clair que $s_\varphi \circ s_\varphi = \mathrm{Id}_{E_2}$, puisque $S_\varphi^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathrm{I}_2$.

1) Déterminons les invariants de s_φ.

Pour tout $X = \begin{pmatrix} x \\ y \end{pmatrix}$ de $\mathbf{M}_{2,1}(\mathbb{R})$, on a :

$$S_\varphi X = X \iff \begin{cases} (1-\cos\varphi)x - \sin\varphi\, y = 0 \\ -\sin\varphi\, x + (1+\cos\varphi)y = 0 \end{cases} \iff \begin{cases} 2\sin\dfrac{\varphi}{2}\left(\sin\dfrac{\varphi}{2}\, x - \cos\dfrac{\varphi}{2}\, y\right) = 0 \\ 2\cos\dfrac{\varphi}{2}\left(-\sin\dfrac{\varphi}{2}\, x + \cos\dfrac{\varphi}{2}\, y\right) = 0 \end{cases}$$

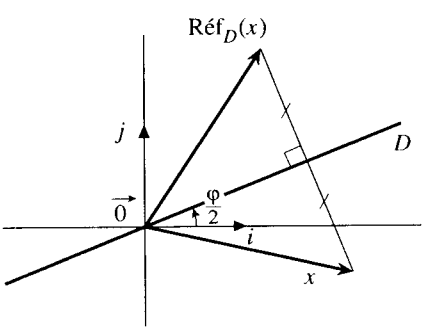
$$\iff x\sin\frac{\varphi}{2} - y\cos\frac{\varphi}{2} = 0.$$

Ainsi, l'ensemble des invariants de s_φ est la droite vectorielle $D_{\frac{\varphi}{2}}$ d'angle polaire $\dfrac{\varphi}{2}$, c'est-à-dire engendrée par $\cos\dfrac{\varphi}{2}\, i + \sin\dfrac{\varphi}{2}\, j$.

2) Un calcul analogue montre que l'ensemble des anti-invariants de s_φ (c'est-à-dire l'ensemble des u de E_2 tels que $s_\varphi(u) = -u$) est la droite vectorielle $D_{\frac{\varphi}{2}+\frac{\pi}{2}}$ d'angle polaire $\dfrac{\varphi}{2} + \dfrac{\pi}{2}$, c'est-à-dire engendrée par $-\sin\dfrac{\varphi}{2}\, i + \cos\dfrac{\varphi}{2}\, j$.

Résumons l'étude :

♦ **Proposition 5** Soient $\mathcal{B} = (i, j)$ une b.o.n.d. de E_2, et $\varphi \in \mathbb{R}$. L'endomorphisme de E_2, dont la matrice par rapport à $\mathcal{B}$ est $S_\varphi = \begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix}$, est la réflexion par rapport à la droite vectorielle D d'angle polaire $\dfrac{\varphi}{2}$, et est notée $\mathrm{Réf}_D$.



Le résultat suivant découle des études précédentes.

◆ **Proposition 6**

- $\mathcal{SO}(E_2) = \{\text{Rot}_\theta;\ \theta \in \mathbb{R}\}$
- $\mathcal{O}(E_2) - \mathcal{SO}(E_2) = \{\text{Réf}_D;\ D \in \mathcal{D}\}$,

où $\mathcal{D}$ est l'ensemble des droites vectorielles de E_2. ∎

◆ **Proposition 7** Toute rotation de E_2 est décomposable, d'au moins une manière, en produit de deux réflexions.

Plus précisément, pour toute rotation r de E_2 et toute réflexion s de E_2, il existe une réflexion unique t de E_2 telle que $r = t \circ s$.

Preuve :
En notant $t = r^{-1} \circ s$, t est dans $\mathcal{O}(E)$ et $\det(t) = (\det(r))^{-1} \det(s) = 1^{-1}(-1) = -1$, donc t est une réflexion.

Exercices

◇ **10.4.1** Pour $\theta,\varphi \in \mathbb{R}$, on note $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, et $S_\varphi = \begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix}$ (cf. 10.4 Prop. 1 p. 362).
Calculer les produits $R_\theta R_{\theta'}$, $R_\theta S_\varphi$, $S_\varphi R_\theta$, $S_\varphi S_{\varphi'}$ pour $\theta,\theta',\varphi,\varphi' \in \mathbb{R}$.

◇ **10.4.2** Soient r une rotation et s une réflexion de E_2. Calculer $s \circ r \circ s$ et $r \circ s \circ r$.

◇ **10.4.3** Dans $\mathbb{R}^2$, quel est l'angle de $u = (-2,1)$ et $v = (1,3)$?

◇ **10.4.4** **Gerbe quadratique dans E_2**
Soit $(a,b,c) \in \mathbb{R}^3 - \{(0,0,0)\}$.

a) CNS sur a,b,c pour que l'équation $ax^2 + 2bxy + cy^2 = 0$ représente la réunion de deux droites (éventuellement confondues) ?

On suppose dorénavant $b^2 - ac \geqslant 0$, et on note D, D' les deux droites de E_2 dont la réunion, appelée *gerbe quadratique*, a pour équation $ax^2 + 2bxy + cy^2 = 0$.

b) Calculer $|\widehat{(D,D')}|$ (dans $[0;\ \frac{\pi}{2}]$).

c) Former l'équation de la gerbe quadratique des bissectrices de D et D'.

10.5 Géométrie vectorielle euclidienne en dimension 3

On note E_3 un espace vectoriel euclidien orienté de dimension 3, $\cdot$ le produit scalaire sur E_3.

10.5.1 Endomorphismes orthogonaux de E_3

Soient $f \in \mathcal{O}(E_3)$, $\mathcal{B} = (i,j,k)$ une b.o.n.d. de E_3, $\Omega = \mathrm{Mat}_{\mathcal{B}}(f)$.

• Nous allons d'abord montrer qu'il existe $x \in E_3 - \{0\}$ tel que $f(x) = x$ ou $f(x) = -x$ (c'est-à-dire, voir Tome 6, 2.1 Déf. p. 35, que 1 ou -1 est valeur propre de f).

Soit $\lambda \in \mathbb{R}$. On a :

$$(\exists x \in E_3 - \{0\},\ f(x) = \lambda x) \iff \big((\exists x \in E_3 - \{0\},\ x \in \mathrm{Ker}(f - \lambda \mathrm{Id}_{E_3})\big)$$
$$\iff \big(f - \lambda \mathrm{Id}_{E_3} \text{ non injective}\big) \iff \det\big((f - \lambda \mathrm{Id}_{E_3}\big) = 0.$$

L'application $P : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ \lambda & \longmapsto & \det(\Omega - \lambda \mathrm{I}_n) \end{array}$ est un polynôme de degré 3, de coefficient dominant -1. Comme P est continue sur $\mathbb{R}$ et que $\lim\limits_{-\infty} P = +\infty$, $\lim\limits_{+\infty} P = -\infty$, le théorème des valeurs intermédiaires montre que P admet au moins un zéro réel λ_0.

Ainsi, il existe $\lambda_0 \in \mathbb{R}$ et $x_0 \in E_3 - \{0\}$ tels que $f(x_0) = \lambda_0 x_0$.

Mais, comme $f \in \mathcal{O}(E_3)$, on a $||f(x_0)|| = ||x_0||$, d'où $|\lambda_0| = 1$, c'est-à-dire $\lambda_0 \in \{-1,1\}$.

Autrement dit, on a montré que 1 ou -1 est valeur propre de f.

• Notons $I = \dfrac{1}{||x_0||} x_0$ et $H = I^{\perp}$. Le plan vectoriel H est stable par f car, pour tout y de H : $f(y) \cdot I = f(y) \cdot \left(\dfrac{1}{\lambda_0} f(I)\right) = \dfrac{1}{\lambda_0}\big(f(y) \cdot I\big) = \dfrac{1}{\lambda_0}\,(y \cdot I) = 0.$

Considérons l'endomorphisme g de H induit par f, $g : \begin{array}{ccc} H & \longrightarrow & H \\ y & \longmapsto & f(y) \end{array}$, et munissons H du produit scalaire restriction de $\cdot$ à $H \times H$ et d'une b.o.n. (J,K).

Comme $f \in \mathcal{O}(E_3)$, il est clair que $g \in \mathcal{O}(H)$:

$$\forall (y,z) \in H^2,\quad g(y) \cdot g(z) = f(y) \cdot f(z) = y \cdot z.$$

D'après 10.4 Prop. 6 p. 366, g est une rotation ou une réflexion.

Ceci fait apparaître quatre cas pour l'étude de f.

1er Cas : $\lambda_0 = 1$ et g est une rotation

La matrice de f dans la b.o.n (I,J,K) de E_3 est de la forme $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$, $\theta \in \mathbb{R}$.

2ème Cas : $\lambda_0 = 1$ et g est une réflexion

Notons J' (resp. K') un vecteur normé dirigeant $\mathrm{Ker}(g - \mathrm{Id}_H)$ (resp. $\mathrm{Ker}(g + \mathrm{Id}_H)$).

Alors (I,J',K') est une b.o.n., dans laquelle la matrice de f est : $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$,

donc f est la réflexion par rapport au plan vectoriel engendré par $\{I,J'\}$.

3ème Cas : $\lambda_0 = -1$ et g est une réflexion

Avec les notations du 2ème cas, la matrice de f dans la b.o.n. (I, J', K') est $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$.

Donc f est la symétrie orthogonale par rapport à la droite vectorielle engendrée par J'.

La matrice de f dans la b.o.n. (J', I, K') est $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$; ainsi, f est aussi la rotation d'axe dirigé (et orienté) par J' et d'angle π.

4ème Cas : $\lambda_0 = -1$ et g est une rotation

La matrice de f dans la b.o.n. (I, J, K) est de la forme $\begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}, \theta \in \mathbb{R}$.

Remarquons : $\begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$. ■

Nous supposons dorénavant que E_3 est orienté.

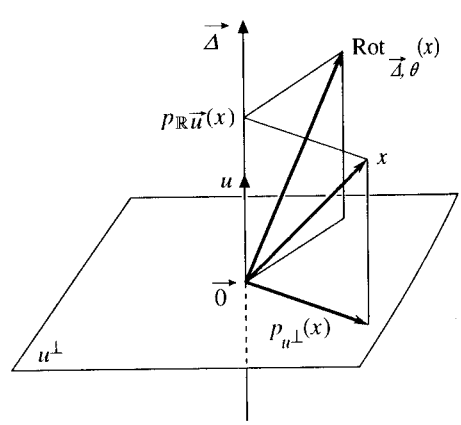
La description géométrique du 1er cas amène le Déf. suivante.

◆ **Définition 1** Soient $u \in E_3$ tel que $||u|| = 1$, $\overrightarrow{\Delta}$ l'axe dirigé et orienté par u, et $\theta \in \mathbb{R}$. On appelle, **rotation d'axe $\overrightarrow{\Delta}$ et d'angle θ**, et on note $\mathrm{Rot}_{\overrightarrow{\Delta},\theta}$, l'endomorphisme de E_3 dont la matrice dans une b.o.n.d. (u, v, w), commençant par u, est $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$.

On a donc, pour tout x de E_3 :

$$\mathrm{Rot}_{\overrightarrow{\Delta},\theta}(x) = \mathrm{Rot}_\theta\left(p_{u^\perp}(x)\right) + p_{\mathbb{R}u}(x),$$

où :
- $p_{u^\perp}(x)$ est la projection orthogonale de x sur le plan $u^\perp$
- $p_{\mathbb{R}u}(x)$ et la projection orthogonale de x sur la droite $\mathbb{R}u$
- Rot_θ est la rotation d'angle θ, dans le plan $u^\perp$ orienté par la base directe (v, w).



Remarques :

1) Soient $\overrightarrow{\Delta}$ un axe, $\theta \in \mathbb{R} - 2\pi\mathbb{Z}$. D'après l'étude précédente, il existe une b.o.n.d. (u,v,w) telle que u dirige et oriente $\overrightarrow{\Delta}$ et dans laquelle la matrice de $\mathrm{Rot}_{\overrightarrow{\Delta},\theta}$ est

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}.$$

Il est alors clair que l'ensemble des invariants de $\mathrm{Rot}_{\overrightarrow{\Delta},\theta}$ est la droite vectorielle $\mathbb{R}u$, puisque la rotation $g : \begin{array}{ccc} u^\perp & \longrightarrow & u^\perp \\ y & \longmapsto & f(y) \end{array}$ n'admet que $\overrightarrow{0}$ pour invariant.

Ceci montre qu'une rotation n'admet que deux axes, de même direction et de sens opposés.

2) Soient $\overrightarrow{\Delta_1}, \overrightarrow{\Delta_2}$ deux axes, $\theta_1, \theta_2 \in \mathbb{R} - 2\pi\mathbb{Z}$. On déduit de *1)* :

$$\mathrm{Rot}_{\overrightarrow{\Delta_1},\theta_1} = \mathrm{Rot}_{\overrightarrow{\Delta_2},\theta_2} \iff \left(\begin{cases} \overrightarrow{\Delta_2} = \overrightarrow{\Delta_1} \\ \theta_2 \equiv \theta_1 [2\pi] \end{cases} \text{ ou } \begin{cases} \overrightarrow{\Delta_2} = -\overrightarrow{\Delta_1} \\ \theta_2 \equiv -\theta_1 [2\pi] \end{cases} \right),$$

où $-\overrightarrow{\Delta_1}$ désigne l'axe de même direction que $\overrightarrow{\Delta_1}$ et de sens contraire. ■

La description géométrique du 3ème cas amène la Déf. suivante.

♦ **Définition 2** On appelle **retournement** (ou : **demi-tour**) de E_3 toute rotation de E_3 d'angle $\pi \quad [2\pi]$. ■

L'étude précédente montre :

♦ **Théorème** **(Classification des endomorphismes orthogonaux de E_3)**

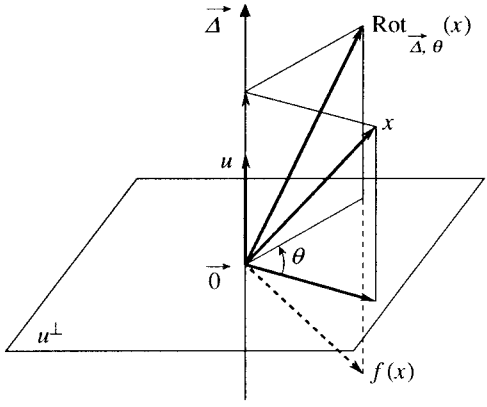
Soit $f \in \mathcal{O}(E_3) - \{\mathrm{Id}_{E_3}\}$.

1) Si $\det(f) = 1$, alors f est une rotation de E_3.

2) Si $\det(f) = -1$, alors :

- ou bien f est une réflexion de E_3
- ou bien f est la composée d'une rotation de E_3 et de la réflexion par rapport au plan orthogonal à l'axe de cette rotation.

Cas où f est la composée d'une rotation de E_3 et de la réflexion par rapport au plan orthogonal à l'axe de cette rotation



Détermination de la nature et des éléments caractéristiques d'un endomorphisme orthogonal de E_3

Soient $\Omega \in \mathbf{O}_3(\mathbb{R}) - \{I_3\}$, f l'endomorphisme orthogonal de E_3 représenté par Ω dans une b.o.n.d. $\mathcal{B}$ de E_3.

1) Supposons $\det(\Omega) = 1$.

Alors f est une rotation de E_3.

La droite supportant l'axe de f est l'ensemble des invariants de f, donc est déterminée par la résolution de l'équation $\Omega X = X$, d'inconnue $X \in \mathbf{M}_{3,1}(\mathbb{R})$.

D'après l'étude précédente :

$$\mathrm{tr}(\Omega) = \mathrm{tr}(f) = \mathrm{tr}\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} = 1 + 2\cos\theta,$$

ce qui permet de déterminer $\cos\theta$.

Notons I le vecteur normé dirigeant et orientant l'axe de f, et (J,K) une b.o.n. de $I^{\perp}$ de sorte que (I,J,K) soit une b.o.n.d. de E_3.

Soit $x \in E_3$, non colinéaire à I. Notons (α,β,γ) les composantes de x dans la b.o.n.d. (I,J,K).

La colonne des composantes de $f(x)$ dans (I,J,K) est :

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta\cos\theta - \gamma\sin\theta \\ \beta\sin\theta + \gamma\cos\theta \end{pmatrix} \quad \text{et donc :}$$

$$[x, f(x), I] = \det_{(I,J,K)}(x, f(x), I) = \begin{vmatrix} \alpha & \alpha & 1 \\ \beta & \beta\cos\theta - \gamma\sin\theta & 0 \\ \gamma & \beta\sin\theta + \gamma\cos\theta & 0 \end{vmatrix} = (\beta^2 + \gamma^2)\sin\theta.$$

Ainsi, comme $\beta^2 + \gamma^2 > 0$ (car x n'est pas colinéaire à I), $\sin\theta$ est du signe du produit mixte $[x, f(x), I]$. En pratique, on calcule ce produit mixte par un déterminant dans la b.o.n.d. (i,j,k). En résumé :

1) La droite supportant l'axe $\overrightarrow{\Delta}$ de f est l'ensemble des invariants de f, obtenu en résolvant $\Omega X = X$, d'inconnue $X \in \mathbf{M}_{3,1}(\mathbb{R})$.

2) On détermine θ par :

- $\mathrm{tr}(\Omega) = 1 + 2\cos\theta$
- $\sin\theta$ est du signe du produit mixte $[x, f(x), I]$ pour n'importe quel x non colinéaire à I, où I est le vecteur normé dirigeant et orientant l'axe de f.

EXEMPLE :

Reconnaître l'endomorphisme f de $\mathbb{R}^3$ dont la matrice dans la base canonique est :

$$\Omega = \frac{1}{3}\begin{pmatrix} -2 & -1 & 2 \\ 2 & -2 & 1 \\ 1 & 2 & 2 \end{pmatrix}.$$

Il est clair que $\Omega \in \mathbf{O}_3(\mathbb{R})$ (les colonnes de Ω sont normées et deux à deux orthogonales).

De plus : $\det(\Omega) = 1$.

Donc f est une rotation.

L'axe $\overrightarrow{\Delta}$ de f est dirigé par $xi + yj + zk$, où (x,y,z) est déterminé par :

$$\frac{1}{3}\begin{pmatrix} -2 & -1 & 2 \\ 2 & -2 & 1 \\ 1 & 2 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \iff \begin{cases} -2x - y + 2z = 3x \\ 2x - 2y + z = 3y \\ x + 2y + 2z = 3z \end{cases}$$

$$\iff \begin{cases} 5x + y - 2z = 0 \\ 2x - 5y + z = 0 \\ x + 2y - z = 0 \end{cases} \iff \begin{cases} y = -5x + 2z \\ 27x - 9z = 0 \\ -9x + 3z = 0 \end{cases} \iff \begin{cases} y = x \\ z = 3x. \end{cases}$$

Un vecteur dirigeant et orientant l'axe $\overrightarrow{\Delta}$ de f est $u = i + j + 3k$, et un vecteur normé dirigeant et orientant $\overrightarrow{\Delta}$ est $I = \frac{1}{\sqrt{11}}(i + j + 3k)$.

Notons θ l'angle de f.

Comme $1 + 2\cos\theta = \mathrm{tr}(\Omega) = -\frac{2}{3}$, on déduit $\cos\theta = -\frac{5}{6}$.

Enfin, $\sin\theta$ est du signe du produit mixte :

$$[i, f(i), I] = \det_{(i,j,k)}(i, f(i), I) = \begin{vmatrix} 1 & -\frac{2}{3} & \frac{1}{\sqrt{11}} \\ 0 & \frac{2}{3} & \frac{1}{\sqrt{11}} \\ 0 & \frac{1}{3} & \frac{3}{\sqrt{11}} \end{vmatrix} = \frac{5}{3\sqrt{11}} > 0.$$

On conclut : f est la rotation d'axe dirigé et orienté par $I = \frac{1}{\sqrt{11}}(i + j + 3k)$ et d'angle $\theta = \mathrm{Arccos}\left(-\frac{5}{6}\right)$ $[2\pi]$.

2) Supposons $\det(\Omega) = -1$.

Alors f est soit une réflexion, soit la composée d'une rotation et d'une réflexion.

Remarquons que, pour $\Omega \in \mathbf{O}_3(\mathbb{R})$, les relations $\Omega^2 = \mathrm{I}_3$ et ${}^t\Omega = \Omega$ sont équivalentes, puisque ${}^t\Omega\Omega = \mathrm{I}_3$.

a) Supposons Ω symétrique.

Puisque $\Omega^2 = \mathrm{I}_3$, f est une symétrie orthogonale.

Comme de plus $\det(\Omega) = -1$, si $\Omega \neq -\mathrm{I}_3$, alors f est une réflexion. Le plan de la réflexion f est l'ensemble des invariants de f.

EXEMPLE :

Reconnaître l'endomorphisme f de $\mathbb{R}^3$ dont la matrice dans la base canonique est :

$$\Omega = -\frac{1}{9}\begin{pmatrix} -8 & 4 & 1 \\ 4 & 7 & 4 \\ 1 & 4 & -8 \end{pmatrix}.$$

Il est clair que $\Omega \in \mathbf{O}_3(\mathbb{R})$, $\det(\Omega) = -1$, ${}^t\Omega = \Omega$. Donc f est une réflexion.

Le plan de la réflexion f est défini par : $\Omega X = X$. Pour $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$:

$$\Omega X = X \Longleftrightarrow \left\{ \begin{array}{l} -8x + 4y + z = -9x \\ 4x + 7y + 4z = -9y \\ x + 4y - 8z = -9z \end{array} \right| \Longleftrightarrow x + 4y + z = 0.$$

On conclut : f est la réflexion par rapport au plan vectoriel d'équation $x + 4y + z = 0$.
(Vérification : $(1,4,1)$ est bien anti-invariant par f).

b) Supposons Ω non symétrique.

Alors f est la composée commutative d'une rotation $\mathrm{Rot}_{\overrightarrow{\Delta},\theta}$ et d'une réflexion $\mathrm{Réf}_P$ par rapport au plan P orthogonal à l'axe $\overrightarrow{\Delta}$.

Les éléments de $\overrightarrow{\Delta}$ sont caractérisés par : $\Omega X = -X$.

On a :

$$\mathrm{tr}(\Omega) = \mathrm{tr}(f) = \mathrm{tr}\begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} = -1 + 2\cos\theta,$$

ce qui permet de déterminer $\cos\theta$.

Comme en *1)* plus haut p. 370, $\sin\theta$ est du signe du produit mixte $[x, f(x), I]$ pour n'importe quel x non colinéaire à I, où I est le vecteur normé dirigeant et orientant $\overrightarrow{\Delta}$.

Enfin : $P = \Delta^{\perp}$.

EXEMPLE :

Reconnaître l'endomorphisme f de $\mathbb{R}^3$ dont la matrice dans la base canonique est :

$$\Omega = -\frac{1}{4}\begin{pmatrix} 3 & 1 & \sqrt{6} \\ 1 & 3 & -\sqrt{6} \\ -\sqrt{6} & \sqrt{6} & 2 \end{pmatrix}.$$

Il est clair que $\Omega \in \mathbf{O}_3(\mathbb{R})$, Ω n'est pas symétrique, et $\det(\Omega) = -1$. Donc f est la composée commutative d'une rotation $\mathrm{Rot}_{\overrightarrow{\Delta},\theta}$ et de la réflexion $\mathrm{Réf}_P$ où $P = \Delta^{\perp}$.

Les éléments de Δ sont déterminés par : $\Omega X = -X$.

Pour $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$, on a :

$$\Omega X = -X \iff \begin{cases} 3x + y + \sqrt{6}z = 4x \\ x + 3y - \sqrt{6}z = 4y \\ -\sqrt{6}x + \sqrt{6}y + 2z = 4z \end{cases} \iff \begin{cases} -x + y + \sqrt{6}z = 0 \\ \sqrt{6}x - \sqrt{6}y + 2z = 0 \end{cases} \iff \begin{cases} x = y \\ z = 0 \end{cases}.$$

Un vecteur normé dirigeant et orientant $\overrightarrow{\Delta}$ est $I = \dfrac{1}{\sqrt{2}}(i + j)$.

Comme $-1 + 2\cos\theta = \mathrm{tr}(\Omega) = -2$, on déduit $\cos\theta = -\dfrac{1}{2}$.

Enfin, $\sin\theta$ est du signe de :

$$[i, f(i), I] = \begin{vmatrix} 1 & -\frac{3}{4} & \frac{1}{\sqrt{2}} \\ 0 & -\frac{1}{4} & \frac{1}{\sqrt{2}} \\ 0 & \frac{\sqrt{6}}{4} & 0 \end{vmatrix} = -\frac{\sqrt{3}}{4} < 0,$$

d'où $\theta \equiv -\dfrac{2\pi}{3}$ $[2\pi]$.

On conclut : f est la composée $\mathrm{Rot}_{\overrightarrow{\Delta},\theta} \circ \mathrm{Réf}_P$, où $\overrightarrow{\Delta}$ est dirigé et orienté par $I = \dfrac{1}{\sqrt{2}}(i+j)$, $\theta \equiv -\dfrac{2\pi}{3}[2\pi]$, P est le plan orthogonal à Δ, d'équation $x + y = 0$. ■

◆ **Proposition 1**

Tout endomorphisme orthogonal de E_3 est décomposable en produit d'au plus trois réflexions.

Preuve :

Soit $f \in \mathcal{O}(E_3)$.

• Si $f = \mathrm{Id}_{E_3}$, f est clairement la composée de deux réflexions (deux fois la même), ou encore f est la composée vide.

• Le résultat est évident si f est une réflexion.

• Cas où f est une rotation.

Avec les notations de la p. 368, il existe deux droites vectorielles D_1, D_2 de $\Delta^\perp$ telles que $g = \mathrm{Réf}_{D_2} \circ \mathrm{Réf}_{D_1}$, dans le plan $\Delta^\perp$.

En notant P_1 (resp. P_2) le plan vectoriel engendré par $D_1 \cup \Delta$ (resp. $D_2 \cup \Delta$), il est clair que :

$$f = \mathrm{Réf}_{P_2} \circ \mathrm{Réf}_{P_1}.$$

• Si f est la composée d'une rotation et d'une réflexion, alors, d'après le cas précédent, f est décomposable en un produit de trois réflexions.

• Si $f = -\mathrm{Id}_{E_3}$, alors f est la composée des trois réflexions par rapport aux trois plans de coordonnées. ■

◆ **Définition 3** Soient $u,v \in E_3 - \{0\}$. On définit l'angle de u et v, noté $\widehat{(u,v)}$ par :

$\widehat{(u,v)} = 0$ si $\exists \alpha \in \mathbb{R}_+^*$, $v = \alpha u$

$\widehat{(u,v)} = \pi$ si $\exists \alpha \in \mathbb{R}_-^*$, $v = \alpha u$

$\widehat{(u,v)}$ est la valeur absolue de l'angle (compté dans $]-\pi;\pi[$) de u et v dans le plan euclidien orienté par u et v si (u,v) est libre.

On remarquera qu'ainsi un angle dans E_3 n'est pas, a priori, «orienté». De façon imagée, on peut regarder le plan Vect (u,v) par dessus ou par dessous.

On déduit de 10.4 Prop. 3 p. 364 le résultat suivant.

◆ **Proposition 2**

$$\forall u,v \in E_3 - \{0\},\ u \bullet v = ||u||\ ||v|| \cos \widehat{(u,v)}.$$

Exercices

◇ **10.5.1** Déterminer la nature de l'endomorphisme f de E_3, dont la matrice Ω relativement à une b.o.n.d. (i,j,k) de E_3 est donnée ci-après, et préciser les éléments caractéristiques de f :

a) $-\frac{1}{27}\begin{pmatrix} 2 & -26 & 7 \\ -23 & 2 & 14 \\ 14 & 7 & 22 \end{pmatrix}$ *b)* $\frac{1}{9}\begin{pmatrix} -7 & 4 & -4 \\ 4 & -1 & -8 \\ -4 & -8 & -1 \end{pmatrix}$

c) $\frac{1}{9}\begin{pmatrix} 7 & 4 & 4 \\ 4 & 1 & -8 \\ 4 & -8 & 1 \end{pmatrix}$ *d)* $\frac{1}{9}\begin{pmatrix} 7 & -4 & 4 \\ 4 & 8 & 1 \\ 4 & -1 & -8 \end{pmatrix}$

e) $\begin{pmatrix} a^2 & ab-c & ac+b \\ ab+c & b^2 & bc-a \\ ac-b & bc+a & c^2 \end{pmatrix}$, $(a,b,c) \in \mathbb{R}^3$, $a^2+b^2+c^2 = 1$.

◇ **10.5.2** Former la matrice Ω, dans une b.o.n.d. (i,j,k) de E_3, de la rotation f d'axe dirigé orienté par $i+j+k$ et d'angle $\frac{\pi}{3}$ $[2\pi]$.

◇ **10.5.3** Soient $f,g \in \mathcal{SO}(E_3) - \{\mathrm{Id}_{E_3}\}$. Montrer que f et g commutent si et seulement si :

f et g sont deux rotations de même axe
ou
f et g sont deux retournements d'axes orthogonaux.

◇ **10.5.4** Démontrer que toute rotation de E_3 est décomposable, d'au moins une façon, en produit d'au plus deux retournements.

10.5.2 Produit vectoriel

Rappelons (cf. 10.3.2 Prop. - Déf. 7 p. 360) que le produit mixte $[u,v,w]$ de trois éléments u,v,w de E_3 est défini par : $[u,v,w] = \det_{\mathcal{B}}(u,v,w)$,

où $\mathcal{B}$ est n'importe quelle b.o.n.d. de E_3.

D'après 9.2.2 Prop. 2 p. 306, on a : $[u,v,w] = 0 \iff (u,v,w)$ lié.

Puisque, pour (u,v) fixé, l'application $\begin{array}{ccc} E_3 & \longrightarrow & \mathbb{R} \\ w & \longmapsto & [u,v,w] \end{array}$ est une forme linéaire, la Prop. suivante résulte de 10.2.3 Prop. 2 p. 354.

♦ **Proposition - Définition 1** Soit $(u,v) \in E_3^2$. Il existe un élément unique x de E_3 tel que : $\forall\, w \in E_3, \quad [u,v,w] = x \cdot w$.

Cet élément x de E_3 s'appelle le **produit vectoriel** de u par v, et est noté $u \wedge v$ (ou : $u \times v$).

On a donc, par définition : $\forall\, u,v,w \in E_3,\ [u,v,w] = (u \wedge v) \cdot w$,

ce qui justifie, a posteriori, l'expression «produit mixte » comme mélange d'un produit vectoriel et d'un produit scalaire.

Remarques :

1) On a , pour tous u,v,w de E_3 :

$$\begin{cases} [u,v,w] = (u \wedge v) \cdot w \\ [u,v,w] = [v,w,u] = (v \wedge w) \cdot u \\ [u,v,w] = [w,u,v] = (w \wedge u) \cdot v. \end{cases}$$

2) Si $\mathcal{B} = (i,j,k)$ est une b.o.n.d. de E_3, alors : $i \wedge j = k, \quad j \wedge k = i, \quad k \wedge i = j$, puisque, par exemple :

$$\begin{aligned} i \wedge j &= \big((i \wedge j) \cdot i\big)i + \big((i \wedge j) \cdot j\big)j + \big((i \wedge j) \cdot k\big)k \\ &= [i,j,i]i + [i,j,j]j + [i,j,k]k = k. \end{aligned}$$

♦ **Proposition 2**

L'application $\begin{array}{ccc} E_3 \times E_3 & \longrightarrow & E_3 \\ (u,v) & \longmapsto & u \wedge v \end{array}$ est bilinéaire alternée.

Preuve :

Soient $\alpha \in \mathbb{R}, u,v,v' \in E_3$.

• $\forall\, w \in E_3,\ (v \wedge u) \cdot w = [v,u,w] = -[u,v,w] = -(u \wedge v) \cdot w$,

d'où, par unicité de $v \wedge u$: $v \wedge u = -u \wedge v$.

• $\forall\, w \in E_3,\ \big(u \wedge (\alpha v + v')\big) \cdot w = [u,\alpha v + v', w] = \alpha[u,v,w] + [u,v',w]$

$$= \alpha(u \wedge v) \cdot w + (u \wedge v') \cdot w = \big(\alpha(u \wedge v) + (u \wedge v')\big) \cdot w,$$

d'où, par unicité de $u \wedge (\alpha v + v')$: $u \wedge (\alpha v + v') = \alpha(u \wedge v) + (u \wedge v')$.

La linéarité par rapport à la 1ère place résulte de la linéarité par rapport à la 2ème place et de l'alternance.

◆ **Proposition 3**

$$\forall u,v \in E_3, \quad (u \wedge v = 0 \Longleftrightarrow (u,v) \text{ lié}).$$

Preuve :

1) Si (u,v) est lié, alors $u \wedge v = 0$ (cf. 9.1.2 Prop. 2 p. 303).

2) Réciproquement, supposons $u \wedge v = 0$.

Si (u,v) est libre, alors, d'après le théorème de la base incomplète, forme faible (6.4 Th.2 p. 229), il existe $w \in E_3$ tel que (u,v,w) soit une base de E_3, et alors $(u \wedge v) \cdot w = [u,v,w] \neq 0$ (cf. 9.2.2 Prop. 2 p. 306), contradiction.

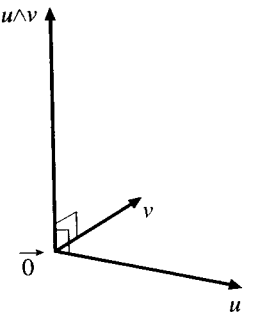
Donc (u,v) est lié.

◆ **Corollaire**

Si (u,v) est libre, alors $(u,v,\ u \wedge v)$ est une base directe de E_3.

Preuve :

$$\begin{aligned}[u,v,u \wedge v] &= (u \wedge v) \cdot (u \wedge v) \\ &= \|u \wedge v\|^2 > 0.\end{aligned}$$



◆ **Proposition 4**

$$\forall u,v \in E_3, \ (u \wedge v \perp u \text{ et } u \wedge v \perp v).$$

Preuve : $(u \wedge v) \cdot u = [u,v,u] = 0, \quad (u \wedge v) \cdot v = [u,v,v] = 0.$

◆ **Proposition 5** Soient $\mathcal{B} = (i,j,k)$ une b.o.n.d. de E_3, $u,v \in E_3$, (x,y,z) (resp. (x',y',z')) les composantes de u (resp. v) dans $\mathcal{B}$. On a :

$$u \wedge v = (yz' - zy')i + (zx' - xz')j + (xy' - yx')k.$$

Preuve :

Comme $\wedge$ est bilinéaire alterné, et d'après la Prop. précédente, on a :

$$\begin{aligned}u \wedge v &= (xi + yj + zk) \wedge (x'i + y'j + z'k) \\ &= (yz' - zy')i + (zx' - xz')j + (xy' - yx')k.\end{aligned}$$

Remarque :

On peut retenir ce résultat sous la forme schématique :

$$u \wedge v = \begin{vmatrix} x & x' & i \\ y & y' & j \\ z & z' & k \end{vmatrix}$$

«faux déterminant» (car i,j,k sont des vecteurs) que l'on développe par rapport à la 3ème colonne.

♦ **Proposition 6** **(Double produit vectoriel)**

$$\forall u,v,w \in E_3, \quad u \wedge (v \wedge w) = (u \bullet w)v - (u \bullet v)w.$$

Preuve :

1) Si $v = 0$, la propriété est immédiate.

2) Si $v \neq 0$ et si w est colinéaire à v, il existe $\lambda \in \mathbb{R}$ tel que $w = \lambda v$, d'où :

$$(u \bullet w)v - (u \bullet v)w = \lambda(u \bullet v)v - \lambda(u \bullet v)v = 0 = u \wedge (v \wedge w).$$

3) Supposons (u,v) libre. D'après le procédé d'orthogonalisation de Schmidt, il existe une b.o.n.d. (I,J,K) de E_3 et $\alpha,\beta,\gamma,a,b,c \in \mathbb{R}$ tels que :

$$v = \alpha I, \quad w = \beta I + \gamma J, \quad u = aI + bJ + cK.$$

On a alors :

- $v \wedge w = \alpha\gamma K$, d'où $u \wedge (v \wedge w) = -\alpha\gamma aJ + \alpha\gamma bI$
- $(u \bullet w)v - (u \bullet v)w = (a\beta + b\gamma)v - a\alpha w = b\gamma\alpha I - a\alpha\gamma J$,

d'où la formule voulue.

♦ **Proposition 7**

1) $\forall u,v \in E_3, \quad ||u \wedge v||^2 + (u \bullet v)^2 = ||u||^2 \, ||v||^2$

(Identité de Lagrange)

2) $\forall u,v \in E_3 - \{0\}, \quad ||u \wedge v|| = ||u|| \, ||v|| \, \left|\sin(\widehat{u,v})\right|$.

Preuve : *1)*

$$\begin{aligned} ||u \wedge v||^2 &= (u \wedge v) \bullet (u \wedge v) = [u,v,u \wedge v,u] = [v,u \wedge v,u] = (v \wedge (u \wedge v)) \bullet u \\ &= \big((v \bullet v)u - (v \bullet u)v\big) \bullet u = (v \bullet v)(u \bullet u) - (v \bullet u)(v \bullet u) = ||v||^2 \, ||u||^2 - (v \bullet u)^2. \end{aligned}$$

2) D'après 10.5.1 Prop. 2 p. 374 :

$$||u \wedge v||^2 = ||u||^2 \, ||v||^2 \left(1 - \cos^2(\widehat{u,v})\right) = ||u||^2 \, ||v||^2 \sin^2(\widehat{u,v}).$$

Remarques :

1) En particulier : $\forall u,v \in E_3, \ (u \perp v \iff ||u \wedge v|| = ||u|| \, ||v||)$.

2) Si u et v sont normés et orthogonaux, alors $(u,v,u \wedge v)$ est une b.o.n.d. de E_3.

◆ **Proposition 8**

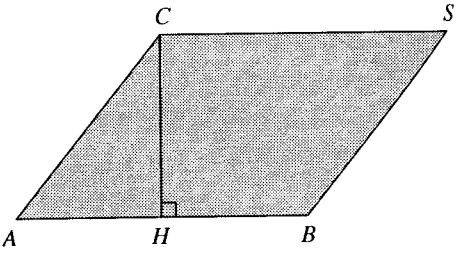
1) Pour tout (u,v) de E_3^2, $||u \wedge v||$ vaut l'aire du parallélogramme construit sur u,v.

2) Pour tout (u,v,w) de E_3^3, $|[u,v,w]|$ vaut le volume du parallélépipède construit sur u,v,w.

Preuve :

1) Dans le (un) plan affine euclidien (orienté) (voir Tome de Géométrie), soient A,B,C,S tels que $\overrightarrow{AB} = u$, $\overrightarrow{AC} = v$, $\overrightarrow{BS} = \overrightarrow{AC}$, et soit H la projection orthogonale de C sur (AB) (le cas $u = 0$ étant trivial).

L'aire $\mathcal{A}$ du parallélogramme $ABSC$ est $AB \times CH$.



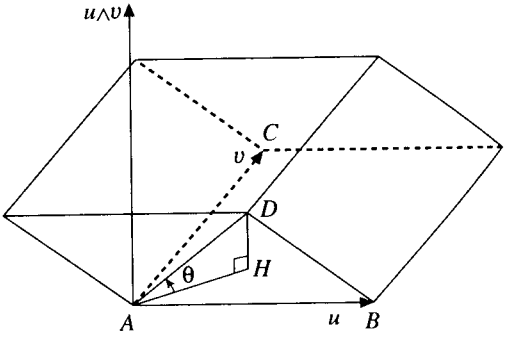
Comme $AB = ||u||$ et $CH = AC \sin \widehat{CAH} = ||v|| \, |\sin (\widehat{u,v})|$, on conclut :

$$\mathcal{A} = ||u|| \, ||v|| \, |\sin (\widehat{u,v})| = ||u \wedge v||.$$

En conséquence, l'aire du triangle ABC vaut $\frac{1}{2}||\overrightarrow{AB} \wedge \overrightarrow{AC}||$.

2) Dans l' (un) espace affine euclidien (orienté) de dimension 3, soient A,B,C,D tels que $\overrightarrow{AB} = u$, $\overrightarrow{AC} = v$, $\overrightarrow{AD} = w$, et soit H la projection orthogonale de D sur le plan ABC (le cas où (u,v) est lié étant trivial).

Le volume $\mathcal{V}$ du parallélépipède construit sur A,B,C,D est $DH \times \mathcal{A}$, où $\mathcal{A}$ est l'aire du parallélogramme construit sur ABC.



Notons $\theta = \widehat{DAH}$, l'angle entre $\overrightarrow{AD}$ et le plan ABC.

Puisque $u \wedge v \perp ABC$, on a : $\left(\widehat{\overrightarrow{AD}, u \wedge v}\right) = \frac{\pi}{2} - \theta$,

d'où $DH = AD|\sin\theta| = AD \cdot \left|\cos (\widehat{\overrightarrow{AD}, u \wedge v})\right|$, puis, en utilisant *1)* :

$$\mathcal{V} = ||u \wedge v|| \cdot AD \cdot \left|\cos (\widehat{\overrightarrow{AD}, u \wedge v})\right| = |(u \wedge v) \cdot w| = |[u,v,w]|.$$

Exercices

◇ **10.5.5** **Division vectorielle**

Pour $(a,b) \in (E_3)^2$ donné, résoudre $a \wedge x = b$, d'inconnue $x \in E_3$.

◇ **10.5.6** Soit $(a,b) \in (E_3)^2$ libre; montrer qu'il n'existe aucun c de E_3 tel que :

$$\forall x \in E_3,\ a \wedge (b \wedge x) = c \wedge x.$$

◇ **10.5.7** Pour $a \in E_3$ donné, résoudre $\begin{cases} a \wedge x + y = a \\ a \wedge y + x = a \end{cases}$, d'inconnue $(x,y) \in (E_3)^2$.

◇ **10.5.8** Pour $(a,b) \in (E_3)^2$ libre, résoudre $(a \wedge x) \wedge b = a \wedge (x \wedge b)$, d'inconnue $x \in E_3$.

◇ **10.5.9** Pour $(a,b) \in (E_3)^2$ libre, résoudre (S) $\begin{cases} a \wedge x = b \wedge y \\ a \wedge y = b \wedge x \\ x \wedge y = a \wedge b \end{cases}$, d'inconnue $(x,y) \in (E_3)^2$.

◇ **10.5.10** Etablir, pour tous x,y,z,u,v,w de E_3 :

$$[x \wedge u,\ y \wedge v,\ z \wedge w] + [x \wedge v,\ y \wedge w,\ z \wedge u] + [x \wedge w,\ y \wedge u,\ z \wedge v] = 0.$$

◇ **10.5.11** Soient $a \in E_3$, $f_a : (E_3)^2 \longrightarrow E_3$ définie par :

$$\forall (x,y) \in (E_3)^2,\ f_a(x,y) = (a \wedge x) \wedge y + (a \wedge y) \wedge x.$$

a) Vérifier que f_a est une application bilinéaire symétrique, c'est-à-dire :

$$\begin{cases} \forall (x,y) \in (E_3)^2,\ f_a(y,x) = f_a(x,y) \\ \forall \lambda \in \mathbb{R}, \forall (x,y,z) \in (E_3)^3,\ f_a(x,y+\lambda z) = f_a(x,y) + \lambda f_a(x,z). \end{cases}$$

b) Montrer que, pour tout (x,y) de $(E_3 - \{0\})^2$ tel que $x \cdot y = 0$, on a :

$$f_a(x,y) = 0 \Longleftrightarrow a \in \mathbb{R}(x \wedge y).$$

◇ **10.5.12** Soient $u \in E_3$ normé, $f : \begin{array}{ccc} E_3 & \longrightarrow & E_3 \\ x & \longmapsto & x \wedge u \end{array}$.

Vérifier : $f^3 = -f$.

◇ **10.5.13** Soient $u \in E_3$ normé, $(\alpha,\beta,\gamma) \in \mathbb{R}^3$, $f : E_3 \longrightarrow E_3$ définie par :

$$\forall x \in E_3,\ f(x) = \alpha x + \beta(u \cdot x)u + \gamma u \wedge x.$$

CNS sur (α,β,γ) pour que f soit une rotation, et dans ce cas déterminer ses éléments caractéristiques (axe, angle).

Complément

◇ C 10.1 Polynômes de Legendre

On note E l'ensemble des applications polynomiales de $[-1;1]$ dans $\mathbb{R}$ et, pour chaque n de $\mathbb{N}$, E_n l'ensemble des applications polynomiales de $[-1;1]$ dans $\mathbb{R}$ de degré $\leqslant n$. On pourra confondre polynôme et application polynomiale de $[-1;1]$ dans $\mathbb{R}$ (puisque $[-1;1]$ est infini, cf. 5.1.7 Prop. 2 p. 150). Il est immédiat que E est un $\mathbb{R}$-ev pour les lois usuelles.

On définit une application $< \cdot,\cdot >$ de E^2 dans $\mathbb{R}$ par :

$$\forall (P,Q) \in E^2,\ < P,Q >= \int_{-1}^{1} P(x)Q(x)\,dx.$$

I Polynômes orthogonaux

1) Vérifier que $< \cdot,\cdot >$ est un produit scalaire sur E, et que :

$$\forall P,Q,R \in E,\ < PQ,R >=< P,QR > .$$

On note $||\cdot||$ la norme sur E associée à $< \cdot,\cdot >$.

2) Etablir qu'il existe une suite unique $(P_n)_{n\in\mathbb{N}}$ d'éléments de E telle que :

$$\begin{cases} \forall (m,n) \in \mathbb{N}^2,\quad < P_m,P_n >= \begin{cases} 1 & \text{si } m = n \\ 0 & \text{si } m \neq n \end{cases} \\ \text{Pour tout } n \text{ de } \mathbb{N},\ P_n \text{ est de degré } n \text{ et à coefficient dominant} > 0. \end{cases}$$

3) Montrer : $\forall n \in \mathbb{N}^*, P_n \in E_{n-1}^{\perp}$, où $E_{n-1}^{\perp}$ est l'orthogonal de E_{n-1} pour le produit scalaire $< \cdot,\cdot >$.

II Pour $n \in \mathbb{N}$, on note $U_n = \left((X^2-1)^n\right)^{(n)}$ (dérivée $n^{\text{ème}}$ de $(X^2-1)^n$).

1) a) Soit $n \in \mathbb{N}$. Montrer que, si n est pair (resp. impair), alors U_n est pair (resp. impair).

b) Montrer que, pour tout n de $\mathbb{N}$, U_n est de degré n, et calculer son coefficient dominant.

Pour $n \in \mathbb{N}$, on note $L_n = \dfrac{1}{2^n n!} U_n$, appelé $n^{\text{ème}}$ **polynôme de Legendre**.

2) a) Etablir : $\forall (m,n) \in \mathbb{N}^2, (m \neq n \Longrightarrow < U_m,U_n > = 0)$.
(On pourra utiliser une intégration par parties).

b) Calculer $||U_n||$ pour tout n de $\mathbb{N}$.

c) Montrer : $\forall n \in \mathbb{N}, P_n = \dfrac{1}{2^n n!}\sqrt{\dfrac{2n+1}{2}}\, U_n$ **(formule de Rodrigues)** .

d) En déduire, pour tout n de $\mathbb{N}$, le coefficient dominant de P_n.

3) **Equation différentielle satisfaite par L_n**
Démontrer : $\forall n \in \mathbb{N},\ (1-X^2)L_n'' - 2XL_n' + n(n+1)L_n = 0$.
(On pourra, en notant $M_n = (X^2-1)^n$, remarquer $(X^2-1)M_n' = 2nXM_n$, puis prendre la dérivée $(n+1)$ ème).

4) **Relation de récurrence sur les L_n**

a) Démontrer : $\forall n \in \mathbb{N}^*$, $(n+1)L_{n+1} = (2n+1)XL_n - nL_{n-1}$.

(En notant c_k le coefficient dominant de L_k pour $k \in \mathbb{N}$, et $D_n = c_n L_{n+1} - c_{n+1} X L_n$, montrer que $\deg(D_n) \leqslant n$ et que D_n est orthogonal à $L_0, \ldots, L_{n-2}, L_n$.

Puis faire intervenir $R_{k-1} \in E$ tel que (pour $k = n-1, n$) $L_k = c_k X^k + R_{k-1}$ et $\deg(R_{k-1}) \leqslant k-1$).

b) En déduire L_n pour $n \in \{0, \ldots, 6\}$.

c) Calculer $L_n(1)$ et $L_n'(1)$ pour tout n de $\mathbb{N}$.

III Etude des zéros de L_n

1) **Formule de Christoffel et Darboux**

Démontrer : $\forall n \in \mathbb{N}$, $\forall (x,y) \in \mathbb{R}^2$,

$$(x-y)\sum_{k=0}^{n}(2k+1)L_k(x)L_k(y) = (n+1)\big(L_{n+1}(x)L_n(y) - L_n(x)L_{n+1}(y)\big).$$

2) Démontrer que, pour tout n de $\mathbb{N}^*$, L_n est scindé sur $\mathbb{R}$ et admet exactement n zéros deux à deux distincts et situés dans $]-1;1[$.

(Cette question est indépendante de *1)*).

On note $(\xi_{n,i})_{1 \leqslant i \leqslant n}$ les zéros de L_n, rangés de façon que :

$$-1 < \xi_{n,1} < \xi_{n,2} < \ldots < \xi_{n,n-1} < \xi_{n,n} < 1.$$

3) a) Déduire de *1)* : $\forall n \in \mathbb{N}$, $\forall x \in \mathbb{R}$,

$$\sum_{k=0}^{n}(2k+1)\big(L_k(x)\big)^2 = (n+1)\big(L_{n+1}'(x)L_n(x) - L_n'(x)L_{n+1}(x)\big).$$

b) On note $F_n = \dfrac{L_n}{L_{n+1}} \in \mathbb{R}(X)$, *pour* $n \in \mathbb{N}$.

Montrer que les coefficients de la décomposition en éléments simples de F_n (dans $\mathbb{R}(X)$) sont tous > 0. (Utiliser *2)* et *3) a)*).

4) **Entrelacement des zéros de L_{n-1} et L_n.**

Soit $n \in \mathbb{N} - \{0,1\}$. Etablir :

$$\xi_{n,1} < \xi_{n-1,1} < \xi_{n,2} < \xi_{n-1,2} < \ldots < \xi_{n-1,n-2} < \xi_{n,n-1} < \xi_{n-1,n-1} < \xi_{n,n}.$$

5) Soient $n \in \mathbb{N}^*$, $c \in \mathbb{R}$. Montrer que $L_n + cL_{n-1}$ est scindé sur $\mathbb{R}$ et à zéros tous simples.

Indications et réponses

Indications et réponses
pour les exercices du chapitre 1

1.1.1 *a)* $(p \iff q) \iff \begin{cases} p \implies q \\ q \implies p \end{cases} \iff \begin{cases} q \implies p \\ p \implies q \end{cases} \iff (q \iff p)$

b) $\begin{cases} \begin{cases} p \implies q \\ q \implies r \end{cases} \implies \begin{cases} p \implies r \\ r \implies p \end{cases} \implies (p \iff r), \ldots \\ r \implies p \end{cases}$

c) $\big(p \implies (q \implies r)\big) \iff \big(\neg p \text{ ou } (\neg q \text{ ou } r)\big) \iff \big((\neg p \text{ ou } \neg q) \text{ ou } r\big) \iff \big(\neg(p \text{ et } q) \text{ ou } r\big)$
$\iff \big((p \text{ et } q) \implies r\big)$.

d) $\big((p \text{ ou } q) \implies r\big) \iff \big(\neg(p \text{ ou } q) \text{ ou } r\big) \iff \big((\neg p \text{ et } \neg q) \text{ ou } r\big) \iff \big((\neg p \text{ ou } r) \text{ et } (\neg q \text{ ou } r)\big)$
$\iff \big((p \implies r) \text{ et } (q \implies r)\big)$.

1.1.2 *a)* Immédiat.

b) $A \cap B = \big(A \cap B \cap (C \cup \overline{C})\big) = (A \cap B \cap C) \cup (A \cap B \cap \overline{C}) \subset (A \cap C) \cup (B \cap \overline{C})$.

c) $\implies$: $B \subset A \cup B = A \cap C \subset A$ et $A \subset A \cup B = A \cap C \subset C$

$\impliedby$: immédiat.

d) $\implies$: $B = (A \cup B) \cap B = (A \cup C) \cap B = (A \cap B) \cup (C \cap B) = (A \cap C) \cup (C \cap B) = (A \cup B) \cap C$
$= (A \cup C) \cap C = C$

$\impliedby$: évident.

e) $(A - B) \cup (A - C) = (A \cap \overline{B}) \cup (A \cap \overline{C}) = A \cap (\overline{B} \cup \overline{C}) = A \cap (\overline{B \cap C}) = A - (B \cap C)$.

f) $(A - B) - (A - C) = (A \cap \overline{B}) \cap \overline{A \cap \overline{C}} = A \cap \overline{B} \cap (\overline{A} \cup C) = (A \cap B \cap \overline{A}) \cup (A \cap \overline{B} \cap C)$
$= A \cap \overline{B} \cap C = (A - B) \cap C = (A \cap C) - B$.

g) $\implies$: $A = A \cap (C \cup \overline{C}) = (A \cap C) \cup (A \cap \overline{C}) \subset (B \cap C) \cup (B \cap \overline{C}) = B \cap (C \cup \overline{C}) = B$

$\impliedby$: évident.

h) $A \cup (B \cap (A \cup C)) = (A \cup B) \cap (A \cup C) = A \cup (B \cap C)$.

i) Analogue à *h)*.

j) $\big(A \cup (B \cap C)\big) \cap \big(A \cup (B \cap D)\big) = A \cup \big((B \cap C) \cap (B \cap D)\big) = A \cup (B \cap C \cap D) = A \cup (B \cap A \cap B) = A$.

k) $A = A \cap (C \cup D) \subset A \cap (C \cup B) = (A \cap C) \cup (A \cap B) = C \cup (C \cap D) = C$.

1.1.3 $X' = X' \cap E = X' \cap (X \cup Y \cup Z) = (X' \cap X) \cup (X' \cap Y) \cup (X' \cap Z) \subset X \cup (X' \cap Y') \cup (X' \cap Z')$
$= X \cup (X \cap Y) \cup (X \cap Z) = X$.

1.1.4 ◇ **Réponses :**

a) $\varnothing$ si $A \not\subset B$, $\{(B - A) \cup Y;\ Y \in \mathfrak{P}(A)\}$ si $A \subset B$

b) $\varnothing$ si $B \not\subset A$, $\{B \cup Y;\ Y \in \mathfrak{P}(\complement_E(A))\}$ si $B \subset A$

c) $\varnothing$ si $A \cap B \neq \varnothing$, $\{B \cup Y;\ Y \in \mathfrak{P}(A)\}$ si $A \cap B = \varnothing$

d) $\{A \triangle B\}$.

1.1.5 *a)* • Soit $A \in \mathcal{A}$. Pour tout x de A, on a $x \in F$ (par définition de F), donc $A \in \mathfrak{P}(F)$. Ceci prouve : $\mathcal{A} \subset \mathfrak{P}(F)$.

- $(\forall A \in \mathcal{A},\ A \neq \varnothing)$ car $\mathcal{P}$ est une partition de E.
- $(\forall (A,B) \in \mathcal{A}^2, (A \neq B \Longrightarrow A \cap B = \varnothing))$ car $\mathcal{P}$ est une partition de E.
- $(\forall x \in F,\ \exists A \in \mathcal{A},\ x \in A)$ par définition de F.

Ceci montre que $\mathcal{A}$ est une partition de F. En échangeant $(\mathcal{A}, F)$ et $(\mathcal{B}, G)$, on conclut que $\mathcal{B}$ est une partition de G.

b) • Soit $x \in F \cap G$. Il existe $A \in \mathcal{A}$, $B \in \mathcal{B}$ tels que $x \in A$ et $x \in B$. Comme $\mathcal{P}$ est une partition de E, on a alors $A = B$, d'où $\mathcal{A} \cap \mathcal{B} \neq \varnothing$, contradiction. Donc $F \cap G = \varnothing$.

• Soit $x \in E$. Il existe $P \in \mathcal{P}$ tel que $x \in P$. Comme $\mathcal{P} = \mathcal{A} \cup \mathcal{B}$, on a ($P \in \mathcal{A}$ ou $P \in \mathcal{B}$), d'où, par définition de F et G : $x \in F$ ou $x \in G$. Ceci montre : $F \cup G = E$.

1.1.6 • $\forall i \in \{1, \ldots, n\}$, $B_i \neq \varnothing$.

• Soient $i, j \in \{1, \ldots, n\}$ tels que $i < j$. On a : $B_i \subset A_i$ et $B_j = A_j - A_{j-1} \subset A_j - A_i$, donc $B_i \cap B_j = \varnothing$.

• Soit $x \in E$. Il existe $i \in \{1, \ldots, n\}$ tel que $x \in A_i$ et $x \notin A_{i-1}$, d'où $x \in B_i$.

1.2.1 • $x\mathcal{R}y \Longrightarrow \begin{cases} x\mathcal{R}y \\ y\mathcal{R}y \end{cases} \Longrightarrow y\mathcal{R}x.$

• $\begin{cases} x\mathcal{R}y \\ y\mathcal{R}z \end{cases} \Longrightarrow z\mathcal{R}x \Longrightarrow x\mathcal{R}z.$

1.2.2 • $\mathcal{S}$ est réflexive car $\mathcal{R}$ l'est.

• $\mathcal{S}$ est à l'évidence symétrique.

• $\begin{cases} x\mathcal{S}y \\ y\mathcal{S}z \end{cases} \Longrightarrow \begin{cases} x\mathcal{R}y \text{ et } y\mathcal{R}x \\ y\mathcal{R}z \text{ et } z\mathcal{R}y \end{cases} \Longrightarrow \begin{cases} x\mathcal{R}z \\ z\mathcal{R}x \end{cases} \Longrightarrow x\mathcal{S}z.$

1.2.3 *a)* Remarquer : $\forall (x,y) \in \mathbb{R}^2, (x\mathcal{R}y \Longleftrightarrow f(x) = f(y))$, où $f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 - x \end{array}$.

b) ◇ **Réponse :** $\mathrm{cl}_{\mathcal{R}}(x) = \begin{cases} \{x, 1-x\} & \text{si } x \neq \dfrac{1}{2} \\ \dfrac{1}{2} & \text{si } x = \dfrac{1}{2} \end{cases}$.

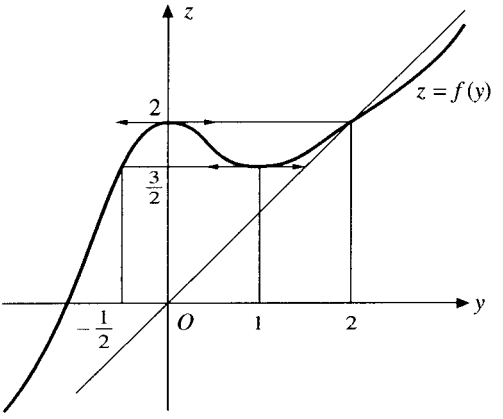
1.2.4 *a)* Remarquer : $\forall (x,y) \in \mathbb{R}^2$, $(x \mathcal{R} y \iff f(x) = f(y))$, où $f : \mathbb{R} \longrightarrow \mathbb{R}$, $x \longmapsto \dfrac{x^3+2}{x^2+1}$.

b) Etudier les variations de f :

f est dérivable sur $\mathbb{R}$ et :

$$\forall y \in \mathbb{R},\ f'(y) = \frac{y(y-1)(y^2+y+4)}{(y^2+1)^2}.$$

y	$-\infty$		0		1		$+\infty$
$f'(y)$		$+$	0	$-$	0	$+$	
$f(y)$	$-\infty$	$\nearrow$	2	$\searrow$	$\frac{3}{2}$	$\nearrow$	$+\infty$



Pour tout x de $\mathbb{R}$, on a : $\mathrm{cl}_{\mathcal{R}}(x) = \{y \in \mathbb{R};\ f(y) = f(x)\}$; étudier l'intersection de la courbe représentative de f avec l'horizontale d'ordonnée $f(x)$.

◇ **Réponse :** Le nombre d'éléments de $\mathrm{cl}_{\mathcal{R}}(x)$ est :

$$\begin{cases} 1 & \text{si } x \in \left]-\infty; -\frac{1}{2}\right[\cup]2; +\infty[\\ 2 & \text{si } x \in \{-\frac{1}{2}, 0, 1, 2\} \\ 3 & \text{si } x \in \left]-\frac{1}{2}; 0\right[\cup]0; 1[\cup]1; 2[. \end{cases}$$

1.2.5 ◇ **Réponse :**

	Ensemble des majorants dans E	Ensembles des éléments maximaux	borne supérieure	plus grand élément
A	$\{5\}$	$\{2, 3\}$	5	n'existe pas
B	$\varnothing$	$\{2, 4\}$	n'existe pas	n'existe pas
C	$\{5\}$	$\{5\}$	5	5

1.2.6 *a)* $\mathrm{Sup}_E(B)$ est un majorant de B donc de A (dans E) et $\mathrm{Sup}_E(A)$ est le plus petit majorant de A dans E, d'où : $\mathrm{Sup}_E(A) \leqslant \mathrm{Sup}_E(B)$.

b) ◇ **Réponse :**

1) $E = \mathbb{R}$, $\leqslant$ usuel, $A = \mathbb{R}_-$, $B = \mathbb{R}$

2) $E = \mathbb{Q}$, $\leqslant$ usuel, $A = \{x \in \mathbb{Q};\ x^2 < 2\}$, $B = \{x \in \mathbb{Q};\ x \leqslant 2\}$

3) $E = \mathbb{R}$, $\leqslant$ usuel, $A = \{x \in \mathbb{Q};\ x^2 < 2\}$, $B = A \cup \{2\}$.

1.2.7 *a)* Immédiat.

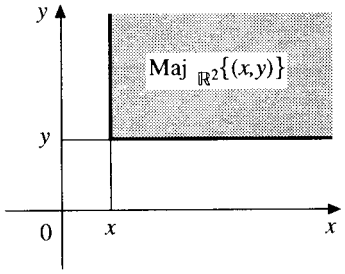
b) α) ◇ **Réponse :**
$\mathrm{Maj}_{\mathbb{R}^2}\{(x,y)\} = [x;\infty[\times[y;+\infty[$.

β) $\mathcal{P}$ n'est pas total dans $\mathbb{R}^2$ car $(1,0)$ et $(0,1)$ ne sont pas comparables.

γ) ◇ **Réponse :** $\{(x,y)\in\mathbb{R}^2;\ x+y=0\}$.

δ) $\mathrm{Maj}_{\mathbb{R}^2}(\mathbb{R}_-^*)^2 = (\mathbb{R}_+)^2$ et $(\mathbb{R}_+)^2$ admet $(0,0)$ pour plus petit élément.

◇ **Réponse :** $(\mathbb{R}_-^*)^2$ admet une borne supérieure dans $\mathbb{R}^2$, qui est $(0,0)$.



1.2.8 *a)* • La réflexivité est immédiate.

• Soient $(x,y),(x',y')\in E\times F$ tels que $\begin{cases}(x,y)\mathcal{L}(x',y')\\(x',y')\mathcal{L}(x,y)\end{cases}$, c'est-à-dire :

$$\begin{vmatrix} x\prec x' & (1)\\ \text{ou} & \\ (x=x' \text{ et } y\preccurlyeq y') & (2)\end{vmatrix} \quad\text{et}\quad \begin{vmatrix} x'\prec x & (3)\\ \text{ou} & \\ (x'=x \text{ et } y'\preccurlyeq y) & (4)\end{vmatrix}.$$

Seuls les cas (2) et (4) sont non-contradictoires. D'où $(x,y)=(x',y')$.

Ceci montre que $\mathcal{L}$ est antisymétrique.

• Soient $(x,y),(x',y'),(x'',y'')\in E\times F$ tels que : $\begin{cases}(x,y)\mathcal{L}(x',y')\\(x',y')\mathcal{L}(x'',y'')\end{cases}$. On a alors :

$$\begin{vmatrix} x\prec x' & (1)\\ \text{ou} & \\ (x=x' \text{ et } y\preccurlyeq y') & (2)\end{vmatrix} \quad\text{et}\quad \begin{vmatrix} x'\prec x'' & (3)\\ \text{ou} & \\ (x'=x'' \text{ et } y'\preccurlyeq y'') & (4)\end{vmatrix}.$$

Les conditions ((1) et (3)), ((1) et (4)), ((2) et (3)) entraînent $x\prec x''$, et donc $(x,y)\mathcal{L}(x'',y'')$.

Enfin : $\begin{cases}(2)\\(4)\end{cases}\Longrightarrow\begin{cases}x=x''\\y\preccurlyeq y''\end{cases}\Longrightarrow(x,y)\mathcal{L}(x'',y'')$. Ainsi, $\mathcal{L}$ est transitive.

b) Soient $(x,y),(x',y')\in E\times F$.

Comme $\preccurlyeq$ est total dans E, on a : $x\prec x'$ ou $x=x'$ ou $x'\prec x$.

Si $x\prec x'$, alors $(x,y)\mathcal{L}(x',y')$.

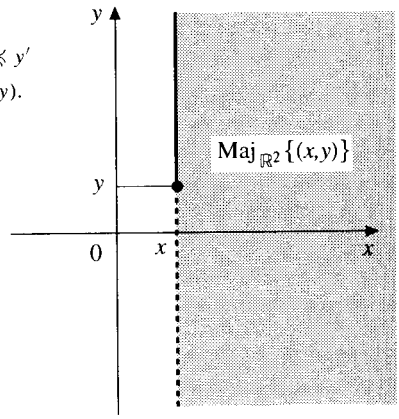
Si $x'\prec x$, alors $(x',y')\mathcal{L}(x,y)$.

Si $x=x'$, comme $\preccurlyeq$ est total dans F, on a $y\preccurlyeq y'$ ou $y'\preccurlyeq y$, d'où $(x,y)\mathcal{L}(x',y')$ ou $(x',y')\mathcal{L}(x,y)$.

c) α) ◇ **Réponse :** $\mathrm{Maj}_{\mathbb{R}^2}[(x,y)] = (\{x\}\times[y;+\infty[)\cup(]x;\infty[\times\mathbb{R})$.

β) $\mathrm{Maj}_{\mathbb{R}^2}(\mathbb{R}_-^*\times\mathbb{R}) = \mathbb{R}_+\times\mathbb{R}$, et $\mathbb{R}_+\times\mathbb{R}$ n'a pas de plus petit élément pour $\mathcal{L}$.

◇ **Réponse :** $\mathbb{R}_-^*\times\mathbb{R}$ n'admet pas de borne supérieure dans $\mathbb{R}^2$ pour $\mathcal{L}$.



1.3.1 Les preuves sont immédiates. Par exemple, pour *6)* :

$$\varphi_{A\cup B} = 1 - \varphi_{\overline{A\cup B}} = 1 - \varphi_{\overline{A}\cap\overline{B}} = 1 - (1-\varphi_A)(1-\varphi_B) = \varphi_A + \varphi_B - \varphi_A\varphi_B.$$

1.3.2 *a)* La réflexivité, l'antisymétrie, la transitivité sont immédiates.

b) ◇ **Réponse :** • Les éléments maximaux de $\mathcal{U}$ pour $\mathcal{R}$ sont les (E,f) où $f \in F^E$.

• Les éléments minimaux de $\mathcal{U}$ pour $\mathcal{R}$ sont les $(\{x\},f)$ où $x \in E$ et $f \in F^{\{x\}}$.

1.3.3 $(g' \circ f') \circ u = g' \circ (f' \circ u) = g' \circ (v \circ f) = (g' \circ v) \circ f = (w \circ g) \circ f = w \circ (g \circ f)$.

1.3.4 *a) 1)* Supposons qu'il existe $h : F \longrightarrow G$ telle que $h \circ f = g$. On a, pour tout (x,x') de E^2 :

$$f(x) = f(x') \Longrightarrow h(f(x)) = h(f(x')) \Longrightarrow g(x) = g(x').$$

2) Réciproquement, supposons : $\forall (x,x') \in E^2, \quad (f(x) = f(x') \Longrightarrow g(x) = g(x'))$.

Soit $y \in F$.

• Si y n'a pas d'antécédent par f, on note $h(y) = e$ où e est n'importe quel élément fixé de G.

• Si y admet au moins un antécédent x par f, on note $h(y) = g(x)$, ce qui est correct car si y admet au moins deux antécédents x,x' par f, alors $g(x) = g(x')$.

On a ainsi défini une application $h : F \longrightarrow G$ qui vérifie : $\forall x \in E,\ h(f(x)) = g(x)$, c'est-à-dire $h \circ f = g$.

b) 1) Supposons qu'il existe $f : E \longrightarrow F$ telle que $h \circ f = g$. On a alors : $\forall x \in E, g(x) = h(f(x))$, et donc : $\forall x \in E, \exists y \in F, g(x) = h(y)$.

2) Réciproquement, supposons : $\forall x \in E, \exists y \in F, g(x) = h(y)$. Soit $x \in E$.

Par hypothèse, il existe $y \in F$ tel que $g(x) = h(y)$. Considérons l'application $f : \begin{matrix} E \longrightarrow F \\ x \longmapsto y \end{matrix}$, où y est un élément tel que $g(x) = h(y)$. (Cette construction utilise l'«axiome du choix»).

On a ainsi défini une application $f : E \longrightarrow F$ qui vérifie : $\forall x \in E,\ g(x) = h(f(x))$, c'est-à-dire : $h \circ f = g$.

1.3.5 • $f \circ g \circ f$ bijective $\Longrightarrow \begin{cases} f\circ g\circ f & \text{injective} \\ f\circ g\circ f & \text{surjective} \end{cases} \Longrightarrow \begin{cases} f & \text{injective} \\ f & \text{surjective} \end{cases} \Longrightarrow f$ bijective

(cf. 1.3.2 Prop. 2 p. 27)

• Puis : $g = f^{-1} \circ (f \circ g \circ f) \circ f^{-1}$.

1.3.6 *a)* $\begin{cases} g\circ f & \text{injective} \\ f & \text{surjective} \end{cases} \Longrightarrow \begin{cases} f & \text{injective} \\ f & \text{surjective} \end{cases} \Longrightarrow f$ bijective, puis $g = (g \circ f) \circ f^{-1}$

est injective.

b) $\begin{cases} g\circ f & \text{surjective} \\ g & \text{injective} \end{cases} \Longrightarrow \begin{cases} g & \text{surjective} \\ g & \text{injective} \end{cases} \Longrightarrow g$ bijective, puis $f = g^{-1} \circ (g \circ f)$ est surjective.

1.3.7 *a)* En appliquant l'exercice 1.3.4 *a)* p. 26 à E,F,E,f,Id_E au lieu de E,F,G,f,g, on obtient : f est injective si et seulement s'il existe $h : F \longrightarrow E$ telle que $h \circ f = \mathrm{Id}_E$. De plus, si $h \circ f = \mathrm{Id}_E$, alors h est surjective (cf. 1.3.2 Prop. 2 p. 27).

b) En appliquant l'exercice 1.3.4 *b)* p. 26 à F,E,F,Id_F,f au lieu de E,F,G,g,h, on obtient : f est surjective si et seulement s'il existe $g : F \longrightarrow E$ telle que $f \circ g = \mathrm{Id}_F$. De plus, si $f \circ g = \mathrm{Id}_F$, alors g est injective (cf. 1.3.2 Prop. 2 p. 27).

1.3.8 Résulte de l'exercice 1.3.7 p. 29.

1.3.9 *a)* ◇ **Réponse :** • f est injective, non surjective.

• g est surjective, non injective.

b) ◇ **Réponse :** $g \circ f = \mathrm{Id}_{\mathbb{N}}$, $f \circ g : \mathbb{N} \longrightarrow \mathbb{N}$, $x \longmapsto \begin{cases} x & \text{si } x \text{ est pair} \\ x-1 & \text{si } x \text{ est impair} \end{cases}$

1.3.10 *a)* Immédiat.

b) Les applications : $\varphi : E/\mathcal{R} \times F/\mathcal{S} \longrightarrow (E \times F)/\mathcal{T}$, $\big(\mathrm{cl}_{\mathcal{R}}(x), \mathrm{cl}_{\mathcal{S}}(y)\big) \longmapsto \mathrm{cl}_{\mathcal{T}}(x,y)$ et $\psi : (E \times F)/\mathcal{T} \longrightarrow E/\mathcal{R} \times F/\mathcal{S}$, $\mathrm{cl}_{\mathcal{T}}(x,y) \longmapsto \big(\mathrm{cl}_{\mathcal{R}}(x), \mathrm{cl}_{\mathcal{S}}(y)\big)$ sont correctement définies car, pour tous (x,y), (x',y') de $E \times F$:

$$\big(\mathrm{cl}_{\mathcal{R}}(x), \mathrm{cl}_{\mathcal{S}}(y)\big) = \big(\mathrm{cl}_{\mathcal{R}}(x'), \mathrm{cl}_{\mathcal{S}}(y')\big) \Longleftrightarrow \begin{cases} \mathrm{cl}_{\mathcal{R}}(x) = \mathrm{cl}_{\mathcal{R}}(x') \\ \mathrm{cl}_{\mathcal{S}}(y) = \mathrm{cl}_{\mathcal{S}}(y') \end{cases} \Longleftrightarrow \begin{cases} x \mathcal{R} x' \\ y \mathcal{S} y' \end{cases} \Longleftrightarrow (x,y)\mathcal{T}(x',y')$$
$$\Longleftrightarrow \mathrm{cl}_{\mathcal{T}}(x,y) = \mathrm{cl}_{\mathcal{T}}(x',y').$$

Clairement : $\psi \circ \varphi = \mathrm{Id}_{E/\mathcal{R} \times F/\mathcal{S}}$ et $\varphi \circ \psi = \mathrm{Id}_{(E \times F)/\mathcal{T}}$. D'après 1.3.2 Prop. 5 p. 28, on conclut que φ et ψ sont des bijections réciproques l'une de l'autre.

1.3.11 *a) 1)* Pour tout f de E, $f \mathcal{R} f$ car $\mathrm{Id}_{\mathbb{R}} \circ f = f \circ \mathrm{Id}_{\mathbb{R}}$.

2) Soit $(f,g) \in E^2$ tel que $f \mathcal{R} g$; il existe $\varphi \in E$ bijective telle que $\varphi \circ f = g \circ \varphi$. Alors $\varphi^{-1} \in E$, φ^{-1} est bijective, et :

$$\varphi^{-1} \circ g = \varphi^{-1} \circ (g \circ \varphi) \circ \varphi^{-1} = \varphi^{-1} \circ (\varphi \circ f) \circ \varphi^{-1} = f \circ \varphi^{-1}, \quad \text{et donc } g \mathcal{R} f.$$

3) Soit $(f,g,h) \in E^3$ tel que $f \mathcal{R} g$ et $g \mathcal{R} h$; il existe $\varphi, \psi \in E$, bijectives, telles que :

$$\varphi \circ f = g \circ \varphi \quad \text{et} \quad \psi \circ g = h \circ \psi.$$

Alors $\psi \circ \varphi \in E$, $\psi \circ \varphi$ est bijective, et :

$$(\psi \circ \varphi) \circ f = \psi \circ (\varphi \circ f) = \psi \circ (g \circ \varphi) = (\psi \circ g) \circ \varphi = (h \circ \psi) \circ \varphi = h \circ (\psi \circ \varphi),$$

d'où $f \mathcal{R} h$.

b) 1) Si ch$\mathcal{R}$sh, il existe $\varphi \in E$ bijective telle que $\varphi \circ \mathrm{ch} = \mathrm{sh} \circ \varphi$; alors $\mathrm{ch} = \varphi^{-1} \circ \mathrm{sh} \circ \varphi$, donc ch est bijective, contradiction.

2) Supposons cos$\mathcal{R}$sin. Il existe une bijection $\varphi : \mathbb{R} \longrightarrow \mathbb{R}$ telle que $\varphi \circ \cos = \sin \circ \varphi$, c'est-à-dire : $\forall x \in \mathbb{R}$, $\varphi(\cos x) = \sin(\varphi(x))$. On a : $\begin{cases} \varphi(1) = \varphi(\cos 0) = \sin(\varphi(0)) \in [-1\,;\,1] \\ \varphi(-1) = \varphi(\cos \pi) = \sin(\varphi(\pi)) \in [-1\,;\,1] \\ \sin(\varphi(1)) = \varphi(\cos 1) = \varphi(\cos(-1)) = \sin(\varphi(-1)), \end{cases}$

d'où $\varphi(1) = \varphi(-1)$, contradiction avec la bijectivité de φ.

◇ **Réponse :** ch $\not\mathcal{R}$ sh et cos $\not\mathcal{R}$ sin.

c) 1) Supposons $f \mathcal{R} g$. Il existe $\varphi : \mathbb{R} \longrightarrow \mathbb{R}$ bijective telle que $\varphi \circ f = g \circ \varphi$.

Considérons $\psi : \mathbb{R} \longrightarrow \mathbb{R}$, $x \longmapsto \varphi(x) + \dfrac{p}{2}$, qui est à l'évidence bijective. On a, pour tout x de $\mathbb{R}$:

$$\psi(x^2) = \varphi(f(x)) + \frac{p}{2} = g(\varphi(x)) + \frac{p}{2} = (\varphi(x))^2 + p\varphi(x) + q + \frac{p}{2} = (\psi(x))^2 + C,$$

où $C = \dfrac{p}{2} - \dfrac{p^2}{4} + q$.

On a donc : $\forall x \in \mathbb{R}, (\psi(-x))^2 = \psi(x^2) - C = (\psi(x))^2$, d'où : $\forall x \in \mathbb{R}, \psi(-x) = \left|\begin{array}{l}\psi(x)\\ \text{ou}\\ -\psi(x)\end{array}\right.$

Soit $x \in \mathbb{R}^*$; comme $x \neq -x$ et que ψ est bijective, on a alors $\psi(-x) = -\psi(x)$ et $\psi(x) \neq 0$. Il en résulte $\psi(0) = 0$ et $C = \psi(0^2) - (\psi(0))^2 = 0$.

2) Réciproquement, si $\dfrac{p}{2} - \dfrac{p^2}{4} + q = 0$, l'application $\varphi : \begin{array}{ccc}\mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & -\dfrac{p}{2}\end{array}$ est bijective et vérifie :

$\varphi \circ f = g \circ \varphi$.

◇ **Réponse :** $f : \begin{array}{ccc}\mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2\end{array}$ et $g : \begin{array}{ccc}\mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2+px+q\end{array}$ sont équivalentes si et seulement si $\dfrac{p}{2} - \dfrac{p^2}{4} + q = 0$.

1.3.12 *1)* • La réflexivité est évidente.

• $\left\{\begin{array}{l}x\mathcal{R}y\\ y\mathcal{R}x\end{array}\right. \Longrightarrow \left\{\begin{array}{l}f(x) \preccurlyeq f(y)\\ f(y) \preccurlyeq f(x)\end{array}\right. \Longrightarrow f(x) = f(y) \Longrightarrow x = y.$

• $\left\{\begin{array}{l}x\mathcal{R}y\\ y\mathcal{R}z\end{array}\right. \Longrightarrow \left\{\begin{array}{l}f(x) \preccurlyeq f(y)\\ f(y) \preccurlyeq f(z)\end{array}\right. \Longrightarrow f(x) \preccurlyeq f(z) \Longrightarrow x\mathcal{R}z.$

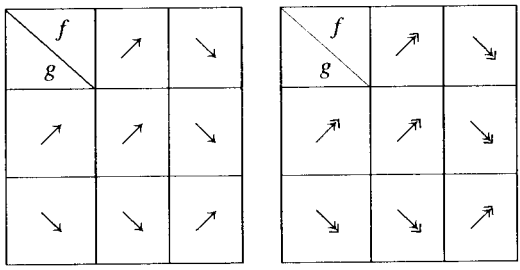
1.3.13 *a)* ◇ **Réponse :**

↗ signifie : croissante

↘ signifie : décroissante

↗̸ signifie : strictement croissante

↘̸ signifie : strictement décroissante.



b) ◇ **Réponse :** $E = F = \{0,1\}$, $=$ dans E, $\leqslant$ usuel dans F, $f = \mathrm{Id}_E$.

c) Soit $(x,x') \in E^2$ tel que $x \prec x'$. Puisque f est croissante et injective : $f(x) \preccurlyeq f(x')$ et $f(x) \neq f(x')$, d'où $f(x) \prec f(x')$.

d) Soit $(x,x') \in E^2$ tel que $f(x) = f(x')$. Puisque $\preccurlyeq$ est total dans E, on a : $x \prec x'$ ou $x' \prec x$ ou $x = x'$. Si $x \prec x'$ (resp. $x' \prec x$), alors, comme f est strictement croissante, $f(x) \prec f(x')$ (resp. $f(x') \prec f(x)$), contradiction. Donc $x = x'$.

1.3.14 *1)* (i) $\Longrightarrow$ (ii) :

• En remplaçant Y par X : $f(X) \supset f(f(X)) \cup f(X) \cup X$, d'où $f(X) \supset X$ et $f(X) \supset f(f(X))$. En remplaçant X par $f(X)$ dans $f(X) \supset X$, on obtient $f(f(X)) \supset f(X)$, et donc $f(f(X)) = f(X)$.

• Si $X \subset Y$, alors : $f(Y) = f(X \cup Y) \supset f(f(X)) \cup f(Y) \cup Y \supset f(f(X)) = f(X)$.

2) (ii) $\Longrightarrow$ (i) :

$\left\{\begin{array}{l}X \subset X \cup Y\\ Y \subset X \cup Y\end{array}\right.$ d'où $\left\{\begin{array}{l}f(X) \subset f(X \cup Y)\\ f(Y) \subset f(X \cup Y)\end{array}\right.$, puis $f(X \cup Y) \supset f(X) \cup f(Y) = f(f(X)) \cup f(Y) \cup Y$.

1.3.15 *a)* • $\forall x \in A, (f \circ g)(f(x)) = f((g \circ f)(x)) = f(x)$, donc : $\forall x \in A, f(x) \in B$.

De même : $\forall y \in B, g(y) \in A$.

Ceci permet de définir les applications $f' : \begin{array}{ccc} A & \longrightarrow & B \\ x & \longmapsto & f(x) \end{array}$ et $g' : \begin{array}{ccc} B & \longrightarrow & A \\ y & \longmapsto & g(y) \end{array}$.

b) 1) Soit $(a,a') \in A^2$ tel que $a \prec a'$.

Puisque f est croissante : $f(a) \preccurlyeq f(a')$, et donc $f'(a) \preccurlyeq f'(a')$.

Si $f'(a) = f'(a')$, alors : $a = (g \circ f)(a) = g(f'(a)) = g(f'(a')) = (g \circ f)(a') = a'$, contradiction.

Ceci montre : $\forall (a,a') \in A^2, (a \prec a' \Longrightarrow f'(a) \prec f'(a'))$, c'est-à-dire : f' est strictement croissante.
De même, g' est strictement croissante.

2) $\forall a \in A, (g' \circ f')(a) = g'(f'(a)) = g(f(a)) = (g \circ f)(a) = a$, donc $g' \circ f' = \mathrm{Id}_A$.

De même, $f' \circ g' = \mathrm{Id}_B$.

D'après 1.3.2 Prop. 5 p. 28, f' et g' sont des bijections réciproques l'une de l'autre.

1.3.16 Puisque $f \circ g = \mathrm{Id}_F$, f est surjective (cf. 1.3.2 Prop. 2 p. 27), d'où $f(E) = F$, puis $(g \circ f)(E) = g(f(E)) = g(F)$.

1.3.17 *1)* Soit $y \in f(f^{-1}(A'))$; il existe $x \in f^{-1}(A')$ tel que $y = f(x)$. Alors $y \in A'$ et $y \in f(E)$, d'où $y \in A' \cap f(E)$.

2) Réciproquement, soit $y \in A' \cap f(E)$. Puisque $y \in f(E)$, il existe $x \in E$ tel que $y = f(x)$. Comme $y = f(x) \in A'$, on a : $x \in f^{-1}(A')$, et donc $y = f(x) \in f(f^{-1}(A'))$.

1.3.18 *1)* Supposons f bijective.

• Soit $y \in f(\complement_E(A))$; il existe $x \in \complement_E(A)$ tel que $y = f(x)$.

Si $y \in f(A)$, alors il existe $a \in A$ tel que $y = f(a)$, d'où $f(x) = f(a)$ avec $x \neq a$, contradiction (f est bijective). Donc $y \in \complement_{E'}(f(A))$.

Ceci montre : $f(\complement_E(A)) \subset \complement_{E'}(f(A))$.

• Soit $y \in \complement_{E'}(f(A))$. Comme f est bijective, il existe $x \in E$ tel que $y = f(x)$.

Si $x \in A$, alors $y = f(x) \in f(A)$, contradiction. Donc $x \in \complement_E(A)$, puis $y = f(x) \in f(\complement_E(A))$.

Ceci montre : $\complement_{E'}(f(A)) \subset f(\complement_E(A))$.

2) Réciproquement, supposons : $\forall A \in \mathfrak{P}(E), f(\complement_E(A)) = \complement_{E'}(f(A))$.

• En particulier : $f(E) = f(\complement_E(\varnothing)) = \complement_{E'}(f(\varnothing)) = \complement_{E'}(\varnothing) = E'$, donc f est surjective.

• Soit $(x,y) \in E^2$ tel que $f(x) = f(y)$. Si $y \neq x$, alors $f(x) = f(y) \in f(\complement_E\{x\}) = \complement_{E'}(f(\{x\})) = \complement_{E'}\{f(x)\}$, contradiction, donc $x = y$. Ceci montre que f est injective.

1.3.19 (i) $\Longrightarrow$ (ii) :

• Soit $y \in E'$. Il existe $x \in E$ tel que $y = f(x)$, d'où $x \in f^{-1}(\{y\})$, puis $y = f(x) \in f(f^{-1}(\{y\}))$.

Ceci montre : $\{y\} \subset f(f^{-1}(\{y\}))$.

• L'inclusion $f(f^{-1}(\{y\})) \subset \{y\}$ est connue (cf. 1.3.5 Prop. *3)* p. 33).

(ii) $\Longrightarrow$ (iii) :

Soit $A' \in \mathfrak{P}(E)$.

• L'inclusion $f(f^{-1}(A')) \subset A'$ est connue (cf. 1.3.5 Prop. *3)* p. 33).

• Soit $y \in A'$. Puisque $f(f^{-1}(\{y\})) = \{y\}$, il existe $x \in f^{-1}(\{y\})$ tel que $y = f(x)$. Alors $y = f(x)$ et $x \in f^{-1}(A')$, donc $y \in f(f(^{-1}(A'))$, ce qui montre : $A' \subset f(f^{-1}(A'))$.

(iii) $\Longrightarrow$ (iv) :

Soit $A' \in \mathfrak{P}(E')$ telle que $f^{-1}(A') = \varnothing$. Alors : $A' = f(f^{-1}(A')) = f(\varnothing) = \varnothing$.

(iv) $\Longrightarrow$ (i) :

Soit $y \in F$; comme $\{y\} \neq \varnothing$, on a $f^{-1}(\{y\}) \neq \varnothing$, et donc il existe $x \in E$ tel que $y = f(x)$.

1.3.20 *a)* D'après 1.3.5 Prop. p. 33, on a :

$$f^{-1}(A'_{\triangle}B') = f^{-1}\big((A' \cap \overline{B'}) \cup (\overline{A'} \cap B')\big) = \big(f^{-1}(A') \cap \overline{f^{-1}(B')}\big) \cup \big(\overline{f^{-1}(A')} \cap f^{-1}(B')\big)$$
$$= f^{-1}(A')_{\triangle} f^{-1}(B').$$

b) 1) Supposons f injective et soit $(A,B) \in (\mathfrak{P}(E))^2$.

α) $f(A_{\triangle}B) = f\big((A \cap \overline{B}) \cup (\overline{A} \cap B)\big) = f(A \cap \overline{B}) \cup f(\overline{A} \cap B) \subset \big(f(A) \cap f(\overline{B})\big) \cup \big(f(\overline{A}) \cap f(B)\big)$.

Montrons $f(\overline{B}) \subset \overline{f(B)}$.

Soit $y \in f(\overline{B})$. Si $y \in f(B)$, il existe $b \in B$ et $c \in \overline{B}$ tels que $y = f(b) = f(c)$, contradiction avec l'injectivité de f. Donc $y \in \overline{f(B)}$.

De même : $f(\overline{A}) \subset \overline{f(A)}$.

Alors : $f(A_{\triangle}B) \subset \big(f(A) \cap \overline{f(B)}\big) \cup \big(\overline{f(A)} \cap f(B)\big) = f(A)_{\triangle} f(B)$.

β) Soit $y \in f(A) \cap \overline{f(B)}$.

Il existe $a \in A$ tel que $y = f(a)$.

Si $a \in B$, alors $y = f(a) \in f(B)$, contradiction. Donc $a \notin B$, $y = f(a) \in f(A \cap \overline{B})$.

Ceci montre : $f(A) \cap \overline{f(B)} \subset f(A \cap \overline{B})$.

De même : $\overline{f(A)} \cap f(B) \subset f(\overline{A} \cap B)$. D'où :

$$f(A)_{\triangle} f(B) = \big(f(A) \cap \overline{f(B)}\big) \cup \big(\overline{f(A)} \cap f(B)\big) \subset f(A \cap \overline{B}) \cup f(\overline{A} \cap B)$$
$$= f\big((A \cap \overline{B}) \cup (\overline{A} \cap B)\big) = f(A_{\triangle}B).$$

2) Réciproquement, supposons : $\forall (A,B) \in (\mathfrak{P}(E))^2$, $f(A_{\triangle}B) = f(A)_{\triangle} f(B)$.

Soit $(x,y) \in E^2$ tel que $f(x) = f(y)$.

Si $x \neq y$, alors : $\begin{cases} f(\{x\}_{\triangle}\{y\}) = f(\{x,y\}) = \{f(x)\} \neq \varnothing \\ f(\{x\})_{\triangle} f(\{y\}) = \{f(x)\}_{\triangle}\{f(x)\} = \varnothing \end{cases}$, contradiction. Donc $x = y$.

Ceci montre que f est injective.

1.3.21 ◇ **Réponse :** Toute partie non vide $\mathcal{G}$ de $\mathcal{F}$ admet une borne supérieure et une borne inférieure dans $\mathcal{F}$ pour l'inclusion, qui sont respectivement $\{x \in E;\ \exists X \in \mathcal{G},\ x \in X\}$ et $\{x \in E;\ \forall X \in \mathcal{G},\ x \in X\}$, c'est-à-dire, avec les notations de 1.3.6 p. 34, $\bigcup_{X \in \mathcal{G}} X$ et $\bigcap_{X \in \mathcal{G}} X$.

1.3.22 *a)* • $x \in \complement_E\left(\bigcup_{i \in I} A_i\right) \Longleftrightarrow \text{non}(\exists i \in I,\ x \in A_i) \Longleftrightarrow \big(\forall i \in I,\ x \in \complement_E(A_i)\big)$

$\Longleftrightarrow x \in \bigcap_{i \in I} \complement_E(A_i)$.

• De même pour l'autre relation.

b) • $x \in \left(\bigcup_{i\in I} A_i\right) \cap B \iff \begin{cases} \exists i \in I, x \in A_i \\ x \in B \end{cases} \iff (\exists i \in I, x \in A_i \cap B) \iff x \in \bigcup_{i\in I}(A_i \cap B).$

• De même pour l'autre relation.

c) • $x \in \left(\bigcup_{i\in I} A_i\right) \cap \left(\bigcup_{j\in J} B_j\right) \iff \begin{cases} \exists i \in I, x \in A_i \\ \exists j \in J, x \in B_j \end{cases} \iff \big(\exists (i,j) \in I \times J, x \in A_i \cap B_j\big)$

$$\iff x \in \bigcup_{(i,j)\in I\times J} A_i \cap B_j$$

• $x \in \left(\bigcap_{i\in I} A_i\right) \cup \left(\bigcap_{j\in J} B_j\right) \iff \begin{vmatrix} \forall i \in I, x \in A_i \\ \text{ou} \\ \forall j \in J, x \in B_j \end{vmatrix} \iff \big(\forall (i,j) \in I \times J, x \in A_i \cup B_j\big)$

$$\iff x \in \bigcap_{(i,j)\in I\times J} (A_i \cup B_j).$$

La question *c)* est une généralisation de *b)*.

d) Immédiat.

e) $\bigcap_{i\in I}(A_i - B_i) = \bigcap_{i\in I}\big(A_i \cap \complement_E(B_i)\big) = \left(\bigcap_{i\in I} A_i\right) \cap \left(\bigcap_{i\in I} \complement_E(B_i)\right) = \left(\bigcap_{i\in I} A_i\right) \cap \complement_E \left(\bigcup_{i\in I} B_i\right)$

$$= \left(\bigcap_{i\in I} A_i\right) - \left(\bigcup_{i\in I} B_i\right).$$

1.3.23 *a)* • Pour tout x de E :

$$x \in f^{-1}\left(\bigcup_{i\in I} A'_i\right) \iff \left(f(x) \in \bigcup_{i\in I} A'_i\right) \iff \big(\exists i \in I, f(x) \in A'_i\big) \iff \big(\exists i \in I, x \in f^{-1}(A'_i)\big)$$

$$\iff x \in \bigcup_{i\in I} f^{-1}(A'_i).$$

• De même pour l'autre relation.

b) Pour tout y de E' :

• $y \in f\left(\bigcup_{i\in I} A_i\right) \iff \left(\exists x \in \bigcup_{i\in I} A_i, y = f(x)\right) \iff \big(\exists i \in I, \exists x \in A_i, y = f(x)\big)$

$$\iff \big(\exists i \in I, y \in f(A_i)\big) \iff y \in \bigcup_{i\in I} f(A_i).$$

• $y \in f\left(\bigcap_{i\in I} A_i\right) \iff \left(\exists x \in \bigcap_{i\in I} A_i, y = f(x)\right) \iff \left(\exists x \in E, \begin{cases} y = f(x) \\ \forall i \in I, x \in A_i \end{cases}\right)$

$$\implies \big(\forall i \in I, \exists x \in A_i, y = f(x)\big) \iff \big(\forall i \in I, y \in f(A_i)\big) \iff y \in \bigcap_{i\in I} f(A_i).$$

Les questions *a), b)* généralisent des résultats vus en 1.3.5 p. 33.

c) Supposons f injective.

Soit $y \in \bigcap_{i\in I} f(A_i)$. Pour chaque i de I, il existe $a_i \in A_i$ tel que $y = f(a_i)$.

Comme f est injective, on a : $\forall (i,j) \in I^2, a_i = a_j$.

Il existe donc $a \in E$ tel que : $\forall i \in I, a_i = a$. Alors $y = f(a) \in f\left(\bigcap_{i\in I} A_i\right)$.

1.3.24 *a)* α) $(g \circ f)(A) = g(f(A)) \subset g(A) \subset A$.

β) Immédiat à partir de α).

γ) $A \supset f(A) \supset f^2(A) \supset \ldots \supset f^n(A) = A$,

donc $A = f(A) = f^2(A) = \ldots = f^n(A)$.

b) D'après l'exercice 1.3.23 *b)* p. 35 : $\begin{cases} f\left(\bigcup\limits_{i\in I} A_i\right) = \bigcup\limits_{i\in I} f(A_i) \subset \bigcup\limits_{i\in I} A_i \\ f\left(\bigcap\limits_{i\in I} A_i\right) \subset \bigcap\limits_{i\in I} f(A_i) \subset \bigcap\limits_{i\in I} A_i. \end{cases}$

1.3.25 *a)* • Soit $i \in I$. Puisque $A'_i \neq \varnothing$ et que f est surjective, on a $f^{-1}(A'_i) \neq \varnothing$.

• Soit $(i,j) \in I^2$ tel que $f^{-1}(A'_i) \cap f^{-1}(A'_j) \neq \varnothing$.

Alors $f^{-1}(A'_i \cap A'_j) = f^{-1}(A'_i) \cap f^{-1}(A'_j) \neq \varnothing$, donc $A'_i \cap A'_j \neq \varnothing$, $i = j$.

• Soit $x \in E$. Il existe $i \in I$ tel que $f(x) \in A'_i$, d'où $x \in f^{-1}(A'_i)$.

Ceci montre que $(f^{-1}(A'_i))_{i\in I}$ est une partition de E.

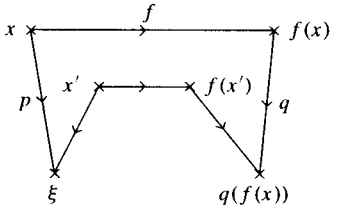
b) ◇ **Réponse :** $E = \{0,1\}$, $E' = \{0\}$, $f : \begin{array}{ccc} E & \longrightarrow & E' \\ x & \longmapsto & 0 \end{array}$, $(A_i)_{i\in I} = (\{0\},\{1\})$.

C.1.1 *A* *1)* α) Supposons que f soit compatible avec $\mathcal{R}$ et $\mathcal{S}$.

Existence

Soit $\xi \in E/\mathcal{R}$; il existe $x \in E$ tel que $\xi = p(x)$. On définit $\varphi(\xi)$ par : $\varphi(\xi) = q(f(x))$, ce qui est correct car, si x' est un (autre) élément de E tel que $\xi = p(x')$, alors $x\mathcal{R}x'$, donc $f(x)\mathcal{S}f(x')$, c'est-à-dire $q(f(x)) = q(f(x'))$.

Autrement dit, tous les éléments de ξ ont la même image par $q \circ f$.



Par construction : $\forall x \in E, \varphi(p(x)) = q(f(x))$, c'est-à-dire : $\varphi \circ p = q \circ f$.

Unicité

Soient $\varphi, \psi : E/\mathcal{R} \longrightarrow F/\mathcal{S}$ telles que $\varphi \circ p = q \circ f$ et $\psi \circ p = q \circ f$.

On a alors : $\forall x \in E, \varphi(p(x)) = \psi(p(x))$, d'où, puisque p est surjective : $\forall \xi \in E/\mathcal{R}, \varphi(\xi) = \psi(\xi)$.

β) Réciproquement, supposons qu'il existe $\varphi : E/\mathcal{R} \longrightarrow F/\mathcal{S}$ telle que $\varphi \circ p = q \circ f$.

On a, pour tout (x,x') de E^2 :

$$x\mathcal{R}x' \Longleftrightarrow p(x) = p(x') \Longrightarrow \varphi(p(x)) = \varphi(p(x')) \Longleftrightarrow q(f(x)) = q(f(x')) \Longleftrightarrow f(x)\mathcal{S}f(x').$$

Ainsi, f est compatible avec $\mathcal{R}$ et $\mathcal{S}$.

2) a) • $\forall (x,x') \in E^2, \big(x\mathcal{R}x' \Longrightarrow f(x)\mathcal{S}f(x') \Longrightarrow g(f(x))\mathcal{T}g(f(x'))\big)$, donc $g \circ f$ est compatible avec $\mathcal{R}$ et $\mathcal{T}$.

• L'application $\widetilde{g} \circ \widetilde{f} : E/\mathcal{R} \longrightarrow G/\mathcal{T}$ vérifie :

$$(\widetilde{g} \circ \widetilde{f}) \circ p = \widetilde{g} \circ (\widetilde{f} \circ p) = \widetilde{g} \circ (q \circ f) = (\widetilde{g} \circ q) \circ f = (r \circ g) \circ f = r \circ (g \circ f),$$

où $r : G \longrightarrow G/\mathcal{T}$ est la surjection canonique. Par unicité de $\widetilde{g \circ f}$, on conclut : $\widetilde{g} \circ \widetilde{f} = \widetilde{g \circ f}$.

b) Immédiat.

B *1) a)* Réflexivité, symétrie, transitivité sont immédiates.

b) **Existence**

Soit $\xi \in E/\mathcal{R}_f$; il existe $x \in E$ tel que $\xi = p(x)$. On définit $\widehat{f}(\xi)$ par : $\widehat{f}(\xi) = f(x)$, ce qui est correct car, si x' est un (autre) élément de ξ, alors $x\mathcal{R}_f x'$, donc $f(x) = f(x')$.

L'application $\widehat{f} : E/\mathcal{R}_f \longrightarrow f(E)$ ainsi définie vérifie $f = i \circ \widehat{f} \circ p$, puisque :

$$\forall x \in E, \quad (i \circ \widehat{f} \circ p)(x) = \widehat{f}(p(x)) = f(x).$$

• Soit $(\xi,\xi') \in (E/\mathcal{R}_f)^2$ tel que $\widehat{f}(\xi) = \widehat{f}(\xi')$.

Il existe $(x,x') \in E^2$ tel que : $\xi = p(x)$, $\xi' = p(x')$.

On a : $f(x) = \widehat{f}(\xi) = \widehat{f}(\xi') = f(x')$, donc $x\mathcal{R}_f x'$, $\xi = \xi'$.

Ceci montre que $\widehat{f}$ est injective.

• Pour tout y de $f(E)$, il existe $x \in E$ tel que $y = f(x)$, et on a, par définition de $\widehat{f}$: $\widehat{f}(p(x)) = f(x) = y$.

Ceci montre que $\widehat{f}$ est surjective.

Unicité

Soient $\varphi_1,\varphi_2 : E/\mathcal{R}_f \longrightarrow f(E)$ telles que : $f = i \circ \varphi_1 \circ p$ et $f = i \circ \varphi_2 \circ p$.

On a alors : $\forall x \in E, \varphi_1(p(x)) = \varphi_2(p(x))$, et donc, puisque p est surjective : $\varphi_1 = \varphi_2$.

Remarque : En notant $q : F \longrightarrow F/_{=}$ la surjection canonique, on a : $q \circ i \circ \widehat{f} = \widetilde{f}$. On aurait pu déduire le théorème de décomposition canonique de la propriété de passage aux quotients (*A 1*)).

2) a) ◇ **Réponse :** $\mathrm{E} = i \circ \widehat{\mathrm{E}} \circ p$, où :

$$i : \underset{n}{\mathbb{Z}} \longrightarrow \underset{n}{\mathbb{R}}, \qquad \mathbb{R}/\mathcal{R}_{\mathrm{E}} = \{[n; n+1[; n \in \mathbb{Z}\},$$

$$p : \mathbb{R} \longrightarrow \mathbb{R}/\mathcal{R}_{\mathrm{E}}, \qquad \widehat{\mathrm{E}} : \mathbb{R}/\mathcal{R}_{\mathrm{E}} \longrightarrow \mathbb{Z}.$$
$$x \longmapsto [\mathrm{E}(x); \mathrm{E}(x)+1[\qquad [n; n+1[\longrightarrow n$$

b) ◇ **Réponse :**

$$\widehat{f} : \mathfrak{P}(E)/\mathcal{R}_f \longrightarrow \mathfrak{P}(A),$$
$$\mathrm{cl}_{\mathcal{R}_f}(X) = \{X' \in \mathfrak{P}(E);\ X' \cap A = X \cap A\} \longmapsto X \cap A$$

$$\widehat{g} : \mathfrak{P}(E)/\mathcal{R}_g \longrightarrow g(\mathfrak{P}(E)) = \{Y \in \mathfrak{P}(E);\ A \subset Y\}.$$
$$\mathrm{cl}_{\mathcal{R}_g}(X) = \{X' \in \mathfrak{P}(E);\ X' \cup A = X \cup A\} \longmapsto X \cup A$$

Remarque : L'application $\mathfrak{P}\big(\complement_E(A)\big) \longrightarrow g(\mathfrak{P}(E))$ est une bijection.
$$Y \longmapsto Y \cup A$$

Indications et réponses
pour les exercices du chapitre 2

2.1.1 *a)* La commutativité est évidente.
Comme $(-1 * 0) * 2 = 0 * 2 = -3$ et $(-1) * (0 * 2) = (-1) * (-3) = 3$, $*$ n'est pas associative.
Il est clair que 1 est neutre.

b) ◇ **Réponse :** *1)* $\left\{-2, \frac{4}{3}\right\}$ *2)* $\{-1,0,1\}$.

2.1.2 $a * (b * c) = (0 * (-a)) * (b * c) = (0 * (0 * a)) * (b * c) = (a * (0 * 0)) * (b * c)$
$= (a * 0) * (b * c) = c * (b * (a * 0)) = c * (0 * (a * b)) = (a * b) * (0 * c) = (a * b) * (-c)$.
Un exemple : $* = -$.

2.1.3 $(x \top y) \top z = (x * a * y) * a * z = x * a * (y * a * z) = x \top (y \top z)$.

2.1.4 *1)* Montrons, par récurrence sur n : $\forall n \in \mathbb{N}^*, x^n y = y x^n$.

- $n = 1$: $xy = yx$ par hypothèse.
- Si $x^n y = y x^n$, alors : $x^{n+1} y = x(x^n y) = x(y x^n) = (xy)x^n = (yx)x^n = y x^{n+1}$.

2) En appliquant le résultat précédent à (p, y, x^n) au lieu de (n, x, y), on conclut : $y^p x^n = x^n y^p$.

2.1.5 *1)* Si $x \in E$ est symétrisable pour $*$, alors, pour tout (y,z) de E^2 :

$$x * y = x * z \Longrightarrow x^{-1} * (x * y) = x^{-1} * (x * z) \Longrightarrow (x^{-1} * x) * y = (x^{-1} * x) * z \Longrightarrow y = z,$$

et donc x est régulier à gauche. De même, x est régulier à droite.

2) Dans $(\mathbb{N}, +)$, 1 est régulier mais n'est pas symétrisable.

2.1.6 *a)* γ_a est injective si et seulement si : $\forall (x,y) \in E^2, (a * x = a * y \Longrightarrow x = y)$, c'est-à-dire si et seulement si a est régulier à gauche.

b) $\big(\forall (a,b,c) \in E^3, \quad (a * x) * b = a * (x * b)\big)$
$\Longleftrightarrow \forall (a,b) \in E^2, \forall x \in E, \delta_b(\gamma_a(x)) = \gamma_a(\delta_b(x)) \Longleftrightarrow \forall (a,b) \in E^2, \delta_b \circ \gamma_a = \gamma_a \circ \delta_b$.

2.1.7 Notons $\gamma_x : \begin{matrix} E \longrightarrow E \\ y \longmapsto x*y \end{matrix}$ et $\delta_x : \begin{matrix} E \longrightarrow E \\ y \longmapsto y*x \end{matrix}$.

Puisque x est régulier, γ_x et δ_x sont injectives (cf. exercice 2.1.6 *a)*). Comme E est fini, il en résulte (cf. aussi plus loin 3.2.2 Prop. 6 p. 000) que γ_x et δ_x sont bijectives.

• Il existe donc $(a,b) \in E^2$ tel que $\gamma_x(a) = x$ et $\delta_x(b) = x$, c'est-à-dire : $x*a = x$ et $b*x = x$.

On a : $\forall y \in E, x*(a*y) = (x*a)*y = x*y$ et donc, puisque x est régulier : $\forall y \in E \quad a*y = y$.

De même : $\forall y \in E \quad y*b = y$.

Ainsi, a est neutre à gauche et b neutre à droite; alors : $a*b = b$ et $a*b = a$, donc en notant $e = a = b$, e est neutre.

• Il existe $(x',x'') \in E^2$ tel que $\gamma_x(x') = e$ et $\delta_x(x'') = e$, c'est-à-dire : $x*x' = e$ et $x''*x = e$.

On a : $x' = (x''*x)*x' = x''*(x*x') = x''$, et donc x est symétrisable.

2.1.8 *a)* $(x*y)*(x*y) = (x*(y*x))*y = (x*(x*y))*y = (x*x)*(y*y) = x*y$.

b) $x^{-1}*x^{-1} = (x*x)^{-1} = x^{-1}$ (cf. 2.1 Prop. 4 p. 42).

D'ailleurs : $x = x*(x*x^{-1}) = (x*x)*x^{-1} = x*x^{-1} = e$.

2.1.9 *a)* $(x*y)\top(x'*y') = \big(x\top(x'*y')\big)*\big(y\top(x'*y')\big) = (x\top x')*(x\top y')*(y\top x')*(y\top y')$

et $(x*y)\top(x'*y') = \big((x*y)\top x'\big)*\big((x*y)\top y'\big) = (x\top x')*(y\top x')*(x\top y')*(y\top y')$,

d'où, puisque $x\top x'$ et $y\top y'$ sont réguliers pour $*$:

$$(x\top y')*(y\top x') = (y\top x')*(x\top y').$$

b) En notant ε le neutre de $\top$, le résultat de *a)*, appliqué à $(x,y,\varepsilon,\varepsilon)$ au lieu de (x,y,x',y') montre que $x\top\varepsilon$ et $y\top\varepsilon$ sont permutables pour $*$, c'est-à-dire : $x*y = y*x$.

c) Conséquence évidente de *b)*.

2.1.10 *a)* L'application $f : \begin{matrix}]0;+\infty[\longrightarrow]0;+\infty[\\ x \longmapsto x^2 \end{matrix}$ est un isomorphisme de magmas de $(]0;+\infty[,*)$ sur $(]0;+\infty[,+)$.

◇ **Réponse :** $*$ est associative, commutative, et n'admet pas de neutre.

b) $f(a*\ldots*a) = f(a)+\ldots+f(a) = na^2$, donc $a*\ldots*a = f^{-1}(na^2) = \sqrt{n}\,a$.

◇ **Réponse :** $\sqrt{n}\,a$.

2.1.11 *a)* L'application $f : \begin{matrix} \mathbb{R} \longrightarrow \mathbb{R} \\ x \longmapsto 1-x \end{matrix}$ est un isomorphisme de magmas de $(\mathbb{R},*)$ sur $(\mathbb{R},\cdot)$.

◇ **Réponse :** $*$ est associative, commutative, admet 0 pour neutre. Tout élément x de $\mathbb{R}-\{1\}$ admet un symétrique pour $*$, qui est $\mathrm{sym}(x) = \dfrac{x}{x-1}$; 1 n'admet pas de symétrique pour $*$.

b) ◇ **Réponse :** $1-(1-a)^n$.

2.1.12 *a)* $\forall (a,a') \in A^2,\ f(a) \top f(a') = f(a * a') \in f(A)$.

b) $\forall (x,x') \in (f^{-1}(B))^2,\ f(x * x') = f(x) \top f(x') \in B$.

2.1.13 *1)* Pour tout x de X : $\big((f * g) * h\big)(x) = (f * g)(x) * h(x) = \big(f(x) * g(x)\big) * h(x)$
$= f(x) * \big(g(x) * h(x)\big) = f(x) * (g * h)(x) = \big(f * (g * h)\big)(x)$.

2) Pour tout x de X : $(g * f)(x) = g(x) * f(x) = f(x) * g(x) = (f * g)(x)$.

3) En notant e le neutre de E pour $*$, l'application constante $e : \begin{array}{ccc} X & \longrightarrow & E \\ x & \longmapsto & e \end{array}$ est neutre pour $*$ dans E^X.

4) Pour $f \in E^X$, l'application $\begin{array}{ccc} X & \longrightarrow & E \\ x & \longmapsto & (f(x))^{-1} \end{array}$ est symétrique de f pour $*$.

2.1.14 *a) 1)* Evident.

2) • Soit $x \in (A * B) * C$. Il existe $(a,b,c) \in E^3$ tel que $x = (a * b) * c$. Alors : $x = a * (b * c) \in A * (B * C)$. Ceci prouve l'inclusion $(A * B) * C \subset A * (B * C)$. L'autre inclusion se prouve de la même façon.

• Même démarche pour la commutativité.

3) Evident.

b) Prenons $E = \mathbb{R}$, $* = +$, $A = \{0,1\}$. Il n'existe pas de partie B de $\mathbb{R}$ telle que $A + B = \{0\}$.

◊ **Réponse :** non.

2.1.15

- $(a * x) * (a * y) = a * (x * a * y) \in \{a\} * E$
- $(x * b) * (y * b) = (x * b * y) * b \in E * \{b\}$
- $(a * x * b) * (a * y * b) = a * (x * b * a * y) * b \in \{a\} * E * \{b\}$
- $(x * a * y) * (x' * a * y') = x * a * (y * x' * a * y') \in E * \{a\} * E$.

2.1.16 *a) 1)* $B \subset B \cup C$ et $C \subset B \cup C$ donc (cf. exercice 2.1.14 *a) 1)*) :

$$A * B \subset A * (B \cup C) \quad \text{et} \quad A * C \subset A * (B \cup C),$$

d'où : $(A * B) \cup (A * C) \subset A * (B \cup C)$.

2) Soit $x \in A * (B \cup C)$. Il existe $(a,y) \in A \times (B \cup C)$ tel que $x = a * y$.
Si $y \in B$ (resp. C), alors $x \in A * B$ (resp. $A * C$). Donc $x \in (A * B) \cup (A * C)$.

◊ **Réponse :** $A * (B \cup C) = (A * B) \cup (A * C)$.

b) 1) $B \cap C \subset B$ et $B \cap C \subset C$ donc (cf. exercice 2.1.14 *a) 1)*) :

$$A * (B \cap C) \subset A * B \quad \text{et} \quad A * (B \cap C) \subset A * C,$$

d'où : $A * (B \cap C) \subset (A * B) \cap (A * C)$.

2) L'inclusion réciproque peut être fausse, comme le montre l'exemple :

$$E = \mathbb{R}, * = +, A = \mathbb{R}_+, B = \mathbb{R}_+, C = \mathbb{R}_-^*,$$

dans lequel on a : $A * (B \cap C) = \varnothing$ et $(A * B) \cap (A * C) = \mathbb{R}_+$.

◊ **Réponse :** $A * (B \cap C) \subset (A * B) \cap (A * C)$.

2.1.17 Soit $(x,a) \in E \times A$; supposons $x * a \notin A$ (c'est-à-dire : $x * a$ est régulier pour $*$).
Alors pour tout (y,z) de E^2 :

$$a * y = a * z \Longrightarrow x * (a * y) = x * (a * z) \Longrightarrow (x * a) * y = (x * a) * z \Longrightarrow y = z,$$

et donc a est régulier à gauche.
De même, a est régulier à droite, et donc a est régulier, contradiction.

2.1.18 *a)* $\forall (a,b,c,d) \in A^4$, $(a * b) * (c * d) \in A * A$.

b) Soit $(x,y) \in (A^c)^2$, on a :

$$\forall a \in A,\ (x * y) * a = x * (y * a) = x * (a * y) = (x * a) * y = (a * x) * y = a * (x * y),$$

et donc $x * y \in A^c$.

2.1.19 *a)* Soit $(a,a') \in A^2$; on a; pour tout (y,z) de E^2 :

$$\big((a * a') * y\big) * z = \big(a * (a' * y)\big) * z = a * \big((a' * y) * z\big) = a * \big(a' * (y * z)\big) = (a * a') * (y * z),$$

et donc $a * a' \in A$.

b) $\forall (x,y,z) \in A^3$, $(x * y) * z = x * (y * z)$ car $x \in A$ et $(y,z) \in E^2$.

2.1.20 *a)* Soit $(a,a') \in C^2$; on a, pour tout x de E :

$$(a * a') * x = a * (a' * x) = a * (x * a') = (a * x) * a' = (x * a) * a' = x * (a * a'),$$

et donc $a * a' \in C$.
On peut aussi remarquer $C = E^c$ (cf. exercice 2.1.18).

b) $\forall (a,b) \in C^2$, $a * b = b * a$ (car $a \in C$ et $b \in E$).

2.1.21 *1)* $\big((x,y) * (x',y')\big) * (x'',y'') = (x \top x', y \perp y') * (x'',y'') = \big((x \top x') \top x'', (y \perp y') \perp y''\big)$
$= \big(x \top (x' \top x''), y \perp (y' \perp y'')\big) = (x,y) * (x' \top x'', y' \perp y'') = (x,y) * \big((x',y') * (x'',y'')\big)$.

2) $(x',y') * (x,y) = (x' \top x, y' \perp y) = (x \top x', y \perp y') = (x,y) * (x',y')$.

3) Si e (resp. ε) est neutre pour $\top$ (resp. $\perp$), alors (e,ε) est neutre pour $*$ car :

$$\forall (x,y) \in E \times F, \quad \begin{cases} (x,y) * (e,\varepsilon) = (x \top e, y \perp \varepsilon) = (x,y) \\ (e,\varepsilon) * (x,y) = (e \top x, \varepsilon \perp y) = (x,y) \end{cases}.$$

4) Si x (resp. y) admet un symétrique x' (resp. y') pour $\top$ (resp. $\perp$), alors (x,y) admet (x',y') pour symétrique pour $*$ car :

$$\begin{cases} (x,y) * (x',y') = (x \top x', y \perp y') = (e,\varepsilon) \\ (x',y') * (x,y) = (x' \top x, y' \perp y) = (e,\varepsilon). \end{cases}$$

2.1.22 *a) 1)* Supposons f injective. On a, pour tout (g,h) de E^2 :

$$f \circ g = f \circ h \Longrightarrow \big(\forall x \in X, f(g(x)) = f(h(x))\big) \Longrightarrow \big(\forall x \in X, g(x) = h(x)\big) \Longrightarrow g = h,$$

et donc f est régulière à gauche pour $\circ$ dans E.

2) Réciproquement, supposons f régulière à gauche pour $\circ$ dans E. Soit $(x,x') \in X^2$ tel que $f(x) = f(x')$. Si $x \neq x'$, considérons $g : X \longrightarrow X$ définie par : $\begin{cases} g(x) = x', \quad g(x') = x \\ \forall t \in X - \{x,x'\}, \quad g(t) = t \end{cases}$.

On a alors $f \circ g = f = f \circ \mathrm{Id}_X$, donc $g = \mathrm{Id}_X$, $x = x'$, contradiction.

Donc $x = x'$.

b) 1) Supposons f surjective. Soient $(g,h) \in E^2$ tel que $g \circ f = h \circ f$, et $y \in X$. Il existe $x \in X$ tel que $y = f(x)$; on a : $g(y) = g(f(x)) = h(f(x)) = h(y)$.

Ceci prouve $g = h$, et donc f est régulière à droite pour $\circ$ dans E.

2) Réciproquement supposons f régulière à droite pour $\circ$ dans E. Raisonnons par l'absurde : supposons f non surjective. Il existe alors $\beta \in X$ tel que $\beta \notin f(X)$. Considérons $g : X \longrightarrow X$ définie par : $g(t) = \begin{cases} t & \text{si } t \in f(X) \\ f(\beta) & \text{si } t \notin f(X) \end{cases}$.

On a : $\forall x \in X$, $(g \circ f)(x) = g(f(x)) = f(x)$,

donc : $g \circ f = f = \mathrm{Id}_X \circ f$,

d'où : $g = \mathrm{Id}_X$.

En particulier : $\beta = g(\beta)$.

Mais $\beta \notin f(X)$, donc $g(\beta) = f(\beta)$.

Ainsi : $\beta = f(\beta) \in f(X)$, contradiction.

2.1.23 *a)* • $\begin{cases} a * b \leqslant b \\ a * b \leqslant a \end{cases}$, donc $a * b \leqslant b * a$

• $\begin{cases} b * a \leqslant a \\ b * a \leqslant b \end{cases}$, donc $b * a \leqslant a * b$.

b) • $a * a \leqslant a$

• $\begin{cases} a \leqslant a \\ a \leqslant a \end{cases}$, donc $a \leqslant a * a$.

c) $\begin{cases} a * c \leqslant a \leqslant b \\ a * c \leqslant c \end{cases} \Longrightarrow a * c \leqslant b * c$.

d) $\begin{cases} a \leqslant b \\ c \leqslant d \end{cases} \Longrightarrow \begin{cases} a * c \leqslant b * c \\ c * b \leqslant d * b \end{cases} \Longrightarrow a * c \leqslant b * d$.

e) • $\begin{cases} b * c \leqslant b \Longrightarrow a * (b * c) \leqslant a * b \\ a * (b * c) \leqslant b * c \leqslant c \end{cases}$ donc $a * (b * c) \leqslant (a * b) * c$.

• $\begin{cases} a * b \leqslant b \Longrightarrow (a * b) * c \leqslant b * c \\ (a * b) * c \leqslant a * b \leqslant a \end{cases}$ donc $(a * b) * c \leqslant a * (b * c)$.

2.2.1 Soit $(x,y) \in G^2$. On a : $\begin{cases} (xy)^2 = (xy)(xy) = x(yx)y \\ (xy)^2 = xy = x^2y^2 = x(xy)y \end{cases}$, d'où, puisque x et y sont réguliers : $yx = xy$.

2.2.2 Soit $x \in G$; pour montrer qu'il existe $(a,b) \in A \times B$ tel que $x = ab$, ce qui revient à $a^{-1}x = b$, nous allons montrer que les parties $A^{-1}x$ (définie par $A^{-1}x = \{a^{-1}x;\ a \in A\}$) et B de G ne sont pas disjointes.

Puisque $a \longmapsto a^{-1}x$ est une bijection de A sur $A^{-1}x$, on a $\mathrm{Card}(A^{-1}x) = \mathrm{Card}(A)$, et donc : $\mathrm{Card}(A^{-1}x) + \mathrm{Card}(B) = \mathrm{Card}(A) + \mathrm{Card}(B) > \mathrm{Card}(G)$. Il en résulte : $(A^{-1}x) \cap B \neq \varnothing$. Il existe donc $y \in (A^{-1}x) \cap B$, puis $a \in A$ tel que $y = a^{-1}x$. Alors : $x = ay \in AB$.

2.2.3 *a)* La réflexivité et la symétrie sont évidentes. Si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors ($y = x$ et $z = y$) ou ($y = x$ et $z = y^{-1}$) ou ($y = x^{-1}$ et $z = y$) ou ($y = x^{-1}$ et $z = y^{-1}$), d'où : $z = x$ ou $z = x^{-1}$.

b) $G/\mathcal{R}$ est formé de $\{e\}$, les singletons $\{x\}$ ($x \in S$) et les ensembles à deux éléments $\{x,x^{-1}\}$ ($x \in G - (S \cup \{e\})$). En notant $\alpha = \mathrm{Card}(S)$, $\beta = \mathrm{Card}(G - (S \cup \{e\}))$, on a donc : $1 + \alpha + 2\beta = \mathrm{Card}(G)$, et donc α et $\mathrm{Card}(G)$ sont de parités contraires.

2.2.4 *1)* Soient $(a,b), (c,d) \in \mathbb{R}^* \times \mathbb{R}$; on a : $\forall x \in \mathbb{R}, (f_{a,b} \circ f_{c,d})(x) = a(cx+d)+b = f_{ac,ad+b}(x)$, donc $f_{a,b} \circ f_{c,d} = f_{ac,ad+b}$, ce qui montre que $\circ$ est interne dans $\mathcal{A}$.

2) $f_{1,0} = \mathrm{Id}_{\mathbb{R}}$, neutre pour $\circ$.

3) $\circ$ est associative dans $\mathbb{R}^{\mathbb{R}}$, donc dans $\mathcal{A}$.

4) Tout élément $f_{a,b}$ de $\mathcal{A}$ admet un symétrique pour $\circ$, qui est $f_{\frac{1}{a},-\frac{b}{a}}$.

5) $f_{1,1} \circ f_{2,0} = f_{2,1}$, $f_{2,0} \circ f_{1,1} = f_{2,2}$, et $f_{2,1} \neq f_{2,2}$.

Voir aussi ex. 2.2.6 p. 451.

◇ **Réponse :** $(\mathcal{A}, \circ)$ est un groupe non commutatif.

2.2.5 *1)* Le sens $\Longleftarrow$ est évident.

2) Supposons $H \cup K = G$.

Raisonnons par l'absurde : supposons $H \neq G$ et $K \neq G$. Il existe $x \in G$ tel que $x \notin H$ et il existe $y \in G$ tel que $y \notin K$. Comme $H \cup K = G$, on a alors $x \in K$ et $y \in H$.

Considérons l'élément xy de G.

Comme $xy \in G = H \cup K$, on a : $xy \in H$ ou $xy \in K$.

Si $xy \in H$, alors $x = (xy)y^{-1} \in H$, contradiction.

Si $xy \in K$, alors $y = x^{-1}(xy) \in K$, contradiction.

2.2.6 *a) 1)* Il est clair que $*$ est interne dans G.

2) $\big((x,y) * (x',y')\big) * (x'',y'') = (xx',xy'+y) * (x'',y'') = (xx'x'',xx'y''+xy'+y)$

et $(x,y) * \big((x',y') * (x'',y'')\big) = (x,y) * (x'x'',x'y''+y') = (xx'x'',xx'y''+xy'+y)$,

donc $*$ est associative.

3) $(1,0)$ est neutre pour $*$

4) La résolution de $(x,y) * (x',y') = (x',y') * (x,y) = (1,0)$ montre que tout élément (x,y) de $\mathbb{R}^* \times \mathbb{R}$ admet un symétrique pour $*$, qui est $\left(\frac{1}{x}, -\frac{y}{x}\right)$.

5) $(1,1) * (2,0) = (2,1)$ et $(2,0) * (1,1) = (2,2)$, donc $*$ n'est pas commutative.

Remarque : On peut aussi utiliser un transfert de la structure de groupe (cf. 2.2.3 Prop. 3 p. 53) en remarquant que l'application $(x,y) \longmapsto f_{x,y}$ (définie dans l'exercice 2.2.4 p. 48) est un isomorphisme de magmas et que $\mathcal{A} = \{f_{x,y};\ (x,y) \in \mathbb{R}^* \times \mathbb{R}\}$ est un groupe.

b) Notons $H = \mathbb{R}_+^* \times \mathbb{R}$ $\quad (H \subset G)$.

1) $(1,0) \in H$

2) $\forall\big((x,y),(x',y')\big) \in H^2,\ (x,y) * (x',y') = (xx', xy' + y) \in H$ (car $xx' > 0$).

3) $\forall (x,y) \in H,\ (x,y)^{-1} = \left(\frac{1}{x}, -\frac{y}{x}\right) \in H$ (car $\frac{1}{x} > 0$).

2.2.7 *1)* $e \in C$.

2) Soit $(x,x') \in C^2$; on a : $\forall y \in G,\ (xx')y = x(x'y) = x(yx') = (xy)x' = (yx)x' = y(xx')$, donc $xx' \in G$ (cf. aussi exercice 2.1.20 *a)* p. 46).

3) Soit $x \in C$; on a, pour tout y de G : $\quad xy = yx \Longrightarrow x^{-1}(xy)x^{-1} = x^{-1}(yx)x^{-1} \Longrightarrow yx^{-1} = x^{-1}y$, et donc $x^{-1} \in C$.

2.2.8 *a)* Analogue à l'exercice 2.2.6 *a)* p. 402.

b) Soit $(a,b) \in G$, on a, pour tout (x,y) de G :

$$(a,b) * (x,y) = (x,y) * (a,b) \Longleftrightarrow ay + \frac{b}{x} = xb + \frac{y}{a} \Longleftrightarrow (a^2 - 1)xy + ab(1 - x^2) = 0.$$

Donc :

$$\big(\forall (x,y) \in G, (a,b) * (x,y) = (x,y) * (a,b)\big) \Longleftrightarrow \big(\forall (x,y) \in \mathbb{R}^* \times \mathbb{R}, (a^2 - 1)xy + ab(1 - x^2) = 0\big)$$
$$\Longleftrightarrow \begin{cases} a^2 - 1 = 0 \\ ab = 0 \end{cases} \Longleftrightarrow \left(\begin{cases} a = 1 \\ b = 0 \end{cases} \quad \text{ou} \quad \begin{cases} a = -1 \\ b = 0 \end{cases}\right).$$

◊ **Réponse :** $\{(1,0),(-1,0)\}$.

c) Les vérifications sont immédiates.

d) De même que pour *c)*, on montre facilement que H_k est un sous-groupe de G. De plus, pour tout (x,x') de $(\mathbb{R}^*)^2$:

$$\left(x, k\left(x - \frac{1}{x}\right)\right) * \left(x', k\left(x' - \frac{1}{x'}\right)\right) = \left(xx', k\left(xx' - \frac{1}{xx'}\right)\right) = \left(x', k\left(x' - \frac{1}{x'}\right)\right) * \left(x, k\left(x - \frac{1}{x}\right)\right).$$

2.2.9 *Raisonnement par l'absurde*

Supposons $H \neq G$. Il existe $x \in G$ tel que $x \notin H$. L'application $h \longmapsto hx$ est une bijection de H sur Hx (car x est symétrisable). On a donc :

$$\mathrm{Card}(Hx) + \mathrm{Card}(H) = 2\mathrm{Card}(H) > \mathrm{Card}(G).$$

Il en résulte $(Hx) \cap H \neq \varnothing$. Il existe donc $y \in (Hx) \cap H$, puis $z \in H$ tel que $y = zx$. On a alors $x = yz^{-1} \in H$, contradiction.

Comparer avec l'exercice 2.2.2 p. 48.

2.2.10 Les vérifications sont immédiates.

2.2.11 *1)* On a, pour tout x de $[0;1]$:

$$\begin{cases} x+\mathrm{i}x^2 \in G \\ (1-x)+\mathrm{i}(1-x)^2 \in G \end{cases} \Longrightarrow x+\mathrm{i}x^2-(1-x)-\mathrm{i}(1-x)^2 \in G \Longrightarrow (2x-1)(1+\mathrm{i}) \in G.$$

Comme $x \longmapsto 2x-1$ est une surjection de $[0;1]$ sur $[-1;1]$, il en résulte en particulier :

$$\forall t \in [0;1], \quad t+\mathrm{i}t = t(1+\mathrm{i}) \in G.$$

2) Soit $x \in [0;1]$; on a $x+\mathrm{i}x^2 \in G$ et $x^2+\mathrm{i}x^2 \in G$ (cf. *1)*), donc $x-x^2 \in G$.

Comme $x \longmapsto x-x^2$ est une surjection $[0;1]$ sur $\left[0;\frac{1}{4}\right]$, on déduit $\left[0;\frac{1}{4}\right] \subset G$.

Il est clair que : $\forall x \in \mathbb{R}, \exists n \in \mathbb{Z}, \exists u \in \left[0;\frac{1}{4}\right], x = nu$, d'où $\mathbb{R} \subset G$.

3) Soit $x \in [0;1]$; on a $x+\mathrm{i}x^2 \in G$ et $x+\mathrm{i}x \in G$ (cf. *1)*), d'où $\mathrm{i}(x-x^2) \in G$. Comme en *2)*, on déduit $\mathrm{i}\mathbb{R} \subset G$.

4) Enfin, puisque G est un sous-groupe de $\mathbb{C}$, on conclut $\mathbb{C} = \mathbb{R}+\mathrm{i}\mathbb{R} \subset G$.

2.2.12 *a)* • $e' = f(e) \in f(H)$.

• Si $(x',y') \in (f(H))^2$, il existe $(x,y) \in H^2$ tel que $x' = f(x)$, $y' = f(y)$, d'où : $x' \perp y' = f(x) \perp f(y) = f(x \top y) \in f(H)$, car $x \top y \in H$.

• Si $x' \in f(H)$, il existe $x \in H$ tel que $x' = f(x)$, d'où :
$x'^{-1} = (f(x))^{-1} = f(x^{-1}) \in f(H)$, car $x^{-1} \in H$.

b) • $f(e) = e' \in H'$, donc $e \in f^{-1}(H')$.

• Si $(x,y) \in \left(f^{-1}(H')\right)^2$, alors $f(x), f(y) \in H'$, d'où : $f(x \top y) = f(x) \perp f(y) \in H'$, donc $x \top y \in f^{-1}(H')$.

• Si $x \in f^{-1}(H')$, alors $f(x) \in H'$, d'où : $f(x^{-1}) = (f(x))^{-1} \in H'$, donc $x^{-1} \in f^{-1}(H')$.

2.2.13 Résulte de 2.1 Prop. 5 p. 43.

2.2.14 *1)* Supposons f injectif.

L'inclusion $\{e\} \subset \mathrm{Ker}(f)$ est triviale.

Soit $x \in \mathrm{Ker}(f)$; on a $f(x) = e' = f(e)$, donc $x = e$, et ainsi $\mathrm{Ker}(f) \subset \{e\}$.

2) Réciproquement, supposons $\mathrm{Ker}(f) = \{e\}$. Soit $(x_1,x_2) \in G^2$ tel que $f(x_1) = f(x_2)$. On a :

$$f(x_1x_2^{-1}) = f(x_1)\left(f(x_2)\right)^{-1} = f(x_1)\left(f(x_1)\right)^{-1} = e',$$

donc $x_1x_2^{-1} \in \mathrm{Ker}(f) = \{e\}$, d'où $x_1x_2^{-1} = e$, puis $x_1 = x_2$. Ceci montre que f est injective.

2.2.15 Raisonnement par l'absurde.

Supposons $f^2 \neq \mathrm{Id}_G$, et notons $A = \{x \in G;\ f(x) = x^{-1}\}$.

Il existe $x \in G$ tel que $f^2(x) \neq x$.

Si $x \in A$, alors $f^2(x) = f(f(x)) = f(x^{-1}) = (f(x))^{-1} = (x^{-1})^{-1} = x$, contradiction, donc $x \notin A$.

Montrons $xA \cap A = \varnothing$. Supposons qu'il existe $y \in xA \cap A$. Alors il existe $a \in A$ tel que $y = xa$, et : $f(y) = f(x)f(a)$, $f(y) = y^{-1}, f(a) = a^{-1}$, donc $f(x) = y^{-1}a$, puis $f^2(x) = f(y^{-1}a) = (f(y))^{-1}f(a) = ya^{-1} = (xa)a^{-1} = x$, contradiction.

Ceci montre $xA \cap A = \varnothing$.

D'autre part, $a \longmapsto xa$ est une bijection de A sur xA.

On en déduit : $\mathrm{Card}(G) \geqslant \mathrm{Card}(A) + \mathrm{Card}(xA) = 2\mathrm{Card}(A)$, contradiction.

On peut aussi se ramener à l'ex. 2.2.9 p. 51, en montrant que la partie B de G définie par

$B = \{x \in G;\ f^2(x) = x\}$ est un sous-groupe de G contenant A.

2.2.16 Soit $f : H \times K \longrightarrow HK$, qui est clairement surjective.
$(h,k) \longmapsto hk$

Soit $(h,k) \in H \times K$, nous allons montrer : $\mathrm{Card}\big(f^{-1}(\{hk\})\big) = \mathrm{Card}(H \cap K)$.

1) Soit $(h',k') \in H \times K$ tel que $f(h,k) = f(h',k')$. On a $kk'^{-1} = h^{-1}h'$, donc $h^{-1}h' \in H \cap K$, $h' \in h(H \cap K)$. Il existe $z \in H \cap K$ tel que $h' = hz$; puis $k' = h'^{-1}hk = z^{-1}k$.

2) Réciproquement, pour tout z de $H \cap K$: $hz \in H, z^{-1}k \in K$, et $f(hz,z^{-1}k) = (hz)(z^{-1}k) = hk$.

Ainsi, $H \cap K \longrightarrow f^{-1}(\{hk\})$ est une bijection.
$z \longmapsto (hz,z^{-1}k)$

En notant $\alpha = \mathrm{Card}(H \cap K)$, chaque élément de HK admet exactement α antécédents par f, d'où :

$$\mathrm{Card}(H)\mathrm{Card}(K) = \mathrm{Card}(H \times K) = \mathrm{Card}(HK)\mathrm{Card}(H \cap K).$$

Remarque : $H, K, H \cap K$ sont des sous-groupes de G, mais HK peut ne pas être un sous-groupe de G.

2.2.17 *1)* Soit $y \in G$. Puisque f est surjectif, il existe $z \in G$ tel que $y = z^3$.

Soit $x \in G$. Comme f est un morphisme, on a : $(xyx^{-1})^3 = x^3z^3x^{-3}$, d'où :

$$xyx^{-1} = xz^3x^{-1} = (xzx^{-1})^3 = x^3z^3x^{-3} = x^3yx^{-3}, \quad \text{donc } yx^2 = x^2y.$$

2) $x(yx)^2y = (xy)^3 = x^3y^3 = x(x^2y^2)y$, donc $(yx)^2 = x^2y^2 = (x^2y)y = (yx^2)y = (yx)(xy)$, d'où $yx = xy$.

2.2.18 Comme dans la solution de l'exercice 2.2.17 *1)*.

2.2.19 Il existe $a \in G$ tel que $G = < a >$.

Soit $x' \in G'$. Il existe $x \in G$ tel que $x' = f(x)$, puis il existe $n \in \mathbb{Z}$ tel que $x = a^n$. On a alors : $x' = f(x) = f(a^n) = (f(a))^n$, ce qui montre : $G' = < f(a) >$.

Si, de plus, G est fini, alors G' est fini puisque f est surjective.

2.2.20 Supposons qu'il existe un isomorphisme de groupes $f : (\mathbb{Q},+) \longrightarrow (\mathbb{Q}_+^*,\times)$.

Puisque $2 \in \mathbb{Q}_+^*$, en notant $\alpha = f^{-1}(2)$ et $\beta = \dfrac{\alpha}{2}$, on a : $2 = f(\alpha) = f(\beta + \beta) = (f(\beta))^2$.

Mais on sait que l'équation $x^2 = 2$ n'a pas de solution dans $\mathbb{Q}$ (cf. Tome 1, exercice 1.1.1 p. 1), contradiction.

2.2.21 Supposons qu'il existe un isomorphisme de groupes $f : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{C}^*, \times)$.
Puisque $i \in \mathbb{C}^*$, en notant $\alpha = f^{-1}(i)$, on a :

$$f(\alpha^2) = (f(\alpha))^2 = i^2 = -1 = f(-1)$$

(car $(f(-1))^2 = f((-1)^2) = f(1) = 1$, $f(1) = 1$, et $f(-1) \neq f(1)$),
et donc $\alpha^2 = -1$, contradiction ($\alpha \in \mathbb{R}$).

2.3.1 *a)* $x^2 = x$, $x^2 = (-x)^2 = -x$, d'où $2x = 0$.

b) $x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$, d'où $xy + yx = 0$, puis $xy = xy + 2yx = (xy + yx) + yx = yx$.

c) 1) Si $(x + y)z = 0$, alors $yz = -xz = xz$, d'où : $x(y + 1)z = xyz + xz = x^2z + xz = xz + xz = 0$ et $(x + 1)yz = xyz + yz = x^2z + xz = 0$.

2) Réciproquement, si $x(y + 1)z = (x + 1)yz = 0$, alors $xyz + xz = xyz + yz$, donc $xz = yz$, $(x + y)z = xz + yz = 2xz = 0$.

2.3.2 *a)* Montrer d'abord que C est un sous-groupe de $(A, +)$.
Soit $(x, y) \in A^2$; on a :

$$(x + y)^2 - (x + y) = (x^2 - x) + (y^2 - y) + (xy + yx),$$

d'où $xy + yx \in C$.

b) D'après *a)*, $x(xy + yx) = (xy + yx)x$, d'où $x^2y = yx^2$.
Mais aussi $(x^2 - x)y = y(x^2 - x)$ (car $x^2 - x \in C$), d'où $xy = yx$.

2.3.3 *a)* Il existe $(n, p) \in (\mathbb{N}^*)^2$ tel que $x^n = y^p = 0$. D'après la formule du binôme de Newton :

$$\begin{aligned}(x + y)^{n+p-1} &= \sum_{k=0}^{n+p-1} C_{n+p-1}^k x^k y^{n+p-1-k} \\ &= \left(\sum_{k=0}^{n-1} C_{n+p-1}^k x^k y^{n-1-k}\right) y^p + x^n \left(\sum_{k=n}^{n+p-1} C_{n+p-1}^k x^{k-n} y^{n+p-1-k}\right) = 0,\end{aligned}$$

et donc $x + y$ est nilpotent.

b) Si $x^n = 0$, alors $(xy)^n = x^n y^n = 0$.

c) Si $x^n = 0$, en notant $y = \sum_{k=0}^{n-1} x^k$, on a : $(1 - x)y = y(1 - x) = 1 - x^n = 1$.

◇ **Réponse :** Si $x^n = 0$, alors $1 - x$ est inversible, et $(1 - x)^{-1} = \sum_{k=0}^{n-1} x^k$.

2.3.4 ◇ **Réponse :** La caractéristique de $\mathbb{Z}$ (resp. $\mathbb{Z}/n\mathbb{Z}$) est 0 (resp. n).

2.3.5 Par hypothèse, il existe $b \in A$ tel que $ba = 1$.

Considérons, pour $n \in \mathbb{N}$, $c_n = b + a^n(1 - ab)$ (où, par convention, $a^0 = 1$).

Pour tout n de $\mathbb{N}$, c_n est inverse de a à gauche car :

$$c_n a = ba + a^{n+1} - a^{n+1}ba = 1 + a^{n+1} - a^{n+1} = 1.$$

Montrons que les c_n ($n \in \mathbb{N}$) sont deux à deux distincts. Soit $(n,p) \in \mathbb{N}^2$ tel que, par exemple, $n > p$, et supposons $c_n = c_p$.

On a : $c_n = c_p \iff a^n(1 - ab) = a^p(1 - ab) \implies b^n a^n(1 - ab) = b^n a^p(1 - ab)$.

Comme $ba = 1$, une récurrence facile montre : $\forall k \in \mathbb{N}$, $b^k a^k = 1$.

On obtient donc : $1 - ab = b^{n-p}(1 - ab) = b^{n-p} - b^{n-p-1}(ba)b = b^{n-p} - b^{n-p-1}b = 0$, d'où $ab = 1$, contradiction.

2.3.6 *a)* Les vérifications sont immédiates (cf. aussi exercice 2.1.13 p. 45).

b) • L'application $\psi : (\mathbb{Z}/2\mathbb{Z})^X \longrightarrow \mathfrak{P}(X)$ définie par : $\forall f \in (\mathbb{Z}/2\mathbb{Z})^X$, $\psi(f) = \{x \in X ; f(x) = \widehat{1}\}$ vérifie clairement : $\psi \circ \theta = \mathrm{Id}_{\mathfrak{P}(X)}$ et $\theta \circ \psi = \mathrm{Id}_{(\mathbb{Z}/2\mathbb{Z})^X}$, ce qui montre que θ est bijective.

• Pour tout (A,B) de $(\mathfrak{P}(X))^2$, $\theta(A_\triangle B) = \theta_{A_\triangle B} = \theta_A + \theta_B - 2\theta_A\theta_B = \theta_A + \theta_B = \theta(A) + \theta(B)$, (cf. exercice 1.3.1 p. 25) et $\theta(A \cap B) = \theta_{A\cap B} = \theta_A\theta_B = \theta(A)\theta(B)$.

2.4.1

- $xy = x(x^{-1} + y^{-1})y = y + x = -1$ et de même $yx = -1$; ainsi $xy = yx = -1$.
- $1 = (x + y)^2 = x^2 + 2xy + y^2$, d'où $x^2 + y^2 = 3$.
- $9 = (x^2 + y^2)^2 = x^4 + 2x^2y^2 + y^4$, d'où $x^4 + y^4 = 7$.

2.4.2 Supposons que la caractéristique n de K soit $\neq 0$. Si n n'est pas premier, il existe $(a,b) \in (\mathbb{N}^*)^2$ tel que $n = ab$, $a < n$, $b < n$, d'où $a1_K \neq 0$, $b1_K \neq 0$ et $(a1_K)(b1_K) = n1_K = 0$, contradiction.

Remarque : le raisonnement précédent montre plus généralement que la caractéristique d'un anneau intègre est 0 ou un nombre premier.

2.4.3 Notons $f : \begin{array}{ccc} K & \longrightarrow & K \\ x & \longmapsto & x^2 \end{array}$ et $E = f(K)$.

Tout élément de $K - \{0\}$ admet au plus deux antécédents par f, car :

$$f(x) = f(y) \iff x^2 = y^2 \iff (x - y)(x + y) = 0 \iff (y = x \text{ ou } y = -x),$$

et 0 admet 0 pour seul antécédent.

Donc : $\mathrm{Card}(E) \geqslant \dfrac{\mathrm{Card}(K) - 1}{2} + 1$, c'est-à-dire : $\mathrm{Card}(E) > \dfrac{1}{2}\mathrm{Card}(K)$.

D'après l'exercice 2.2.2 p. 48, on conclut $K = E + E$, c'est-à-dire : $\forall x \in K, \exists (a,b) \in K^2, x = a^2 + b^2$.

On démontre (théorème de Wedderburn) que tout corps fini est commutatif.

2.4.4 Supposons qu'il existe un corps K tel qu'il existe un isomorphisme de groupes $f : (K,+) \longrightarrow (K - \{0\}, \times)$.

1er cas : $1_K + 1_K = 0_K$.

Soit $x \in K$. On a successivement :

$$x + x = x(1_K + 1_K) = x0_K = 0_K,$$
$$(f(x))^2 = f(x + x) = f(0_K) = 1_K,$$
$$f(x) = 1_K \quad \text{ou} \quad f(x) = -1_K = 1_K.$$

Ainsi $f(K) = \{1_K\}$, K est fini. Mais alors K et $K - \{0\}$ n'ont pas le même cardinal, contradiction.

2ème cas : $1_K + 1_K \neq 0_K$.

Notons $\alpha = f^{-1}(1_K)$, $\beta = f^{-1}(-1_K)$. On a : $\begin{cases} f(2\alpha) = f(\alpha + \alpha) = (f(\alpha))^2 = 1_K^2 = 1_K \\ f(2\beta) = f(\beta + \beta) = (f(\beta))^2 = (-1_K)^2 = 1_K \end{cases}$,

d'où $2\alpha = 2\beta$, puisque f est bijective.

Comme $2 \cdot 1_K \neq 0$ et $(2 \cdot 1_K)(\alpha - \beta) = 0$, on déduit $\alpha - \beta = 0$, puis $1_K = -1_K$, contradiction.

◇ **Réponse :** non.

C 2.1 *1) a)* • $\overline{e} \neq \varnothing$ car $e \in \overline{e}$.

• $(x,y) \in (\overline{e})^2 \iff \begin{cases} x\mathcal{R}e \\ y\mathcal{R}e \end{cases} \Longrightarrow \begin{cases} x\mathcal{R}e \\ xy\mathcal{R}xe \end{cases} \Longrightarrow xy\mathcal{R}e \Longrightarrow xy \in \overline{e}$.

• $x \in \overline{e} \iff x\mathcal{R}e \Longrightarrow x^{-1}x\mathcal{R}x^{-1}e \iff e\mathcal{R}x^{-1} \iff x^{-1} \in \overline{e}$.

b) • $x\mathcal{R}x' \Longrightarrow x^{-1}x\mathcal{R}x^{-1}x' \iff x^{-1}x' \in \overline{e}$.

• $x^{-1}x' \in \overline{e} \iff x^{-1}x'\mathcal{R}e \Longrightarrow x(x^{-1}x')\mathcal{R}xe \iff x'\mathcal{R}x$.

• $x\mathcal{R}x' \iff x^{-1}x' \in \overline{e} \iff x' \in x\overline{e}$.

2) a) 1) • Soit $x \in G$; comme $x^{-1}x = e \in H$, on a : $x\mathcal{R}_H x$, d'où la réflexivité.

• Soit $(x,x') \in G^2$. On a :

$x\mathcal{R}_H x' \iff x^{-1}x' \in H \Longrightarrow x'^{-1}x = (x^{-1}x')^{-1} \in H \iff x'\mathcal{R}_H x$, d'où la symétrie.

• $\begin{cases} x\mathcal{R}_H x' \\ x'\mathcal{R}_H x'' \end{cases} \iff \begin{cases} x^{-1}x' \in H \\ x'^{-1}x'' \in H \end{cases} \Longrightarrow x^{-1}x'' = (x^{-1}x')(x'^{-1}x'') \in H \iff x\mathcal{R}_H x''$, d'où la transitivité.

Ceci montre que $\mathcal{R}_H$ est une relation d'équivalence dans G.

2) Soit $(x,x',y) \in G^3$. Comme $(yx)^{-1}(yx') = x^{-1}x'$, on a : $x\mathcal{R}_H x' \Longrightarrow yx\mathcal{R}yx'$.

Ainsi, $\mathcal{R}_H$ est compatible à gauche avec la loi de G.

3) $x \in H \iff e^{-1}x \in H \iff e\mathcal{R}_H x \iff x \in \overline{e}$, d'où $H = \overline{e}$.

b) Comme $\overline{x} = xH = x\overline{e}$, il est clair que : $\forall y \in H, xy \in \overline{x}$. Notons $\varphi : \begin{array}{ccc} \overline{e} & \longrightarrow & \overline{x} \\ y & \longmapsto & xy \end{array}$.

• Soit $z \in \overline{x}$. En notant $y = x^{-1}z$, on a : $y \in \overline{e}$ et $\varphi(y) = z$. Ceci montre la surjectivité de φ.

• Si $(y_1,y_2) \in (\overline{e})^2$ est tel que $\varphi(y_1) = \varphi(y_2)$, alors $y_1 = x^{-1}(xy_1) = x^{-1}(xy_2) = y_2$, ce qui montre l'injectivité de φ.

Plus généralement, pour tout (x,x') de G^2, l'application $y \longmapsto x'x^{-1}y$ est une bijection de $\overline{x}$ sur $\overline{x'}$.

3) • Puisque $\mathcal{R}_H$ est une relation d'équivalence dans G, $G/\mathcal{R}_H$ est une partition de G, donc :

$$\text{Card}(G) = \sum_{\xi \in G/\mathcal{R}_H} \text{Card}(\xi).$$

De plus, les classes modulo $\mathcal{R}_H$ ont toutes le même cardinal, d'après *2) b)*; donc :

$$\forall \xi \in G/\mathcal{R}_H, \quad \mathrm{Card}(\xi) = \mathrm{Card}(\overline{e}) = \mathrm{Card}(H).$$

On obtient ainsi : $\mathrm{Card}(G) = \mathrm{Card}(G/\mathcal{R}_H)\mathrm{Card}(H)$ (égalité souvent appelée **équation aux classes**). En particulier : $\mathrm{Card}(H)|\mathrm{Card}(G)$.

4) a) 10 ne divise pas 24.

◇ **Réponse :** non.

b) Puisque $H \cap K$ est un sous-groupe de H et de K, d'après le théorème de Lagrange, $\mathrm{Card}(H \cap K)$ divise $\mathrm{Card}(H)$ et divise $\mathrm{Card}(K)$. Comme $\mathrm{pgcd}\big(\mathrm{Card}(H),\mathrm{Card}(K)\big) = 1$, il en résulte $\mathrm{Card}(H \cap K) = 1$, donc $H \cap K = \{e\}$.

C 2.2 *I 1)* • D'après C 2.1 *1) a)* p. 63, $\overline{e}$ est un sous-groupe de G.

• $y \in \overline{e} \iff y\mathcal{R}e \Longrightarrow xyx^{-1}\mathcal{R}xex^{-1} = e \iff xyx^{-1} \in \overline{e}$.

2) • D'après C 2.1 *2) a)* p. 63, $\mathcal{R}_H$ est une relation d'équivalence dans G, compatible à gauche avec la loi de G, et $H = \overline{e}$.

• Soit $(x,x',y) \in G^3$. On a :

$x\mathcal{R}_H x' \iff x^{-1}x' \in H \Longrightarrow y^{-1}(x^{-1}x')y \in H \iff (xy)^{-1}(x'y) \in H \iff x'y\mathcal{R}_H xy$, ce qui montre que $\mathcal{R}_H$ est compatible à droite avec la loi de G.

Remarque : Un sous-groupe H de G est distingué dans G si et seulement si : $\forall x \in G, xH = Hx$.

3) a) Evident.

b) ◇ **Réponse :** $G = \mathfrak{S}_3$, $H = \{e,\tau_{1,2}\}$ (cf. 3.4.2 Exemple p. 87); $\tau_{13} \circ \tau_{12} \circ \tau_{13}^{-1} = \tau_{23} \notin H$.

4) a) • D'après ex. 2.2.12 *b)* p. 54, $f^{-1}(H')$ est un sous-groupe de G.

• Soient $x \in f^{-1}(H')$, $y \in G$.

On a : $f(yxy^{-1}) = f(y)f(x)(f(y))^{-1} \in H'$, car $f(x) \in H'$ et $H' \lhd G'$.

Ainsi $yxy^{-1} \in f^{-1}(H')$, et finalement $f^{-1}(H') \lhd G$. En particulier : $\mathrm{Ker}(f) \lhd G$.

b) ◇ **Réponse :** $G = \mathfrak{S}_2$, $G' = \mathfrak{S}_3$, $H = \mathfrak{S}_2$, $f : \mathfrak{S}_2 \longrightarrow \mathfrak{S}_3$ définie par $f(\mathrm{Id}) = \mathrm{Id}$ et $f(\tau_{12}) = \tau_{12}$ (cf. 3.4.2 Exemple p. 87 et *3) b)* ci-dessus).

c) • D'après l'ex. 2.2.12 *a)* p. 54, $f(H)$ est un sous-groupe de G'.

• Soient $x' \in f(H)$, $y' \in G'$. Il existe $x \in H$ tel que $x' = f(x)$ et, puisque f est surjective, il existe $y \in G$ tel que $y' = f(y)$. On a : $y'x'y'^{-1} = f(y)f(x)(f(y))^{-1} = f(yxy^{-1}) \in f(H)$, car $x \in H$ et $H \lhd G$.

Finalement : $f(H) \lhd G'$.

5) a) • $e \in C(G)$: évident.

• Soit $(a,b) \in \big(C(G)\big)^2$. On a : $\forall x \in G, (ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$, d'où : $ab \in C(G)$.

• Soit $a \in C(G)$. On a : $\forall x \in G, a^{-1}x = a^{-1}(xa)a^{-1} = a^{-1}(ax)a^{-1} = xa^{-1}$, d'où : $a^{-1} \in C(G)$.

• Soient $a \in C(G)$, $y \in G$. On a : $yay^{-1} = yy^{-1}a = a \in C(G)$.

b) Soit H un sous-groupe de G tel que $\text{Card}(H) = n$.

1) Soit $x \in G$.

• Si $x \in H$, alors $xH = H = Hx$.

• Si $x \notin H$, alors $(xH) \cap H = \varnothing$ et $(Hx) \cap H = \varnothing$, d'où, puisque $\text{Card}(xH) = \text{Card}(Hx) = \text{Card}(H) = n$, $xH = Hx$.

On a ainsi prouvé : $\forall x \in G, xH = Hx$.

2) Soit $(h,x) \in H \times G$. Puisque $xh \in xH = Hx$, il existe $k \in H$ tel que $xh = kx$, d'où : $xhx^{-1} = (kx)x^{-1} = k \in H$.

Finalement : $H \lhd G$.

II *1)* $\left.\begin{matrix} x\mathcal{R}x' \\ y\mathcal{R}y' \end{matrix}\right\} \Longrightarrow \left\{\begin{matrix} xy\mathcal{R}x'y \\ x'y\mathcal{R}x'y' \end{matrix}\right. \Longrightarrow xy\mathcal{R}x'y'.$

2) Soit $(\xi,\zeta) \in (G/H)^2$.

Si $(x,y,x',y') \in G^4$ est tel que $\xi = \overline{x} = \overline{x'}$ et $\zeta = \overline{y} = \overline{y'}$, alors, d'après *1)*, $\overline{xy} = \overline{x'y'}$. On peut donc définir $\xi\zeta$ par $\xi\zeta = \overline{xy}$.

3) • $\forall x \in G, \left\{\begin{matrix} \overline{x}\,\overline{e} = \overline{xe} = \overline{x} \\ \overline{e}\,\overline{x} = \overline{ex} = \overline{x} \end{matrix}\right.$, donc $\overline{e}$ est neutre dans G/H.

• $\forall (x,y,z) \in G^3$, $(\overline{x}\,\overline{y})\overline{z} = \overline{xy}\,\overline{z} = \overline{(xy)z} = \overline{x(yz)} = \overline{x}\,\overline{yz} = \overline{x}(\overline{y}\,\overline{z})$, donc $\cdot$ est associative dans G/H.

• $\forall x \in G, \left\{\begin{matrix} \overline{x}\,\overline{x^{-1}} = \overline{xx^{-1}} = \overline{e} \\ \overline{x^{-1}}\,\overline{x} = \overline{x^{-1}x} = \overline{e} \end{matrix}\right.$, donc tout élément de G/H admet un symétrique pour $\cdot$.

Finalement, G/H est un groupe.

4) a) • On a, pour tout (x,y) de G^2 :

$$x\mathcal{R}_H y \Longleftrightarrow x^{-1}y \in H \Longrightarrow f(x^{-1}y) \in H' \Longleftrightarrow (f(x))^{-1}f(y) \in H' \Longleftrightarrow f(x)\mathcal{R}_{H'}f(y),$$

ce qui montre que f est compatible avec $\mathcal{R}_H$ et $\mathcal{R}_{H'}$.

• Pour tout (x,y) de G^2 :

$$\begin{aligned} \widetilde{f}(\overline{x}\,\overline{y}) = \widetilde{f}(\overline{xy}) = (\widetilde{f} \circ p)(xy) = (p' \circ f)(xy) = (p' \circ f)(x)(p' \circ f)(y) \\ = (\widetilde{f} \circ p)(x)(\widetilde{f} \circ p)(y) = \widetilde{f}(\overline{x})\widetilde{f}(\overline{y}), \end{aligned}$$

donc $\widetilde{f}$ est un morphisme de groupes.

b) On a vu *(1 4) a)* : $\text{Ker}(f) \lhd G$. La relation $\mathcal{R}$ définie dans G par :

$$x\mathcal{R}y \Longleftrightarrow x^{-1}y \in \text{Ker}(f)$$

est donc une relation d'équivalence compatible avec la loi de G.

D'après C 1.1 *B 1) b)* p. 37, il existe une application unique : $\widehat{f} : G/\mathcal{R} \longrightarrow \text{Im}(f)$ telle que $f = i \circ \widehat{f} \circ p$, et $\widehat{f}$ est bijective.

Enfin, $\widehat{f}$ est un morphisme de groupes car, pour tout (x,y) de G^2 :

$$\begin{aligned} \widehat{f}\big(p(x)p(y)\big) = \widehat{f}\big(p(xy)\big) = (i \circ \widehat{f} \circ p)(xy) = f(xy) = f(x)f(y) \\ = (i \circ \widehat{f} \circ p)(x)(i \circ \widehat{f} \circ p)(y) = \widehat{f}\big(p(x)\big)\widehat{f}\big(p(y)\big). \end{aligned}$$

Dans l'exemple, $\text{Ker}(f) = n\mathbb{Z}$, $\text{Im}(f) = \mathbb{Z}/n\mathbb{Z}$, $\begin{array}{ccc} \mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/n\mathbb{Z} \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ \mathbb{Z}/n\mathbb{Z} & \xrightarrow[\widehat{f}]{} & \mathbb{Z}/n\mathbb{Z} \end{array}$, f est surjective, et $\widehat{f} = \text{Id}_{\mathbb{Z}/n\mathbb{Z}}$.

C 2.3 *I 1) a)* Puisque $(\mathbb{Z}/2\mathbb{Z},+,\cdot)$ est un anneau, $\left((\mathbb{Z}/2\mathbb{Z})^E,+,\cdot\right)$ est aussi un anneau (cf. ex. 2.3.6 p. 59 ou 2.1.13 p. 45). Soient $\varphi \in (\mathbb{Z}/2\mathbb{Z})^E$, $x \in E$; on a : $\varphi^2(x) = (\varphi(x))^2 = \varphi(x)$, car $\varphi(x) \in \widehat{\{0,1\}}$. Ainsi : $\forall \varphi \in (\mathbb{Z}/2\mathbb{Z})^E$, $\varphi^2 = \varphi$, et donc $\left((\mathbb{Z}/2\mathbb{Z})^E,+,\cdot\right)$ est un anneau booléien.

b) On sait que $(\mathfrak{P}(E),\Delta,\cap)$ est un anneau isomorphe à $\left((\mathbb{Z}/2\mathbb{Z})^E,+,\cdot\right)$ (cf. ex. 2.3.6 p. 59, notion de fonction caractéristique). De plus : $\forall A \in \mathfrak{P}(E)$, $A \cap A = A$, donc $(\mathfrak{P}(E),\Delta,\cap)$ est un anneau booléien.

On peut remarquer plus généralement que, si A est un anneau booléien et $\theta : A \longrightarrow B$ un isomorphisme d'anneaux, alors B est booléien puisque :

$$\forall b \in B, \quad b^2 = \left(\theta(\theta^{-1}(b))\right)^2 = \theta\left((\theta^{-1}(b))^2\right) = \theta\left(\theta^{-1}(b)\right) = b.$$

2) a) $x + x = (x + x)^2 = x^2 + x^2 + x^2 + x^2 = x + x + x + x$, d'où $x + x = 0$.

Autrement dit : $\forall x \in A$, $x = -x$.

b) $x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$, d'où $xy + yx = 0$, puis, comme $yx + yx = 0$ (cf. *a)*), $xy - yx = (xy + yx) - (yx + yx) = 0$, et finalement : $xy = yx$.

c) $xy(x + y) = xyx + xy^2 = x^2y + xy^2 = xy + xy = 0$.

d) Supposons $A \neq \{0\}$.

Soit $x \in A$. D'après *c)* (appliqué à $y = 1$), $x(x + 1) = 0$. Comme A est intègre, on déduit $x = 0$ ou $x = -1 = 1$. Ainsi, $A \subset \{0,1\}$. Finalement : $A = \{0\}$ ou $A = \{0,1\}$.

II 1) Réflexivité : Pour tout x de A, $x \leqslant x$, car $x^2 = x$.

Antisymétrique : $\begin{cases} x \leqslant y \\ y \leqslant x \end{cases} \iff \begin{cases} xy = x \\ yx = y \end{cases} \implies x = y$

Transitivité : $\begin{cases} x \leqslant y \\ y \leqslant z \end{cases} \iff \begin{cases} xy = x \\ yz = y \end{cases} \implies xz = (xy)z = x(yz) = xy = x \implies x \leqslant z.$

2) a) 1) • $(xy)x = x^2y = xy$, donc $xy \leqslant x$; de même, $xy \leqslant y$.

• Soit $z \in A$ tel que $\begin{cases} z \leqslant x \\ z \leqslant y \end{cases}$. Alors $\begin{cases} zx = z \\ zy = z \end{cases}$, d'où $z(xy) = (zx)y = zy = z$ et donc $z \leqslant xy$.

Ceci montre que xy est le plus grand des minorants (dans A) de l'ensemble formé par x et y, donc $\mathrm{Inf}(x,y)$ existe et vaut xy.

2) • $(x + y + xy)x = x^2 + yx + xyx = x + xy + xy = x$, donc $x \leqslant x + y + xy$; de même, $y \leqslant x + y + xy$.

• Soit $z \in A$ tel que $\begin{cases} x \leqslant z \\ y \leqslant z \end{cases}$. Alors $\begin{cases} xz = x \\ yz = y \end{cases}$, d'où $(x+y+xy)z = xz+yz+xyz = x+y+xy$, et donc $x + y + xy \leqslant z$.

Ceci montre que $x + y + xy$ est le plus petit des majorants (dans A) de l'ensemble formé par x et y, donc $\mathrm{Sup}(x,y)$ existe et vaut $x + y + xy$.

b) • $\wedge$ est commutative : $x \wedge y = xy = yx = y \wedge x$.

• $\vee$ est commutative : $x \vee y = x + y + xy = y + x + yx = y \vee x$.

• $\wedge$ est assoviative : $(x \wedge y) \wedge z = (xy)z = x(yz) = x \wedge (y \wedge z)$.

• $\vee$ est associative : $(x \vee y) \vee z = (x+y+xy)+z+(x+y+xy)z = x+y+z+xy+xz+yz+xyz = x + (y + z + yz) + x(y + z + yz) = x \vee (y \vee z)$.

• $\wedge$ est distributive sur $\vee$:

$$\begin{cases} x \wedge (y \vee z) = x(y + z + yz) = xy + xz + xyz \\ (x \wedge y) \vee (x \wedge z) = xy + xz + (xy)(xz) = xy + xz + xyz. \end{cases}$$

• $\vee$ est distributive sur $\wedge$:

$$\begin{cases} x \vee (y \wedge z) = x + yz + xyz \\ (x \vee y) \wedge (x \vee z) = (x + y + xy)(x + z + xz) \\ \qquad\qquad = x + (xy + xy) + (xz + xz) + yz + (xyz + xyz) + xyz \\ \qquad\qquad = x + yz + xyz. \end{cases}$$

Remarque : A l'aide de $x \longmapsto x^* = 1 + x$ (voir plus loin, *3)*), on peut déduire une distributivité de l'autre.

3) a) $\forall x \in A, 0 \leqslant x$ (car $0x = 0$).

b) Soit $x \in A$.

• S'il existe $y \in A$ tel que $\begin{cases} x \wedge y = 0 \\ x \vee y = 1 \end{cases}$, alors $\begin{cases} xy = 0 \\ x + y + xy = 1 \end{cases}$, d'où $y = 1 - x = 1 + x$ et l'unicité de y.

• Réciproquement, on a :

$$\begin{cases} x \wedge (1 + x) = x(1 + x) = x + x^2 = x + x = 0 \\ x \vee (1 + x) = x + (1 + x) + x(1 + x) = x + (1 + x) = 1. \end{cases}$$

Ainsi, pour tout x de A, il existe un élément et un seul x^* de A, tel que $\begin{cases} x \wedge x^* = 0 \\ x \vee x^* = 1 \end{cases}$, et on a : $x^* = 1 + x$.

c) 1) $0^* = 1 + 0 = 1, \quad 1^* = 1 + 1 = 0$.

2) $x^{**} = 1 + (1 + x) = (1 + 1) + x = x$.

3) • $(x \vee y)^* = 1 + (x + y + xy) = (1 + x)(1 + y) = x^* \wedge y^*$.

• $(x \wedge y)^* = (x^{**} \wedge y^{**})^* = ((x^* \vee y^*)^*)^* = x^* \vee y^*$.

4) $x \leqslant y \iff xy = x \iff 1 + x + y + xy = 1 + x + y + x \iff (1 + x)(1 + y) = 1 + y$
$\iff y^* \leqslant x^*$.

5) $x \leqslant y \iff xy = x \iff xy + x = 0 \iff x(1 + y) = 0 \iff x \wedge y^* = 0$
$\iff (x \wedge y^*)^* = 1 \iff x^* \vee y = 1$.

4) a) Soit $(x,m) \in A \times M$. On a : $mx = x \iff x \leqslant m \iff \mathrm{Sup}(x,m) = m$.
D'autre part, comme m est maximal dans $A - \{1\}$ et que $m \leqslant \mathrm{Sup}(x,m)$, on a : $\mathrm{Sup}(x,m) \in \{m,1\}$. Donc :

$$\big(\mathrm{non}(x \leqslant m)\big) \iff mx \neq m \iff \mathrm{Sup}(x,m) \neq m \iff x \vee m = 1 \iff x^* \leqslant m$$
$$\iff x^* \wedge m^* = 0 \iff (1 + x)(1 + m) = 0.$$

b) Soit $(x,y,m) \in A \times A \times M$. En utilisant *a)* :

$$\left(\mathrm{non}\left|\begin{matrix} x \leqslant m \\ \mathrm{ou} \\ y \leqslant m \end{matrix}\right.\right) \iff \begin{cases} x^* \leqslant m \\ y^* \leqslant m \end{cases} \iff x^* \vee y^* \leqslant m \iff (x \wedge y)^* \leqslant m \iff \mathrm{non}(x \wedge y \leqslant m).$$

c) 1) • On a : $(\forall m \in M, 0 \leqslant m)$, donc $\phi(0) = \varnothing$.

• Réciproquement, soit $x \in A$ tel que $\phi(x) = \varnothing$. Supposons $x \neq 0$, c'est-à-dire $1 + x \neq 1$. Puisque A est fini, il existe $m_0 \in M$ tel que $1 + x \leqslant m_0$ (montrer que, dans tout ensemble ordonné fini $(E, \leqslant)$, pour tout a de E, il existe au moins un élément maximal m de E tel que $a \leqslant m$).

On a alors $x \leqslant m_0$ (car $m_0 \notin \phi(x)$) et $x^* = 1 + x \leqslant m_0$, d'où : $1 = x \vee x^* \leqslant m_0$, contradiction.

Ceci montre : $x = 0$.

2) Soit $x \in A$. On a, pour tout m de M : $m \in \phi(x^*) \iff (x^*)^* \leqslant m \iff x \leqslant m \iff m \notin \phi(x)$, ce qui montre : $\phi(x^*) = \complement_M(\phi(x))$.

3) Soit $(x,y) \in A^2$.

- On a, pour tout m de M :

$$m \in \phi(x \wedge y) \iff (x \wedge y)^* \leqslant m \iff x^* \vee y^* \leqslant m \iff \begin{cases} x^* \leqslant m \\ y^* \leqslant m \end{cases} \iff \begin{cases} m \in \phi(x) \\ m \in \phi(y) \end{cases},$$

d'où : $\phi(x \wedge y) = \phi(x) \cap \phi(y)$.

$$4)\ \phi(x \vee y) = \phi\big((x^* \wedge y^*)^*\big) = \complement_M\big(\phi(x^*) \cap \phi(y^*)\big) = \complement_M\Big(\complement_M\big(\phi(x)\big)\Big) \cap \Big(\complement_M\big(\phi(y)\big)\Big)$$
$$= \phi(x) \cup \phi(y).$$

d) 1) ϕ **est un morphisme d'anneaux**

Soit $(x,y) \in A^2$. On a, en utilisant *b)* :

- $\phi(xy) = \phi(x \wedge y) = \phi(x) \cap \phi(y)$
- $\phi(x + y) = \phi\big(x(1 + y) + y(1 + x) + x(1 + y)y(1 + x)\big) = \phi\big((xy^*) \vee (x^*y)\big)$

$= \phi(xy^*) \cup \phi(x^*y) = \Big(\phi(x) \cap \complement_M\big(\phi(y)\big)\Big) \cup \Big(\Big(\complement_M\big(\phi(x)\big)\Big) \cap \phi(y)\Big) = \phi(x) \triangle \phi(y)$.

- $\phi(1) = \{m \in M;\ 0 \leqslant m\} = M$, neutre pour $\cap$ dans $\mathfrak{P}(M)$.

2) ϕ **est injective**

Soit $(x,y) \in A^2$ tel que $\phi(x) = \phi(y)$. On a, en utilisant *b)* :

$$\phi(x \wedge y^*) = \phi(x) \cap \complement_M(\phi(y)) = \varnothing,$$

donc $x \wedge y^* = 0$, et, de même, $x^* \wedge y = 0$.

Alors (cf. *3) c)*) : $\begin{cases} x \leqslant y \\ y \leqslant x \end{cases}$, donc $x = y$.

3) ϕ **est surjective**

Soit $F \in \mathfrak{P}(M)$.

Si $F = \varnothing$, alors $F = \phi(0)$.

Supposons donc $F \neq \varnothing$, et notons $N = \mathrm{Card}(F)$, $F = \{m_1, \ldots, m_N\}$, $p = m_1 \wedge \ldots \wedge m_N$. Montrons : $F = \phi(p^*)$.

On a, pour tout m de M, d'après *a)* et *b)* :

$$m \in \phi(p^*) \iff p \leqslant m \iff m_1 \wedge \ldots \wedge m_N \leqslant m$$
$$\iff \left| \begin{array}{c} m_1 \leqslant m \\ \text{ou} \\ \vdots \\ \text{ou} \\ m_N \leqslant m \end{array} \right. \iff \left| \begin{array}{c} m_1 = m \\ \text{ou} \\ \vdots \\ \text{ou} \\ m_N = m \end{array} \right.$$

puisque $m_1, \ldots, m_N$ sont maximaux dans $A - \{1\}$ et que $m \in A - \{1\}$.

Ainsi, $\phi(p^*) = \{m_1, \ldots, m_N\} = F$, d'où la surjectivité de ϕ.

Finalement, ϕ est un isomorphisme d'anneaux.

Indications et réponses
pour les exercices du chapitre 3

3.1.1 En notant $\alpha = a - 1 \in \mathbb{N}$, $\beta = b - 1 \in \mathbb{N}$, $\gamma = c - 1 \in \mathbb{N}$, on a :

$$ab < c \iff \alpha\beta + \alpha + \beta < \gamma \implies \alpha + \beta < \gamma \iff \alpha + \beta + 2 \leqslant \gamma + 1 \iff a + b \leqslant c.$$

3.1.2 Si (x,y,z) est solution, alors y est impair : $y = 2Y + 1$, $Y \in \mathbb{N}$. L'équation se ramène à :

$$5x + 15Y + 3z = 59. \tag{2}$$

Si (x,Y,z) est solution de (2), alors $3|2x - 2$, $3|x - 1$, donc $x = 3X + 1$, $X \in \mathbb{N}$. Puis (2) se ramène à :

$$5X + 5Y + z = 18. \tag{3}$$

Si (X,Y,z) est solution de (3), alors $5|z - 3$, donc $z = 5Z + 3$, $Z \in \mathbb{N}$. Puis (3) se ramène à : $X + Y + Z = 3$.

◊ **Réponse :**
$\{(10, 1, 3), (7, 3, 3), (7, 1, 8), (4, 5, 3), (4, 3, 8), (4, 1, 13), (1, 7, 3), (1, 5, 8), (1, 3, 13), (1, 1, 18)\}$.

3.1.3 (i) La formule est facilement vérifiée pour $n = 0,1,2$. Pour $n \geqslant 3$:

$1^{2n} + 2^{2n} + 3^{2n} > 3^{2n} \geqslant 2 \cdot 7^n$ car $\left(\frac{9}{7}\right)^n \geqslant \left(\frac{9}{7}\right)^3 \geqslant 2$ (en anticipant sur les fractions).

(ii) La formule est facilement vérifiée pour $n = 0,1,2$. Pour $n \geqslant 3$:

$1^{2n+1} + 2^{2n+1} + 3^{2n+1} > 3 \cdot 9^n \geqslant 6^{n+1}$ car $\left(\frac{3}{2}\right)^n \geqslant \left(\frac{3}{2}\right)^3 \geqslant 2$.

◊ **Réponse :** Il y a égalité dans (i) (resp. (ii)) si et seulement si $n \in \{1,2\}$ (resp. $n \in \{0,1\}$).

3.1.4 *a)* La formule est facilement vérifiée pour $n = 2$. Supposons-la vraie pour un n de $\mathbb{N} - \{0,1\}$. Alors : $\displaystyle\sum_{k=1}^{n+1} \frac{1}{k^2} > \frac{3n}{2n+1} + \frac{1}{(n+1)^2}$, et on a :

$$\frac{3n}{2n+1} + \frac{1}{(n+1)^2} \geqslant \frac{3(n+1)}{2(n+1)+1}$$
$$\iff \big(3n(n+1)^2 + (2n+1)\big)(2n+3) \geqslant 3(n+1)^3(2n+1) \iff n^2 + 2n \geqslant 0.$$

D'où : $\displaystyle\sum_{k=1}^{n+1} \frac{1}{k^2} > \frac{3(n+1)}{2(n+1)+1}$.

b) La formule est évidente pour $n = 1$. Supposons-la vraie pour un n de $\mathbb{N}^*$. Alors :

$$4^{n+1}\big((n+1)!\big)^3 = \big(4^n(n!)^3\big) \cdot 4(n+1)^3 < (n+1)^{3n} 4(n+1)^3 = 4(n+1)^{3n+3}.$$

D'après la formule du binôme de Newton :

$$\left(1+\frac{1}{n+1}\right)^{3n+3} \geqslant 1+C_{3n+3}^{1}\frac{1}{n+1}=4,$$

d'où : $4(n+1)^{3n+3} \leqslant (n+2)^{3n+3}$, et donc : $4^{n+1}\big((n+1)!\big)^3 < (n+2)^{3(n+1)}$.

c) La formule est évidente pour $n=1$. Supposons-la vraie pour un n de $\mathbb{N}^*$. Alors :

$$1!3!\ldots(2n+3)! = \big(1!3!\ldots(2n+1)!\big)\big((2n+3)!\big) \geqslant \big((n+1)!\big)^{n+1}(2n+3)!.$$

On a :

$$\big((n+1)!\big)^{n+1}(2n+3)! \geqslant \big((n+2)!\big)^{n+2} \Longleftrightarrow (2n+3)! \geqslant (n+1)!(n+2)^{n+2}$$
$$\Longleftrightarrow (n+2)(n+3)\ldots(2n+3) \geqslant (n+2)^{n+2},$$

et cette dernière inégalité est vraie, car $n+2, n+3, \ldots, 2n+3$ sont $\geqslant n+2$.

d) La formule est facilement vérifiée pour $n=1$. Supposons-la vraie pour un n de $\mathbb{N}$. Il suffit alors de prouver :

$$\frac{4n+5}{4n+7}\sqrt{\frac{3}{4n+3}} > \sqrt{\frac{3}{4n+7}} \tag{1}$$

et

$$\frac{4n+5}{4n+7}\sqrt{\frac{5}{4n+5}} < \sqrt{\frac{5}{4n+9}}. \tag{2}$$

Enfin :

$$(1) \Longleftrightarrow (4n+5)^2 > (4n+7)(4n+3) \Longleftrightarrow 25 > 21$$
$$(2) \Longleftrightarrow (4n+5)(4n+9) < (4n+7)^2 \Longleftrightarrow 45 < 49.$$

3.1.5 La propriété est vraie pour $n=2$ par définition de $\triangle$. Supposons-la vraie pour un n de $\mathbb{N}-\{0,1\}$, et soient $A_1,\ldots,A_{n+1}$ des parties de E.

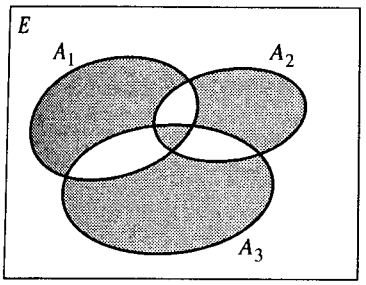
Comme $\triangle$ est associative (exercice 2.3.6 p. 59), on a :

$$\bigtriangleup_{i=1}^{n+1} A_i = \left(\bigtriangleup_{i=1}^{n} A_i\right) \triangle A_{n+1} = \left\{ x \in E ; \left| \begin{array}{lll} x \in \bigtriangleup_{i=1}^{n} A_i & \text{et} & x \notin A_{n+1} \\ \text{ou} & & \\ x \notin \bigtriangleup_{i=1}^{n} A_i & \text{et} & x \in A_{n+1} \end{array} \right. \right\}.$$

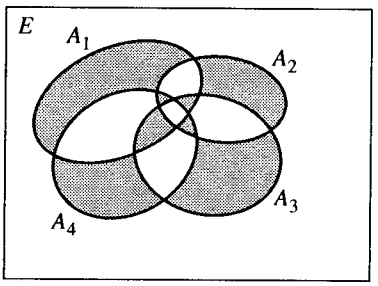
Ainsi, $\bigtriangleup_{i=1}^{n+1} A_i$ est l'ensemble des x de E tels que :

$$\left| \begin{array}{l} x \text{ appartient à un nombre impair des } A_i \ (1 \leqslant i \leqslant n) \text{ et } x \notin A_{n+1} \\ \text{ou} \\ x \text{ appartient à un nombre pair des } A_i \ (1 \leqslant i \leqslant n) \text{ et } x \in A_{n+1}. \end{array} \right.$$

Donc $\bigtriangleup_{i=1}^{n+1} A_i$ est l'ensemble des x de E appartenant à un nombre impair des A_i $(1 \leqslant i \leqslant n+1)$.



$n = 3$



$n = 4$

3.1.6 Soient $(x,y),(u,v) \in \mathbb{N} \times \mathbb{N}^*$ tels que $f(x,y) = f(u,v)$.

Si $x + y < u + v$, alors :

$$f(u,v) = (u+v)^2 + v \geqslant (x+y+1)^2 + v = (x+y)^2 + y + (2x+y+1+v) > f(x,y).$$

Donc $x + y \geqslant u + v$, et de même $u + v \geqslant x + y$, donc $u + v = x + y$.

Alors, comme $(x+y)^2 + y = (u+v)^2 + v$, on déduit $v = y$, $u = x$.

Voir aussi l'exercice 3.2.6 p. 77.

3.1.7 • Soit (f,g) convenant.

Avec $x = y = 1$, on obtient $f(1) = 1$.

Avec $x = 2$, $y = 1$, on obtient $(f(2))^{g(1)} = 2$, donc $g(1) = 1$ (et $f(2) = 2$).

Avec $x \in \mathbb{N}^*$ et $y = 1$, on obtient : $f(x) = x$.

Avec $x = y \geqslant 2$, on obtient : $g(x) = 1$.

• Réciproque triviale.

◊ **Réponse :** $\left\{\left(f : \mathbb{N}^* \underset{x \longmapsto x}{\longrightarrow} \mathbb{N}^*,\ \mathbb{N}^* \underset{x \longmapsto 1}{\longrightarrow} \mathbb{N}^*\right)\right\}$.

3.1.8 Soit (f,g,h) convenant.

Avec $x = y = z = 1$, on obtient $f(1) = g(1) = h(1) = 1$.

Avec $x \in \mathbb{N}^*$, $y = z = 1$, on obtient $f(x) = x$. Puis, de même, $g = h = \mathrm{Id}_{\mathbb{N}^*}$.

Mais alors, en remplaçant (x,y,z) par $(2,2,1)$, on obtient une contradiction.

◊ **Réponse :** $\mathcal{S} = \varnothing$.

3.1.9 Soit f convenant. Nous allons montrer, par une récurrence forte sur n : $\forall n \in \mathbb{N}$, $f(n) = n$.

• Puisque $f : \mathbb{N} \longrightarrow \mathbb{N}$ est strictement croissante et que $f(2) = 2$, on a : $f(0) = 0$, $f(1) = 1$.

• Soit $n \in \mathbb{N} - \{0,1\}$; supposons : $\forall k \in \{0,\ldots,n\}$, $f(k) = k$.

1) Si $n + 1$ est pair, il existe $p \in \mathbb{N}^*$ tel que $n + 1 = 2p$, d'où :

$$f(n+1) = f(2p) = f(2)f(p) = 2p = n + 1,$$

car $p \leqslant n$.

2) Supposons $n+1$ impair; il existe $q \in \mathbb{N}^*$ tel que $n+2 = 2q$. Comme $n \geqslant 2$, on a $q \leqslant n$, d'où :

$$f(n+2) = f(2q) = f(2)f(q) = 2q = n+2.$$

Alors : $f(n) = n$, $f(n+2) = n+2$, d'où $f(n+1) = n+1$ puisque f est strictement croissante.

3.1.10 $\displaystyle\sum_{k=1}^{n} k(n+1-k) = (n+1)\sum_{k=1}^{n} k - \sum_{k=1}^{n} k^2 = (n+1)\frac{n(n+1)}{2} - \frac{n(n+1)(2n+1)}{6}.$

◇ **Réponse :** $\dfrac{n(n+1)(n+2)}{6}$.

3.1.11 *1)* Déterminons, pour $p \in \mathbb{N}$ fixé, la partie principale de $S_p(n)$ lorsque n tend vers l'infini. On a :

$$S_p(n) = n^{p+1}\frac{1}{n}\sum_{k=1}^{n}\left(\frac{k}{n}\right)^p \quad \text{et} \quad \frac{1}{n}\sum_{k=1}^{n}\left(\frac{k}{n}\right)^p \underset{n\infty}{\longrightarrow} \int_0^1 x^p\,\mathrm{d}x = \frac{1}{p+1},$$

d'où $S_p(n) \underset{n\infty}{\sim} \dfrac{n^{p+1}}{p+1}$.

2) Soit (p,q,r) convenant. D'après *1)*, on a alors : $\dfrac{n^{p+1}}{p+1} \underset{n\infty}{\sim} \left(\dfrac{n^{q+1}}{q+1}\right)^r$, d'où, par unicité de la partie principale :

$$p+1 = (q+1)r \quad \text{et} \quad p+1 = (q+1)^r.$$

On déduit : $(q+1)^{r-1} = r$.

Montrer, par récurrence : $\forall r \geqslant 3, \quad 2^{r-1} > r$.

Donc, si $r \geqslant 3$, alors :

$$(q+1)^{r-1} = r < 2^{r-1} \leqslant (q+1)^{r-1}, \quad \text{contradiction.}$$

D'où $r = 2$, puis $q = 1$, $p = 3$.

◇ **Réponse :** $\{(3,1,2)\}$.

3.2.1 *1ère méthode :*

Récurrence sur $n = \#(E)$.

La propriété est triviale pour $n = 0$, car alors : $E = \varnothing$ et $\mathfrak{P}(E) = \{\varnothing\}$.

Supposons la propriété vraie pour un n de $\mathbb{N}$, et soit E un ensemble fini de cardinal $n+1$. Considérons un élément ω fixé de E. On a : $\mathfrak{P}(E) = \mathcal{A} \cup \mathcal{B}$ où $\mathcal{A} = \{X \in \mathfrak{P}(E);\ \omega \notin X\} = \mathfrak{P}(E - \{\omega\})$ et $\mathcal{B} = \{X \in \mathfrak{P}(E);\ \omega \in X\}$.

Il est clair que $\begin{array}{ccc} Y & \longmapsto & Y \cup \{\omega\} \\ \mathfrak{P}(E-\{\omega\}) & \longrightarrow & \mathcal{B} \end{array}$ est une bijection, d'où $\#(\mathcal{B}) = \#\,\mathfrak{P}(E - \{\omega\}) = 2^n$.

Comme $\mathcal{A} \cap \mathcal{B} = \varnothing$, on obtient :

$$\#(\mathfrak{P}(E)) = \#(\mathcal{A}) + \#(\mathcal{B}) = 2^n + 2^n = 2^{n+1}.$$

2ème méthode : L'application $A \longmapsto \chi_A$ (où χ_A est la fonction caractéristique de A, cf. 1.3.1 Exemple 5 p. 24) est une bijection de $\mathfrak{P}(E)$ sur $\{0,1\}^E$, donc : $\#\,\mathfrak{P}(E) = \#(\{0,1\}^E) = 2^{\#(E)}$.

3.2.2 Appliquer 3.2.2 Prop. 3 *1)* p. 73 en remarquant que $\begin{array}{ccc} E & \longrightarrow & \mathfrak{P}(E) \\ x & \longmapsto & \{x\} \end{array}$ est injective.

3.2.3 Soit $(u_n)_{n\in\mathbb{N}}$ une suite décroissante à termes dans $\mathbb{N}$. Supposons $(u_n)_{n\in\mathbb{N}}$ non stationnaire; alors : $\forall n \in \mathbb{N},\ \exists k \in \mathbb{N},\ (k > n \text{ et } u_k < u_n)$.

Il existe une application $\sigma : \mathbb{N} \longrightarrow \mathbb{N}$ telle que : $\begin{cases} \sigma(0) = 0 \\ \forall n \in \mathbb{N}, \quad \big(\sigma(n+1) > \sigma(n) \quad \text{et} \quad u_{\sigma(n+1)} < u_{\sigma(n)}\big). \end{cases}$

On a alors : $u_0 \geqslant u_{\sigma(0)} \geqslant u_{\sigma(1)} + 1 \geqslant u_{\sigma(2)} + 2 \geqslant \ldots$, et donc : $\forall n \in \mathbb{N}, u_0 \geqslant u_{\sigma(n)} + n \geqslant n$, contradiction (choisir $n = u_0 + 1$).

3.2.4 *a)* L'application induite $\begin{array}{ccc} A & \longrightarrow & f(A) \\ x & \longmapsto & f(x) \end{array}$ est surjective et A est finie, donc (cf. 3.2.2 Prop. 3 *2)*, p. 73) $f(A)$ est finie et $\#(f(A)) \leqslant \#(A)$.

b) • $f^{-1}(B)$ peut ne pas être finie, comme le montre l'exemple $\begin{array}{ccc} f : \mathbb{N} & \longrightarrow & \mathbb{N}, \\ x & \longmapsto & 0 \end{array}$ $B = \{0\}$, $f^{-1}(B) = \mathbb{N}$.

• Si f est injective, l'application induite $\begin{array}{ccc} f^{-1}(B) & \longrightarrow & B \\ x & \longmapsto & f(x) \end{array}$ est injective et donc (cf. 3.2.2 Prop. 3 *1)* p. 000), $f^{-1}(B)$ est finie et $\#(f^{-1}(B)) \leqslant \#(B)$.

3.2.5 Montrer, en utilisant $f^2 = \mathrm{Id}_E$, que la relation $\mathcal{R}$ définie dans E par :

$$x\mathcal{R}y \Longleftrightarrow (y = x \quad \text{ou} \quad y = f(x))$$

est une relation d'équivalence.

Notons $\mathcal{R}_A$ la relation d'équivalence sur A induite par $\mathcal{R}$: $\forall (x,y) \in A^2, (x\mathcal{R}_A y \Longleftrightarrow x\mathcal{R}y)$.

Comme $(\forall x \in A, x \neq f(x))$, chaque classe modulo $\mathcal{R}_A$ est finie et a exactement deux éléments.

Il en résulte que Card(A) est pair.

3.2.6 *1)* **Injectivité :** comme dans la solution de l'exercice 3.1.6 p. 417.

2) **Surjectivité**

Soit $N \in \mathbb{N}$. Il existe $n \in \mathbb{N}$ tel que :

$$\frac{n(n+1)}{2} \leqslant N < \frac{(n+1)(n+2)}{2}.$$

Notons $x = N - \dfrac{n(n+1)}{2}$, $y = n - x$.

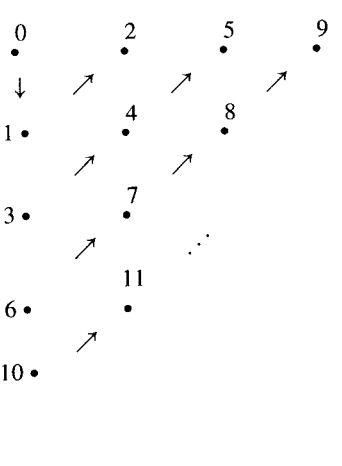
On a : $x \in \mathbb{N}$ et

$$x < \frac{(n+1)(n+2)}{2} - \frac{n(n+1)}{2} = n + 1,$$

donc $x \leqslant n$, d'où $y \in \mathbb{N}$.

Par construction de n, x, y :

$$\begin{aligned} f(x,y) &= \frac{(x+y)(x+y+1)}{2} + x \\ &= \frac{n(n+1)}{2} + x = N. \end{aligned}$$



3.2.7 *Récurrence sur n.*

La formule est triviale pour $n = 1$, et connue pour $n = 2$ (cf. 3.2.2 Prop. 5 p. 73).

Supposons-la vraie pour un n de $\mathbb{N}^*$, et soient $E_1, \ldots, E_{n+1}$ des ensembles finis. On a :

$$\begin{aligned}
\#\left(\bigcup_{i=1}^{n+1} E_i\right) &= \#\left(\left(\bigcup_{i=1}^{n} E_i\right) \cup E_{n+1}\right) = \#\left(\bigcup_{i=1}^{n} E_i\right) + \#(E_{n+1}) - \#\left(\left(\bigcup_{i=1}^{n} E_i\right) \cap E_{n+1}\right) \\
&= \#\left(\bigcup_{i=1}^{n} E_i\right) + \#(E_{n+1}) - \#\bigcup_{i=1}^{n}(E_i \cap E_{n+1}) \\
&= \sum_{k=1}^{n}(-1)^{k-1} \sum_{I \in \mathfrak{P}_k(\{1,\ldots,n\})} \#\left(\bigcap_{i\in I} E_i\right) + \#(E_{n+1}) - \sum_{k=1}^{n}(-1)^{k-1} \sum_{I \in \mathfrak{P}_k(\{1,\ldots,n\})} \#\left(\left(\bigcap_{i\in I} E_i\right) \cap E_{n+1}\right) \\
&= \sum_{k=1}^{n+1}(-1)^{k-1} \sum_{\substack{I \in \mathfrak{P}_k(\{1,\ldots,n+1\}) \\ n+1 \notin I}} \#\left(\bigcap_{i\in I} E_i\right) + \sum_{l=1}^{n+1}(-1)^{l-1} \sum_{\substack{J \in \mathfrak{P}_l(\{1,\ldots,n+1\}) \\ n+1 \in I}} \#\left(\bigcap_{j\in J} E_j\right) \\
&= \sum_{k=1}^{n+1}(-1)^{k-1} \sum_{I \in \mathfrak{P}_k(\{1,\ldots,n+1\})} \#\left(\bigcap_{i\in I} E_i\right).
\end{aligned}$$

3.2.8 *a)* Comme $\{(x,y) \in E^2;\ x\mathcal{R}y\} = \bigcup_{i=1}^{N} E_i^2$ et que les E_i^2 sont deux à deux disjoints, on a :

$$v = \sum_{i=1}^{N} \#(E_i^2) = \sum_{i=1}^{N} \big(\#(E_i)\big)^2.$$

b) En appliquant l'inégalité de Cauchy-Schwarz (Tome 1, 1.2.2) on a :

$$\left(\sum_{i=1}^{N} 1 \cdot \#(E_i)\right)^2 \leqslant \left(\sum_{i=1}^{N} 1^2\right)\left(\sum_{i=1}^{N} \big(\#(E_i)\big)^2\right),$$

c'est-à-dire : $n^2 \leqslant Nv$.

3.2.9 S'il existe (p,q) tel que $p \neq q$ et $a_p = a_q$, alors (p,q) ou (q,p) convient.

Supposons donc $\mathbb{N} \underset{n \longmapsto a_n}{\longrightarrow} \mathbb{N}$ injective.

L'ensemble $\{b_n;\ n \in \mathbb{N}\}$ admet un plus petit élément; il existe donc $p \in \mathbb{N}$ tel que : $\forall n \in \mathbb{N},\quad b_p \leqslant b_n$.

Comme $\mathbb{N} \underset{n \longmapsto a_n}{\longrightarrow} \mathbb{N}$ est injective, il existe $q \in \mathbb{N}$ tel que : $q > p$ et $a_p \leqslant a_q$.

On a alors : $p \neq q$, $a_p \leqslant a_q$, $b_p \leqslant b_q$, donc (p,q) convient.

3.2.10 La relation $\mathcal{R}$ définie dans $\{1,\ldots,n\}$ par : $i\mathcal{R}j \iff x_i = x_j$ est une relation d'équivalence.

Notons $N = \#(\{1,\ldots,n\}/\mathcal{R})$, et $X_1, \ldots, X_N$ les classes modulo $\mathcal{R}$. On a donc :

$$\sum_{i=1}^{N} \#(X_i) = \#(\{1,\ldots,n\}) = n.$$

Si $\left\{\begin{array}{l} N \leqslant p \\ \forall i \in \{1,\ldots,N\},\quad \#(X_i) \leqslant p \end{array}\right.$, alors $n \leqslant p^2$, contradiction.

Donc : $\left|\begin{array}{l} (1)\quad N > p \\ \text{ou} \\ (2)\quad \exists i \in \{1,\ldots,N\},\quad \#(X_i) > p. \end{array}\right.$

Dans le cas (1), au moins $p+1$ des nombres $x_1, \ldots, x_n$ sont deux à deux différents.

Dans le cas (2), au moins $p+1$ des nombres $x_1, \ldots, x_n$ sont égaux.

3.2.11 *1)* Soit $(X, \leqslant)$ un ensemble ordonné. Montrons que toute partie finie non vide Y de X admet au moins un élément maximal.

Puisque $Y \neq \varnothing$, Y admet au moins un élément y_1. Si y_1 n'est pas maximal (dans Y), il existe $y_2 \in Y$ tel que $y_1 < y_2$. Si y_2 n'est pas maximal, il existe $y_3 \in Y$ tel que $y_2 < y_3, \ldots$

Si Y n'admet aucun élément maximal, on construit une suite $(y_n)_{n\in\mathbb{N}^*}$ strictement croissante. Alors Y serait infini, contradiction.

Si E est fini, en appliquant le résultat précédent à $(\mathfrak{P}(E), \subset)$, on conclut : toute partie non vide de $\mathfrak{P}(E)$ admet au moins un élément maximal.

2) Réciproquement, supposons E infini. L'ensemble $\mathfrak{F}(E)$ des parties finies de E est une partie non vide de $\mathfrak{P}(E)$; montrons que $\mathfrak{F}(E)$ n'admet aucun élément maximal. Soit $F \in \mathfrak{F}(E)$. Comme F est finie, incluse dans E infini, il existe $x \in E - F$. Alors $F \underset{\neq}{\subset} F \cup \{x\}$ et $F \cup \{x\} \in \mathfrak{F}(E)$. Ceci montre que F n'est pas maximal dans $\mathfrak{F}(E)$.

3.3.1 $\mathrm{C}_{\mathrm{C}_n^2}^2 = \dfrac{\mathrm{C}_n^2(\mathrm{C}_n^2 - 1)}{2} = \dfrac{n(n-1)(n^2-n-2)}{8}$ et $3\mathrm{C}_{n+1}^4 = \dfrac{(n+1)n(n-1)(n-2)}{8}$.

3.3.2 $\mathrm{C}_n^p - \mathrm{C}_{n-1}^p = \mathrm{C}_{n-1}^{p-1} = \dfrac{(n-1)!}{(p-1)!(n-p)!}$,

donc $\mathrm{C}_n^p = \mathrm{C}_{n-1}^p + \mathrm{C}_{n-x}^{p-x} \iff \begin{cases} 0 \leqslant x \leqslant p \\ \dfrac{(n-x)!}{(p-x)!} = \dfrac{(n-1)!}{(p-1)!} \end{cases}$.

Si $x \geqslant 2$, alors $\forall k \in \{1, \ldots, n-p\}$, $1 \leqslant p - x + k < p - 1 + k$,

d'où $(n-x)(n-x-1)\ldots(p-x+1) < (n-1)(n-2)\ldots p$, et donc $\dfrac{(n-x)!}{(p-x)!} < \dfrac{(n-1)!}{(p-1)!}$.

◊ **Réponse :** $\{1\}$.

3.3.3 $(k+1)\dfrac{\mathrm{C}_n^{k+1}}{\mathrm{C}_n^k} = n - k$.

◊ **Réponse :** $\dfrac{n(n+1)}{2}$.

3.3.4 $P_n = \displaystyle\prod_{k=0}^{n} \frac{n!}{k!(n-k)!} = \frac{(n!)^{n+1}}{\left(\displaystyle\prod_{k=0}^{n} k!\right)^2}$, d'où $\dfrac{P_n}{P_{n-1}} = \dfrac{n^{n+1}(n-1)!}{(n!)^2} = \dfrac{n^n}{n!}$.

3.3.5 $\displaystyle\sum_{k=0}^{q} \frac{p}{p+q-k} \cdot \frac{\mathrm{C}_q^k}{\mathrm{C}_{p+q}^k} = \sum_{k=0}^{q} \frac{p \cdot q!(p+q-k-1)!}{(q-k)!(p+q)!} = \frac{p \cdot q!}{(p+q)!} \sum_{k=0}^{q} \frac{(p+q-k-1)!}{(q-k)!}$

$$= \frac{1}{\mathrm{C}_{p+q}^p} \sum_{k=0}^{q} \mathrm{C}_{p+q-k-1}^{p-1} = \frac{1}{\mathrm{C}_{p+q}^p} \sum_{j=0}^{q} \mathrm{C}_{p+j-1}^{p-1}.$$

Montrer, par récurrence sur q : $\displaystyle\sum_{j=0}^{q} \mathrm{C}_{p+j-1}^{p-1} = \mathrm{C}_{p+q}^p$.

◊ **Réponse :** 1.

3.3.6 Même démarche que pour l'exercice 3.3.5.

3.3.7 $(n!)! = \sum_{i=1}^{n!} i = \prod_{k=1}^{(n-1)!} u_{n,k}$, où $u_{n,k} = \prod_{i=kn-n+1}^{kn} i = (kn-n+1)(kn-n+2)\dots(kn)$

$$= \frac{(kn)!}{(kn-n)!} = \mathrm{A}_{kn}^{n} = n!\mathrm{C}_{kn}^{n}, \quad \text{donc :} \quad (n!)! = (n!)^{(n-1)!}\left(\prod_{k=1}^{(n-1)!} \mathrm{C}_{kn}^{n}\right).$$

3.3.8 Récurrence sur q (pour p fixé).

La propriété est triviale pour $q = 1$.

Supposons-la vraie pour un q de $\mathbb{N}^*$. On a :

$$\sum_{k=0}^{q}(p-2k)\mathrm{C}_p^k = \sum_{k=0}^{q-1}(p-2k)\mathrm{C}_p^k + (p-2q)\mathrm{C}_p^q$$
$$= q\mathrm{C}_p^q + (p-2q)\mathrm{C}_p^q = (p-q)\mathrm{C}_p^q = \frac{p!}{q!(p-q-1)!} = (q+1)\mathrm{C}_p^{q+1}.$$

3.3.9 Récurrence sur n.

La propriété est triviale pour $n = 0$.

Si elle est vraie pour un n de $\mathbb{N}$, alors :

$$\sum_{k=0}^{n+1}\mathrm{C}_{p-k}^q = \sum_{k=0}^{n}\mathrm{C}_{p-k}^q + \mathrm{C}_{p-n-1}^q = \mathrm{C}_{p+1}^{q+1} - \mathrm{C}_{p-n}^{q+1} + \mathrm{C}_{p-n-1}^q = \mathrm{C}_{p+1}^{q+1} - \mathrm{C}_{p-n-1}^{q+1}.$$

3.3.10 $$\sum_{i=1}^{n}\prod_{j=0}^{p-1}(i+j) = \sum_{i=1}^{n}\frac{(i+p-1)!}{(i-1)!} = \sum_{i=0}^{n-1}\frac{(i+p)!}{i!} = p!\sum_{i=0}^{n-1}\mathrm{C}_{p+i}^{p}.$$

Montrons, par récurrence sur n : $\forall n \in \mathbb{N}^*$, $\sum_{i=0}^{n-1}\mathrm{C}_{p+i}^{p} = \mathrm{C}_{p+n}^{p+1}$.

La propriété est triviale pour $n = 1$.

Si elle est vraie pour un n de $\mathbb{N}^*$, alors : $\sum_{i=0}^{n}\mathrm{C}_{p+i}^{p} = \left(\sum_{i=0}^{n-1}\mathrm{C}_{p+i}^{p}\right) + \mathrm{C}_{p+n}^{p} = \mathrm{C}_{p+n}^{p+1} + \mathrm{C}_{p+n}^{p} = \mathrm{C}_{p+n+1}^{p+1}$.

◇ **Réponse :** $\dfrac{(p+n)!}{(p+1)\cdot(n-1)!}$.

3.3.11 En notant $A = \sum_{k=0}^{\mathrm{E}(\frac{n}{2})}\mathrm{C}_n^{2k}$ et $B = \sum_{k=0}^{\mathrm{E}(\frac{n}{2})}\mathrm{C}_n^{2k+1}$, la formule du binôme de Newton donne :

$$A + B = \sum_{k=0}^{n}\mathrm{C}_n^k = 2^n \quad \text{et} \quad A - B = \sum_{k=0}^{n}(-1)^k\mathrm{C}_n^k = 0.$$

◇ **Réponse :** $\sum_{k=0}^{\mathrm{E}(\frac{n}{2})}\mathrm{C}_n^{2k} = \sum_{k=0}^{\mathrm{E}(\frac{n}{2})}\mathrm{C}_n^{2k+1} = 2^{n-1}$.

3.3.12 La considération des coefficients de X^{2p} dans $(1+X)^n(1+X)^n$ et $(1+X)^{2n}$ permet d'obtenir : $\sum_{k=0}^{2p} C_n^k C_n^{2p-k} = C_{2n}^{2p}$.

Remarquer ensuite : $\sum_{k=0}^{2p} C_n^k C_n^{2p-k} = 2\sum_{k=0}^{p} C_n^{p-k} C_n^{p+k} - \left(C_n^p\right)^2$.

◊ **Réponse :** $\frac{1}{2}\left(C_{2n}^{2p} + \left(C_n^p\right)^2\right)$.

3.3.13 En utilisant la formule du binôme de Newton, le coefficient de X^k dans $(X+1)^q$ est C_q^k, et le coefficient de X^{n-k-1} dans $p(X+1)^{p-1}$ (dérivée de $(X+1)^p$) est $(n-k)C_p^{n-k}$. Ainsi, $\sum_{k=0}^{n}(n-k)C_p^{n-k}C_q^k$ est le coefficient de X^{n-1} dans $p(X+1)^{p+q-1}$, qui est aussi :

$$pC_{p+q-1}^{n-1} = p\frac{(p+q-1)!}{(n-1)!(p+q-n)!} = \frac{pn}{p+q}\frac{(p+q)!}{n!(p+q-n)!} = \frac{pn}{p+q}C_{p+q}^n.$$

3.3.14 *a)* D'après la formule du binôme de Newton : $(X-1)^n = \sum_{k=0}^{n} C_n^k (-1)^{n-k} X^k$.

En dérivant p fois, on déduit : $\frac{n!}{(n-p)!}(X-1)^{n-p} = \sum_{k=p}^{n} C_n^k (-1)^{n-k}\frac{k!}{(k-p)!}X^{k-p}$.

En remplaçant X par 1, on obtient, si $n > p$:

$$0 = \sum_{k=p}^{n} C_n^k (-1)^{n-k}\frac{k!}{(k-p)!} = p!\sum_{k=p}^{n} C_n^k (-1)^{n-k} C_k^p = p!\sum_{k=0}^{n}(-1)^{n-k} C_n^k C_k^p.$$

D'autre part, si $n = p$: $\sum_{k=0}^{n}(-1)^{n-k}C_n^k C_k^p = \left(C_n^n\right)^2 = 1$.

b) $\sum_{k=0}^{n}(-1)^{n-k}C_n^k y_k = \sum_{k=0}^{n}(-1)^{n-k}C_n^k \sum_{p=0}^{k} C_k^p x_p = \sum_{k=0}^{n}(-1)^{n-k}C_n^k \sum_{p=0}^{n} C_k^p x_p = \sum_{p=0}^{n}\left(\sum_{k=0}^{n}(-1)^{n-k}C_n^k C_k^p\right)x_p$
$= x_n$.

3.3.15 *a)* Cf. 3.3.3 p. 81.

b) $2\sum_{k=0}^{E\left(\frac{n-1}{2}\right)}\left(\frac{n-2k}{n}C_n^k\right)^2 = \sum_{k=0}^{n}\left(\frac{n-2k}{n}C_n^k\right)^2 = \sum_{k=0}^{n}\left(C_n^k - 2\frac{k}{n}C_n^k\right)^2 = \sum_{k=0}^{n}\left(C_n^k - 2C_{n-1}^{k-1}\right)^2$

$= \sum_{k=0}^{n}\left(C_n^k\right)^2 - 4\sum_{k=0}^{n} C_n^k C_{n-1}^{k-1} + 4\sum_{k=0}^{n}\left(C_{n-1}^{k-1}\right)^2 = \sum_{k=0}^{n} C_n^k C_n^{n-k} - 4\sum_{k=0}^{n} C_n^k C_{n-1}^{n-k} + 4\sum_{k=0}^{n-1} C_{n-1}^{k-1} C_{n-1}^{n-k}$

$= C_{2n}^n - 4C_{2n-1}^n + 4C_{2n-2}^{n-1}$

$= \frac{(2n-2)!}{(n!)^2}(2n(2n-1) - 4(2n-1)n + 4n^2) = \frac{(2n-2)!2n}{(n!)^2} = \frac{2}{n}C_{2n-2}^{n-1}$.

3.3.16 *a)* L'inégalité voulue est triviale pour $i = k$. Supposons $i < k$; on a :

$$C_n^i = C_n^k \frac{k(k-1)\dots(i+1)}{(n-i)(n-i-1)\dots(n-k+1)} \leqslant C_n^k \left(\frac{k}{n-k+1}\right)^{k-i},$$

et $0 \leqslant \dfrac{k}{n-k+1} \leqslant \dfrac{1}{2}$ car $3k \leqslant n+1$.

b) $\displaystyle\sum_{i=0}^{k} C_n^i \leqslant \left(\sum_{i=0}^{k} \frac{1}{2^{k-i}}\right) C_n^k = 2\left(1 - \frac{1}{2^{k+1}}\right) C_n^k \leqslant 2C_n^k.$

3.3.17 Il existe $m \in \mathbb{N}^*$ et $(p_1,\dots,p_m) \in \mathbb{N}^m$ tels que : $n = 2^{p_1} + 2^{p_2} + \dots + 2^{p_m}$ et $0 \leqslant p_1 < p_2 < \dots < p_m$.

Par exemple : $13 = 2^0 + 2^2 + 2^3$ et, en base 2 : $13 = \overline{1101}$.

Montrer (par récurrence ou par la formule du binôme de Newton) que, pour tout p de $\mathbb{N}$, il existe A_p dans $\mathbb{Z}[X]$ tel que : $(X+1)^{2^p} = X^{2^p} + 1 + 2A_p$.

Alors : $\displaystyle(X+1)^n = \prod_{i=1}^{m} (X+1)^{2^{p_i}} = \prod_{i=1}^{m} \left((X^{2^{p_i}} + 1) + 2A_{p_i}\right)$

Il existe donc $A \in \mathbb{Z}[X]$ tel que : $\displaystyle(X+1)^n = \prod_{i=1}^{m} (X^{2^{p_i}} + 1) + 2A$.

D'autre part, en développant $\displaystyle\prod_{i=1}^{m} (X^{2^{p_i}} + 1)$, on obtient 2^m monômes de degrés deux à deux distincts, et de coefficient 1. Il s'ensuit que le nombre d'entiers impairs parmi les C_n^k $(0 \leqslant k \leqslant n)$ vaut 2^m.

◇ **Réponse :** 2^m où m est le nombre de 1 dans l'écriture de n en base 2. Par exemple, pour $n = 13 = \overline{1101}$, il y a exactement 8 $(= 2^3)$ coefficients C_n^k $(0 \leqslant k \leqslant n)$ impairs, et donc 5 pairs.

3.3.18 Pour toute application $f : \{1,\dots,n\} \longrightarrow \{1,\dots,p\}$, l'application $\begin{array}{ccc} \{1,\dots,n\} & \longrightarrow & f(\{1,\dots,n\}) \\ i & \longmapsto & f(i) \end{array}$ est surjective, et, pour tout k de $\{0,1,\dots,p\}$, il y a C_p^k parties à k éléments dans $\{1,\dots,p\}$. On en déduit :

$$p^n = \text{Card}\left(\{1,\dots,p\}^{\{1,\dots,n\}}\right) = \sum_{k=1}^{p} C_p^k S_n^k.$$

◇ **Réponse :**

p	1	2	3	4	5
S_5^p	1	30	150	240	120

3.3.19 *a)* $S_{p+1}(n+1) = \sum_{k=0}^{n+1} k^{p+1} = \sum_{k=1}^{n+1} k^{p+1} = \sum_{q=0}^{n} (q+1)^{p+1} = \sum_{q=0}^{n} \left(\sum_{k=0}^{p+1} C_{p+1}^{k} q^k \right)$

$= \sum_{k=0}^{p+1} \left(\sum_{q=0}^{n} C_{p+1}^{k} q^k \right) = \sum_{k=0}^{p+1} C_{p+1}^{k} S_k(n).$

b) $(n+1)^{p+1} = S_{p+1}(n+1) - S_{p+1}(n) = \sum_{k=0}^{p} C_{p+1}^{k} S_k(n).$

c) • $n+1 = C_1^0 S_0(n)$, d'où $S_0(n) = n+1$. D'ailleurs : $S_0(n) = 0^0 + 1^1 + \ldots + n^0 = n+1$.

Remarquer ici $0^0 = 1$.

• De $(n+1)^2 = C_2^0 S_0(n) + C_2^1 S_1(n)$, on déduit $S_1(n) = \dfrac{n(n+1)}{2}$.

Remarquer, pour $p \geqslant 1$: $S_p(n) = \sum_{k=0}^{n} k^p = \sum_{k=1}^{n} k^p$ car $0^p = 0$.

• De $(n+1)^3 = C_3^0 S_0(n) + C_3^1 S_1(n) + C_3^2 S_2(n)$, on déduit $S_2(n) = \dfrac{n(n+1)(2n+1)}{6}$.

• De même, on obtient $S_3(n) = \left(\dfrac{n(n+1)}{2} \right)^2$.

3.3.20 *a)* La donnée d'un élément de A_k revient à :

• la donnée de $x_1, \ldots, x_{p+k}$ tels que p exactement d'entre eux vaillent 1 (il y a donc C_{p+k}^{p} choix)

• la donnée de $x_{p+k+2}, \ldots, x_{p+q+1}$ quelconques dans $\{0,1\}$ (il y a donc 2^{q-k} choix).

On en déduit : $\mathrm{Card}(A_k) = C_{p+k}^{p} 2^{q-k}$.

b) • A est la réunion des A_k $(0 \leqslant k \leqslant q)$ et les A_k sont deux à deux disjoints, donc :

$$\mathrm{Card}(A) = \sum_{k=0}^{q} \mathrm{Card}(A_k) = \sum_{k=0}^{q} C_{p+k}^{p} 2^{q-k}.$$

• En échangeant les rôles de 0 et 1, on obtient : $\mathrm{Card}(B) = \sum_{k=0}^{p} C_{q+k}^{q} 2^{p-k}$.

◊ **Réponse :** $\mathrm{Card}(A) = \sum_{k=0}^{q} C_{p+k}^{p} 2^{q-k}$, $\mathrm{Card}(B) = \sum_{k=0}^{p} C_{q+k}^{q} 2^{p-k}$.

c) Puisque $B = \complement_E(A)$, on a : $\mathrm{Card}(E) = \mathrm{Card}(A) + \mathrm{Card}(B)$,

$$2^{p+q+1} = \sum_{k=0}^{q} C_{p+k}^{p} 2^{q-k} + \sum_{k=0}^{p} C_{q+k}^{q} 2^{p-k},$$

d'où la relation voulue.

d) Appliquer *c)* avec $q = p$.

3.3.21 Notons, pour $n \in \mathbb{N}$: $S_n = \sum_{k=0}^{n} \frac{1}{C_n^k}$.

On a, pour tout n de $\mathbb{N}^*$:

$$\frac{2^{n+1}}{n+1} S_n - \frac{2^n}{n} S_{n-1} = \frac{2^{n+1}}{n+1} + T_n,$$

où $T_n = \sum_{k=0}^{n-1} \left(\frac{2^{n+1}}{(n+1)C_n^k} - \frac{2^n}{nC_{n-1}^k} \right)$.

Et : $T_n = 2^n \sum_{k=0}^{n-1} \left(\frac{2 \cdot k!(n-k)!}{(n+1)!} - \frac{k!(n-1-k)!}{n!} \right)$

$$= \frac{2^n}{(n+1)!} \sum_{k=0}^{n-1} \left(2 \cdot k!(n-k)! - (n+1)k!(n-1-k)!\right)$$

$$= \frac{2^n}{(n+1)!} \sum_{k=0}^{n-1} k!(n-1-k)!(n-2k-1) \underset{[i=n-1-k]}{=} \frac{2^n}{(n+1)!} \sum_{i=0}^{n-1} (n-1-i)!i!(-n+2i+1) = -T_n,$$

d'où $T_n = 0$.

Ainsi : $\forall n \in \mathbb{N}^*$, $\frac{2^{n+1}}{n+1} S_n = \frac{2^n}{n} S_{n-1} + \frac{2^{n+1}}{n+1}$,

d'où en sommant : $\forall n \in \mathbb{N}^*$, $\frac{2^{n+1}}{n+1} S_n = \sum_{k=0}^{n+1} \frac{2^k}{k} + 2S_0 = \sum_{k=1}^{n+1} \frac{2^k}{k}$.

3.4.1 $\tau_{13} \circ \tau_{12}(2) = 3$ et $\tau_{12} \circ \tau_{13}(2) = 1$, donc $\tau_{13} \circ \tau_{12} \neq \tau_{12} \circ \tau_{13}$.

3.4.2 **1re méthode**

Le nombre d'inversions de $\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ n & n-1 & \dots & 2 & 1 \end{pmatrix}$ est : $(n-1) + (n-2) + \dots + 1$,

d'où $\varepsilon(\sigma) = (-1)^{\frac{(n-1)n}{2}}$.

2ème méthode

On décompose σ en transpositions :

- n pair, $n = 2p$ ($p \in \mathbb{N}^*$), $\sigma = \tau_{1,2p} \circ \tau_{2,2p-1} \circ \dots \circ \tau_{p,p+1}$, d'où $\varepsilon(\sigma) = (-1)^p$
- n impair, $n = 2p+1$ ($p \in \mathbb{N}$), $\sigma = \tau_{1,2p+1} \circ \tau_{2,2p} \circ \dots \circ \tau_{p,p+2}$, d'où $\varepsilon(\sigma) = (-1)^p$.

◇ **Réponse :** $\varepsilon(\sigma) = (-1)^{\frac{n(n-1)}{2}} = (-1)^{E(\frac{n}{2})}$, ou encore : $\varepsilon(\sigma) = \begin{cases} 1 & \text{si } n \equiv 0 \text{ ou } 1 \quad [4] \\ -1 & \text{si } n \equiv 2 \text{ ou } 3 \quad [4] \end{cases}$.

3.4.3 On compte les inversions de σ ; ce sont les couples : $(2, 1)$, $(4, 1)$, $(4, 3)$, $(6, 1)$, $(6, 3)$, $(6, 5)$, $\dots$, $(2n, 1)$, $(2n, 3)$, $\dots$, $(2n, 2n-1)$. Il y en a donc $1 + 2 + 3 + \dots + n$.

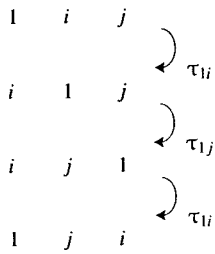
◇ **Réponse :** $\varepsilon(\sigma) = (-1)^{\frac{n(n+1)}{2}}$.

3.4.4 *a)* ◇ **Réponse :** $l(\sigma) = 27$, σ est impaire.

b) ◇ **Réponse :** $\sigma = \tau_{1,2} \circ \tau_{3,5} \circ \tau_{3,6} \circ \tau_{2,7} \circ \tau_{4,8} \circ \tau_{2,9} \circ \tau_{8,10} \circ \tau_{8,11} \circ \tau_{10,12}$.

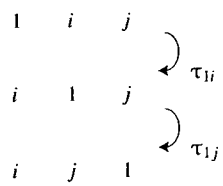
c) ◇ **Réponse :** $\sigma = (1,7,9,2) \circ (3,5,6) \circ (4,12,10,11,8)$, $\varepsilon(\sigma) = (-1)^{4-1}(-1)^{3-1}(-1)^{5-1} = -1$.

3.4.5 *a)*



Comme les transpositions engendrent $\mathfrak{S}_n$ et que toute transposition se décompose sur les τ_{1i} $(2 \leqslant i \leqslant n)$, on en déduit que $\{\tau_{1i};\ 2 \leqslant i \leqslant n\}$ engendre $\mathfrak{S}_n$.

b)



d'où $\tau_{1j} \circ \tau_{1i} = (1,i,j)$.

Soit $\sigma \in \mathcal{A}_n$. D'après *a)*, il existe $N \in \mathbb{N}^*$, $i_1,\ldots,i_N \in \{2,\ldots,n\}$ tels que $\sigma = \tau_{1i_1} \circ \ldots \circ \tau_{1i_N}$. Puisque σ est paire et que toute transposition est impaire, N est pair. En groupant les τ_{1i_k} $(1 \leqslant k \leqslant N)$ deux par deux, on conclut que σ se décompose sur les 3-cycles $(1,i,j)$, $(i,j) \in \{2,\ldots,n\}^2$, $i \neq j$.

c) D'après *b)*, $\tau_{1k} \circ \tau_{12} = (1,2,k)$ et $\tau_{12} \circ \tau_{1k} = (1,k,2) = (1,2,k)^2$.

D'où : $\gamma_i \circ \gamma_j^2 = (\tau_{1i} \circ \tau_{12}) \circ (\tau_{12} \circ \tau_{1j}) = \tau_{1i} \circ \tau_{1j}$.

On déduit alors de *b)* que toute σ de $\mathcal{A}_n$ se décompose sur les γ_i $(3 \leqslant i \leqslant n)$.

3.5.1 Il existe un objet ω n'appartenant pas à F. Notons $G = F \cup \{\omega\}$, $\mathcal{F}(E,F)$ l'ensemble des fonctions de E vers F. L'application qui, à tout f de $\mathcal{F}(E,F)$ associe l'application

$$E \longrightarrow G$$
$$x \longmapsto \begin{cases} f(x) \text{ si } x \text{ a une image par } f \\ \omega \text{ si } x \text{ n'a pas d'image par } f. \end{cases}$$

est une bijection.

Donc : $\#\big(\mathcal{F}(E,F)\big) = \#(G^E) = (\#(G))^{\#(E)}$.

◊ **Réponse :** $(p+1)^n$.

3.5.2 Soit a un élément fixé de $\{1,\ldots,n+1\}$ (par exemple $a = n+1$). La donnée d'une partition de $\{1,\ldots,n+1\}$ est définie par :

- la donnée d'une partie A de $\{1,\ldots,n+1\}$ telle que $a \in A$ (il y a C_n^k possibilités, où $k = \#(A) - 1$)
- puis la donnée d'une partition de $\{1,\ldots,n+1\} - A$.

On en déduit : $P_{n+1} = \sum_{k=0}^{n} C_n^k P_k$.

◊ **Réponse :**

n	0	1	2	3	4	5
P_n	1	1	2	5	15	52

3.5.3 *a)* Les partitions de $\{1,\dots,n+1\}$ en $p+1$ parties sont :

- d'une part, celles qui contiennent le singleton $\{n+1\}$ (il y en a $P_{n,p}$)
- d'autre part, celles qui ne contiennent pas le singleton $\{n+1\}$ (il y en a $(p+1)P_{n,p+1}$).

b) ◇ **Réponse :**

n \ p	1	2	3	4	5
1	1	0	0	0	0
2	1	1	0	0	0
3	1	3	1	0	0
4	1	7	6	1	0
5	1	15	25	10	1

c) • La donnée d'une partition de $\{1,\dots,n+1\}$ en n parties (donc non vides) revient à la donnée d'une paire de $\{1,\dots,n+1\}$, d'où $P_{n+1,n} = C_{n+1}^2 = \dfrac{n(n+1)}{2}$.

• La donnée d'une partition de $\{1,\dots,n+1\}$ en 2 parties (donc non vides) revient à la donnée d'une paire $\left(A, \complement_{\{1,\dots,n+1\}}(A)\right)$ où $A \neq \varnothing$, d'où $P_{n+1,2} = \dfrac{1}{2}(2^{n+1}-2) = 2^n - 1$.

• *Récurrence sur n*

La formule $P_{n+1,3} = \dfrac{3^n - 2^{n+1} + 1}{2}$ est évidente pour $n = 2$.

Si elle est vraie pour un n ($\geqslant 2$), alors :

$$P_{n+2,3} = P_{n+1,2} + 3P_{n+1,3} = 2^n - 1 + \frac{3}{2}(3^n - 2^{n+1} + 1)$$
$$= \frac{3^{n+1}}{2} - 2^{n+1} + \frac{1}{2} = \frac{3^{n+1} - 2^{n+2} + 1}{2}.$$

3.5.4 *a) 1)* Soit $x_1 \in E$ fixé. On a :

$$b_{n,k} = \#\Big(\Big\{f : E \longrightarrow \mathbb{N};\ \sum_{x\in E} f(x) = k\Big\}\Big) = \#\Big(\Big\{g : E - \{x_1\} \longrightarrow \mathbb{N};\ \sum_{x\in E-\{x_1\}} g(x) \leqslant k\Big\}\Big) = a_{n-1,k}.$$

2) L'ensemble $A_{n,k}$ est la réunion disjointe de $B_{n,k}$ et de $A_{n,k-1}$, d'où $a_{n,k} = b_{n,k} + a_{n,k-1}$.

b) 1) Récurrence sur $n+k$, pour montrer $a_{n,k} = C_{n+k}^k$.

- Si $n+k = 0$, alors $n = k = 0$, et $a_{0,0} = 1 = C_0^0$.
- Soit $p \in \mathbb{N}$, et supposons $a_{n,k} = C_{n+k}^k$ pour tout couple (n,k) de $\mathbb{N}^2$ tel que $n+k = p$.

Soit $(n,k) \in \mathbb{N}^2$ tel que $n+k = p+1$.

Si $n \geqslant 1$ et $k \geqslant 1$, alors $(n-1,k) \in \mathbb{N}^2$, $(n,k-1) \in \mathbb{N}^2$, et $(n-1)+k = n+(k-1) = p$, d'où, d'après l'hypothèse de récurrence :

$$a_{n,k} = a_{n-1,k} + a_{n,k-1} = C_{n-1+k}^k + C_{n+k-1}^{k-1} = C_{n+k}^k.$$

De plus : $a_{0,k} = a_{n,0} = 1$.

Indications et réponses
pour les exercices du chapitre 4

4.1.1 • Si $n = 2p$ ($p \in \mathbb{Z}$), alors $n^2 = 4p^2$, donc $n^2 \equiv 0$ [4], d'où $n^2 \equiv 0$ ou 4 [8].

• Si $n = 2p + 1$ ($p \in \mathbb{Z}$), alors $n^2 = 4p(p + 1) + 1$, donc $n^2 \equiv 1$ [8], car $p(p + 1)$ est pair, vu que p ou $p + 1$ est pair.

4.1.2 Remarquer : $5^{2^{n-2}} - 1 = 4\prod_{k=0}^{n-3}(5^{2^k} + 1)$ (si $n \geqslant 3$), et chacun des facteurs $5^{2^k} + 1$ ($k \in \mathbb{N}$) est pair, mais congru à 2 modulo 4.

4.1.3 $$\sum_{k=1}^{2n} \frac{(2n)!}{k} = \sum_{k=1}^{n} \frac{(2n)!}{k} + \sum_{k=n+1}^{2n} \frac{(2n)!}{k} = \sum_{k=1}^{n} \frac{(2n)!}{k} + \sum_{l=1}^{n} \frac{(2n)!}{2n+1-l}$$
$$= \sum_{k=1}^{n} (2n)! \left(\frac{1}{k} + \frac{1}{2n+1-k} \right) = (2n+1) \sum_{k=1}^{n} \frac{(2n)!}{k(2n+1-k)}.$$

Comme, pour tout k de $\{1, \ldots, n\}$, k et $2n+1-k$ sont distincts et inférieurs à $2n$, le rationnel $\dfrac{(2n)!}{k(2n+1-k)}$ est un entier.

4.1.4 Récurrence sur n.

La propriété est immédiate pour $n = 1$.

Supposons-la vraie pour un n de $\mathbb{N}^*$. Comme $\big(5(n+1)\big)! = (5n)! \cdot (5n+1)(5n+2)(5n+3)(5n+4)(5n+5)$ et $40^{n+1}(n+1)! = (40^n n!)40(n+1)$, il suffit alors de prouver : $8 \mid (5n+1)(5n+2)(5n+3)(5n+4)$.

Parmi les quatre nombres consécutifs $5n+1$, $5n+2$, $5n+3$, $5n+4$, il y en deux qui sont pairs, et l'un de ces deux derniers est multiple de 4. On peut aussi remarquer : $C_{5n+4}^4 \in \mathbb{N}$.

4.1.5 En notant $\alpha = 2n - 1$ et $u_n = (3n^2-3n+1)(3n^2-3n+2)$, on a $u_n = \dfrac{1}{16}(3\alpha^2+1)(3\alpha^2+5)$, d'où :

$$2n - 1 \mid u_n \Longrightarrow \alpha \mid (3\alpha^2 + 1)(3\alpha^2 + 5) \Longrightarrow \alpha \mid 5 \Longrightarrow \alpha \in \{1,5\} \Longrightarrow n = 3.$$

Réciproquement, $u_3 = 380$ est divisible par 5.

4.1.6 Notons $E_n = \{k \in \mathbb{N};\ n! < k < (n+1)!\}$. Pour qu'il existe $k \in E_n$ tel que $n^3 | k$, il suffit que E_n contienne au moins n^3 nombres consécutifs (parmi lesquels il y aura alors un multiple de n^3). Comme $\mathrm{Card}(E_n) = (n+1)! - n! - 1 = n \cdot n! - 1$, il suffit que : $\forall n \geqslant 4$, $n \cdot n! \geqslant n^3 + 1$, ce qui se montre facilement (par récurrence sur n).

4.1.7 En notant $m = ad + bc$, il existe $(\alpha,\beta,\gamma,\delta) \in \mathbb{Z}^4$ tel que $a = m\alpha,\ldots,d = m\delta$. Alors : $m = ad + bc = m^2(\alpha\delta + \beta\gamma)$, d'où $m^2 | m$, $m \in \{-1,0,1\}$.

4.1.8 En notant $r_1 = \dfrac{3-\sqrt{5}}{2}$, $r_2 = \dfrac{3+\sqrt{5}}{2}$, et $u_n = r_1^n + r_2^n$ $(n \in \mathbb{N})$, $(u_n)_{n\geqslant 0}$ est une suite récurrente linéaire du second ordre à coefficients constants (cf. Tome 1, 3.4.2 2)), et on a :

$$\forall n \in \mathbb{N},\quad u_{n+2} - (r_1 + r_2)u_{n+1} + r_1 r_2 u_n = 0,$$

c'est-à-dire : $\forall n \in \mathbb{N}, u_{n+2} = 3u_{n+1} - u_n$.

Comme $u_0 = 2$ et $u_1 = 3$, il est alors clair (par récurrence à deux pas sur n) que : $\forall n \in \mathbb{N}, u_n \in \mathbb{Z}$, et même, comme $r_1 \geqslant 0$ et $r_2 \geqslant 0$: $\forall n \in \mathbb{N}, u_n \in \mathbb{N}$.

Ainsi, pour tout n de $\mathbb{N}$, $(3+\sqrt{5})^n + (3-\sqrt{5})^n = 2^n u_n$, donc est un entier divisible par 2^n.

4.1.9 *a)* Remarquer d'abord : $\forall n \in \mathbb{Z}, 3n + 4 \neq 0$.

En notant $m = n + 1$, on a : $\dfrac{11n+8}{3n+4} = \dfrac{11m-3}{3m+1} \xrightarrow[|m|\infty]{} \dfrac{11}{3} < 4$.

Notons $k = \dfrac{11m-3}{3m+1} \in \mathbb{Q}$.

- Si $k \in \mathbb{Z}$ et $|k| \geqslant 4$, alors : $11|m| + 3 \geqslant |11m + 3| = |k|\,|3m + 1| \geqslant 4(3|m| - 1)$, d'où : $|m| \leqslant 7$.

Tester les valeurs $-7,-6,\ldots,7$ de m.

- Tester les valeurs $-3,-2,\ldots,3$ de k.

Remarque : la question revient à déterminer les points à coordonnées entières sur l'hyperbole d'équation $y = \dfrac{11x+8}{3x+4}$.

◇ **Réponse :** $\{-8,-3,-2,-1,0,2\}$.

b) Montrer d'abord : $\forall n \in \mathbb{Z}$, $\begin{cases} n^2 - 6 \neq 0,\ n^2 + 3n - 2 \neq 0 \\ \dfrac{n^2-6}{n^2+3n-2} \neq 1 \quad \text{et} \quad \neq -1 \end{cases}$.

Alors, si $\dfrac{n^2-6}{n^2+3n-2} \in \mathbb{Z}$:

$$n^2 + 6 \geqslant |n^2 - 6| \geqslant 2|n^2 + 3n - 2| \geqslant 2(n^2 - 3|n| - 2),$$

d'où $n^2 - 6|n| - 10 \leqslant 0$, et donc $|n| \leqslant 3 + \sqrt{19} < 8$.

Tester les valeurs $-7,-6,\ldots,7$ de n.

◇ **Réponse :** $\{-4,0\}$.

4.1.10 Remarquer : $a^3 + b^3 + c^3 - 3abc = (a + b + c)(a^2 + b^2 + c^2 - ab - ac - bc)$.

4.1.11 • On a : $\forall k \in \mathbb{N}^*, (k|n \Longrightarrow a^k - 1 \mid a^n - 1)$.

En effet, si $n = km$, $(k,m) \in (\mathbb{N}^*)^2$, alors : $a^n - 1 = (a^k)^m - 1 = (a^k - 1)\displaystyle\sum_{i=0}^{m-1}(a^k)^i$.

- Comme l'application $\begin{array}{ccc} \mathbb{N}^* & \longrightarrow & \mathbb{N}^* \\ k & \longmapsto & a^k - 1 \end{array}$ est injective (car $a \geqslant 2$), on conclut : $\mathrm{d}(a^n - 1) \geqslant \mathrm{d}(n)$.

4.1.12 1^er^ **cas : k impair,** $k = 2l+1, l \in \mathbb{N}$.

Alors : $m = d_1 d_{2l+1} = d_2 d_{2l} = \ldots = d_l d_{l+2} = d_{l+1}^2$, d'où $\left(\sum_{i=1}^{k} d_i\right)^2 = \prod_{i=1}^{k} d_i d_{2l+2-i} = n^k$.

2^ème^ **cas : k pair,** analogue.

4.1.13 *a)* $xy = 2x + 3y \iff (x-3)(y-2) = 6$.

◊ **Réponse :** $\{(-3,1),(0,0),(1,-1),(2,-4),(4,8),(5,5),(6,4),(9,3)\}$.

b) $x^2 - y^2 - x + 3y = 30 \iff \left(x - \frac{1}{2}\right)^2 - \left(y - \frac{3}{2}\right)^2 = 28 \iff (x+y-2)(x-y+1) = 28$.

◊ **Réponse :** $\{(-14,-12),(-5,0),(-5,3),(-14,15),(15,-12),(6,0),(6,3),(15,15)\}$.

c) $\frac{1}{x} + \frac{1}{y} = \frac{1}{5} \iff xy = 5(x+y) \iff (x-5)(y-5) = 25$.

◊ **Réponse :** $\{(-20,4),(4,-20),(6,30),(10,10),(30,6)\}$.

d) $x^2 - 3xy + 2y^2 + x - 3y - 6 = 0 \iff (x-y+2)(x-2y-1) = 4$.

◊ **Réponse :** $\{(-12,-6),(-7,-3),(-3,0),(-7,-6),(-3,-3),(2,0)\}$.

e) $2x^3 + xy - 7 = 0 \iff x(2x^2+y) = 7$.

◊ **Réponse :** $\{(-7,-99),(-1,-9),(1,5),(7,-97)\}$.

f) Remarquer d'abord les rôles symétriques de x et y, ce qui permet de se ramener à $x \leqslant y$.

Si $x^3 + xy + y^3 = 209$, alors :

- $y^3 \leqslant 209$, donc $y \leqslant 5$
- $209 \leqslant y^3 + y^2 + y^3 \leqslant 3y^3$, donc $y \geqslant 5$.

◊ **Réponse :** $\{(4,5),(5,4)\}$.

g) En notant $t = x + 4$, l'équation se ramène à : $(t^2-9)(t^2-16) = y^2$, et on a alors $t^2 \leqslant 9$ ou $t^2 \geqslant 16$.

- Tester les valeurs $-3,-2,\ldots,3$ de t.
- Si $t^2 \geqslant 16$, alors $(t^2-16)^2 \leqslant y^2 \leqslant (t^2-9)^2$; résoudre chacune des équations $(t^2-k)^2 = (t^2-9)(t^2-16)$, pour $k \in \{9,\ldots,16\}$.

◊ **Réponse :** $\{(-9,12),(-8,0),(-7,0),(-4,-12),(-4,12),(-1,0),(0,0),(1,12)\}$.

h) $x^2 = 9y^2 - 39y + 40 \iff (2x - 6y + 13)(2x + 6y - 13) = -9$.

◊ **Réponse :** $\{(-2,3),(2,3)\}$.

i) Soit (x,y,z) convenant. On a : $x^3 = y^3 + z^3 + 3xyz \geqslant y^3$, donc $x \geqslant y$, et aussi $x \geqslant z$.

Puis $x^2 = 2(y+z) \leqslant 4x$ et x est pair, donc $x \in \{0,2,4\}$.

◊ **Réponse :** $\{(0,0,0),\ (2,0,2),\ (2,1,1),\ (2,2,0)\}$.

j) Si (x,y,z) convient, alors : $4(x^2+y^2) = 4z^2 = \big(xy - 2(x+y)\big)^2$, d'où $xy\big(xy - 4(x+y) + 8\big) = 0$, et donc $(x-4)(y-4) = 8$.

◊ **Réponse :** $\{(5,12,13),\ (6,8,10),\ (8,6,10),\ (12,5,13)\}$.

k) Soit (x,y) convenant.

Comme 3^x est impair, y est impair, et donc (cf. exercice 4.1.1 p. 103), $y^2 \equiv 1$ [8].

D'autre part, si x est impair, $3^x \equiv 3$ [8], contradiction. Donc x est pair, $x = 2X$, $X \in \mathbb{N}$. Alors : $(3^X - y)(3^X + y) = 8$, d'où $3^X \leqslant 8$, $X \in \{0,1\}$.

◇ **Réponse :** $\{(2,1)\}$.

4.1.14 *1)* Dans les exemples ne faisant intervenir n qu'en exposant, on peut souvent utiliser des congruences. Par exemple, pour *a)* :

$$2^{2n+1} + 3^{2n+1} = 4^n \cdot 2 + 9^n \cdot 3 \underset{[5]}{\equiv} 4^n(2+3) \underset{[5]}{\equiv} 0.$$

On peut résoudre ainsi les exemples : *a), c), e), f), h), l), m), o), p), q), r).*

2) Dans les exemples mélangeant des exponentielles et des polynômes, une récurrence permettra souvent de conclure. Par exemple, pour *b)*, en notant $u_n = 4^n - 1 - 3n$, on a $u_0 = 0$, et, si $u_n \equiv 0$ [9], alors

$$u_{n+1} = 4^{n+1} - 1 - 3(n+1) = 4(u_n + 1 + 3n) - 3n - 4 = 4u_n + 9n \equiv 0 \quad [9].$$

On peut résoudre ainsi les exemples : *b), d), g), i), j), k), n), s), t).*

u) Notons $u_n = 3 \cdot 81^{n+1} + (16n - 54)9^{n+1} - 320n^2 - 144n + 243$.

On a : $u_n = \big(3 \cdot 9^{n+1} + (40n - 27)\big)\big(9^{n+1} + (-8n - 9)\big) = 64\alpha_n\beta_n$,

où $\alpha_n = \dfrac{1}{8}\big(27(9^n - 1) + 40n\big) = 27\displaystyle\sum_{k=0}^{n-1} 9^k + 5n$ et $\beta_n = \dfrac{1}{8}\big(9(9^n - 1) - 8n\big) = 9\displaystyle\sum_{k=0}^{n-1} 9^k - n$.

Comme $9 \equiv 1$ [8], on a : $\alpha_n \underset{[8]}{\equiv} 27\displaystyle\sum_{k=0}^{n-1} 1 + 5n = 32n \underset{[8]}{\equiv} 0$ et $\beta_n \underset{[8]}{\equiv} 9\displaystyle\sum_{k=0}^{n-1} 1 - n = 8n \underset{[8]}{\equiv} 0$.

Ainsi : $8|\alpha_n$ et $8|\beta_n$, d'où $2^{12} = 64^2 \mid u_n$.

4.1.15 Récurrence sur n (pour $a \in \mathbb{Z}$ impair fixé).

- $n = 3$: $a^{2^{n-2}} = a^2 \equiv 1$ [8] (cf. exercice 4.1.1 p. 103).
- Supposons $a^{2^{n-2}} \equiv 1$ [2^n] ; il existe $\lambda \in \mathbb{Z}$ tel que : $a^{2^{n-2}} = 1 + \lambda 2^n$. On a alors :

$$a^{2^{n-1}} = \left(a^{2^{n-2}}\right)^2 = (1 + \lambda 2^n)^2 = 1 + \lambda 2^{n+1} + \lambda^2 2^{2n} \equiv 1 \quad [2^{n+1}],$$

car $2n \geqslant n + 1$.

4.1.16 • Dans $\mathbb{Z}/7\mathbb{Z}$:

$\widehat{x}$	$\widehat{-3}$	$\widehat{-2}$	$\widehat{-1}$	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$
x^3	$\widehat{1}$	$\widehat{-1}$	$\widehat{-1}$	$\widehat{0}$	$\widehat{1}$	$\widehat{1}$	$\widehat{-1}$

• Soit $(a,b,c) \in \mathbb{Z}^3$ tel que $7 \nmid abc$. Alors $\widehat{a} \neq \widehat{0}$, $\widehat{b} \neq \widehat{0}$, $\widehat{c} \neq \widehat{0}$, donc $(\widehat{a}^3, \widehat{b}^3, \widehat{c}^3) \in \{\widehat{-1},\widehat{1}\}^3$, d'où $\widehat{a}^3 + \widehat{b}^3 + \widehat{c}^3 \in \{\widehat{-3},\widehat{-1},\widehat{1},\widehat{3}\}$ et donc $7 \nmid a^3 + b^3 + c^3$.

4.1.17 $n^2 + (n+1)^2 + (n+3)^2 = 3n^2 + 8n + 10 \underset{[10]}{\equiv} 3n^2 - 2n$.

Modulo 10 :

n	-4	-3	-2	-1	0	1	2	3	4	5
$3n^2 - 2n$	-4	3	-4	5	0	1	-2	1	0	5

◊ **Réponse :** $n \equiv 0$ ou 4 [10].

4.1.18 • Si n est pair, $n = 2k$ ($k \in \mathbb{N}$), alors :

$$3^n + 4n + 1 = 9^k + 8k + 1 \underset{[8]}{\equiv} 1 + 8k + 1 \underset{[8]}{\equiv} 2.$$

• Si n est impair, $n = 2k + 1$ ($k \in \mathbb{N}$), alors :

$$3^n + 4n + 1 = 3 \cdot 9^k + 8k + 5 \underset{[8]}{\equiv} 3 + 8k + 5 \underset{[8]}{\equiv} 0.$$

◊ **Réponse :** n impair.

4.1.19 *a)* Comme $2^6 = 64 \equiv 1$ [21], la classe de 2^n modulo 21 dépend de la classe de n modulo 6 :

n mod. 6	0	1	2	3	4	5
2^n mod. 21	1	2	4	8	-5	-10
2^{2n} mod. 21	1	4	-5	1	4	-5
$2^{2n} + 2^n + 1$ mod. 21	3	7	0	10	0	-14

◊ **Réponse :** $n \equiv 2$ ou 4 [6].

b) Comme $2^3 = 8 \equiv 1$ [7], la classe de 2^n modulo 7 dépend de la classe de n modulo 3. D'autre part, puisque $2^2 = 4 \equiv 1$ [3], la classe de 2^n modulo 3 dépend de la classe de n modulo 2. D'où le tableau :

n mod. 6	0	1	2	3	4	5
2^n mod. 7	1	2	4	1	2	4
2^n mod. 3	1	2	1	2	1	2
2^{2^n} mod. 7	2	4	2	4	2	4
$2^{2^n} + 2^n + 1$ mod. 7	4	0	0	6	5	2

◊ **Réponse :** $n \equiv 1$ ou 2 [6].

4.1.20 Comme $3^2 \equiv 1$ [8], on a : $3^n \equiv 1$ ou 3 [8], et donc $3^n + 1 \equiv 2$ ou 4 [8]. Ceci prouve : $8 \nmid 3^n + 1$. Par ailleurs, l'étude du cas $n = 2$ est immédiate.

4.1.21 Calculer les classes modulo 23 de 2^k et 3^k pour $k = 0, 1, 2, \ldots$. On remarque : $2^{11} \equiv 1$ [23] et $3^{11} \equiv 1$ [23]. Ainsi, les classes de 2^k et 3^k modulo 23 dépendent de la classe de k modulo 11.

k mod. 11	0	1	2	3	4	5	6	7	8	9	10
2^k mod. 23	1	2	4	8	-7	9	-5	-10	3	6	12
3^k mod. 23	1	3	9	4	12	-10	-7	2	6	-5	8

En notant $A = \{\widehat{1},\widehat{2},\widehat{4},\widehat{8},\widehat{-7},\widehat{9},\widehat{-5},\widehat{-10},\widehat{3},\widehat{6},\widehat{-11}\}$ et $B = \{\widehat{-1},\widehat{-3},\widehat{-9},\widehat{-4},\widehat{11},\widehat{10},\widehat{7},\widehat{-2},\widehat{-6},\widehat{5},\widehat{-8}\}$,

on a : $\begin{cases} \forall a \in \mathbb{N}, \quad \widehat{2^a} \in A \\ \forall b \in \mathbb{N}, \quad \widehat{-3^b} \in B \\ A \cap B = \varnothing. \end{cases}$

On conclut : $\forall (a,b) \in \mathbb{N}^2,\ 23 \nmid 2^a + 3^b$.

4.1.22 *a)* Si (x,y) est solution, alors $5y^2 \leqslant 3$, d'où $y^2 < 1$, $y = 0$, puis $x^2 = 3$, contradiction.

b) Passer modulo 5 :

x mod. 5	0	1	2
x^2 mod. 5	0	1	-1

Ainsi : $\forall x \in \mathbb{Z}, x^2 \equiv -1,0$ ou 1 [5].
Mais, si $x^2 - 5y^2 = 3$, alors $x^2 \equiv 3$ [5], contradiction.

c) Soit (x,y) une solution. Alors $3|7y^2$, donc $3|y$ (car 3 est premier, au bien en séparant en cas : $y \equiv -1,0,1$ [3]). Il existe donc $Y \in \mathbb{Z}$ tel que $y = 3Y$, et : $5x^2 - 21Y^2 = 3$. De même, $3|5x^2$, $3|x$.
Il existe donc $X \in \mathbb{Z}$ tel que $x = 3X$, et : $15X^2 - 7Y^2 = 1$.
En passant modulo 3, on déduit $Y^2 \equiv -1$ [3]. Mais on a : $\forall Y \in Z, Y^2 \equiv 0$ ou 1 [3], d'où une contradiction.

d) Passer modulo 8 et utiliser l'exercice 4.1.1 p. 103.

e) Si (x,y) est solution, en passant modulo 3, on déduit $x^3 - x - 1 \equiv 0$ [3].
Mais d'autre part : $\forall x \in \mathbb{Z}, x^3 - x - 1 \equiv -1$ [3], comme on le voit en séparant en cas $x \equiv -1,0,1$ [3].

f) Supposons qu'il existe une solution (x,y).

1) $x^3 + 11^3 \geqslant 12^3 \Longrightarrow x^3 \geqslant 397 \Longrightarrow x \geqslant 8$.

2) • $y^3 = x^3 + 11^3 > x^3 \Longrightarrow y > x \Longrightarrow y \geqslant x + 1$.

- Modulo 2 : $x^3 \equiv x$, $y^3 \equiv y$, $11^3 \equiv 1$, donc $y \equiv x + 1$ [2]. En particulier $y \neq x + 2$.
- Modulo 3 : $x^3 \equiv x$, $y^3 \equiv y$, $11^3 \equiv -1$, donc $y \equiv x - 1$ [3]. En particulier $y \neq x + 1$.

On a donc $y \geqslant x + 3$, puis :

$$11^3 = y^3 - x^3 \geqslant (x+3)^3 - x^3 = 9x^2 + 27x + 27,$$

d'où $9x^2 + 27x - 1304 \leqslant 0$, et donc $x \leqslant 10$.
Tester les valeurs 8, 9, 10 de x.
Finalement, l'équation proposée n'a pas de solution.

4.1.23 α) Soit (x,y,z) convenant. À cause des rôles symétriques de x,y,z, on peut se ramener au cas : $1 \leqslant x \leqslant y \leqslant z$.

Alors : $\left\{\begin{array}{l} 1 \leqslant x + y - 1 \leqslant 2z - 1 \\ z \mid x + y - 1 \end{array}\right.$, donc $z = x + y - 1$.

Puis : $\left\{\begin{array}{l} 1 \leqslant z + x - 1 = 2x + y - 2 \leqslant 3y - 2 \\ y \mid 2x + y - 2 \end{array}\right.$, donc $2x + y - 2 \in \{y, 2y\}$.

1) Si $2x + y - 2 = y$, alors $x = 1$ et $z = y$.

2) Supposons $2x + y - 2 = 2y$; alors $y = 2x - 2$ et $z = 3x - 3$. Dans ce cas, on a :

$$\begin{cases} x+y \equiv 1 \quad [z] \\ y+z \equiv 1 \quad [x] \\ z+x \equiv 1 \quad [y] \end{cases} \iff \begin{cases} 3x-3 \equiv 0 \quad [3x-3] \\ 5x-6 \equiv 0 \quad [x] \\ 4x-4 \equiv 0 \quad [2x-2] \end{cases} \iff 5x \equiv 6\,[x] \iff x|6 \iff x \in \{1,2,3,6\}.$$

β) Vérifier que les triplets obtenus conviennent.

◇ **Réponse :** $\{(1,y,y);\ y \in \mathbb{N}^*\} \cup \{(2,2,3),\ (3,4,6),\ (6,10,15)\}$.

4.1.24 D'après l'exercice 4.1.1 p. 103 : $n^2 \equiv 1\ [8]$. Il existe donc $\lambda \in \mathbb{Z}$ tel que $n^2 = 1 + 8\lambda$, d'où : $n^4 = 1 + 16\lambda + 64\lambda^2 \equiv 1\ [16]$.

4.1.25 Modulo 10 :

- $2^{100} = (2^5)^{20} \equiv 2^{20} = (2^5)^4 \equiv 2^4 \equiv 6$
- $3^{100} = (3^4)^{25} \equiv 1^{25} = 1$
- $4^{100} = (2^{100})^2 \equiv 6^2 \equiv 6$
- $5^{100} \equiv 5$
- $6^{100} \equiv (-4)^{100} = 4^{100} \equiv 6$, ... en passant par les opposés.

◇ **Réponse :** 3.

4.1.26 Puisque $2^4 \equiv 1\ [5]$, $3^4 \equiv 1\ [5]$, $4^4 \equiv 1\ [5]$, les classes de $2^n, 3^n, 4^n, 5^n$ modulo 5 dépendent de la classe de n modulo 4 :

n mod. 4	1	2	3	4
2^n mod. 5	2	−1	−2	1
3^n mod. 5	−2	−1	2	1
4^n mod. 5	−1	1	−1	1
$1^n + 2^n + 3^n + 4^n$ mod. 5	0	0	0	4

Ainsi : $5 \mid 1^n + 2^n + 3^n + 4^n \iff n \equiv 1$ ou 2 ou 3 $[4] \iff 4 \nmid n$.

4.1.27 $3^4 = 81 \equiv 1\ [10]$, donc, modulo 10 : $3^{a+4b} = 3^a \cdot (3^4)^b \equiv 3^a \equiv -1$, $3^{a-4b} \cdot 3^{4b} = 3^a \equiv -1$ et $3^{a-4b} \cdot 3^{4b} \equiv 3^{a-4b}$.

Cet exercice évident revient aussi à : $\forall n \in \mathbb{N},\ 3^{2+4n} \equiv -1\ [10]$.

4.1.28 Soit $k \in \mathbb{N} - \{0,1\}$. S'il existe $N \in \mathbb{N}^*$ tel que $(\phi_N = \phi_0$ et $\phi_{N+1} = \phi_1)$, alors, à l'aide d'un raisonnement par récurrence, on voit que la suite $(\phi_n \bmod k)_{n\in\mathbb{N}}$ est N-périodique, et donc $\phi_n \bmod k$ ne dépend que de la classe de n modulo N.

a)

n	0	1	2	3	4
ϕ_n mod. 2	0	1	1	0	1

La suite $(\phi_n \bmod 2)_{n\in\mathbb{N}}$ est 3-périodique et répète la séquence $(0,1,1)$.

Donc : $2|\phi_n \iff n \equiv 0\ [3] \iff 3|n$.

b)

n	0	1	2	3	4	5	6	7	8	9
$\phi_n \bmod 3$	0	1	1	−1	0	−1	−1	1	0	1

La suite $(\phi_n \bmod 3)_{n\in\mathbb{N}}$ est 8-périodique et : $3|\phi_n \iff n \equiv 0$ ou $4\ [8] \iff n \equiv 0\ [4] \iff 4|n$.

c)

n	0	1	2	3	4	5	6	7
$\phi_n \bmod 4$	0	1	1	2	−1	1	0	1

La suite $(\phi_n \bmod 4)_{n\in\mathbb{N}}$ est 6-périodique, et : $4|\phi_n \iff n \equiv 0\ [6] \iff 6|n$.

4.1.29 $2^{2^n} \equiv -1\ [F_n]$, d'où : $2^{F_n} = 2\cdot 2^{2^{2^n}} = 2\left(2^{2^n}\right)^{2^{2^n}-n} \underset{[F_n]}{\equiv} 2(-1)^{2^{2^n}-n} \equiv 2$, car $2^{2^n}-n$ est pair, vu que $2^n - n \geqslant 1$.

4.1.30 D'abord, il est clair que les $k\mathbb{Z}$ $(k \in \mathbb{N})$ sont des sous-groupes de $(\mathbb{Z},+)$.

Soit G un sous-groupe de $\mathbb{Z}$; supposons $G \neq \{0\}$. Il existe $a \in G$ tel que $a \neq 0$.

Si $a > 0$, alors $G \cap \mathbb{N}^* \neq \varnothing$.

Si $a < 0$, alors $-a \in G$, et donc $G \cap \mathbb{N}^* \neq \varnothing$.

Ainsi, $G \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}^*$, donc admet un plus petit élément, noté k.

Montrons $G = k\mathbb{Z}$.

1) Comme $k \in G$, un raisonnement par récurrence montre : $\forall n \in \mathbb{N}$, $kn \in G$, puis, en passant aux opposés : $\forall n \in \mathbb{Z}$, $kn \in G$. On conclut : $k\mathbb{Z} \subset G$.

2) Réciproquement, soit $x \in G$. Par division euclidienne de x par k, il existe $(q,r) \in \mathbb{Z}^2$ tel que :

$$x = kq + r \text{ et } 0 \leqslant r < k.$$

Comme $x \in G$, $kq \in G$, et que G est un sous-groupe de $\mathbb{Z}$, on obtient $r \in G$, puis, par définition de k, $r = 0$.

Ainsi : $x = kq \in k\mathbb{Z}$.

4.1.31 Soit H un sous-groupe de $(\mathbb{Z}/n\mathbb{Z},+)$. Puisque la surjection canonique $s : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ est un morphisme de groupes, $s^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$ (cf. exercice 2.2.12 *b)* p. 54).

D'après l'exercice 4.1.30, il existe $k \in \mathbb{Z}$ tel que $s^{-1}(H) = k\mathbb{Z}$.

Comme s est surjective, on a : $H = s(s^{-1}(H)) = s(k\mathbb{Z}) = \widehat{k}\,\mathbb{Z}/n\mathbb{Z}$.

◇ **Réponse :** Les sous-groupes de $(\mathbb{Z}/n\mathbb{Z},+)$ sont les $\widehat{k}\,\mathbb{Z}/n\mathbb{Z}$, $k \in \mathbb{Z}$.

4.1.32 Notons a un générateur du groupe monogène G : $G =< \{a\} >$. L'application $\varphi : \mathbb{Z} \longrightarrow G$, $n \longmapsto a^n$ est un morphisme de groupes puisque :

$$\forall (m,n) \in \mathbb{Z}^2,\quad \varphi(m+n) = a^{m+n} = a^m a^n = \varphi(m)\varphi(n).$$

De plus, φ est surjectif, puisque $G = \{a^n ; n \in \mathbb{Z}\}$.

1er cas

Si φ est injectif, alors φ est un isomorphisme de groupes, et donc $G \simeq \mathbb{Z}$. En particulier, G est infini.

2ème cas

Supposons φ non injectif. Comme $\mathrm{Ker}(\varphi)$ est un sous-groupe de $\mathbb{Z}$ (cf. 2.2 Prop. 2. p. 52), d'après l'exercice 4.1.30, il existe $n \in \mathbb{N}$ tel que $\mathrm{Ker}(\varphi) = n\mathbb{Z}$.

Comme $\mathrm{Ker}(\varphi) \neq \{0\}$, on a : $n \in \mathbb{N}^*$.

Les éléments $e,a,a^2,\ldots,a^{n-1}$ de G sont deux à deux distincts car, si $(k,l) \in \{0,\ldots,n-1\}^2$ vérifie $a^k = a^l$, alors $l - k \in \mathrm{Ker}(\varphi)$, $n \mid l - k$, et donc $l = k$.

Ainsi : $G = \{e,a,a^2,\ldots,a^{n-1}\}$.

Vérifier que l'application $\psi : G \longrightarrow \mathbb{Z}/n\mathbb{Z}$ $(0 \leqslant k \leqslant n-1)$ est un isomorphisme de groupes.
$a^k \longmapsto \widehat{k}$

4.1.33 Dans $\mathbb{Z}/17\mathbb{Z}$:

• $2\widehat{x} + 3\widehat{y} = \widehat{0} \iff \widehat{3}\,\widehat{y} = -\widehat{2}\,\widehat{x} \iff \widehat{y} = \widehat{6}(-\widehat{2}\,\widehat{x}) = \widehat{5}\,\widehat{x}$, car $\widehat{6}\cdot\widehat{3} = \widehat{1}$

• $9\widehat{x} + 5\widehat{y} = \widehat{0} \iff \widehat{5}\,\widehat{y} = -\widehat{9}\,\widehat{x} \iff \widehat{y} = \widehat{7}\cdot(-\widehat{9}\,\widehat{x}) = \widehat{5}\widehat{x}$, car $\widehat{7}\cdot\widehat{5} = \widehat{1}$.

4.1.34 *a)* $x^2 + x + \widehat{7} = \widehat{0} \iff x^2 + \widehat{14}x + \widehat{7} = 0 \iff (x + \widehat{7})^2 - \widehat{42} = 0 \iff (x + \widehat{7})^2 = \widehat{3}$.
On remarque $\widehat{3} = \widehat{4}^2$. D'où :

$$(x + \widehat{7})^2 = \widehat{3} \iff (x + \widehat{7} - \widehat{4})(x + \widehat{7} + \widehat{4}) = \widehat{0} \iff (\widehat{x} = -3 \text{ ou } \widehat{x} = -\widehat{11}),$$

car $\mathbb{Z}/13\mathbb{Z}$ est un corps (13 est premier).

◇ **Réponse :** $\{-\widehat{3},\widehat{2}\}$.

b) $x^2 - \widehat{4}x + \widehat{3} = \widehat{0} \iff (x - \widehat{2})^2 = \widehat{1}$.
On calcule les carrés dans $\mathbb{Z}/12\mathbb{Z}$:

t	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$	$\widehat{4}$	$\widehat{5}$	$\widehat{6}$
t^2	$\widehat{0}$	$\widehat{1}$	$\widehat{4}$	$-\widehat{3}$	$\widehat{4}$	$\widehat{1}$	$\widehat{0}$

Ainsi : $\forall t \in \mathbb{Z}/12\mathbb{Z}$, $(t^2 = \widehat{1} \iff t \in \{-\widehat{5},-\widehat{1},\widehat{1},\widehat{5}\})$.

◇ **Réponse :** $\{-\widehat{5},-\widehat{3},\widehat{1},\widehat{3}\}$.

4.1.35 Soient $x_1,\ldots,x_5 \in \mathbb{Z}$.

• Si $-\widehat{1},\widehat{0},\widehat{1}$ (dans $\mathbb{Z}/3\mathbb{Z}$) figurent parmi $\widehat{x_1},\ldots,\widehat{x_5}$, alors l'une au moins des sommes de trois termes est $\widehat{0}$.

• Sinon, l'un au moins des éléments $-\widehat{1},\widehat{0},\widehat{1}$ est répété trois fois et l'une des sommes de trois termes vaut $\widehat{0}$.

4.1.36 Soient $n \in \mathbb{N}^*$, $(a,b,c,d) \in \mathbb{N}^4$ tel que $2^n = a^2 + b^2 + c^2 + d^2$. Comme a,b,c,d jouent des rôles symétriques, en permutant éventuellement a,b,c,d, il existe $\alpha \in \mathbb{N}$ tel que : $2^\alpha \mid a$, $2^\alpha \mid b$, $2^\alpha \mid c$, $2^\alpha \mid d$, $2^{\alpha+1} \nmid a$, puis il existe a' impair, $(b',c',d') \in \mathbb{N}^3$ tels que : $a = 2^\alpha a'$, $b = 2^\alpha b'$, $c = 2^\alpha c'$, $d = 2^\alpha d'$.
Alors : $a'^2 + b'^2 + c'^2 + d'^2 = 2^{n-2\alpha}$, et donc $n - 2\alpha \geqslant 0$.

1er cas : a',b',c',d' impairs.

Alors (cf. exercice 4.1.1 p. 103) : $a'^2 \equiv 1\ [8], \ldots, d'^2 \equiv 1\ [8]$, d'où $2^{n-2\alpha} \equiv 4\ [8]$, donc $n-2\alpha = 2$, puis $a' = b' = c' = d' = 1$, $a = b = c = d = 2^\alpha$.

2ème cas : a',b' impairs, c',d' pairs (à l'ordre près). Alors $a'^2 \underset{[4]}{\equiv} 1$, $b'^2 \underset{[4]}{\equiv} 1$, $c'^2 \underset{[4]}{\equiv} 0$, $d'^2 \underset{[4]}{\equiv} 0$, d'où $2^{n-2\alpha} \equiv 2\ [4]$, $n-2\alpha = 1$, puis $a' = b' = 1$, $c' = d' = 0$, $a = b = 2^\alpha$, $c = d = 0$.

3ème cas : a' impair, b',c',d' pairs. Alors $n-2\alpha = 0, a' = 1, b' = c' = d' = 0, a = 2^\alpha, b = c = d = 0$.

◇ **Réponse :**

	Solutions (a,b,c,d)	Nombre de solutions
n pair, $n = 2\alpha+2$, $\alpha \in \mathbb{N}$	$(2^\alpha,2^\alpha,2^\alpha,2^\alpha)$, $(2^{\alpha+1},0,0,0)$ et ses permutés	5
n impair, $n = 2\alpha+1$, $\alpha \in \mathbb{N}$	$(2^\alpha,2^\alpha,0,0)$ et ses permutés	6

4.1.37 Remarquer que tout entier $\geqslant 1$ s'écrit, d'une façon unique, sous la forme $2^\alpha(2\beta+1)$, $(\alpha,\beta) \in \mathbb{N}^2$. Pour chaque i de $\{0,\ldots,n\}$, il existe donc $(\alpha_i,\beta_i) \in \mathbb{N}^2$ tel que $a_i = 2^{\alpha_i}(2\beta_i+1)$. Les $n+1$ entiers $\beta_0,\ldots,\beta_n$ sont dans $\{0,\ldots,n-1\}$, qui est de cardinal n ; il existe donc $(i,j) \in \{0,\ldots,n\}^2$ tel que : $i \neq j$ et $\beta_i = \beta_j$. On a alors $(\alpha_i \leqslant \alpha_j$ ou $\alpha_j \leqslant \alpha_i)$, d'où $(a_i | a_j$ ou $a_j | a_i)$.

4.1.38 *a)* Evident.

b) • $S(2n+1) = \displaystyle\sum_{k=1}^{2n} \frac{\delta(k)}{k} + \frac{\delta(2n+1)}{2n+1} = S(2n)+1$.

• En séparant en termes d'indices pairs ou impairs :

$$S(2n) = \sum_{\substack{k=1 \\ k \text{ pair}}}^{2n} \frac{\delta(k)}{k} + \sum_{\substack{k=1 \\ k \text{ impair}}}^{2n} \frac{\delta(k)}{k} = \sum_{p=1}^{n} \frac{\delta(2p)}{2p} + n = \frac{1}{2}\sum_{p=1}^{n} \frac{\delta(2p)}{p} + n = \frac{1}{2}S(n) + n.$$

c) • $S(2n+1) = S(2n)+1 \iff F(2n+1) + \dfrac{2(2n+1)}{3} = F(2n) + \dfrac{4n}{3} + 1$, d'où $F(2n+1) = F(2n) + \dfrac{1}{3}$.

• $S(2n) = \dfrac{1}{2}S(n) + n \iff F(2n) + \dfrac{4n}{3} = \dfrac{1}{2}F(n) + \dfrac{n}{3} + n$, d'où $F(2n) = \dfrac{1}{2}F(n)$.

• $F(1) = S(1) - \dfrac{2}{3} = \dfrac{1}{3}$.

• Montrons, par récurrence sur n, la propriété $\mathcal{P}_n$: $\forall k \in \{1,\ldots,n\}$, $\begin{cases} 0 < F(2k) < \dfrac{1}{3} \\ 0 < F(2k+1) < \dfrac{2}{3} \end{cases}$.

1) $\mathcal{P}_1$ est vraie, car $F(2) = \dfrac{1}{2}F(1) = \dfrac{1}{6}$ et $F(3) = F(2) + \dfrac{1}{3} = \dfrac{1}{2}$.

2) Si $\mathcal{P}_n$ est vraie, alors : $\begin{cases} 0 < F(2(n+1)) = \dfrac{1}{2}F(n+1) < \dfrac{1}{2}\cdot\dfrac{2}{3} = \dfrac{1}{3} \\ 0 < F(2(n+1)+1) = F(2n+2) + \dfrac{1}{3} < \dfrac{1}{3} + \dfrac{1}{3} = \dfrac{2}{3}. \end{cases}$

4.2.1 *a)* $\forall d \in \mathbb{N}^*$, $\left(\begin{cases} d \mid n^2+n \\ d \mid 2n+1 \end{cases} \Longrightarrow d \mid (2n+1)^2 - 4(n^2+n) = 1 \Longrightarrow d = 1 \right)$.

b) Par l'algorithme d'Euclide :

	n	n	n
n^4+3n^2+1	n^3+2n	n^2+1	n
n^2+1	n	1	

c) $\forall d \in \mathbb{N}^*$, $\left(\begin{cases} d|n^2+1 \\ d|(n+1)^2+1 \end{cases} \Longrightarrow \begin{cases} d|n^2+1 \\ d|2n+1 \end{cases} \Longrightarrow \begin{cases} d|(2n+1)^2-4(n^2+1)=4n-3 \\ d|2n+1 \end{cases}\right.$

$\left. \Longrightarrow d|2(2n+1)-(4n-3)=5\right)$.

4.2.2 Notons, pour $n \in \mathbb{N}^*$, $u_n = 16^n+10^n-1$, $v_n = u_n+1 = 16^n+10^n$, et $\delta = \text{pgcd}\{u_n ; n \in \mathbb{N}^*\}$.

1) La suite $(v_n)_{n\in\mathbb{N}^*}$ est une suite récurrente linéaire du second ordre à coefficients constants (cf. Tome 1, 3.4.2), dont l'équation caractéristique admet pour solutions 16 et 10; on a donc :

$$\forall n \in \mathbb{N}^*, \quad v_{n+2} - (16+10)v_{n+1} + 16 \cdot 10 v_n = 0,$$

d'où : $\forall n \in \mathbb{N}^*$, $u_{n+2} = 26u_{n+1} - 160u_n - 135$.

Comme $(\delta|u_n, \delta|u_{n+1}, \delta|u_{n+2})$, on déduit $\delta|135$. D'autre part, $\delta|u_1 = 25$.

D'où : $\delta|135 \wedge 25 = 5$.

2) $\forall n \in \mathbb{N}^*$, $u_n \underset{[5]}{\equiv} 1^n + 0^n - 1 = 0$.

◇ **Réponse :** 5.

4.2.3 *a)* En sommant $\begin{cases} r_0 = r_1 q_1 + r_2 \\ \quad\vdots \\ r_{n-2} = r_{n-1}q_{n-1} + r_n \\ r_{n-1} = r_n q_n \end{cases}$, on obtient : $\displaystyle\sum_{i=0}^{n-1} r_i = \sum_{i=1}^{n} r_i q_i + \sum_{i=2}^{n} r_i$,

d'où : $\displaystyle\sum_{i=1}^{n} r_i q_i = r_0 + r_1 - r_n = a + b - a \wedge b$.

b) En sommant $\begin{cases} r_0 r_1 = r_1^2 q_1 + r_1 r_2 \\ \quad\vdots \\ r_{n-2}r_{n-1} = r_{n-1}^2 q_{n-1} + r_{n-1}r_n \\ r_{n-1}r_n = r_n^2 q_n \end{cases}$, on obtient $\displaystyle\sum_{i=0}^{n-1} r_i r_{i+1} = \sum_{i=1}^{n} r_i^2 q_i + \sum_{i=1}^{n-1} r_i r_{i+1}$,

d'où : $\displaystyle\sum_{i=1}^{n} r_i^2 q_i = r_0 r_1 = ab$.

4.2.4 *a)* L'ensemble $\{n \in \mathbb{N}^* ; x^n = e\}$ est une partie non vide de $\mathbb{N}^*$, donc admet un plus petit élément, noté $\omega(x)$.

b) α) • Puisque G est fini, les éléments x^n ($n \in \mathbb{N}$) ne sont pas deux à deux distincts. Il existe donc $(k,l) \in \mathbb{N}^2$ tel que : $k < l$ et $x^k = x^l$.

En notant $n = l - k$, on a : $n \in \mathbb{N}^*$ et $x^n = e$, donc x est d'ordre fini.

• Soit $p \in \mathbb{N}$; par division euclidienne de p par $\omega(x)$, il existe $(q,r) \in \mathbb{N}^2$ tel que : $p = q\omega(x)+r$ et $0 \leqslant r < \omega(x)$, d'où $x^n = (x^{\omega(x)})^q x^r = x^r$.

D'autre part, d'après la définition de $\omega(x)$, on déduit que $e,x,x^2,\ldots,x^{\omega(x)-1}$ sont deux à deux distincts.

Ainsi : $< x >= \{e,x,\ldots,x^{\omega(x)-1}\}$.

D'après le théorème de Lagrange (C 2.1 p. 63), $\text{Card}(< x >) \mid \text{Card}(G)$, donc $\omega(x) \mid \text{Card}(G)$.

$\beta)$ ◇ **Réponse :** Il existe des groupes infinis dont tout élément est d'ordre fini, par exemple $((\mathbb{Z}/2\mathbb{Z})[X],+)$, groupe additif des polynômes à une indéterminée et à coefficients dans le corps $\mathbb{Z}/2\mathbb{Z}$ (cf. plus loin ch. 5 p. 139).

c) Même méthode que dans la solution de *b)* α).

d) α) • Notons $\mu = \omega(x) \vee \omega(y)$. Comme $\omega(x)|\mu$ et $\omega(y)|\mu$, on a $x^\mu = y^\mu = e$ (cf. *c)*), d'où $(xy)^\mu = x^\mu y^\mu = e$, puisque x et y commutent.

Ainsi, xy est d'ordre fini et $\omega(xy)|\mu$ (cf. *c)*).

• En choisissant $G = (\mathbb{Z}/2\mathbb{Z},+)$, $x = y = \widehat{1}$, on a : $\omega(x) = 2$, $\omega(y) = 2$, $x + y = y + x$, $\omega(x + y) = 1 \neq \omega(x) \vee \omega(y)$.

◇ **Réponse :** non.

$\beta)$ ◇ **Réponse :** On peut choisir pour G le groupe des isométries vectorielles du plan euclidien (la loi est $\circ$), x et y deux symétries par rapport à deux droites vectorielles D, Δ telles que $(\widehat{D,\Delta}) = \alpha$, où $\alpha \in \mathbb{R}$ est tel que $\alpha \notin \pi\mathbb{Q}$, par exemple $\alpha = 1$ (sachant que π est irrationnel), ou $\alpha = \pi\sqrt{2}$ (sachant que $\sqrt{2}$ est irrationnel).

4.2.5 *1)* Il est clair que, pour tout cycle c de $\mathfrak{S}_n$, en notant $\gamma(c)$ le cardinal du support de c, on a :

- c est d'ordre $\gamma(c)$
- $\varepsilon(c) = (-1)^{\gamma(c)-1}$.

2) D'après 3.4.3 Th. p. 88, σ admet une décomposition $\sigma = c_1 \circ \ldots \circ c_\nu$ en produit de cycles à supports deux à deux disjoints. Puisque $c_1,\ldots,c_\nu$ commutent deux à deux, on a : $\sigma^N = c_1^N \circ \ldots \circ c_\nu^N$, d'où, par unicité de la décomposition de e en produit de cycles à supports deux à deux disjoints :

$$\forall k \in \{1,\ldots,\nu\}, \quad c_k^N = e.$$

On a alors (cf. exercice 4.2.4 *c)*) : $\forall k \in \{1,\ldots,\nu\}$, $\gamma(c_k)|N$.

Comme N est impair, il en résulte que les $\gamma(c_k)$ sont impairs, puis que les c_k sont paires.

Enfin, $\sigma = c_1 \circ \ldots \circ c_N$ est paire.

4.2.6 Puisque $c_1,\ldots,c_\nu$ commutent deux à deux : $\forall p \in \mathbb{N}^*$, $\sigma^p = c_1^p \circ \ldots \circ c_\nu^p$.

Par unicité de la décomposition de e en produit de cycles à supports deux à deux disjoints, on a, pour tout p de $\mathbb{N}^*$:

$$\sigma^p = e \iff c_1^p = \ldots = c_\nu^p = e \iff (\forall k \in \{1,\ldots,\nu\},\ \omega(c_k)|p) \iff \big(\text{ppcm}((\omega(c_k))_{1\leqslant k\leqslant \nu})|p\big).$$

Exemple : $\sigma = (1,7,3) \circ (2,8,10,11) \circ (4,6,12)$, $\omega(\sigma) = \text{ppcm}(3,4,3) = 12$.

◇ **Réponse :** 12.

4.3.1 D'après l'exercice 4.1.1 p. 103 : $n^2 \equiv 1\ [8]$.

D'autre part : $n \not\equiv 0\ [3] \Longrightarrow n \equiv -1$ ou $1\ [3] \Longrightarrow n^2 \equiv 1\ [3]$.

Comme $3 \wedge 8 = 1$: $\begin{cases} 3|n^2-1 \\ 8|n^2-1 \end{cases} \Longrightarrow 24|n^2-1$.

4.3.2 Soient $(x,y) \in (\mathbb{N}^*)^2$, $\delta = x \wedge y$; il existe $(x',y') \in (\mathbb{N}^*)^2$ tel que : $x = \delta x'$, $y = \delta y'$, $x' \wedge y' = 1$; on a : $x \vee y = \delta x' y'$ (cf. 4.3.3 Prop. 4 p. 117).

a) $\begin{cases} x \wedge y = 18 \\ x \vee y = 540 \end{cases} \iff \begin{cases} \delta = 18 \\ x'y' = 30 \end{cases}$.

◊ **Réponse :** {(18,540), (36,270), (54,180), (90,108) et les couples renversés}.

b) $\begin{cases} x \vee y - x \wedge y = 534 \\ x \vee y - 5(x \wedge y) = 510 \end{cases} \iff \begin{cases} x \wedge y = 6 \\ x \vee y = 540 \end{cases}$ et terminer comme en *a)*.

◊ **Réponse :** {(6,540), (12,270), (30,108), (54,60) et les couples renversés}.

c) $x \vee y - 3(x \wedge y) = 135 \iff \delta(x'y' - 3) = 135$. Par rôles symétriques de x' et y', on peut supposer $x' \leqslant y'$. Les diviseurs de 135 (dans $\mathbb{N}^*$) sont : 1, 3, 5, 9, 15, 27, 45, 135.

	$\begin{cases} \delta = 1 \\ x'y' = 138 \end{cases}$	$\begin{cases} \delta = 3 \\ x'y' = 48 \end{cases}$	$\begin{cases} \delta = 5 \\ x'y' = 30 \end{cases}$	$\begin{cases} \delta = 9 \\ x'y' = 18 \end{cases}$	$\begin{cases} \delta = 15 \\ x'y' = 12 \end{cases}$	$\begin{cases} \delta = 27 \\ x'y' = 8 \end{cases}$	$\begin{cases} \delta = 45 \\ x'y' = 6 \end{cases}$	$\begin{cases} \delta = 135 \\ x'y' = 4 \end{cases}$
x'	1 2 3 6	1 3	1 2 3 5	1 2	1 3	1	1 2	1
y'	138 69 46 23	48 16	30 15 10 6	18 9	12 4	8	6 3	4

◊ **Réponse :** {(1,138), (2,69), (3,46), (3,144), (5,150), (6,23), (9,48), (9,162), (10,75), (15,50), (15,180), (18,81), (25,30), (27,216), (45,60), (45,270), (90,135), (135,540) et les couples renversés}.

d) $\begin{cases} x + y = 1008 \\ x \wedge y = 24 \end{cases} \iff \begin{cases} \delta = 24 \\ x' + y' = 42 \end{cases}$.

x'	1	5	11	13	17	19
y'	41	37	31	29	25	23

◊ **Réponse :** {(24,984), (120,888), (264,744), (312,696), (408,600), (456,552) et les couples renversés}.

e) $\delta^2 | 19476 \Longrightarrow \delta \in \{1,2,3,6\}$.

Pour chaque valeur de δ, résoudre $\begin{cases} x'^2 + y'^2 = \dfrac{19476}{\delta^2} \\ x'y' = \dfrac{1260}{\delta} \end{cases}$, en calculant $(x' + y')^2$.

◊ **Réponse :** {(60,126), (126,60)}.

f) $x \wedge y + x \vee y = y + 9 \iff \delta(1 + x'y' - y') = 9 \Longrightarrow \delta | 9 \Longrightarrow \delta \in \{1,3,9\}$.

Pour chaque valeur de δ, résoudre $(x' - 1)y' = \dfrac{9}{\delta} - 1$.

◊ **Réponse :** {(3,4), (5,2), (9,1), (9,3)} ∪ {(9,9λ); $\lambda \in \mathbb{N}^*$}.

4.3.3 *a)* Appliquer, par exemple, l'algorithme d'Euclide.

b) Comme en 4.3.2 p. 115, on calcule un couple (u_0, v_0) convenant : $(28, -25)$.

- Si (u,v) convient, alors $442u + 495v = 1 = 442u_0 + 495v_0$, d'où $442(u - u_0) = -495(v - v_0)$.

Comme $442 \wedge 495 = 1$, le théorème de Gauss montre : $442 | v - v_0$. Il existe $k \in \mathbb{Z}$ tel que $v = 442k + v_0$, puis $u = -495k + u_0$.

- Réciproque immédiate.

◇ **Réponse :** $\{(28-495k,-25+442k);\ k\in\mathbb{Z}\}$.

c) $\widehat{1}=\widehat{442}\cdot\widehat{28}+\widehat{495}\cdot(\widehat{-25})=\widehat{442}\cdot\widehat{28}$, donc $\widehat{442}$ est inversible et a pour inverse $\widehat{28}$.
Alors : $\widehat{442}x=\widehat{314}\iff x=\widehat{28}\cdot\widehat{314}$.

◇ **Réponse :** $\{\widehat{377}\}$.

4.3.4 D'abord, la résolution dans $\mathbb{Z}$ donne :

$$\{(x,y)\in\mathbb{Z}^2;\ 2x+3y=n\}\ =\ \{(-n+3z,n-2z);\ z\in\mathbb{Z}\}.$$

Soit $z\in\mathbb{Z}$; on a : $\begin{cases}-n+3z\geqslant 0\\ n-2z\geqslant 0\end{cases}\iff \dfrac{n}{3}\leqslant z\leqslant\dfrac{n}{2}$.

Comme l'application $z\longmapsto(-n+3z,n-2z)$ est injective, on en déduit :

$$\mathrm{Card}\{(x,y)\in\mathbb{N}^2;\ 2x+3y=n\}=\mathrm{Card}\{z\in\mathbb{Z};\ \frac{n}{3}\leqslant z\leqslant\frac{n}{2}\}.$$

Séparer en cas modulo 6 pour n.

◇ **Réponse :** $\mathrm{E}\left(\dfrac{n}{6}\right)$ si $n\equiv 1\ [6]$, $1+\mathrm{E}\left(\dfrac{n}{6}\right)$ sinon.

4.3.5 Soit $\delta=a\wedge b$; il existe $(a',b')\in(\mathbb{Z}^*)^2$ tel que : $a=\delta a'$, $b=\delta b'$, $a'\wedge b'=1$.

Notons $\mathcal{S}=\{(x,y)\in\mathbb{Z}^2;\ ax+by=c\}$.

Si $\delta\nmid c$, alors $\mathcal{S}=\varnothing$.

Supposons $\delta\mid c$; il existe $c'\in\mathbb{Z}$ tel que $c=\delta c'$.

• Soit $(x,y)\in\mathbb{Z}^2$ tel que $ax+by=c$. On a alors : $a'x+b'y=c'$. D'après le théorème de Bezout, puisque $a'\wedge b'=1$, il existe $(u,v)\in\mathbb{Z}^2$ tel que $a'u+b'v=1$. D'où : $a'(x-c'u)=b'(c'v-y)$.

Comme $a'\wedge b'=1$, le théorème de Gauss montre $a'|c'v-y$. Il existe donc $k\in\mathbb{Z}$ tel que $c'v-y=ka'$, puis $x-c'u=kb'$.

• Réciproquement, on vérifie aisément que, pour tout k de $\mathbb{Z}$, le couple $(c'u+kb',c'v-ka')$ convient.

◇ **Réponse :** • $\varnothing$ si $a\wedge b\nmid c$

• $\{(c'u+kb',\ c'v-ka');\ k\in\mathbb{Z}\}$ si $a\wedge b\mid c$, où a',b',c' sont définis par :

$\delta=a\wedge b$, $a=\delta a'$, $b=\delta b'$, $c=\delta c'$, et $(u,v)\in\mathbb{Z}^2$ tel que $a'u+b'v=1$.

Exemples : *a)* $\varnothing$; *b)* $\{(5k+12,-3k-6);k\in\mathbb{Z}\}$.

4.3.6 **1) Existence**

D'après 4.3.2 Prop. p. 114, il existe $(u,v)\in\mathbb{Z}^2$ tel que : $au+bv=1$, $|u|<b$, $|v|\leqslant a$.

Il est d'abord clair que u et v sont non nuls, et $|v|\neq a$.

Si $u<0$, notons $(u',v')=(u+b,v-a)$; on a :

$$\begin{cases}au'+bv'=au+bv=1\\ 1\leqslant u'<b\\ |bv'|=|1-au'|\leqslant 1+au'\leqslant 1+ab<(a+1)b,\quad\text{donc } |v'|\leqslant a.\end{cases}$$

Ceci montre qu'en remplaçant éventuellement (u,v) par $(u+b,v-a)$, on peut se ramener à :

$$au+bv=1,\ 1\leqslant u\leqslant b-1,\ 1\leqslant -v\leqslant a-1.$$

a) Cas $0\leqslant u\leqslant\mathrm{E}\left(\dfrac{b}{2}\right)$

Alors $b(-v)=au-1<au<a\dfrac{b}{2}$, donc $-v<\dfrac{a}{2}$, et le couple $(x,y)=(u,v)$ convient.

b) Cas $\mathrm{E}\left(\frac{b}{2}\right)+1 \leqslant u \leqslant b-1$

Notons $x=u-b$, $y=v+a$. Alors :

- $ax+by=au+bv=1$
- $|x|=-x=b-\mathrm{E}\left(\frac{b}{2}\right)-1<\frac{b}{2}$
- $by=1-ax=1+a(-x)\leqslant 1+\frac{ab}{2}$, donc $y<\frac{1}{b}+\frac{a}{2}<1+\frac{a}{2}$. Si $y=\frac{a}{2}$, alors $a(2x+y)=2$, contradiction (car $a\geqslant 3$); d'où $y<\frac{a}{2}$.

2) Unicité

Soient (x,y), (x',y') convenant. On a alors $a(x-x')=b(y'-y)$, d'où, puisque $a\wedge b=1$, $a|y'-y$. Mais d'autre part : $|y'-y|\leqslant |y'|+|y|<\frac{a}{2}+\frac{a}{2}=a$. On déduit $y'-y=0$, puis $x'-x=0$.

4.3.7 Même genre de raisonnement que pour l'exercice 4.3.6.

4.3.8 Notons $u_n=(n^2-1)(n^2-9)(n^2-49)$, et remarquons : $23040=2^9\cdot 3^2\cdot 5$.

1) Modulo 5

$n^2\equiv 1$ ou -1 [5], donc $5\mid n^2-1$ ou $5\mid n^2-9$, d'où $5\mid u_n$.

2) Modulo 9

n	0	1	2	3	4
n^2	0	1	4	0	-2

Si $n^2\equiv 0$ ou 1 ou 4, alors $9\mid n^2-9$ ou $9\mid n^2-1$ ou $9\mid n^2-49$, donc $9\mid u_n$.

Si $n^2\equiv -2$ [9], alors $n^2-1\equiv 0$ [3] et $n^2-49\equiv 0$ [3], donc $9\mid u_n$.

3) Modulo 2^9

D'après l'exercice 4.1.1 p. 103, $n^2\equiv 1$ [8], donc $8\mid n^2-1$, $8\mid n^2-9$, $8\mid n^2-49$, d'où $2^9=8^3\mid u_n$.

Enfin, comme 5, 9, 2^9 sont premiers entre eux deux à deux, on conclut : $23040\mid u_n$.

4.3.9 Supposons qu'il existe $(x,y,z,t)\in\mathbb{Z}^4$ convenant.

Montrer d'abord que x,y,z,t sont tous $\neq 0$.

En notant $\delta=\mathrm{pgcd}(x,y,z,t)$, il existe $(X,Y,Z,T)\in(\mathbb{Z}^*)^4$ tel que : $x=\delta X,\ldots,t=\delta T$, $\mathrm{pgcd}(X,Y,Z,T)=1$, et $X^2+10Y^2=Z^2$, $10X^2+Y^2=T^2$.

1er cas : X impair

Alors Z est impair, $Z-X$ et $Z+X$ sont pairs, $4|Z^2-X^2=10Y^2$, $2|Y$; puis T^2 est pair, T est pair. Mais alors, modulo 4 : $X^2\equiv 1$, $Y^2\equiv 0$, $T^2\equiv 0$; ce qui contredit $10X^2+Y^2=T^2$.

2ème cas : X pair

Alors Z est pair. Si Y est pair, alors T est pair, contradiction. Donc Y et T sont impairs. Mais alors, modulo 4 : $X^2\equiv 0$, $Y^2\equiv 1$, $T^2\equiv 1$; ce qui contredit $X^2+10Y^2=Z^2$.

4.3.10 $(n+1)\mathrm{C}_{2n}^{n+1}=n\mathrm{C}_{2n}^{n}$ et $(n+1)\wedge n=1$, donc $(n+1)|\mathrm{C}_{2n}^{n}$.

4.3.11 *a)* Notons $\delta = a \wedge b$, $(a',b') \in (\mathbb{Z}^*)^2$ tel que : $a = \delta a'$, $b = \delta b'$, $a' \wedge b' = 1$.
On a : $a^2 \wedge b^2 = \delta^2(a'^2 \wedge b'^2) = \delta^2$. Si $a^2 | b^2$, alors $a^2 \wedge b^2 = a^2$, d'où $\delta^2 = a^2$, $\delta = |a|$, $a|b$.

b) Soit $\alpha \in \mathbb{Q}^*$; il existe $(a,b) \in (\mathbb{Z}^*)^2$ tel que $\alpha = \dfrac{b}{a}$. D'après *a)* :
$\alpha^2 \in \mathbb{Z} \iff a^2 | b^2 \implies a|b \iff \alpha \in \mathbb{Z}$.

c) En développant, on se ramène, si $y \neq 0$, à : $2y^2 + (x^2 - 3x)y + 3x^2 + x = 0$ (1)
Montrer : (1) $\iff (4y + (x^2 - 3x))^2 = x(x+1)^2(x-8)$. Examiner les cas $x = -1, 0, 8$.
Supposons maintenant $x \neq -1, 0, 8$. D'après *a)*, $x + 1$ divise $4y + (x^2 - 3x)$.
On en déduit qu'il existe $\lambda \in \mathbb{N}^*$ tel que $x(x-8) = \lambda^2$.
Alors : $(x-4)^2 = 16 + \lambda^2$, donc $|x-4| \geqslant \lambda + 1$, puis : $16 + \lambda^2 \geqslant (\lambda+1)^2$, d'où $\lambda \leqslant 7$.
Tester les valeurs 0, ..., 7 de λ en liaison avec la relation $(x-4)^2 = 16 + \lambda^2$. On déduit $x = 9$.

◇ **Réponse :** $(\mathbb{Z} \times \{0\}) \cup \{(-1,-1), (8,-10), (9,-6), (9,-21)\}$.

4.3.12 Notons $d = a \wedge c$, $\delta = b \wedge c$; il existe $a',c',b'',c'' \in \mathbb{Z}^*$ tels que :

$$\begin{cases} a = da', & c = dc', \quad a' \wedge c' = 1 \\ b = \delta b'', & c = \delta c'', \quad b'' \wedge c'' = 1 \end{cases}.$$

On a $dc' \mid da'\delta b''$, d'où $c' \mid a'\delta b''$. Comme $c' \wedge a' = 1$, on déduit (théorème de Gauss) : $c' \mid \delta b''$.
Puis : $\delta c'' = c = dc' \mid d\delta b''$, d'où $c'' \mid db''$. Comme $c'' \wedge b'' = 1$, on déduit $c'' \mid d$, et enfin : $c = \delta c'' \mid \delta d$.

4.3.13 Comme $\dfrac{a^n - b^n}{a-b} = \sum_{k=0}^{n-1} a^k b^{n-1-k} \equiv na^{n-1}\ [a-b]$,

on a : $\left(\dfrac{a^n - b^n}{a-b}\right) \wedge (a-b) = (na^{n-1}) \wedge (a-b)$.

Notons $\delta = a \wedge b$.

1) Pour tout diviseur d de $(n\delta^{n-1}) \wedge (a-b)$, comme $\delta \mid a$, on déduit : $d \mid (na^{n-1}) \wedge (a-b)$.

2) Réciproquement, soit $d \in \mathbb{N}^*$ tel que $d | (na^{n-1}) \wedge (a-b)$. On a donc : $a \equiv b\ [d]$ et $na^{n-1} \equiv 0\ [d]$.
D'autre part, il existe $(u,v) \in \mathbb{Z}^2$ tel que $\delta = ua + vb$. On déduit $\delta \equiv (u+v)a\ [d]$, puis $n\delta^{n-1} \equiv n(u+v)^{n-1}a^{n-1} \equiv 0\ [d]$. Donc $d | (n\delta^{n-1}) \wedge (a-b)$.
Finalement : $(na^{n-1}) \wedge (a-b) = (n\delta^{n-1}) \wedge (a-b)$.

4.3.14 *1)* Les zéros réels du trinôme $6X^2+5X+1$ sont $-\dfrac{1}{2}$ et $-\dfrac{1}{3}$. Donc l'équation $6x^2+5x+1 = 0$ n'admet pas de solution dans $\mathbb{Z}$.

2) Soit $n \in \mathbb{N}^*$; il existe $(k,m) \in \mathbb{N}^2$ tel que $n = 2^k(2m+1)$.
Puisque $3 \wedge 2^k = 1$, 3 admet un inverse modulo 2^k, noté α : $3\alpha \equiv 1\ [2^k]$. Alors :

$$\forall x \in \mathbb{Z}, \quad \big(3x + 1 \equiv 0\ [2^k] \iff x \equiv -\alpha\ [2^k]\big).$$

De même, puisque $2 \wedge (2m+1) = 1$, 2 admet un inverse modulo $2m+1$, noté β : $2\beta \equiv 1\ [2m+1]$.
Alors : $\forall x \in \mathbb{Z}, \quad \big(2x + 1 \equiv 0\ [2m+1] \iff x \equiv -\beta\ [2m+1]\big)$.
D'autre part, $2^k \wedge (2m+1) = 1$, donc il existe $(u,v) \in \mathbb{Z}^2$ tel que $2^k u + (2m+1)v = 1$. On a alors :
$\alpha - \beta = (\alpha - \beta)(2^k u + (2m+1)v)$, d'où, en notant $\xi = -\alpha + (\alpha - \beta)2^k u = -\beta + (\beta - \alpha)(2m+1)v$:

$$\begin{cases} \xi \equiv -\alpha\ [2^k] \\ \xi \equiv -\beta\ [2m+1] \end{cases}, \quad \text{d'où} \quad \begin{cases} 3\xi + 1 \equiv 0\ [2^k] \\ 2\xi + 1 \equiv 0\ [2m+1] \end{cases},$$

et donc $6\xi^2 + 5\xi + 1 \equiv 0\ [n]$.

On peut remarquer que, d'après le théorème chinois (exercice 4.3.16), le système de congruences simultanées $\begin{cases} x \equiv -\alpha \ [2^k] \\ x \equiv -\beta \ [2m+1] \end{cases}$ admet au moins une solution, puisque $2^k \wedge (2m+1) = 1$.

4.3.15 En notant, pour $i \in \{1,\dots,n\}$, $E_i = \{1,\dots,n\} - \{i\}$, on a :

$$\text{pgcd}(A_1,\dots,A_n) = \prod_{k \in \bigcap_{i=1}^{n} E_i} a_k = \prod_{k \in \varnothing} a_k = 1.$$

4.3.16 *a)* Notons, pour $i \in \{1,\dots,n\}$: $A_i = \dfrac{a}{a_i}$. Soit $i \in \{1,\dots,n\}$; comme $A_i \wedge a_i = 1$, d'après le théorème de Bezout, il existe $c_i \in \mathbb{Z}$ tel que : $A_i c_i \equiv 1 \ [a_i]$.

Notons $x = \sum_{i=1}^{n} A_i b_i c_i$. On a : $\forall i \in \{1,\dots,n\}$, $x \equiv A_i b_i c_i \equiv b_i \ [a_i]$.

Exemple

Sur un tel exemple, nous n'allons pas appliquer la démonstration précédente.

Supposons que x convienne.

Puisque $x \equiv 4 \ [5]$, il existe $\lambda \in \mathbb{Z}$ tel que : $x = 5\lambda + 4$.

On a : $x \equiv 3 \ [6] \iff 5\lambda \equiv -1 \ [6] \iff -\lambda \equiv -1 \ [6] \iff \lambda \equiv 1 \ [6]$.

Il existe donc $\mu \in \mathbb{Z}$ tel que $\lambda = 6\mu + 1$, d'où $x = 30\mu + 9$. Alors :

$$x \equiv 2 \ [7] \iff 30\mu \equiv -7 \ [7] \iff 2\mu \equiv 0 \ [7] \iff \mu \equiv 0 \ [7],$$

car 2 est inversible modulo 7.

Il existe donc $\nu \in \mathbb{Z}$ tel que $\mu = 7\nu$; d'où $x = 210\nu + 9$.

La réciproque est immédiate.

◇ **Réponse :** $\{210\nu + 9;\ \nu \in \mathbb{Z}\}$.

b) Soit $\xi \in \mathbb{Z}/a\mathbb{Z}$. Il existe $x \in \mathbb{Z}$ tel que $\xi = \text{cl}_a(x)$; posons $\theta(\xi) = \big(\text{cl}_{a_1}(x),\dots,\text{cl}_{a_n}(x)\big)$.

Cette définition est correcte car, pour tout (x,y) de $\mathbb{Z}^2$:

$$\text{cl}_a(x) = \text{cl}_a(y) \Longrightarrow a | x-y \Longrightarrow \big(\forall i \in \{1,\dots,n\}, a_i | x-y\big) \Longrightarrow \big(\forall i \in \{1,\dots,n\},\ \text{cl}_{a_i}(x) = \text{cl}_{a_i}(y)\big)$$

- θ est un morphisme de groupes car, pour tout (x,y) de $\mathbb{Z}^2$:

$$\theta\big(\text{cl}_a(x) + \text{cl}_a(y)\big) = \theta\big(\text{cl}_a(x+y)\big) = \big(\text{cl}_{a_1}(x+y),\dots,\text{cl}_{a_n}(x+y)\big)$$
$$= \big(\text{cl}_{a_1}(x) + \text{cl}_{a_1}(y),\dots,\text{cl}_{a_n}(x) + \text{cl}_{a_n}(y)\big) = \theta\big(\text{cl}_a(x)\big) + \theta\big(\text{cl}_a(y)\big).$$

- θ est injective car, pour tout x de $\mathbb{Z}$:

$$\theta\big(\text{cl}_a(x)\big) = 0 \Longrightarrow \text{cl}_{a_1}(x) = \dots = \text{cl}_{a_n}(x) = 0 \Longrightarrow \big(\forall i \in \{1,\dots,n\},\ a_i | x\big) \Longrightarrow a | x \Longrightarrow \text{cl}_a(x) = 0.$$

- Surjectivité de θ

1re méthode

Soit $(\xi_1,\dots,\xi_n) \in \mathbb{Z}/a_1\mathbb{Z} \times \dots \times \mathbb{Z}/a_n\mathbb{Z}$.

Il existe $(b_1,\dots,b_n) \in \mathbb{Z}^n$ tel que : $\forall i \in \{1,\dots,n\}$, $\xi_i = \text{cl}_{a_i}(b_i)$.

D'après *a)*, il existe $\beta \in \mathbb{Z}$ tel que : $\forall i \in \{1,\dots,n\}$, $\beta \equiv b_i \ [a_i]$.

On a alors : $\theta\big(\text{cl}_a(\beta)\big) = \big(\text{cl}_{a_1}(\beta),\dots,\text{cl}_{a_n}(\beta)\big) = \big(\text{cl}_{a_1}(b_1),\dots,\text{cl}_{a_n}(b_n)\big) = (\xi_1,\dots,\xi_n)$.

2ème méthode

Puisque θ est injective et que $\mathbb{Z}/a\mathbb{Z}$ et $\mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_n\mathbb{Z}$ sont finis et ont le même cardinal, θ est bijective. Ceci prouve aussi que le théorème chinois peut se déduire de la seule injectivité de θ.

4.3.17 En remplaçant x par $\dfrac{y-a}{2}$, déduire : $(3y)^2 = 3(4b-a^2)$. Comme $3(4b-a^2) \in \mathbb{Z}$, d'après l'exercice 4.3.11 *b)* p. 119, on a : $3y \in \mathbb{Z}$. En notant $Y = 3y$: $Y^2 = 3(4b-a^2)$, donc $3 \mid Y$, d'où $y \in \mathbb{Z}$.

Enfin, comme $3y^2 = 4b - a^2$, y et a sont de même parité, donc $x = \dfrac{y-a}{2} \in \mathbb{Z}$.

4.3.18 Puisque $(bc-ad)^2 = (bc+ad)^2 - 4(ac)(bd)$, on déduit $n^2 \mid (bc-ad)^2$, puis $n \mid bc-ad$, cf. exercice 4.3.11 *a)* p. 119.

Il existe $(\lambda,\mu) \in \mathbb{Z}^2$ tel que $bc+ad = \lambda n$ et $bc-ad = \mu n$, d'où, en notant $\alpha = \lambda+\mu$ et $\beta = \lambda-\mu$: $2bc = \alpha n$ et $2ad = \beta n$. D'autre part, il existe $(\gamma,\delta) \in \mathbb{Z}^2$ tel que : $ac = \gamma n$ et $bd = \delta n$.

On déduit : $\alpha\beta n^2 = 4abcd = 4\gamma\delta n^2$, d'où $4 \mid \alpha\beta$.

De plus, α et β sont de même parité, puisque $\alpha+\beta = 2\lambda$.

On en déduit que α et β sont pairs, et finalement : $n \mid bc$ et $n \mid ad$.

4.3.19 Soient (x,y,z) convenant, $(\alpha,\beta,\gamma) \in \mathbb{N}^3$ tel que : $xy = 1+\alpha z$, $xz = 1+\beta y$, $yz = 1+\gamma x$.

On a : $(xy-1)x = \alpha z x = \alpha(1+\beta y)$, d'où, en notant $\lambda = x^2 - \alpha\beta$: $\lambda y = x+\alpha$ et $\lambda \in \mathbb{N}^*$.

De même, il existe $\mu \in \mathbb{N}^*$ tel que : $\mu x = y+\alpha$.

On a : $y+\alpha = \mu x = \mu(\lambda y - \alpha)$, d'où : $(\lambda\mu - 1)y = (1+\mu)\alpha$.

Mais, puisque $xy = 1+\alpha z$, $y \wedge \alpha = 1$, et donc $y \mid 1+\mu$. Il existe $k \in \mathbb{N}^*$ tel que $1+\mu = ky$.

Alors : $x+y+\alpha = x+\mu x = kxy$, puis $xz+yz+\alpha z = kxyz$, et donc : $xy+xz+yz-1 = kxyz$.

- $3yz > xy+xz+yz-1 = kxyz \geqslant xyz$, d'où $x < 3$, $x = 2$. On déduit : $2y+2z-1 = (2k-1)yz$.
- $4z > 2y+2z-1 = (2k-1)yz \geqslant yz$, d'où $y < 4$. Comme $x \wedge y = 1$, on déduit $y = 3$.
- $5+2z = 3(2k-1)z$, d'où $z \mid 5$. Comme $z \geqslant y = 4$, on conclut $z = 5$.

La réciproque est évidente.

◇ **Réponse :** $\{(2,3,5)\}$.

4.3.20 Soit $(x,y,z) \in \mathbb{Z}^3 - \{(0,0,0)\}$ une solution telle que $|x|+|y|+|z|$ soit minimum.

On a : $3 \mid x^3$, donc $3 \mid x$, $x = 3X$, $X \in \mathbb{Z}^*$, d'où : $y^3+3z^3+9X^3-9Xyz = 0$.

Ainsi, (y,z,X) est solution; par définition de (x,y,z), on a alors $|y|+|z|+|X| \geqslant |x|+|y|+|z|$, d'où $X = 0$, $x = 0$, $y^3+3z^3 = 0$.

Si $(y,z) \neq (0,0)$, en notant $\delta = y \wedge z$, il existe $(\alpha,\beta) \in (\mathbb{Z}^*)^2$ tel que : $y = \delta\alpha$, $z = \delta\beta$, $\alpha \wedge \beta = 1$, et on a : $\alpha^3 + 3\beta^3 = 0$.

Alors $3 \mid \alpha^3$, donc $3 \mid \alpha$, $\alpha = 3\alpha'$, $\alpha' \in \mathbb{Z}^*$; puis $9\alpha'^3 + \beta^3 = 0$, $3 \mid \beta^3$, $3 \mid \beta$, $3 \mid \alpha \wedge \beta$, contradiction.

On peut aussi terminer en montrant que -3 n'est pas un cube de rationnel (cf. aussi Tome 1, ex. 1.1.1 p. 1).

La solution précédente illustre la méthode de «descente infinie».

4.3.21 $(\exists k \in \mathbb{Z},\ k\widehat{x} = \widehat{1}) \iff (\exists \widehat{y} \in \mathbb{Z}/n\mathbb{Z},\ \widehat{y}\,\widehat{x} = \widehat{1})$, et appliquer 4.3.4 *1)* Prop. p. 118.

◇ **Réponse :** Les générateurs du groupe $(\mathbb{Z}/n\mathbb{Z},+)$ sont les $\widehat{x}$, $x \in \mathbb{Z}$ tel que $x \wedge n = 1$.

4.3.22 Soient $\xi \in \mathbb{Z}/n\mathbb{Z}$, $x \in \mathbb{Z}$ tel que $\xi = \widehat{x}$.

1) Si $x \wedge n = 1$, alors $\widehat{x}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ (cf. 4.3.4 *1)* Prop. p. 118), donc n'est pas diviseur de 0.

2) Si $n \nmid x$ et $x \wedge n \neq 1$, en notant $\delta = x \wedge n$, il existe $(a,b) \in (\mathbb{Z}^*)^2$ tel que $x = \delta a$, $y = \delta b$, $a \wedge b = 1$, et on a : $\widehat{b}\,\widehat{x} = \widehat{\delta a b} = \widehat{an} = \widehat{0}$, $\widehat{x} \neq \widehat{0}$, $b \neq \widehat{0}$ (car $|b| < n$ et $b \neq 0$), donc $\widehat{x}$ est diviseur de 0.

◊ **Réponse :** Les diviseurs de 0 dans $\mathbb{Z}/n\mathbb{Z}$ sont les $\widehat{x}$, $x \in \mathbb{Z}$ et $x \wedge n \neq 1$.

4.4.1 *a)* $n^4 - n^2 + 16 = (n^2+4)^2 - 9n^2 = (n^2-3n+4)(n^2+3n+4)$, et n^2-3n+4, n^2+3n+4 sont pairs car $n^2 - n \equiv 0$ [2].

b) $4n^3 + 6n^2 + 4n + 1 = (2n+1)(2n^2+2n+1)$ et $1 < 2n+1 < 2n^2+2n+1$.

c) $2^{4n+2}+1 = (2^{2n+1}+1)^2 - 2\cdot 2^{2n+1} = (2^{2n+1}+2^{n+1}+1)(2^{2n+1}-2^{n+1}+1)$, et $2^{2n+1}+2^{n+1}+1 > 1$, $2^{2n+1} - 2^{n+1} + 1 > 1$ (car $n \geqslant 1$).

Exemple : $2^{18} + 1 = (2^9 + 2^5 + 1)(2^9 - 2^5 + 1) = 545 \cdot 481 = 5 \cdot 109 \cdot 13 \cdot 37$.

4.4.2 Supposons n composé, $n = ab$, $(a,b) \in (\mathbb{N} - \{0,1\})^2$.

Alors $5^n - 3^n = (5^a)^b - (3^a)^b = (5^a - 3^a)\displaystyle\sum_{k=0}^{b-1}(5^a)^k(3^a)^{b-1-k}$, et les deux facteurs obtenus sont $\geqslant 2$, donc $5^n - 3^n$ est composé.

4.4.3 Notons $\delta = a \wedge c$; il existe $(a',c') \in (\mathbb{N}^*)^2$ tel que : $a = \delta a'$, $c = \delta c'$, $a' \wedge c' = 1$.

Comme $ab = cd$, on a : $a'b = c'd$. Puisque $a' | c'd$ et $a' \wedge c' = 1$, le théorème de Gauss montre : $a' | d$; il existe $D \in \mathbb{N}^*$ tel que $d = a'D$. On déduit : $b = c'D$. On a alors : $a = \delta a'$, $b = Dc'$, $c = \delta c'$, $d = Da'$, d'où : $a^n + b^n + c^n + d^n = (\delta^n + D^n)(a'^n + c'^n)$ et $\delta^n + D^n \geqslant 2$, $a'^n + c'^n \geqslant 2$, donc $a^n + b^n + c^n + d^n$ est composé.

4.4.4 Notons $q = p^3 + p^2 + 11p + 2$ et passons modulo 3 :

p mod. 3	-1	0	1
q mod. 3	0	2	0

Donc, comme $q > 3$, si q est premier, alors $p \equiv 0$ [3], puis, comme p est premier, $p = 3$.

Réciproquement, $p = 3$ et $q = 71$ sont premiers.

◊ **Réponse :** {3}.

4.4.5 Il existe $N \in \mathbb{N}^*$ tel que : $\left\{\dfrac{1}{x_1}, \ldots, \dfrac{1}{x_n}\right\} \subset \left\{\dfrac{1}{2^i 3^j};\ (i,j) \in \{0,\ldots,N\}^2\right\}$, d'où :

$$\sum_{k=1}^{n}\frac{1}{x_k} \leqslant \sum_{\substack{0\leqslant i\leqslant N\\ 0\leqslant j\leqslant N}}\frac{1}{2^i 3^j} = \left(\sum_{i=0}^{N}\frac{1}{2^i}\right)\left(\sum_{j=0}^{N}\frac{1}{3^j}\right) = \frac{1-\frac{1}{2^{N+1}}}{1-\frac{1}{2}}\cdot\frac{1-\frac{1}{3^{N+1}}}{1-\frac{1}{3}} < 3.$$

Ou encore, en utilisant la notion de série (cf. Tome 3, ch. 3) :

$$\sum_{k=1}^{n}\frac{1}{x_k} < \left(\sum_{i=0}^{+\infty}\frac{1}{2^i}\right)\left(\sum_{j=0}^{+\infty}\frac{1}{3^j}\right) = \frac{1}{1-\frac{1}{2}}\cdot\frac{1}{1-\frac{1}{3}} = 3.$$

4.4.6 Récurrence sur n.

La propriété est triviale pour $n = 0$.

Supposons qu'elle soit vraie pour n; il existe $m \in \mathbb{N}$ tel que : $(1+p)^{p^n} = 1 + p^{n+1} + mp^{n+2}$, d'où $(1+p)^{p^{n+1}} = \left((1+p)^{p^n}\right)^p = (1+p^{n+1}+mp^{n+2})^p = 1+p(p^{n+1}+mp^{n+2})+\sum_{k=2}^{p} C_p^k p^{(n+1)k}(1+mp)^k$.

Comme $\forall k \in \{2,\dots,p\}$, $(n+1)k \geqslant n+3$, on conclut : $(1+p)^{p^{n+1}} \equiv 1 + p^{n+2}\ [p^{n+3}]$.

4.4.7 *1)* Soient $m \in \mathbb{N}$, $h \in \{0,\dots,(m+1)^2 - m^2 - 1\}$, $n = m^2 + h$; on a : $\mathrm{E}(\sqrt{n}) = m$, d'où $u_n = n + 5 + \mathrm{E}(\sqrt{n}) = m^2 + m + h + 5$. Ainsi, les u_n $\left(m^2 \leqslant n \leqslant (m+1)^2 - 1\right)$ sont consécutifs.

De plus, $u_{(m+1)^2-1} = m^2 + 3m + 5$ est impair et $u_{(m+1)^2} = m^2 + 3m + 7$.

2) Ceci montre que $(u_n)_{n\geqslant 0}$ contient tous les entiers impairs $\geqslant u_0 = 5$, donc tous les nombres premiers $\geqslant 5$.

4.4.8 Si a et b sont pairs, alors $4 \mid \frac{1}{2}(a^3 + b^3)$, contradiction.

Si a est pair et b impair (ou l'inverse), alors $\frac{1}{2}(a^3 + b^3) \notin \mathbb{N}$.

Donc a et b sont impairs, et : $\frac{1}{2}(a^3 + b^3) = \frac{a+b}{2}(a^2 - ab + b^2)$, $\frac{a+b}{2} \in \mathbb{N}$, $a^2 - ab + b^2 \in \mathbb{N}$.

Comme $\frac{1}{2}(a^3 + b^3)$ est premier, on déduit : $\frac{1}{2}(a+b) = 1$ ou $a^2 - ab + b^2 = 1$.

- Si $a^2 - ab + b^2 = 1$, alors $(2a-b)^2 + 3b^2 = 4$, d'où $b = |2a - b| = 1$, puis $a = b = 1$.
- Si $\frac{a+b}{2} = 1$, alors $a = b = 1$.

4.4.9 Passer modulo 3 : $n - 10 \equiv n + 2$, $n + 10 \equiv n + 1$, $n + 60 \equiv n$. L'un de ces trois nombres est multiple de 3, donc égal à 3, puisqu'ils sont premiers. On obtient $n - 10 = 3$, puis $n + 90 = 103$ qui est premier.

4.4.10 Si $3 \nmid n$, alors $n^2 \equiv 1\ [3]$, $n^2 + 8 \equiv 0\ [3]$, donc $n^2 + 8$ est composé (multiple de 3, et $\neq 3$). Ainsi $3 \mid n$, $n = 3$, $n^3 + 4 = 31$ qui est premier.

4.4.11 $n^4 + 4n^3 + 6n^2 + 4n + 5 = (n+1)^4 + 4 = \left((n+1)^2 + 2\right)^2 - 4(n+1)^2 = \left((n+1)^2 - 2(n+1) + 2\right)\left((n+1)^2 + 2(n+1) + 2\right) = (n^2+1)\left((n+2)^2 + 1\right)$.

Si le nombre proposé est premier, alors $n^2 + 1 = 1$ ou $(n+2)^2 + 1 = 1$, d'où $n = 0$ ou -2.

Vérifier la réciproque.

◇ **Réponse :** $\{-2, 0\}$.

4.4.12

- $p = 2$ ne convient pas, $p = 3$ convient.
- Si p est premier et $\geqslant 5$, alors, en passant modulo 3 : $\begin{cases} 2^p \equiv (-1)^p = -1 \\ p^2 \equiv 1 \end{cases}$,

d'où $2^p + p^2 \equiv 0\ [3]$. Comme $2^p + p^2$ est premier, on a : $2^p + p^2 = 3$, contradiction.

◇ **Réponse :** $\{3\}$.

4.4.13 $\displaystyle\sum_{k=0}^{p-1}(n+k)^2 = n^2\sum_{k=0}^{p-1}1 + 2n\sum_{k=0}^{p-1}k + \sum_{k=0}^{p-1}k^2$

$\displaystyle= n^2p + 2n\frac{(p-1)p}{2} + \frac{(p-1)p(2p-1)}{6} = p\left(n^2 + n(p-1) + \frac{(p-1)(2p-1)}{6}\right).$

Il suffit de prouver : $\dfrac{(p-1)(2p-1)}{6} \in \mathbb{N}$.

Comme p est premier $\geqslant 5$, on a :

- p impair, donc $(p-1)(2p-1) \equiv 0\ [2]$
- $3 \nmid p$, donc $p - 1 \underset{[3]}{\equiv} 0$ ou $2p - 1 \underset{[3]}{\equiv} 0$, d'où $(p-1)(2p-1) \equiv 0\ [3]$.

4.4.14 Supposons qu'il existe p premier impair tel que $p|m$ et $p|n$; il existe $(m',n') \in (\mathbb{N}^*)^2$ tel que : $m = pm'$, $n = pn'$. On a, puisque p est impair :

$$a^m + b^n = (a^{m'})^p + (b^{n'})^p = (a^{m'} + b^{n'})\sum_{k=0}^{p-1}(-1)^k(a^{m'})^k(b^{n'})^{p-1-k}.$$

Ainsi $a^{m'} + b^{n'} \mid a^m + b^n$ et, comme $p \geqslant 2$, $2 \leqslant a^{m'} + b^{n'} < a^m + b^n$, contradiction avec $a^m + b^n$ premier.

Ceci montre que m et n n'admettent comme diviseur premier commun que 2.

4.4.15

- p et $p+2$ sont premiers et non divisibles par 3, donc $p \equiv -1\ [3]$, $3 \mid p+1$.
- p est impair, donc $p \equiv -1\ [2]$, $2 \mid p+1$.
- $2 \wedge 3 = 1$, donc $6 \mid p+1$.

4.4.16 Si $3 \notin \{p,q,r\}$, alors $p \equiv \pm 1\ [3]$, $q \equiv \pm 1\ [3]$, $r \equiv \pm 1\ [3]$, donc $p^2 + q^2 + r^2 \equiv 0\ [3]$, $p^2 + q^2 + r^2 = 3$, contradiction.

4.4.17 Si $n \geqslant 1$, alors $2^{2^n} + 5 \geqslant 9$ et $2^{2^n} + 5 \underset{[3]}{\equiv} 1 + 5 \underset{[3]}{\equiv} 0$, donc $2^{2^n} + 5$ n'est pas premier.

Si $n = 0$, $2^{2^n} + 5 = 7$ qui est premier.

◊ **Réponse :** $\{7\}$.

4.4.18 Il existe $m \in \mathbb{N} - \{0,1\}$ tel que $n = pm$. Supposons m composé ; il existe $(m_1,m_2) \in \mathbb{N}^2$ tel que : $m = m_1m_2$, $1 < m_1 < m$, $1 < m_2 < m$. Comme p est le plus petit diviseur premier de n, on a : $m_1 \geqslant p$ et $m_2 \geqslant p$, d'où $n = pm_1m_2 \geqslant p^3$, contradiction.

4.4.19

- Si $p \geqslant 13$, alors $p = 9 + (p-9)$ où 9 et $p-9$ (qui est pair $\geqslant 4$) sont composés.
- Examiner les cas $p = 2,3,5,7,11$.

◊ **Réponse :** Les nombres premiers $\geqslant 13$.

4.4.20 Montrer d'abord $p \equiv \pm 1$ [6].

Il existe alors $(q,\varepsilon) \in \mathbb{N} \times \{-1,1\}$ tel que : $p = 6q + \varepsilon$ et $q \geqslant 1$. On a :

$$4p^2 + 1 = 144q^2 + 48\varepsilon q + 5 = (8q + 2\varepsilon)^2 + (8q + \varepsilon)^2 + (4q)^2,$$

où $(8q + 2\varepsilon, 8q + \varepsilon, 4q) \in (\mathbb{N}^*)^3$.

4.4.21 *a)* Comme $p! = k!(p-k)!\mathrm{C}_p^k$, p divise $k!(p-k)!\mathrm{C}_p^k$.

On a : $\forall k \in \{1,\ldots,p-1\}$, $p \wedge k = p \wedge (p-k) = 1$, donc $p \wedge \big(k!(p-k)!\big) = 1$.

Le théorème de Gauss permet de conclure : $p|\mathrm{C}_p^k$.

b) $\dfrac{p!}{i_1!\ldots i_n!}$ est un entier, car c'est le coefficient de $\mathrm{X}_1^{i_1}\ldots\mathrm{X}_n^{i_n}$ dans le développement de $(\mathrm{X}_1+\ldots+\mathrm{X}_n)^p$ par la formule du *multinôme de Newton*, généralisation de la formule du binôme de Newton.

Terminer comme en *a)*.

4.4.22 Examiner le cas $p = 2$.

Supposons p premier impair; il existe $k \in \mathbb{N}^*$ tel que $p = 2k + 1$.

On a : $2^p + 3^p = (2+3)a$, où $a = 2^{2k} - 2^{2k-1}\cdot 3 + \ldots + 3^{2k}$, en passant modulo 5 : $a \equiv (2k+1)2^{2k} = p\cdot 2^{2k}$.

Si $p \neq 5$, alors $p \not\equiv 0$ [5], et $2^{2k} \not\equiv 0$ [5], d'où, puisque 5 est premier, $p2^{2k} \not\equiv 0$ [5]. Ceci prouve : $5|2^p + 3^p$ et $5^2 \not| 2^p + 3^p$. Il n'existe donc pas $(a,n) \in (\mathbb{N} - \{0,1\})^2$ tel que $2^p + 3^p = a^n$.

Examiner le cas $p = 5$.

4.4.23 Raisonnons par l'absurde : supposons qu'il existe $n \in \mathbb{Z}$ tel que $49|u_n$, où $u_n = n^3 - n^2 - 2n + 1$. Comme $u_n = (n+2)^3 - 7n^2 - 14n - 7$, on déduit $7|(n+2)^3$, puis $7|n+2$ puisque 7 est premier. Il existe $k \in \mathbb{Z}$ tel que $n = 7k - 2$. On a alors $u_n = 7^2(7k^3 - 7k^2 + 2k) - 7$, donc $7^2 \not| u_n$, contradiction.

4.4.24 *1)* Soit $n \in \mathbb{N}$; notons $\delta = (2n^7 + 1) \wedge (3n^3 + 2)$. En utilisant une division euclidienne :

$$9(2n^7 + 1) = (3n^3 + 2)(6n^4 - 4n) + 8n + 9,$$

d'où $\delta \mid 8n + 9$.

Puis, de la même façon :

$$512(3n^3 + 2) = (8n + 9)(192n^2 - 216n + 243) - 1163,$$

d'où $\delta|1163$.

Comme 1163 est premier, on obtient $\delta = 1163$.

Il existe donc $a \in \mathbb{N}^*$ tel que $8n + 9 = 1163a$. En passant modulo 8 :

$$1163a \equiv 9\ [8] \Longrightarrow 3a \equiv 1\ [8] \Longrightarrow a \equiv 9a \equiv 3\ [8].$$

Il existe donc $b \in \mathbb{N}$ tel que $a = 8b + 3$, puis $n = 1163b + 435$.

2) Réciproquement, soient $b \in \mathbb{N}$ et $n = 1163b + 435$. En utilisant les divisions euclidiennes vues en *1)*, on a : $1163 \mid 8n + 9$, $1163 \mid 3n^3 + 2$, $1163 \mid 2n^7 + 1$, d'où $(2n^7 + 1) \wedge (3n^3 + 2) \neq 1$.

◇ **Réponse :** $\{1163b + 435;\ b \in \mathbb{N}\}$.

4.4.25 *a)* Il existe $(n,a) \in \mathbb{N}^2$ tel que $k = 2^n(2a+1)$. On a :

$$2^k + 1 = (2^{2^n})^{2a+1} + 1 = (2^{2^n}+1)\sum_{i=0}^{2a}(-1)^i(2^{2^n})^i.$$

Comme $2^k + 1$ est premier et $2^{2^n} + 1 \in \mathbb{N}^*$; on déduit $2^k + 1 = 2^{2^n} + 1$, $k = 2^n$.

b) Soit $(m,n) \in \mathbb{N}^2$ tel que $m > n$, par exemple. Passons modulo F_n :

$$F_m - 1 = 2^{2^m} = (2^{2^n})^{2^{m-n}} \underset{[F_n]}{\equiv} (-1)^{2^{m-n}} = 1,$$

d'où $F_m \equiv 2\ [F_n]$.

Il en résulte : $F_m \wedge F_n \mid 2$. Comme F_m et F_n sont impairs, on conclut : $F_m \wedge F_n = 1$.

4.4.26 Il existe $m \in \mathbb{N}^*$ tel que $n = mp$. On a : $4^n - 2^n + 1 = A_p(2^m)$ où $A_p = X^{2p} - X^p + 1 \in \mathbb{Z}[X]$.

En notant $A_1 = X^2 - X + 1 \in \mathbb{Z}[X]$, on montre que A_1 divise A_p dans $\mathbb{C}[X]$:

$$A_1 = (X + j)(X + j^2), \quad A_p(j) = A_p(j^2) = j^{2p} + j^p + 1 = \frac{j^{3p} - 1}{j^p - 1} = 0, \quad A_p(j^2) = 0.$$

Il en résulte que A_1 divise A_p dans $\mathbb{Z}[X]$, puis $A_1(2^m) | A_p(2^m)$ dans $\mathbb{Z}$.

Enfin, montrer $1 < A_1(2^m) < A_p(2^m)$.

4.4.27 Notons, pour tout k de $\mathbb{N}^*$, $\beta_k = 4^k + 2^k + 1$ et $B_k = X^{2k} + X^k + 1 \in \mathbb{Z}[X]$, de sorte que $\beta_k = B_k(2)$.

Examiner le cas $n = 1$.

On suppose $n \geqslant 2$ et β_n premier. Il existe $(k,m) \in \mathbb{N}^2$ tel que : $\begin{cases} n = 3^k m \\ m \not\equiv 0\ [3] \end{cases}$ (k est la 3-valuation de n).

Ainsi : $B_n(X) = (X^{3^k})^{2m} + (X^{3^k})^m + 1 = B_m(X^{3^k})$.

Supposons $m \geqslant 2$.

Comme $m \not\equiv 0\ [3]$, on a $B_m(j) = B_m(j^2) = j^{2m} + j^m + 1 = \dfrac{j^{3m} - 1}{j^m - 1} = 0$, donc $B_1 | B_m$ dans $\mathbb{C}[X]$.

Puisque $(B_1, B_m) \in (\mathbb{Z}[X])^2$, il en résulte $B_1 | B_m$ dans $\mathbb{Z}[X]$, puis $B_1(2^{3^k}) | B_m(2^{3^k}) = B_n(2) = \beta_n$ dans $\mathbb{Z}$.

Comme $1 < B_1(2^{3^k}) < \beta_n$, β_n est composé, contradiction.

On conclut : $m = 1$, $n = 3^k$.

4.4.28 *1)* Si n est composé, il existe $(a,b) \in \mathbb{N}^2$ tel que : $1 < a < n$, $1 < b < n$, $n = ab$, $a \geqslant b$.

Comme $1, a, n$ sont des diviseurs $\geqslant 1$ de n, deux à deux distincts, on a : $\sigma(n) \geqslant 1 + a + n$.

Mais $a^2 \geqslant ab = n$, donc $a \geqslant \sqrt{n}$, d'où $\sigma(n) \geqslant 1 + \sqrt{n} + n > n + \sqrt{n}$.

2) Si n est premier, $\sigma(n) = n + 1 < n + \sqrt{n}$.

4.4.29 *1)* Pour tout diviseur $d(\geqslant 1)$ de a, bd est un diviseur $(\geqslant 1)$ de ab, d'où :

$$\sigma(ab) = \sum_{\delta | ab} \delta \geqslant \sum_{d|a} bd = b\sigma(a), \quad \text{et donc } \frac{\sigma(ab)}{ab} \geqslant \frac{\sigma(a)}{a}.$$

2) • Soit D un diviseur $(\geqslant 1)$ de ab. Notons $d = D \wedge a$; il existe $(a',\delta) \in (\mathbb{N}^*)^2$ tel que : $a = da'$, $D = d\delta$, $a' \wedge \delta = 1$. Comme $\delta | a'b$ et $\delta \wedge a' = 1$, le théorème de Gauss montre : $\delta | b$.

On obtient ainsi : $D = d\delta$, $d|a$, $\delta|b$.

• On en déduit : $\sigma(ab) = \sum_{D|ab} D \leqslant \sum_{\substack{d|a \\ \delta|b}} d\delta = \left(\sum_{d|a} d\right)\left(\sum_{\delta|d} \delta\right) = \sigma(a)\sigma(b)$.

4.4.30 Notons $\delta = a \wedge b$; il existe $(a',b') \in (\mathbb{N}^*)^2$ tel que : $a = \delta a'$, $b = \delta b'$, $a' \wedge b' = 1$.

On a : $(a^2 + ab + b^2) \wedge (ab) = \delta^2 \cdot \big((a'^2 + a'b' + b'^2) \wedge (a'b')\big)$. Supposons qu'il existe un diviseur premier commun p à $a'^2 + a'b' + b'^2$ et $a'b'$. Comme p est premier et $p|a'b'$, on a (quitte à échanger a' et b') : $p|a'$. Ainsi, $p|a'$ et $p|a'^2 + a'b' + b'^2$, donc $p|b'^2$, $p|b'$ (car p est premier). On aboutit à une contradiction avec $a' \wedge b' = 1$.

Ainsi $a'^2 + a'b' + b'^2$ et $a'b'$ n'ont aucun diviseur premier commun, d'où $(a'^2 + a'b' + b'^2) \wedge (a'b') = 1$, puis $(a^2 + ab + b^2) \wedge (ab) = \delta^2 = (a \wedge b)^2$.

4.4.31 ◇ **Réponse :** non; exemple : $a = 4$, $b = 10$.

4.4.32 On écrit les décompositions primaires de a,b sous la forme :

$$a = \left(\prod_{i\in I} p_i^{\alpha_i}\right)\left(\prod_{i\in J} p_i^{\alpha'_i}\right)\left(\prod_{i\in K} p_i^{\alpha''_i}\right), \quad b = \left(\prod_{i\in L} p_i^{\beta_i}\right)\left(\prod_{i\in J} p_i^{\beta'_i}\right)\left(\prod_{i\in K} p_i^{\beta''_i}\right)$$

où $\begin{cases} I, J, K, L \text{ sont deux à deux disjoints} \\ \text{les } p_i \ (i \in I \cup J \cup K \cup L) \text{ sont premiers deux à deux distincts} \\ \forall i \in J, \quad \alpha'_i \geqslant \beta'_i \geqslant 1 \\ \forall i \in K, \quad \beta''_i > \alpha''_i > 1. \end{cases}$

Il suffit alors de prendre : $x = \left(\prod_{i\in I} p_i^{\alpha_i}\right)\left(\prod_{i\in J} p_i^{\alpha'_i}\right)$, $y = \left(\prod_{i\in L} p_i^{\beta_i}\right)\left(\prod_{i\in K} p_i^{\beta''_i}\right)$.

Exemple : $a = 2^4 \cdot 3^2 \cdot 5 \cdot 7$, $b = 2 \cdot 3^2 \cdot 5^2 \cdot 11$; la méthode précédente permet de choisir $x = 2^4 \cdot 3^2 \cdot 7$, $y = 5^2 \cdot 11$.

4.4.33 Considérons les décompositions primaires : $a = \prod_{i=1}^{N} p_i^{r_i}$, $b = \prod_{i=1}^{N} p_i^{s_i}$, où $N \in \mathbb{N}^*$, $p_1,\dots,p_N$ sont premiers deux à deux distincts, et $r_1,\dots,r_N,s_1,\dots,s_N \in \mathbb{N}$.

Comme $a \wedge b = 1$, on a : $\forall i \in \{1,\dots,N\}$, ($r_i = 0$ ou $s_i = 0$). Mais $c^k = \prod_{i=1}^{N} p_i^{r_i+s_i}$, d'où, par unicité de la décomposition primaire de c^k : $\forall i \in \{1,\dots,N\}$, $k \mid r_i + s_i$.

On déduit : $\forall i \in \{1,\dots,N\}$, ($k|r_i$ et $k|s_i$).

Il existe $\alpha_1,\dots,\alpha_N,\beta_1,\dots,\beta_N \in \mathbb{N}$ tels que : $\forall i \in \{1,\dots,N\}$, ($r_i = k\alpha_i$ et $s_i = k\beta_i$).

En notant $\alpha = \prod_{i=1}^{N} p_i^{\alpha_i}$ et $\beta = \prod_{i=1}^{N} p_i^{\beta_i}$, on a : $(\alpha,\beta) \in (\mathbb{N}^*)^2$, $a = \alpha^k$, $b = \beta^k$.

4.4.34 Passer par les décompositions primaires de a et b.

Exemple : $a^3|b^5 \Longrightarrow a|b^2$.

4.4.35 Notons $A = (a \vee b)(a \vee c)(b \vee c)(a \wedge b \wedge c)$ et $B = (a \vee b \vee c)|abc|$. Soient p un nombre premier et α,β,γ les p-valuations de a,b,c respectivement. Vu les rôles symétriques de a,b,c, on peut supposer $\alpha \leqslant \beta \leqslant \gamma$. On a :

- $v_p(A) = v_p(a \vee b) + v_p(a \vee c) + v_p(b \vee c) + v_p(a \wedge b \wedge c)$
  $= \text{Max}(\alpha,\beta) + \text{Max}(\alpha,\gamma) + \text{Max}(\beta,\gamma) + \text{Min}(\alpha,\beta,\gamma) = \beta + \gamma + \gamma + \alpha$
- $v_p(B) = v_p(a \vee b \vee c) + v_p(a) + v_p(b) + v_p(c) = \text{Max}(\alpha,\beta,\gamma) + \alpha + \beta + \gamma = \gamma + \alpha + \beta + \gamma$.

Ainsi : $\begin{cases} \forall p \in \mathcal{P}, \quad v_p(A) = v_p(B) \\ (A,B) \in (\mathbb{N}^*)^2 \end{cases}$, d'où $A = B$.

4.4.36 Raisonner comme dans la solution de l'exercice 4.4.35.

4.4.37 Remarquer que l'application $(s_1,\ldots,s_N) \longmapsto \prod_{i=1}^{N} p_i^{s_i}$ est une bijection de $\prod_{i=1}^{N}\{0,\ldots,r_i\}$ sur l'ensemble des diviseurs ($\geqslant 1$) de n. D'où :

1) $\mathrm{d}(n) = \text{Card}\left(\prod_{i=1}^{N}\{0,\ldots,r_i\}\right) = \prod_{i=1}^{N}(r_i + 1)$

2) $\sigma(n) = \sum_{\substack{1\leqslant i\leqslant N \\ 0\leqslant s_i\leqslant r_i}} \left(\prod_{i=1}^{N} p_i^{s_i}\right) = \prod_{i=1}^{N}\left(\sum_{k=0}^{r_i} p_i^k\right) = \prod_{i=1}^{N} \frac{p_i^{r_i+1} - 1}{p_i - 1}$.

4.4.38 Considérons la décomposition primaire $n = \prod_{i=1}^{N} p_i^{r_i}$, et $\mathrm{d}(n)$ le nombre de diviseurs ($\geqslant 1$) de n. Notons $\mathrm{p}(n)$ le produit des diviseurs ($\geqslant 1$) de n.

1) Si n n'est pas un carré d'entier, on peut grouper les diviseurs de n deux par deux de produit n, d'où : $(\mathrm{p}(n))^2 = n^{\mathrm{d}(n)}$.

2) Si n est un carré d'entier, $n = k^2$ ($k \in \mathbb{N}^*$), on peut grouper les diviseurs de n, autres que k, deux par deux de produit n, d'où : $(\mathrm{p}(n))^2 = k^2 n^{\mathrm{d}(n)-1} = n^{\mathrm{d}(n)}$.

◊ **Réponse :** $n^{\frac{\mathrm{d}(n)}{2}}$.

De plus : $\mathrm{d}(n) = \prod_{i=1}^{N}(r_i + 1)$, cf. exercice 4.4.37.

4.4.39 Notons $q(n) = \prod_{\substack{1\leqslant d<n \\ d|n}} d$.

1) Si n admet au moins trois diviseurs premiers p_1, p_2, p_3 deux à deux distincts, alors :

$q(n) \geqslant p_1 p_2 \dfrac{n}{p_1} > n$.

2) Si n admet exactement deux diviseurs premiers p_1, p_2 distincts, et si, par exemple, $p_1^2 | n$, alors : $q(n) \geqslant p_1 p_1^2 \dfrac{n}{p_1} > n$.

3) Si $n = p_1 p_2$, p_1, p_2 premiers distincts, alors : $q(n) = p_1 p_2 = n$.

4) Si $n = p^\alpha$, p premier, $\alpha \in \mathbb{N}^*$, alors : $q(n) = \displaystyle\prod_{k=0}^{\alpha-1} p^k = p^{\frac{(\alpha-1)\alpha}{2}}$, d'où :

$q(n) = n \iff \dfrac{(\alpha-1)\alpha}{2} = \alpha \iff \alpha = 3.$

4.4.40 *a)* Raisonner comme dans la solution de l'exercice 4.4.37, calcul de $\sigma(n)$ $(= \sigma_1(n))$.

b) Soit $(a,b) \in (\mathbb{N}^*)^2$ tel que $a \wedge b = 1$; considérons les décompositions primaires $a = \displaystyle\prod_{i=1}^{N} p_i^{r_i}$, $b = \displaystyle\prod_{i=1}^{N} p_i^{s_i}$. Comme $a \wedge b = 1$, on a : $\forall i \in \{1,\dots,N\}$, ($r_i = 0$ ou $s_i = 0$). Soit $i \in \{1,\dots,N\}$.

Supposons par exemple $s_i = 0$. Alors : $\dfrac{p_i^{k(r_i+s_i+1)} - 1}{p_i^k - 1} = \dfrac{p_i^{k(r_i+1)} - 1}{p_i^k - 1} \dfrac{p_i^{k(s_i+1)} - 1}{p_i^k - 1}$.

On conclut : $\sigma_k(ab) = \sigma_k(a)\sigma_k(b)$.

4.4.41 D'après l'exercice 4.4.37 p. 128 :

$$\sigma(N) = \frac{2^{n+1}-1}{2-1} \cdot \frac{3^2-1}{3-1} \cdot \frac{p^2-1}{p-1} = (2^{n+1}-1)4(p+1).$$

Donc : $\sigma(N) = 3N \iff (2^{n+1}-1)4(p+1) = 2^n \cdot 3^2 p.$ (1)

Comme $2^n \wedge (2^{n+1}-1) = 1$, on déduit $2^n | 4(p+1)$; il existe alors $\lambda \in \mathbb{N}^*$ tel que $4(p+1) = 2^n\lambda$.

Ainsi : $(1) \iff (2^{n+1}-1)\lambda = 9p \iff 2 \cdot 2^n\lambda = \lambda + 9p \iff \lambda = 8 - p$.

Comme $\lambda \in \mathbb{N}^*$ et $p \geqslant 5$, p premier, on déduit $p \in \{5,7\}$.

- $p = 5 : \lambda = 8 - p = 3, 2^n = 8, n = 3, N = 2^3 \cdot 3 \cdot 5 = 120, \sigma(N) = (2^4-1) \cdot 4 \cdot 6 = 360 = 3N.$
- $p = 7 : \lambda = 8 - p = 1, 2^n = 32, n = 5, N = 2^5 \cdot 3 \cdot 7 = 672, \sigma(N) = (2^6-1)4 \cdot 8 = 2016 = 3N.$

◇ **Réponse :** $\{(3,5), (5,7)\}$.

4.4.42 *a)* $\mathbb{Z}/11\mathbb{Z}$ est un corps (11 est premier) et :

$$x^2 + \widehat{4}x + \widehat{1} = 0 \iff (x+\widehat{2})^2 - \widehat{3} = 0 \iff (x+\widehat{2})^2 - \widehat{25} = 0 \iff (x-\widehat{3})(x-\widehat{4}) = 0.$$

◇ **Réponse :** $\{\widehat{3},\widehat{4}\}$.

2) $\mathbb{Z}/12\mathbb{Z}$ n'est pas un corps (12 n'est pas premier). Puisque $\widehat{5}$ est inversible dans $\mathbb{Z}/12\mathbb{Z}$ $(\widehat{5} \cdot \widehat{5} = \widehat{1})$, on a :

$$\widehat{5}x + \widehat{2}y = \widehat{3} \iff \widehat{5}(\widehat{5}x + \widehat{2}y) = \widehat{5} \cdot \widehat{3} \iff x + \widehat{10}y = \widehat{15} \iff x = \widehat{2}y + \widehat{3}.$$

Puis : $\begin{cases} \widehat{5}x + \widehat{2}y = \widehat{3} \\ \widehat{2}x + \widehat{4}y = \widehat{6} \end{cases} \iff \begin{cases} x = \widehat{2}y + \widehat{3} \\ \widehat{2}(\widehat{2}y + \widehat{3}) + \widehat{4}y = \widehat{6} \end{cases} \iff \begin{cases} x = \widehat{2}y + \widehat{3} \\ \widehat{8}y = 0 \end{cases}$.

On a, pour tout a de $\mathbb{Z}$: $8\widehat{a} = \widehat{0} \iff 12 | 8a \iff 3 | 2a \iff 3 | a \iff \widehat{a} \in \{\widehat{0},\widehat{3},\widehat{6},\widehat{9}\}$.

◇ **Réponse :** $\{(\widehat{3},\widehat{0}), (-\widehat{3},\widehat{3}), (\widehat{3},\widehat{6}), (-\widehat{3},-\widehat{3})\}$.

4.4.43 *a)* Cf. exercice 4.4.21 *a)* p. 127.

b) Récurrence sur f.

1) Cas $f = 1$.

Récurrence sur N.

- La propriété est évidente pour $N = 1$.
- Pour $N = 2$: $(x_1 + x_2)^p = x_1^p + \sum_{k=1}^{p-1} C_p^k x_1^k x_2^{p-k} + x_2^p \equiv x_1^p + x_2^p \ [p]$, d'après *a)*.
- Supposons la formule vraie pour un N de $\mathbb{N}^*$. Soit $(x_1, \ldots, x_{N+1}) \in \mathbb{Z}^{N+1}$; on a :

$$\left(\sum_{i=1}^{N+1} x_i\right)^p = \left(\left(\sum_{i=1}^{N} x_i\right) + x_{N+1}\right)^p \underset{[p]}{\equiv} \left(\sum_{i=1}^{N} x_i\right)^p + x_{N+1}^p \underset{[p]}{\equiv} \sum_{i=1}^{N} x_i^p + x_{N+1}^p = \sum_{i=1}^{N+1} x_i^p.$$

2) Supposons la formule vraie pour un f de $\mathbb{N}^*$. On a alors :

$$\left(\sum_{i=1}^{N} x_i\right)^{p^{f+1}} = \left(\left(\sum_{i=1}^{N} x_i\right)^{p^f}\right)^p \underset{[p]}{\equiv} \left(\sum_{i=1}^{N} x_i^{p^f}\right)^p \underset{[p]}{\equiv} \sum_{i=1}^{N} \left(x_i^{p^f}\right)^p = \sum_{i=1}^{N} x_i^{p^{f+1}}.$$

4.4.44 Supposons qu'il existe $x \in \mathbb{Z}$ tel que $5 | ax^3 + bx^2 + cx + d$. On a : $5 \nmid x$, car sinon $5 | d$.
Puisque 5 est premier, il en résulte $5 \wedge x = 1$ et donc (théorème de Bezout), il existe $(y, v) \in \mathbb{Z}^2$ tel que $xy + 5v = 1$.

Comme $x^3(dy^3 + c^2y + by + a) \underset{[5]}{\equiv} ax^3 + bx^2 + cx + d \underset{[5]}{\equiv} 0$ et que $5 \nmid x^3$,

on conclut : $dy^3 + cy^2 + by + a \equiv 0 \ [5]$.

4.4.45 *1)* $(p-1)! C_{np-1}^{p-1} = \prod_{k=1}^{p-1} (np - k) \underset{[p]}{\equiv} \prod_{k=1}^{p-1} (-k) = (-1)^{p-1}(p-1)!$.

Comme p est premier, $(p-1)! \wedge p = 1$, donc $(p-1)!$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$; on peut donc simplifier par $(p-1)!$ et conclure : $C_{np-1}^{p-1} \equiv (-1)^{p-1} \ [p]$.

- Si p est impair : $C_{np-1}^{p-1} \equiv 1 \ [p]$
- Si p est pair : $p = 2$, $C_{np-1}^{p-1} \equiv -1 \equiv 1 \ [2]$.

2) $C_{np}^{p} = n C_{np-1}^{p-1} \equiv n \ [p]$.

4.4.46 Soit (x, y) une solution; on a :

$$2(x^2 - xy + y^2) = 7(x + y) \tag{1}$$

Comme $2 | 7(x + y)$ et $2 \wedge 7 = 1$, on déduit $2 | x + y$; il existe $u \in \mathbb{N}^*$ tel que $x + y = 2u$.

Vu les rôles symétriques de x et y, on peut supposer $x \geqslant y$. Comme $x + y$ est pair, $x - y$ l'est aussi, et il existe donc $v \in \mathbb{N}$ tel que $x - y = 2v$. On a :

$$(1) \iff u^2 + 3v^2 = 7u \iff u(7 - u) = 3v^2 \implies 1 \leqslant u < 7.$$

Tester $u = 1, 2, 3, 4, 5, 6$.

◊ **Réponse :** $\{(1,5), (2,6), (5,1), (6,2)\}$.

4.4.47 Supposons que l'ensemble des solutions ne soit pas vide. Il existe alors une solution (x,y,z) telle que z soit minimal.

• **Cas** $z \geqslant 2$

Alors $3|y$; $y = 3Y$, $Y \in \mathbb{N}$. Puis : $5x^2 - 12Y^2 = 3^{z-1}$, donc $3|x$; $x = 3X$, $X \in \mathbb{N}$. D'où : $15X^2 - 4Y^2 = 3^{z-2}$, et $(X,Y,z-2)$ est une solution, ce qui contredit la minimalité de z.

• **Cas** $z = 1$

Alors $3|y$; $y = 3Y$, $Y \in \mathbb{N}$. Puis $5x^2 - 12Y^2 = 1$, d'où $x^2 \equiv -1$ [3], contradiction.

• **Cas** $z = 0$

Alors $15x^2 - 4y^2 = 1$, d'où $y^2 \equiv -1$ [3], contradiction.

4.4.48 Il existe $q \in \mathbb{N}^*$ tel que $p = 2q + 1$. On a : $H_{p-1} = \sum_{k=1}^{q}\left(\frac{1}{k} + \frac{1}{p-k}\right) = pK_p$, où

$$K_p = \frac{1}{p}\sum_{k=1}^{q}\left(\frac{1}{k} + \frac{1}{p-k}\right) = \sum_{k=1}^{q}\frac{1}{k(p-k)}.$$

Donc : $(p-1)!K_p = \sum_{k=1}^{q}\alpha_{p,k}$, où $\alpha_{p,k} = \frac{(p-1)!}{k(p-k)} = \prod_{\substack{1\leqslant i\leqslant 2q \\ i\neq k,\ i\neq p-k}} i$.

On a : $\forall k \in \{1,\dots,q\}$, $k(p-k)\alpha_{p,k} = (p-1)!$, d'où dans $\mathbb{Z}/p\mathbb{Z}$: $\widehat{(q-1)!}\widehat{K}_p = -\sum_{k=1}^{q}\widehat{(p-1)!}(\widehat{k^2})^{-1}$.

Comme $\widehat{(p-1)!}$ est inversible, on déduit : $\widehat{K}_p = -\sum_{k=1}^{q}(\widehat{k^2})^{-1}$.

Mais aussi, par le changement d'indice $l = p - k$: $\widehat{K}_p = -\sum_{l=q+1}^{2q}(\widehat{p-l^2})^{-1} = -\sum_{l=q+1}^{2q}(\widehat{l^2})^{-1}$,

d'où : $2\widehat{K}_p = -\sum_{k=1}^{2q}(\widehat{k^2})^{-1} = -\sum_{k=1}^{2q}(\widehat{k^{-1}})^2$.

Comme $\widehat{k} \longmapsto \widehat{k}^{-1}$ est une permutation de $\mathbb{Z}/p\mathbb{Z} - \{0\}$, on déduit :

$$2\widehat{K}_p = -\sum_{k=1}^{2q}\widehat{k}^2 = -\left(\sum_{k=1}^{2q}k^2\right)\widehat{\ } = -\left(\frac{2q(2q+1)(4q+1)}{6}\right)\widehat{\ } = -\left(\frac{q(4q+1)}{3}\,p\right)\widehat{\ }.$$

Si $q \equiv 1$ [3], alors $p \equiv 0$ [3], contradiction; donc $q \equiv -1$ ou 0 [3], d'où $q(4q+1) \equiv 0$ [3].

Ainsi, $\frac{q(4q+1)}{3} \in \mathbb{N}$, et donc $2\widehat{K}_p = \widehat{0}$. Enfin $2 \wedge p = 1$, d'où $\widehat{K}_p = \widehat{0}$, $p|K_p$, $p^2|H_{p-1}$.

4.4.49 *a)* et *b)* Analogue à la solution de l'exercice 4.4.48.

c) On a : $(p-1)!C_{2p-1}^{p-1} = \prod_{k=1}^{p-1}(k+p)$.

En développant, on voit qu'il existe $c \in \mathbb{N}$ tel que :

$$\prod_{k=1}^{p-1}(k+p) = (p-1)! + pa + p^2b + p^3c.$$

Comme $p^2|a$ et $p|b$ (cf. *b)*), on déduit : $(p-1)!\left(C_{2p-1}^{p-1} - 1\right) \equiv 0\ [p^3]$, puis $C_{2p-1}^{p-1} - 1 \equiv 0\ [p^3]$, puisque $(p-1)! \wedge p^3 = 1$.

4.4.50 *a) 1)* Montrons, par récurrence sur n : $\forall n \in \mathbb{N}, n^p \equiv n\ [p]$.

La propriété est évidente pour $n = 0$.

Supposons-la vraie pour un n de $\mathbb{N}$. En utilisant l'exercice 4.4.21 *a)* p. 127, on a :

$$(n+1)^p = n^p + \sum_{k=1}^{p-1} C_p^k n^k + 1 \underset{[p]}{\equiv} n^p + 1 \underset{[p]}{\equiv} n + 1.$$

2) Soit $n \in \mathbb{Z}$.

Si p est impair : $n^p = -(-n)^p \underset{[p]}{\equiv} -(-n) = n$.

Si $p = 2$: $n^2 = (-n)^2 \underset{[2]}{\equiv} -n \underset{[2]}{\equiv} n$.

2) Soit $n \in \mathbb{Z}$ tel que $p \nmid n$. Comme p est premier, on a alors $n \wedge p = 1$, et on peut donc simplifier par n dans la congruence $n^p \equiv n\ [p]$, et obtenir : $n^{p-1} \equiv 1\ [p]$.

4.4.51 Notons $A_n = 5n^7 + 7n^5 + 23n$.

D'après le petit théorème de Fermat (exercice 4.4.50) : $n^5 \equiv n\ [5]$, d'où $A_n \equiv 30n \equiv 0\ [5]$.

De même $n^7 \equiv n\ [7]$, d'où $A_n \equiv 28n \equiv 0\ [7]$. Enfin $5 \wedge 7 = 1$, donc $35 | A_n$.

4.4.52 *a)* D'après le petit théorème de Fermat (exercice 4.4.50) :

Mod. 2 : $n^2 \equiv n$, d'où $n^7 \equiv n$

Mod. 3 : $n^3 \equiv n$, d'où $n^7 \equiv n$

Mod. 7 : $n^7 \equiv n$.

Ainsi, 2, 3, 7, qui sont premiers entre eux deux à deux, divisent $n^7 - n$, d'où : $42 = 2 \cdot 3 \cdot 7 \mid n^7 - n$.

b) $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ et raisonner comme en *a)*.

c) $2^{15} - 2^3 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$.

Mod. 8 : • Si n est pair, alors $8 | n^3$, donc $8 | n^{15} - n^3$.

• Si n est impair, alors $n^2 \equiv 1\ [8]$ (cf. exercice 4.1.1 p. 103), d'où $n^{15} \equiv n\ [8]$ et $n^3 \equiv n\ [8]$, donc $8 \mid n^{15} - n^3$.

Mod. 9 :

n	0	± 1	± 2	± 3	± 4
n^3	0	± 1	∓ 1	0	± 1

On a : $\forall n \in \mathbb{Z}, n^3 \equiv -1, 0$ ou $1\ [9]$. Comme $(-1)^5 = -1, 0^5 = 0, 1^5 = 1$, on déduit :

$\forall n \in \mathbb{Z}, n^{15} = (n^3)^5 \equiv n^3\ [9]$.

Mod. 5, 7, 13 : appliquer le petit théorème de Fermat (exercice 4.4.50).

4.4.53 *a)* $21840 = 2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 13$.

Mod. 16 :

n	± 1	± 3	± 5	± 7
n^{12}	1	1	1	1

En effet : $3^{12} = 9^6 \equiv (-7)^6 = (7^2)^3 \equiv 1^3 = 1$, $5^{12} = 25^6 \equiv (-7)^6 \equiv 1$, $7^{12} = 49^6 \equiv 1^6 = 1$.

Mod. 3, 5, 7, 13 : appliquer le petit théorème de Fermat (exercice 4.4.50).

b) $16320 = 2^6 \cdot 3 \cdot 5 \cdot 17$.

Mod. 64 : Puisque p est impair, il existe $(q,\varepsilon) \in \mathbb{N}^* \times \{-1,1\}$ tel que $p = 4q + \varepsilon$, d'où, en développant par la formule du binôme de Newton :

$$p^{16} = (\varepsilon + 4q)^{16} = 1 + 16 \cdot 4\varepsilon q + \frac{16 \cdot 15}{2}(4q)^2 + \sum_{k=3}^{16} C_{16}^k (4q)^k \varepsilon^{16-k} \equiv 1 \ [64].$$

Mod. 3, 5, 17 : appliquer le petit théorème de Fermat (exercice 4.4.50).

4.4.54 $30 = 2 \cdot 3 \cdot 5$.

Mod 5 : • Si $5 \nmid a$, alors (petit théorème de Fermat, exercice 4.4.50) : $a^4 \equiv 1$ [5], d'où $(a^4)^b \equiv (a^4)^c \equiv 1$ et donc $a^{4b+d} - a^{4c+d} \equiv 0$ [5].

• Si $5|a$, alors $a^{4b+d} - a^{4c+d} \equiv 0$ [5].

Raisonner de même modulo 2 et 3.

4.4.55 Remarquons : $1729 = 7 \cdot 13 \cdot 19$ et 6, 12, 18 divisent $1728 : 1728 = 6 \cdot 288 = 12 \cdot 144 = 18 \cdot 96$. D'après le petit de théorème de Fermat (exercice 4.4.50) :

Mod. 7 : $n^6 \equiv 1$ [7], donc $n^{1728} = (n^6)^{288} \equiv 1$ [7]

Mod. 13 : $n^{12} \equiv 1$ [13], donc $n^{1728} = (n^{12})^{144} \equiv 1$ [13]

Mod. 19 : $n^{18} \equiv 1$ [19], donc $n^{1728} = (n^{18})^{96} \equiv 1$ [19].

Comme 7, 13, 19 sont premiers entre eux deux à deux, on conclut : $n^{1728} \equiv 1$ [1729].

4.4.56 *a)* Remarquer : $\frac{p-1}{2} \in \mathbb{N}^*$.

D'après le petit théorème de Fermat (exercice 4.4.50), p divise $n^{p-1} - 1$.

Comme $n^{p-1} - 1 = \left(n^{\frac{p-1}{2}} - 1\right)\left(n^{\frac{p-1}{2}} + 1\right)$ et que p est premier, on conclut :

$p \mid n^{\frac{p-1}{2}} - 1$, ou $p \mid n^{\frac{p-1}{2}} + 1$.

b) D'après le petit théorème de Fermat, il existe $\lambda \in \mathbb{N}$ tel que : $n^{p-1} = 1 + \lambda p$.

On a alors :

$$n^{p(p-1)} = (1 + \lambda p)^p = 1 + C_p^1 \lambda p + \sum_{k=2}^{p} C_p^k \lambda^k p^k \equiv 1 \ [p^2].$$

Remarquons : $\frac{p(p-1)}{2} \in \mathbb{N}^*$.

En notant $a = n^{\frac{p(p-1)}{2}} - 1$ et $b = n^{\frac{p(p-1)}{2}} + 1$, on a donc : $a \in \mathbb{N}^*$, $b \in \mathbb{N}^*$, $p^2|ab$.

Si $p^2 \nmid a$ et $p^2 \nmid b$, comme p est premier, on a $p|a$ et $p|b$, d'où $p|b - a = 2$, $p = 2$.

Alors n est impair et : $4 \mid n - 1$ ou $4 \mid n + 1$, contradiction.

Ainsi : $p^2 \mid n^{\frac{p(p-1)}{2}} - 1$ ou $p^2 \mid n^{\frac{p(p-1)}{2}} + 1$.

4.4.57 **Mod. *p* :** D'après le petit théorème de Fermat (ex. 4.4.50) : $\begin{cases} (n+1)^p \equiv n+1 & [p] \\ n^p \equiv n & [p] \end{cases}$

d'où $(n+1)^p - (n^p + 1) \equiv 0$ [p].

Mod. 2 : Comme, pour tout x de $\mathbb{Z}$ et tout k de $\mathbb{N}^*$, x^k et x sont de même parité, on a : $\begin{cases}(n+1)^p \equiv n+1 & [2]\\ n^p \equiv n & [2]\end{cases}$, d'où $(n+1)^p - (n^p+1) \equiv 0\ [2]$.

Enfin, comme $2 \wedge p = 1$, on conclut $(n+1)^p - (n^p+1) \equiv 0\ [2p]$.

4.4.58 Récurrence sur k, pour n fixé tel que $n \wedge p = 1$.

Pour $k = 0$, il s'agit du petit théorème de Fermat (exercice 4.4.50).

Supposons la propriété vraie pour un k de $\mathbb{N}$.

Il existe $\lambda \in \mathbb{Z}$ tel que : $(n^{p-1})^{p^k} = 1 + \lambda p^{k+1}$, d'où :

$$(n^{p-1})^{p^{k+1}} = \left((n^{p-1})^{p^k}\right)^p = (1+\lambda p^{k+1})^p = 1 + C_p^1 \lambda p^{k+1} + \sum_{i=2}^{p} C_p^i \lambda^i p^{(k+1)i}.$$

Comme $\forall i \in \{2,\dots,p\}$, $(k+1)i \geqslant k+2$, on déduit : $(n^{p-1})^{p^{k+1}} \equiv 1\ [p^{k+2}]$.

4.4.59 *a)* Vu les rôles symétriques de (a,b) et (α,β), on peut supposer, par exemple $\beta \geqslant b$. Il existe $\lambda \in \mathbb{N}$ tel que : $\beta = b + \lambda(p-1)$. D'après le petit théorème de Fermat (exercice 4.4.50), $a^{p-1} \equiv 1\ [p]$, d'où : $a^\beta = a^b (a^{p-1})^\lambda \equiv a^b\ [p]$.

D'autre part, comme $\alpha \equiv a\ [p]$, on a : $\alpha^\beta \equiv a^\beta\ [p]$.

On conclut : $\alpha^\beta \equiv a^b\ [p]$.

b) Soit $(x,y) \in (\mathbb{N}^*)^2$.

1) Si $5|x$, alors $x^y \equiv 0\ [5]$; on peut donc supposer $5 \nmid x$. Il existe $X \in \{-2,-1,1,2\}$ et $Y = \{0,1,2,3\}$ tels que :

$x \equiv X\ [5]$ et $y \equiv Y\ [4]$.

On calcule X^Y modulo 5 :

X \ Y	0	1	2	3
-2	1	-2	-1	(2)
-1	1	-1	1	-1
1	1	1	1	1
2	1	(2)	-1	-2

Ainsi :

$$X^Y \equiv 2\ [5] \iff \begin{cases}(X=2,\ Y=1)\\ \text{ou}\\ (X=-2,\ Y=3).\end{cases}$$

2) De même, on peut supposer $7 \nmid y$, et il existe $u \in \{-3,-2,-1,1,2,3\}$ et $v \in \{0,1,2,3,4,5\}$ tels que : $y \equiv u\ [7]$ et $x \equiv v\ [6]$.

u \ v	0	1	2	3	4	5
-3	1	-3	2	1	-3	2
-2	1	-2	-3	-1	2	(3)
-1	1	-1	1	-1	1	-1
1	1	1	1	1	1	1
2	1	2	-3	1	2	-3
3	1	(3)	2	-1	-3	-2

Ainsi : $u^v \equiv 3\ [7] \iff \left|\begin{array}{l}(u=3,\ v=1)\\ \text{ou}\\ (u=-2,\ v=5)\end{array}\right.$.

On a donc : $\begin{cases} x^y \equiv 2\ [5] \\ y^x \equiv 3\ [7] \end{cases} \iff \left\{\begin{array}{l} x \equiv\ \ 2\ [5] \quad \text{et} \quad y \equiv 1\ [4] \\ \text{ou} \\ x \equiv -2\ [5] \quad \text{et} \quad y \equiv 3\ [4] \\ x \equiv\ \ 1\ [6] \quad \text{et} \quad y \equiv 3\ [7] \\ \text{ou} \\ x \equiv\ \ 5\ [6] \quad \text{et} \quad y \equiv -2\ [7] \end{array}\right.$.

Résoudre les systèmes de congruences qui apparaissent, en remarquant : $5 \wedge 6 = 1$ et $4 \wedge 7 = 1$.

Par exemple :

$$\begin{cases} x \equiv 2\ [5] \\ x \equiv 1\ [6] \end{cases} \iff \begin{cases} x \equiv 7\ [5] \\ x \equiv 7\ [6] \end{cases} \iff x \equiv 7\ [30].$$

Cf. aussi le théorème chinois, ex. 4.3.16 p. 120.

◇ **Réponse :**

$\big((7+30\mathbb{N})\times(17+28\mathbb{N})\big)\cup\big((17+30\mathbb{N})\times(5+28\mathbb{N})\big)\cup\big((13+30\mathbb{N})\times(3+28\mathbb{N})\big)\cup\big((23+30\mathbb{N})\times(19+28\mathbb{N})\big)$.

4.4.60 D'après le petit théorème de Fermat (ex. 4.4.50) : $a^p \equiv a\ [p]$ et $b^p \equiv b\ [p]$.

Comme $a^p \equiv b^p\ [p]$, on déduit $a \equiv b\ [p]$; il existe $\lambda \in \mathbb{Z}$ tel que $a = b + \lambda p$. On a :

$$a^p = (b+\lambda p)^p = b^p + \mathrm{C}_p^1 b^{p-1}\lambda p + \sum_{k=2}^{p} \mathrm{C}_p^k b^{p-k}(\lambda p)^k \equiv b^p\ [p^2].$$

4.4.61 D'après le petit théorème de Fermat (ex. 4.4.50) : $p^{q-1} \equiv 1\ [q]$.

D'autre part, comme $p - 1 \geqslant 1$: $q^{p-1} \equiv 0\ [q]$. D'où : $p^{q-1} + q^{p-1} \equiv 1\ [q]$.

En échangeant p et q : $p^{q-1} + q^{p-1} \equiv 1\ [p]$.

Comme $p \wedge q = 1$, on conclut : $p^{q-1} + q^{p-1} \equiv 1\ [pq]$.

4.4.62 Puisque p est premier et que $p \nmid a$ et $p \nmid b$, on déduit $p \nmid ab$; ainsi, $F_p(a)$, $F_p(b)$, $F_p(ab)$ existent.

En utilisant le petit théorème de Fermat (ex. 4.4.50) :

$$\begin{cases} a^{p-1} \equiv 1\ [p] \\ b^{p-1} \equiv 1\ [p] \end{cases} \Longrightarrow (a^{p-1}-1)(b^{p-1}-1)) \equiv 0\ [p^2]$$

$$\iff (ab)^{p-1} - 1 \equiv (a^{p-1}-1) + (b^{p-1}-1)\ [p^2]$$

$$\iff \frac{(ab)^{p-1}-1}{p} \equiv \frac{a^{p-1}-1}{p} + \frac{b^{p-1}-1}{p}\ [p].$$

4.4.63 D'après le petit théorème de Fermat (ex. 4.4.50) :

$$\forall z \in \mathbb{Z},\quad z^4 \equiv 0 \text{ ou } 1\ [5].$$

Soit $(x,y) \in \mathbb{Z}^2$. On a : $\begin{cases} x^4 + 781 \equiv 1 \text{ ou } 2\ [5] \\ 3y^4 \equiv 0 \text{ ou } 3\ [5] \end{cases}$, donc $x^4 + 781 \neq 3y^4$.

4.4.64 Soit (x,y) une solution; alors $x > y \geqslant 1$. D'après le petit théorème de Fermat (ex. 4.4.50) par exemple : $x^3 \equiv x\ [3]$ et $y^3 \equiv y\ [3]$, d'où $x - y \equiv x^3 - y^3 = 999 \equiv 0\ [3]$.

On déduit : $x \geqslant y + 3$.

Puis : $999 = x^3 - y^3 \geqslant (y+3)^3 - y^3 = 9y^2 + 27y + 27 > 9y^2$, d'où $y^2 < 111$, $y \leqslant 10$.

Examiner le cas $y = 1$.

Supposons $y \geqslant 2$. Alors $x^3 = 999 + y^3 \geqslant 1007$, d'où $x \geqslant 11$, puis : $y^3 = x^3 - 999 \geqslant 11^3 - 999 = 332$, donc $y \geqslant 7$.

Tester les valeurs 7, 8, 9, 10 de y.

◊ **Réponse :** $\{(10,1), (12,9)\}$.

4.4.65 *a)* D'après le petit théorème de Fermat (ex. 4.4.50) : $\forall \xi \in \mathbb{Z}/p\mathbb{Z} - \{0\}$, $\xi^{p-1} = \widehat{1}$ (où $\widehat{\ }$ désigne la classe modulo p).

Le polynôme $X^{p-1} - \widehat{1}$, de $(\mathbb{Z}/p\mathbb{Z})[X]$, est de degré $p-1$, et admet $\widehat{1}, \ldots, \widehat{p-1}$ pour zéros deux à deux disctincts. On déduit :

$$X^{p-1} - \widehat{1} = \prod_{k=1}^{p-1} (X - \widehat{k}).$$

En remplaçant X par 0 : $-1 \underset{[p]}{\equiv} \prod_{k=1}^{p-1} (-k) = (-1)^{p-1} \cdot (p-1)!$.

Si p est impair, alors : $(p-1)! \equiv -1\ [p]$.

Si p est pair, alors $p = 2$ et : $(p-1)! = 1 \equiv -1\ [2]$.

b) Supposons n composé; il existe $a \in \mathbb{N}^*$ tel que : $2 \leqslant a \leqslant n-1$ et $a|n$. Alors $a|(n-1)!$ et $a|n$, donc $(n-1)! \not\equiv -1\ [n]$.

4.4.66 D'après le théorème de Wilson (ex. 4.4.65 *a)*) : $(n+1)! \equiv -1\ [n+2]$.

Comme $(n+1)! + 1 = (n+2)n! - n! + 1$, on déduit $n+2 | n! - 1$.

En utilisant $n \geqslant 4$, montrer : $n + 2 < n! - 1$.

4.4.67 D'après le théorème de Wilson (ex. 4.4.65 *a)*) : $(p-1)! \equiv -1\ [p]$, c'est-à-dire ici :

$$p | (2n)! + 1.$$

De plus :

$$\begin{aligned}(2n)! + 1 &= (1 \cdot 2 \ldots n)\big((n+1)(n+2)\ldots(2n)\big) + 1 \underset{[p]}{\equiv} (1 \cdot 2 \ldots n)\big((-n)(-n+1)\ldots(-1)\big) + 1 \\ &= (-1)^n (n!)^2 + 1 = (n!)^2 + 1.\end{aligned}$$

4.4.68 Notons $a = 2((p-3)!)$. D'après le théorème de Wilson (ex. 4.4.65 *a)*) :

$$a(p-2)(p-1) = 2((p-1)!) \equiv -2\ [p].$$

D'autre part : $a(p-2)(p-1) \equiv 2a\ [p]$.

D'où $2a \equiv -2\ [p]$, puis, comme $2 \wedge p = 1$: $a \equiv -1\ [p]$.

4.4.69 Il existe $q \in \mathbb{N}$ tel que $p = 4q + 3$. On a :

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 = ((2q+1)!)^2 \underset{[p]}{\equiv} (1 \cdot 2 \dots (2q+1))\Big(\big(-(4q+2)\big)\big(-(4q+1)\big)\dots\big(-(2q+2)\big)\Big)$$
$$= (-1)^{2q+1}(4q+2)! = -(p-1)! \equiv 1\ [p],$$

d'après le théorème de Wilson, ex. 4.4.65 *a)*.

4.4.70 Même genre de solution que pour l'exercice 4.4.69.

4.4.71 *1)* Supposons n et $n+2$ premiers. D'après le théorème de Wilson (ex. 4.4.65 *a)*) :

- $(n+1)! \equiv -1\ [n]$, d'où $4\big((n-1)!+1\big) + n \equiv 0\ [n]$
- $(n+1)! \equiv -1\ [n+2]$, d'où :

$$4\big((n-1)!+1\big) + n = 2\big(2(n-1)!\big) + 4 + n \underset{[n+2]}{\equiv} 2\big((n+1)n(n-1)!\big) + 2 = 2\big((n+1)!+1\big) \underset{[n+2]}{\equiv} 0.$$

Enfin, comme $n \wedge (n+2) = 1$, on conclut : $4\big((n-1)!+1\big) + n \equiv 0\ [n(n+2)]$.

2) Montrer la réciproque en «remontant» les calculs de *1)* et en utilisant l'exercice 4.4.65 *b)* p. 130.

4.4.72 D'après le théorème de Wilson (ex. 4.4.65 *a)*) :

$$-1 \underset{[p]}{\equiv} (p-1)! = (p-n-1)!\big((p-n)(p-n+1)\dots(p-1)\big) \underset{[p]}{\equiv} (p-n-1)!\big((-1)^n n!\big) \underset{[p]}{\equiv} (p-n-1)!$$

Application : Prendre $p = 71$ (qui est premier) et $n = 9$.
On a : $(-1)^n n! = -9! = -2 \cdot 5 \cdot 7(3 \cdot 4 \cdot 6)(8 \cdot 9) \underset{[71]}{\equiv} -70 \underset{[71]}{\equiv} 1$, d'où $61! = (71-9-1)! \equiv -1\ [71]$,
puis $63! = 63 \cdot 62 \cdot 61! \underset{[71]}{\equiv} (-9)(-8)(-1) \underset{[71]}{\equiv} -1$.

4.4.73 Analogue aux exercices 4.4.68 à 4.4.70.

4.4.74 En utilisant les théorèmes de Fermat (ex. 4.4.50) et Wilson (4.4.65 *a)*) :

$$\begin{cases} n^p \equiv n & [p] \\ (p-1)! \equiv -1 & [p] \end{cases}, \quad \text{d'où} \quad n^p + (p-1)!n \equiv 0\ [p].$$

4.4.75 *a)* D'après l'exercice 4.3.16 *b)* p. 120, l'application $\theta : \begin{array}{c} \mathbb{Z}/ab\mathbb{Z} \longrightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ \mathrm{cl}_{ab}(x) \longmapsto \big(\mathrm{cl}_a(x), \mathrm{cl}_b(x)\big) \end{array}$

est correctement définie et est un isomorphisme de groupes additifs. De plus :

- $\forall (x,y) \in \mathbb{Z}^2,\ \theta\big(\mathrm{cl}_{ab}(x)\mathrm{cl}_{ab}(y)\big) = \theta\big(\mathrm{cl}_{ab}(xy)\big) = \big(\mathrm{cl}_a(xy), \mathrm{cl}_b(xy)\big)$
$= \big(\mathrm{cl}_a(x)\mathrm{cl}_a(y), \mathrm{cl}_b(x)\mathrm{cl}_b(y)\big) = \big(\mathrm{cl}_a(x), \mathrm{cl}_b(x)\big)\big(\mathrm{cl}_a(y), \mathrm{cl}_b(y)\big) = \theta\big(\mathrm{cl}_{ab}(x)\big)\theta\big(\mathrm{cl}_{ab}(y)\big)$
- $\theta\big(\mathrm{cl}_{ab}(1)\big) = \big(\mathrm{cl}_a(1), \mathrm{cl}_b(1)\big)$.

Finalement, θ est un isomorphisme d'anneaux.

b) Notons, pour tout n de $\mathbb{N}^*$, U_n l'ensemble des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. D'après 4.3.4 *1)* p. 118 : $\varphi(n) = \text{Card}(U_n)$. Comme θ est un isomorphisme d'anneaux, θ transporte les éléments inversibles, c'est-à-dire : pour tout x de $\mathbb{Z}$, $\text{cl}_{ab}(x)$ est inversible dans $\mathbb{Z}/ab\mathbb{Z}$ si et seulement si $\big(\text{cl}_a(x), \text{cl}_b(x)\big)$ est inversible dans $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. On voit aisément que cette dernière condition revient à ce que $\text{cl}_a(x)$ soit inversible dans $\mathbb{Z}/a\mathbb{Z}$ et $\text{cl}_b(x)$ soit inversible dans $\mathbb{Z}/b\mathbb{Z}$. On déduit : $\varphi(ab) = \text{Card}(U_{ab}) = \text{Card}(U_a \times U_b) = \text{Card}(U_a) \cdot \text{Card}(U_b) = \varphi(a)\varphi(b)$.

c) Comme p est premier, on a, pour tout n de $\{1, \ldots, p^r\}$:

$$n \wedge p^r \neq 1 \iff n \wedge p \neq 1 \iff p | n \iff n \in \{kp;\ 1 \leqslant k \leqslant p^{r-1}\}.$$

D'où : $\varphi(p^r) = p^r - \text{Card}\{kp;\ 1 \leqslant k \leqslant p^{r-1}\} = p^r - p^{r-1}$.

d) En utilisant *b)*, on déduit (par récurrence) que, si $a_1, \ldots, a_N$ sont des entiers premiers entre eux deux à deux, alors : $\varphi\left(\prod_{i=1}^{N} a_i\right) = \prod_{i=1}^{N} \varphi(a_i)$.

D'où : $\varphi(n) = \prod_{i=1}^{N} \varphi(p_i^{r_i}) = \prod_{i=1}^{N} (p_i^{r_i} - p_i^{r_i - 1})$.

4.4.76 L'ensemble U_n des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un groupe multiplicatif de cardinal $\varphi(n)$. D'après le théorème de Lagrange (C 2.1 p. 63) : $\forall \xi \in \mathbb{Z}/n\mathbb{Z}$, $\xi^{\varphi(n)} = \widehat{1}$, c'est-à-dire :

$$\forall a \in \mathbb{Z}^*, (a \wedge n = 1 \Longrightarrow a^{\varphi(n)} \equiv 1\ [n]).$$

Le théorème d'Euler est une généralisation du petit théorème de Fermat puisque, si n est premier, $\varphi(n) = n - 1$.

4.4.77 Notons $n = \prod_{i=1}^{N} p_i^{r_i}$ la décomposition primaire de n. D'après l'exercice 4.4.75 *d)* :

$$\varphi(n^k) = \varphi\left(\prod_{i=1}^{N} p_i^{r_i k}\right) = \prod_{i=1}^{N} \left(p_i^{r_i k} - p_i^{r_i k - 1}\right) = \left(\prod_{i=1}^{N} p_i^{r_i (k-1)}\right)\left(\prod_{i=1}^{N} \left(p_i^{r_i} - p_i^{r_i - 1}\right)\right) = n^{k-1}\varphi(n).$$

4.4.78 $13200 = 2^4 \cdot 3 \cdot 5^2 \cdot 11$

Mod. 16 : D'après l'exercice 4.1.1 p. 103, il existe $\lambda \in \mathbb{Z}$ tel que $n^2 = 1 + 8\lambda$, d'où $n^4 = 1 + 16\lambda + 64\lambda^2 \equiv 1\ [16]$, $n^{20} = (n^4)^5 \equiv 1^5 = 1\ [16]$, et enfin $n^{21} \equiv n\ [16]$.

Mod. 3 : D'après le petit théorème de Fermat (ex. 4.4.50 p. 129) : $n^3 \equiv n\ [3]$, d'où $n^{21} = (n^3)^7 \equiv n^7 = (n^3)^2 n \equiv n^2 n = n^3 \equiv n\ [3]$.

Mod. 25 : D'après le théorème d'Euler (ex. 4.4.76), comme $\varphi(25) = 5^2 - 5 = 20$ et que $5 \wedge n = 1$, on a : $n^{20} \equiv 1\ [25]$, d'où $n^{21} \equiv n\ [25]$.

Mod. 11 : D'après le petit théorème de Fermat : $n^{11} \equiv n\ [11]$, d'où $n^{21} = n^{11} n^{10} \equiv n^{11} \equiv n\ [11]$.

Comme 16, 3, 25, 11 sont premiers entre eux deux à deux, on conclut : $13200 \mid n^{21} - n$.

4.4.79 *a)* Notons $\text{Div}(n)$ l'ensemble des diviseurs $\geqslant 1$ de n. La relation $\mathcal{R}$ définie dans $\{1, \ldots, n\}$ par :

$$i \mathcal{R} j \iff i \wedge n = j \wedge n$$

est clairement une relation d'équivalence.

Chaque classe modulo $\mathcal{R}$ contient un diviseur de n et un seul (la classe de i contient $i \wedge n$). D'où :

$$n = \text{Card}(\{1,\dots,n\}) = \sum_{d\in \text{Div}(n)} \text{Card}(\text{cl}_{\mathcal{R}}(d)).$$

D'autre part, pour tout d de $\text{Div}(n)$, l'application $k \longmapsto kd$ est une bijection de $\left\{k \in \left\{1,\dots,\frac{n}{d}\right\},\ k \wedge \left(\frac{n}{d}\right) = 1\right\}$ sur $\text{cl}_{\mathcal{R}}(d)$, d'où $\text{Card}(\text{cl}_{\mathcal{R}}(d)) = \varphi\left(\frac{n}{d}\right)$.

Ainsi : $n = \sum_{d\in \text{Div}(n)} \varphi\left(\frac{n}{d}\right) = \sum_{d\in \text{Div}(n)} \varphi(d)$, car l'application $\text{Div}(n) \longrightarrow \text{Div}(n)$, $d \longmapsto \frac{n}{d}$ est une permutation.

b) D'après *a)* : $\forall m \in \{1,\dots,n\}$, $\sum_{d|m} \varphi(d) = m$. Pour chaque k de $\{1,\dots,n\}$, $\varphi(k)$ apparaît exactement $\text{E}\left(\frac{n}{k}\right)$ fois dans les sommes précédentes $\sum_{d|m} \varphi(d)$ $(1 \leqslant m \leqslant n)$. D'où :

$$\sum_{k=1}^{n} \text{E}\left(\frac{n}{k}\right) \varphi(k) = \sum_{m=1}^{n} \left(\sum_{d|m} \varphi(d)\right) = \sum_{m=1}^{n} m = \frac{n(n+1)}{2}.$$

4.4.80 Notons $E_n = \{k \in \{1,\dots,n-1\};\ k \wedge n = 1\}$.

L'application $k \longmapsto n - k$, est une involution de E_n, puisque : $\forall k \in E_n$, $\begin{cases} (n-k) \wedge n = 1 \\ 1 \leqslant n-k \leqslant n-1 \\ n-(n-k) = k \end{cases}$.

D'où : $2\sum_{k\in E_n} k = \sum_{k\in E_n} k + \sum_{k\in E_n} (n-k) = n\text{Card}(E_n) = n\varphi(n)$.

4.4.81 Puisque n est pair et $\geqslant 2$, il existe $(q,N) \in (\mathbb{N}^*)^2$ tel que : $n = 2^q N$ et N impair.

1) $\sum_{\substack{d_1|n \\ d_1 \text{ impair}}} \varphi\left(\frac{n}{d_1}\right) = \sum_{d_1|N} \varphi\left(2^q \frac{N}{d_1}\right) = \sum_{d_1|N} \varphi(2^q)\varphi\left(\frac{N}{d_1}\right) = \varphi(2^q) \sum_{d_1|N} \varphi\left(\frac{N}{d_1}\right)$

$= (2^q - 2^{q-1})N = 2^{q-1}N = \frac{n}{2}$, en remarquant $2^q \wedge \frac{N}{d_1} = 1$ et en utilisant l'ex. 4.4.79 *a)*.

2) $\sum_{\substack{d_2|n \\ d_2 \text{ pair}}} \varphi\left(\frac{n}{d_2}\right) = \sum_{\substack{\delta|2^{q-1}N \\ (d_2=2\delta)}} \varphi\left(\frac{2^{q-1}N}{\delta}\right) = 2^{q-1}N = \frac{n}{2}$.

4.4.82 **1er cas :** $n = p^r$, p premier, $r \geqslant 2$. Alors $\varphi(n) = p^r - p^{r-1}$, et on a :

$$\varphi(n) \leqslant n - \sqrt{n} \iff p^{r-1} \geqslant \sqrt{p^r} \iff 2(r-1) \geqslant r \iff r \geqslant 2.$$

2ème cas : n admet au moins deux diviseurs premiers distincts.

Il existe alors $(a,b) \in (\mathbb{N}^*)^2$ tel que : $n = ab$, $a \geqslant 2$, $b \geqslant 2$, $a \wedge b = 1$. On a :

$$\varphi(n) = \varphi(ab) = \varphi(a)\varphi(b) \leqslant (a-1)(b-1) = n - (a+b) + 1.$$

Comme $ab = n$, on a, par exemple, $a \geqslant \sqrt{n}$, d'où : $n - (a+b) + 1 \leqslant n - (\sqrt{n}+2) + 1 < n - \sqrt{n}$.

4.4.83 Soit $(a,b) \in (\mathbb{N}^*)^2$ tel que $a \wedge b = 1$.

D'après le théorème d'Euler (ex. 4.4.76 p. 131) : $a^{\varphi(b)} \equiv 1\ [b]$.

Comme d'autre part $\varphi(a) \geqslant 1$, on a : $b^{\varphi(a)} \equiv 0\ [b]$. D'où : $b \mid a^{\varphi(b)} + b^{\varphi(a)} - 1$.

En échangeant a et b : $a \mid a^{\varphi(b)} + b^{\varphi(a)} - 1$.

Enfin $a \wedge b = 1$, donc $ab \mid a^{\varphi(b)} + b^{\varphi(a)} - 1$.

4.4.84 $\left(\sum_{k=0}^{\varphi(n)-1} a^k\right)(a-1) = a^{\varphi(n)} - 1 \equiv 0\ [n]$, d'après le théorème d'Euler, ex. 4.4.76 p. 131.

Comme $(a-1) \wedge n = 1$, on déduit : $\sum_{k=0}^{\varphi(n)-1} a^k \equiv 0\ [n]$.

4.4.85 Soit $(a,b) \in (\mathbb{N}^*)^2$ tel que $a|b$.

Considérons les décompositions primaires : $a = \prod_{i=1}^{N} p_i^{\alpha_i}$, $b = \prod_{i=1}^{N} p_i^{\beta_i}$ (où : $1 \leqslant \alpha_i \leqslant \beta_i$).

On a : $a\varphi(b) = \left(\prod_{i=1}^{N} p_i^{\alpha_i}\right)\left(\prod_{i=1}^{N}\left(p_i^{\beta_i} - p_i^{\beta_i-1}\right)\right) = \prod_{i=1}^{N}\left(p_i^{\alpha_i-1} p_i^{\beta_i}(p_i-1)\right) = b\varphi(a)$.

4.4.86 Comme $a \wedge b|ab$, $a|ab$, $b|ab$, on a, d'après l'ex. 4.4.85 :

$$ab\varphi(a \wedge b) = (a \wedge b)\varphi(ab), \quad a\varphi(ab) = ab\varphi(a), \quad b\varphi(ab) = ab\varphi(b),$$

d'où, par multiplication : $\varphi(a \wedge b)\varphi(ab) = (a \wedge b)\varphi(a)\varphi(b)$.

4.4.87 Même raisonnement que dans la solution de l'ex. 4.4.86, en remplaçant $a \wedge b$ par c, puisque $c|ab$.

4.4.88 Par division euclidienne de $\varphi(a^k - 1)$ par k, il existe $(q,r) \in \mathbb{N}^2$ tel que :

$$\varphi(a^k - 1) = kq + r \quad \text{et} \quad 0 \leqslant r < k.$$

Comme $a \wedge (a^k - 1) = 1$, le théorème d'Euler (ex. 4.4.76 p. 131) montre : $a^{\varphi(a^k-1)} \equiv 1\ [a^k - 1]$.

Mais : $a^{\varphi(a^k-1)} = (a^k)^q a^r \underset{a^k-1}{\equiv} a^r$.

On déduit : $a^k - 1 \mid a^r - 1$.

D'autre part, $0 \leqslant r < k$, donc $0 \leqslant a^r - 1 < a^k - 1$, d'où $a^r - 1 = 0$, $r = 0$, $k \mid \varphi(a^k - 1)$.

4.4.89 Il est clair que : $\forall m \in \mathbb{N}^*$, $\begin{cases} \varphi(m) \leqslant m-1 & \text{si } m \geqslant 2 \\ \varphi(m) = 1 & \text{si } m = 1 \end{cases}$.

En particulier : $\forall m \in \mathbb{N}^*$, $\varphi(m) \leqslant m$, donc $(u_k)_{k\in\mathbb{N}}$ est décroissante.

Comme $(\forall k \in \mathbb{N},\ u_k \in \mathbb{N})$, on en déduit que $u_k)_{k\in\mathbb{N}}$ est stationnaire. Il existe donc $r \in \mathbb{N}$ tel que $u_{r+1} = u_r$. Puisque $(\forall m \geqslant 2,\ \varphi(m) < m)$, on a nécessairement $u_r = 1$.

C 4.1 *I* *1) a)* Développer les deux membres.

b) Résulte simplement de *a)*.

2) a) Notons $F = f(\mathbb{Z}/p\mathbb{Z})$, $G = g(\mathbb{Z}/p\mathbb{Z})$.

Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, on a : $\forall X_1, X_2 \in \mathbb{Z}/p\mathbb{Z}$, $\left(f(X_1) = f(X_2) \Longleftrightarrow \left| \begin{array}{l} X_2 = -X_1 \\ \text{ou} \\ X_2 = X_1 \end{array} \right.\right)$.

Ainsi, F a exactement $\dfrac{p+1}{2}$ éléments, qui sont $f(\widehat{0}), f(\widehat{1}), \ldots, f\left(\left(\dfrac{\widehat{p-1}}{2}\right)\right)$. De même, G a exactement $\dfrac{p+1}{2}$ éléments, qui sont $g(\widehat{0}), g(\widehat{1}), \ldots, g\left(\left(\dfrac{\widehat{p-1}}{2}\right)\right)$.

Comme $\text{Card}(F) + \text{Card}(G) = p + 1 > p = \text{Card}(\mathbb{Z}/p\mathbb{Z})$, on déduit : $F \cap G \neq \varnothing$.

Il existe donc $(x, y) \in \left\{0, \ldots, \dfrac{p-1}{2}\right\}^2$ tel que $x^2 + y^2 + 1 \equiv 0\ [p]$.

b) Pour $p = 2$, il suffit de choisir : $x = y = 1$, $z = t = 0$, $k = 1$.

Si p est impair, d'après *a)*, il existe $(x, y) \in \left\{0, \ldots, \dfrac{p-1}{2}\right\}^2$ et $k \in \mathbb{Z}$ tels que $x^2 + y^2 + 1 = kp$, et, comme $0 < x^2 + y^2 + 1 \leqslant 2\left(\dfrac{p-1}{2}\right)^2 + 1 < p^2$, on a : $1 \leqslant k \leqslant p - 1$.

Il suffit donc de choisir $z = 1$, $t = 0$.

3) D'après *2) b)*, l'ensemble $\left\{k \in \{1, \ldots, p-1\};\ \exists (x,y,z,t) \in \mathbb{N}^4;\ x^2 + y^2 + z^2 + t^2 = kp\right\}$ est une partie non vide de $\mathbb{N}^*$, donc admet un plus petit élément noté m.

a) Si m et pair, alors, quitte à permuter x, y, z, t, on a : $\left| \begin{array}{l} x, y, z, t \text{ pairs} \\ \text{ou} \\ x, y \text{ pairs et } z, t \text{ impairs} \end{array} \right.$

Alors $\dfrac{x-y}{2}$, $\dfrac{x+y}{2}$, $\dfrac{z-t}{2}$, $\dfrac{z+t}{2}$ sont dans $\mathbb{Z}$, et :

$$\left(\frac{x-y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2 + \left(\frac{z-t}{2}\right)^2 + \left(\frac{z+t}{2}\right)^2 = \frac{1}{2}(x^2 + y^2 + z^2 + t^2) = \frac{m}{2}\,p,$$

ce qui contredit la définition de m.

b) Puisque $a^2 + b^2 + c^2 + d^2 \underset{[m]}{\equiv} x^2 + y^2 + z^2 + t^2 \equiv 0\ [m]$, il existe $q \in \mathbb{N}$ tel que : $a^2 + b^2 + c^2 + d^2 = qm$.

Comme $|a| \leqslant \dfrac{m-1}{2}, \ldots, |d| \leqslant \dfrac{m-1}{2}$, on a $qm \leqslant 4\left(\dfrac{m-1}{2}\right)^2$, donc $q < m$.

- Supposons $q = 0$.

Alors $a = b = c = d = 0$, $x \equiv y \equiv z \equiv t \equiv 0\ [m]$, $m^2 | x^2 + y^2 + z^2 + t^2 = mp$, $m | p$, contradiction avec : $1 < m \leqslant p - 1$ et p premier.

- Supposons $q \geqslant 1$.

On a : $(x^2 + y^2 + z^2 + t^2)(a^2 + b^2 + c^2 + d^2) = m^2 qp$.

En notant $A = ax + by + cz + dt$, $B = ay - bx + ct - dz$, $C = az - bt - cx + dy$, $D = at + bz - cy - dx$, on obtient, d'après *1) a)* : $A^2 + B^2 + C^2 + D^2 = m^2 qp$.

D'autre part, modulo m :

$$A \equiv x^2 + y^2 + z^2 + t^2 \equiv 0, \qquad B \equiv xy - yx + zt - tz = 0,$$

$$C \equiv xz - yt - zx + ty = 0, \qquad D \equiv xt + yz - zy - tx = 0.$$

Il existe donc $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ tels que : $A = m\alpha, \ldots, D = m\delta$. On déduit $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = qp$, ce qui contredit la définition de m.

4) Tout entier naturel ($\geqslant 2$) est décomposable (d'au moins une façon) en un produit de nombres premiers. D'après *3) b)*, chaque facteur premier est décomposable en somme de quatre carrés. Alors, d'après *1) b)*, n est décomposable en somme de quatre carrés.

II *1) a)* On a : $\forall (i,j),\ (x_i+x_j)^4+(x_i-x_j)^4 = 2x_i^4+12x_i^2x_j^2+2x_j^4$, d'où :

$$\sum_{1\leqslant i<j\leqslant 4}\left((x_i+x_j)^4+(x_i-x_j)^4\right) = 2\sum_{1\leqslant i<j\leqslant 4}(x_i^4+x_j^4)+12\sum_{1\leqslant i<j\leqslant 4}x_i^2x_j^2$$

$$= 6\sum_{k=1}^{4}x_k^4+12\sum_{1\leqslant i<j\leqslant 4}x_i^2x_j^2 = 6\left(\sum_{k=1}^{4}x_k^2\right)^2.$$

b) Soit $n\in\mathbb{N}$. D'après ***I** 4)*, il existe $(x_1,\dots,x_4)\in\mathbb{N}^4$ tel que $n = x_1^2+x_2^2+x_3^2+x_4^3$; puis, d'après *a)*, $6n^2$ est somme de 12 bicarrés.

2) D'après ***I** 4)*, il existe $(n_1,\dots,n_4)\in\mathbb{N}^4$ tel que $m = n_1^2+n_2^2+n_3^2+n_4^2$, puis, d'après *1) b)*, chaque $6n_k^2$ $(k=1,\dots,4)$ est décomposable en somme de 12 bicarrés. Donc, $6m$ est décomposable en somme de 48 $(=4\times 12)$ bicarrés.

3) a) $0 = 0^4+0^4$, $1 = 1^4+0^4$, $2 = 1^4+1^4$, $81 = 3^4+0^4$, $16 = 2^4+0^4$, $17 = 2^4+1^4$.

b) Soit $N\in\mathbb{N}$ tel que $N\geqslant 81$. Comme 0, 1, 2, 81, 16, 17 sont respectivement congrus modulo 6 à 0, 1, 2, 3, 4, 5, il existe $r\in\{0,1,2,81,16,17\}$ et $n\in\mathbb{N}$ tels que $N = 6m+r$.

D'après *2)*, $6m$ est décomposable en somme de 48 bicarrés.

D'après *3) a)*, r est décomposable en somme de 2 bicarrés.

Donc N est décomposable en somme de 50 bicarrés.

4) Soit $N\in\{0,\dots,80\}$.

- Si $N\leqslant 50$, alors N est décomposable en somme de 50 bicarrés (N termes égaux à 1^4, $50-N$ termes égaux à 0^4).
- Si $N\in\{51,\dots,80\}$, alors $3\leqslant N-(2^4+2^4+2^4)\leqslant 32$, donc N est décomposable en somme de 35 bicarrés (3 termes égaux à 2^4, $N-3\cdot 2^4$ termes égaux à 1^4).

On obtient ainsi le résultat voulu.

C 4.2 *1) a)* Immédiat.

b) Soit $(x,y,z)\in E$.

D'abord, puisque $xyz = x^2+y^2+2>0$, on a : $x\neq 0$, $y\neq 0$, $z\neq 0$.

Si ($x\geqslant 0$ et $y\geqslant 0$), alors $z\geqslant 0$.

Si ($x\leqslant 0$ et $y\geqslant 0$), alors $z\leqslant 0$ et $(-x,y,-z)\in E$.

Si ($x\geqslant 0$ et $y\leqslant 0$), alors $z\leqslant 0$ et $(x,-y,-z)\in E$.

On peut donc se ramener à : $(x,y,z)\in(\mathbb{N}^*)^3$.

De plus, si $y\geqslant x$, alors $(y,x,z)\in E$ et $y\leqslant x$; on peut donc se ramener à : $(x,y,z)\in(\mathbb{N}^*)^3$ et $x\leqslant y$.

2) a) Soit $(x,y,z)\in G$.

- $(zx-y)^2+x^2+2-(zx-y)xz = -xyz+y^2+x^2+2 = 0$, donc $(zx-y,x,z)\in E$.
- $y(zx-y) = xyz-y^2 = x^2+2>0$ et $y>0$, donc $zx-y>0$.
- Supposons $zx-y>x$.

Alors $y<zx-x$, donc $y^2<y(zx-x) = x^2+y^2+2-xy$, d'où $xy<x^2+2$.

Mais $x<y$, donc $xy<x^2+2<xy+2$, d'où $x^2+2 = xy+1$, $x(y-x) = 1$, $x = 1$ et $y = 2$; puis, comme $x^2+y^2+2 = xyz$, $7 = 2z$, contradiction.

Ceci montre : $(zx - y, x, z) \in F$.

b) Soit $(x,y,z) \in (\mathbb{N}^*)^3$ tel que $x = y$. On a :

$$x^2 + y^2 + 2 = xyz \iff 2x^2 + 2 = x^2 z \iff x^2(z-2) = 2 \iff \begin{cases} (x^2 = 2 \quad \text{et} \quad z - 2 = 1) \\ \text{ou} \\ (x^2 = 1 \quad \text{et} \quad z - 2 = 2) \end{cases}$$

$$\iff (x = 1 \quad \text{et} \quad z = 4).$$

3) Soit $(x,y,z) \in F$.

Supposons : $\forall n \in \mathbb{N},\ f^n(x,y,z) \neq (1,1,4)$.

Montrons, par récurrence : $\forall n \in \mathbb{N},\ f^n(x,y,z) \in G$.

Puisque $(x,y,z) \in F$ et $(x,y,z) \neq (1,1,4)$, d'après *2) b)*, on a : $(x,y,z) \in G$.

Supposons que, pour un n de $\mathbb{N}$, $f^n(x,y,z) \in G$. Alors $f^{n+1}(x,y,z) \in F$ (cf. *2) a)*), et $f^{n+1}(x,y,z) \neq (1,1,4)$ par hypothèse, donc $f^{n+1}(x,y,z) \in G$.

En notant $(x_n, y_n, z_n) = f^n(x,y,z)$ pour $n \in \mathbb{N}$, on a :

$$\begin{cases} \forall n \in \mathbb{N},\ x_n < y_n, & \text{car } (x_n, y_n, z_n) \in G \\ \forall n \in \mathbb{N},\ y_{n+1} = x_n, & \text{car } (x_{n+1}, y_{n+1}, z_{n+1}) = f(x_n, y_n, z_n) \end{cases}.$$

Ainsi, $(y_n)_{n \in \mathbb{N}}$ est strictement décroissante et à valeurs dans $\mathbb{N}^*$, contradiction : c'est le «principe de descente infinie».

Ceci établit : $\exists n \in \mathbb{N},\ f^n(x,y,z) = (1,1,4)$.

Et il est clair que $f : \mathbb{Z}^3 \longrightarrow \mathbb{Z}^3$ est bijective et que $f^{-1} : \begin{matrix} \mathbb{Z}^3 & \longrightarrow & \mathbb{Z}^3 \\ (X,Y,Z) & \longmapsto & (Y, YZ - X, Z) \end{matrix}$.

n	0	1	2	3	4	...
$g^n(1,1,4)$	(1,1,4)	(1,3,4)	(3,11,4)	(11,41,4)	(41,153,4)	...

Référence : The College Mathematics Journal, Vol. 22, N° 4, p. 347.

C 4.3. *I 1) a)* Supposons qu'il existe $\xi_0 \in \mathbb{Z}/p\mathbb{Z}$ tel que $\xi_0^2 = \widehat{a}$. On a, pour tout ξ de $\mathbb{Z}/p\mathbb{Z}$:

$$\xi^2 = \widehat{a} \iff (\xi - \xi_0)(\xi + \xi_0) = 0 \iff \begin{cases} \xi = \xi_0 \\ \text{ou} \\ \xi = -\xi_0 \end{cases},$$

puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps (donc un anneau intègre).

De plus, $\xi_0 \neq -\xi_0$, car sinon, $\widehat{2}\xi_0 = 0$, donc $\xi_0 = 0$ (puisque $2 \wedge p = 1$), puis $\widehat{a} = \xi_0^2 = 0$, $p|a$, contradiction.

Ceci montre que l'équation $\xi^2 = \widehat{a}$, d'inconnue $\xi \in \mathbb{Z}/p\mathbb{Z}$ admet zéro ou deux solutions exactement; de plus, si elle admet deux solutions, celles-ci sont dans $\mathbb{Z}/p\mathbb{Z} - \{0\}$.

b) Notons $G_p = \mathbb{Z}/p\mathbb{Z} - \{0\}$ et $\theta_p : \begin{matrix} G_p & \longrightarrow & G_p \\ \xi & \longmapsto & \xi^2 \end{matrix}$. D'après *a)*, tout élément de $\theta_p(G_p)$ admet exactement deux antécédents, donc $\text{Card}(\theta_p(G_p)) = \dfrac{1}{2}\text{Card}(G_p) = \dfrac{p-1}{2}$. Il y a ainsi exactement $\dfrac{p-1}{2}$ RQ mod p, et donc aussi $\dfrac{p-1}{2}$ $\left(= (p-1) - \dfrac{p-1}{2}\right)$ NRQ mod p.

α) Soit $a \in \mathbb{Z}$ tel que $p \nmid a$. Pour chaque k de $\{1, \ldots, p-1\}$, notons r_k le reste de la division euclidienne de ka par p.

Supposons qu'il existe $(i,j) \in \{1,\dots,p-1\}^2$ tel que $r_i = r_j$. On a alors $(i-j)a = ia - ja \underset{[p]}{\equiv} r_i - r_j = 0$.

Comme p est premier et que $p \nmid a$, on déduit $p \mid i-j$, et donc $i = j$.

Ceci montre que $r_1,\dots,r_{p-1}$ sont deux à deux distincts. De même, $r_1,\dots,r_{p-1}$ sont tous non nuls.

On en déduit que $k \longmapsto r_k$ est une permutation de $\{1,\dots,p-1\}$.

D'après *b)*, $\dfrac{p-1}{2}$ des nombres $r_1,\dots,r_{p-1}$ sont des RQ mod p, et $\dfrac{p-1}{2}$ aussi sont des NRQ mod p.

On conclut : $\displaystyle\sum_{k=1}^{p-1}\left(\frac{ka}{p}\right) = \frac{p-1}{2}\cdot 1 + \frac{p-1}{2}(-1) = 0.$

β) 1) Pour $k \in \{1,\dots,p-2\}$, il existe bien k' unique dans $\{1,\dots,p-1\}$ tel que $kk' \equiv 1\ [p]$, puisque $\widehat{k}$ (classe de k modulo p) admet un inverse dans $\mathbb{Z}/p\mathbb{Z}$. De plus, $k' \neq p-1$ car :

$$k' = p-1 \Longrightarrow \widehat{k'} = \widehat{-1} \Longrightarrow \widehat{k} = \widehat{-1} \Longrightarrow k = p-1.$$

- Supposons qu'il existe $x \in \mathbb{Z}$ tel que $x^2 \equiv k(k+1)\ [p]$. Alors : $(k'x)^2 = k'^2x^2 \equiv 1 + k'\ [p]$.
- Réciproquement, s'il existe $y \in \mathbb{Z}$ tel que $y^2 \equiv 1 + k'\ [p]$, alors : $(ky)^2 = k^2y^2 \equiv k^2 + k\ [p]$.

Ceci montre que $k(k+1)$ est un RQ mod p si et seulement si $k'+1$ l'est, donc $\left(\dfrac{k(k+1)}{p}\right) = \left(\dfrac{k'+1}{p}\right)$.

2) Lorsque k décrit $\{1,\dots,p-2\}$, k' (inverse de k modulo p) décrit aussi $\{1,\dots,p-2\}$, d'où, en utilisant 1) et α) :

$$\sum_{k=1}^{p-2}\left(\frac{k(k+1)}{p}\right) = \sum_{k'=1}^{p-2}\left(\frac{k'+1}{p}\right) = \sum_{k=2}^{p-1}\left(\frac{k}{p}\right) = -1.$$

2) a) Distinguons deux cas :

1^er^ cas : $\left(\dfrac{a}{p}\right) = 1$.

Il existe donc $x_0 \in \mathbb{Z}$ tel que $x_0^2 \equiv a\ [p]$. D'après le petit théorème de Fermat (ex. 4.4.50 p. 129), $a^{\frac{p-1}{2}} = x_0^{p-1} \equiv 1\ [p]$ (car $x_0 \wedge p = 1$), et donc $\left(\dfrac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ [p]$.

2^ème^ cas : $\left(\dfrac{a}{p}\right) = -1$.

Notons $G_p = \mathbb{Z}/p\mathbb{Z} - \{0\}$ et $f : G_p \longrightarrow G_p$, $\xi \longmapsto \xi^{-1}\widehat{a}$, de sorte que : $\forall \xi \in G_p,\ \xi f(\xi) = \widehat{a}$.

Il est clair que f est une bijection (c'est même une involution).

S'il existe $\xi \in G_p$ tel que $f(\xi) = \xi$, alors $\xi^2 = \widehat{a}$, donc a est un RQ mod p, contradiction.

Ainsi : $\forall \xi \in G_p,\ f(\xi) \neq \xi$.

Les éléments de G_p peuvent donc être groupés par deux de produit $\widehat{a}$, d'où, en faisant le produit :

$$\widehat{(p-1)!} = \prod_{\widehat{k} \in G_p} \widehat{k} = \widehat{(a)}^{\frac{1}{2}\,\mathrm{Card}(G_p)} = \widehat{(a)}^{\frac{p-1}{2}}.$$

Mais, d'après le théorème de Wilson (ex. 4.4.65 *a)* p. 130) : $(p-1)! \equiv -1\ [p]$.

On déduit $a^{\frac{p-1}{2}} \equiv -1\ [p]$, et donc $\left(\dfrac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ [p]$.

Exemple : $\left(\dfrac{10}{31}\right) \underset{[31]}{\equiv} 10^{\frac{31-1}{2}} = (10^3)^5 \equiv 8^5 \equiv 1.$

◇ **Réponse :** $\left(\dfrac{10}{31}\right) = 1$; 10 est un RQ mod 31. (D'ailleurs : $14^2 = 196 \equiv 10\ [31]$).

b) Si $p = 4k+1$ ($k \in \mathbb{N}^*$), alors $(-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1$.

Si $p = 4k+3$ ($k \in \mathbb{N}$), alors $(-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1$.

c) α) Raisonnons par l'absurde : supposons qu'aucun facteur premier de n ne soit congru à 3 modulo 4, et notons $n = \prod_{i=1}^{N} p_i^{\alpha_i}$ la DP de n.

D'abord, $2 \nmid n$ (puisque $n \equiv 3$ [4]). Et, par hypothèse : $\forall i \in \{1,\dots,N\}$, $p_i \equiv 1$ [4].

On a alors : $\forall i \in \{1,\dots,N\}$, $p_i^{\alpha_i} \equiv 1$ [4], d'où : $n \equiv 1$ [4], contradiction.

β) Raisonnons par l'absurde : supposons qu'il existe (x,y,z) dans $\mathbb{Z}^3$ tel que

$$x^2 + y^3 - 8(2z+1)^3 + 1 = 0.$$

- Montrons d'abord que y est impair.

En effet, si y est pair, alors $y^3 \equiv 0$ [8], d'où $x^2 + 1 = 8(2z+1)^3 - y^3 \equiv 0$ [8], et donc $x^2 \equiv -1$ [8], contradiction puisqu'un carré d'entier ne peut être congru, modulo 8, qu'à 0, 1, 4 (cf. ex. 4.1.1 p. 103).

- On a : $x^2 + 1 = 8(2z+1)^3 - y^3 = \big(2(2z+1) - y\big)A$, où $A = 4(2z+1)^2 + 2(2z+1)y + y^2$.

Modulo 4, en notant $y = 2Y+1$ ($Y \in \mathbb{Z}$) : $A \equiv 2y + y^2 = 4Y^2 + 8Y + 3 \equiv 3$ [4].

D'après α), A admet au moins un diviseur premier q tel que $q \equiv 3$ [4]. Comme $A \mid x^2+1$, on déduit $q \mid x^2+1$, c'est-à-dire que -1 est RQ mod q.

Mais (cf. *b)*) : $\left(\frac{-1}{q}\right) = -1$ (car $q \equiv 3$ [4]), donc -1 est NRQ mod q, contradiction.

L'équation de Lebesgue s'obtient en choisissant $z = 0$.

3) a) 1), 2), 3) sont évidentes.

4) En utilisant le théorème d'Euler *(2) a)*) : $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \underset{[p]}{\equiv} a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} \underset{[p]}{\equiv} \left(\frac{ab}{p}\right)$.

Comme $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ et $\left(\frac{ab}{p}\right)$ sont dans $\{-1,1\}$ et que $p \geqslant 3$, on conclut : $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

b) Soit $i \in \{1,\dots,N\}$.

- Si $i \in I$, alors $\left(\frac{p_i^{r_i}}{p}\right) = \left(\frac{\left(p_i^{\frac{r_i-1}{2}}\right)^2 p_i}{p}\right) = \left(\frac{\left(p_i^{\frac{r_i-1}{2}}\right)^2}{p}\right)\left(\frac{p_i}{p}\right) = \left(\frac{p_i}{p}\right)$.

- Si $i \notin I$, alors r_i est pair et : $\left(\frac{p_i^{r_i}}{p}\right) = \left(\frac{\left(p_i^{\frac{r_i}{2}}\right)^2}{p}\right) = 1$.

D'où : $\left(\frac{a}{p}\right) = \prod_{i \in I}\left(\frac{p_i^{r_i}}{p}\right) = \prod_{i \in I}\left(\frac{p_i}{p}\right) = \left(\frac{a'}{p}\right)$.

4) a) Comme dans *1) c)* α).

b) 1) Par définition, $u_1,\dots,u_s$ sont deux à deux distincts, $v_1,\dots,v_t$ sont deux à deux distincts, et :

$$\forall (i,k) \in \{1,\dots,s\} \times \{1,\dots,t\}, \quad u_i \leqslant \frac{p-1}{2} < \frac{p+1}{2} \leqslant v_k.$$

Il en résulte que $u_1,\dots,u_s,v_1,\dots,v_t$ sont deux à deux distincts.

De plus, comme tout élément de $\left\{r_1,\dots,r_{\frac{p-1}{2}}\right\}$ est soit $\leqslant \dfrac{p-1}{2}$, soit $\geqslant \dfrac{p+1}{2}$, on obtient :

$$\{u_1,\dots,u_s,v_1,\dots,v_t\} = \left\{r_1,\dots,r_{\frac{p-1}{2}}\right\}.$$

2) Par définition, $v_1,\dots,v_t$ sont deux à deux distincts, donc $p-v_1,\dots,p-v_t$ sont deux à deux distincts. Soit $(i,k) \in \{1,\dots,s\} \times \{1,\dots,t\}$. Supposons $u_i = p - v_k$. Il existe $(m,n) \in \left\{1,\dots,\dfrac{p-1}{2}\right\}^2$ tel que $u_i \equiv ma\ [p]$ et $v_k \equiv na\ [p]$. On a alors : $(m+n)a = u_i + v_k \equiv 0\ [p]$, donc $p|(m+n)$ (puisque p est premier et $p\nmid a$). Mais $2 \leqslant m+n \leqslant p-1$, d'où une contradiction.

Ceci montre $\{u_1,\dots,u_s\} \cap \{p-v_1,\dots,p-v_t\} = \varnothing$.

Finalement, $u_1,\dots,u_s,p-v_1,\dots,p-v_t$ sont deux à deux distincts.

De plus : $\begin{cases} \forall i \in \{1,\dots,s\}, & 1 \leqslant u_i \leqslant \dfrac{p-1}{2} \\ \forall k \in \{1,\dots,t\}, & 1 \leqslant p - v_k \leqslant \dfrac{p-1}{2} \quad (\text{car } \dfrac{p+1}{2} \leqslant v_k \leqslant p-1) \end{cases}$.

Et d'après 1), $s+t = \dfrac{p-1}{2}$.

Ainsi, $u_1,\dots,u_s,p-v_1,\dots,p-v_t$ sont $\dfrac{p-1}{2}$ entiers deux à deux distincts et situés dans $\left\{1,\dots,\dfrac{p-1}{2}\right\}$;

donc : $\{u_1,\dots,u_s,p-v_1,\dots,p-v_t\} = \left\{1,\dots,\dfrac{p-1}{2}\right\}$.

c) De *b)* 1), on déduit :

$$u_1\dots u_s(p-v_1)\dots(p-v_t) = r_1\dots r_{\frac{p-1}{2}} \underset{[p]}{\equiv} (a)(2a)\dots\left(\frac{p-1}{2}a\right) = a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!.$$

De *b)* 2), on déduit :

$$u_1\dots u_s(p-v_1)\dots(p-v_t) \underset{[p]}{\equiv} (-1)^t u_1\dots u_s v_1\dots v_t = (-1)^t 1\cdot 2\cdot\dots\cdot\frac{p-1}{2} = (-1)^t\left(\frac{p-1}{2}\right)!.$$

D'où : $a^{\frac{p-1}{2}}\left(\dfrac{p-1}{2}\right)! \equiv (-1)^t\left(\dfrac{p-1}{2}\right)!\ [p]$.

Comme $1 \wedge p = 1$, $2 \wedge p = 1, \dots, \dfrac{p-1}{2} \wedge p = 1$, on a $\left(\dfrac{p-1}{2}\right)! \wedge p = 1$; on peut donc simplifier par $\left(\dfrac{p-1}{2}\right)!$, et on obtient : $a^{\frac{p-1}{2}} \equiv (-1)^t\ [p]$.

D'après le théorème d'Euler, $a^{\frac{p-1}{2}} \equiv \left(\dfrac{a}{p}\right)\ [p]$, donc $\left(\dfrac{a}{p}\right) \equiv (-1)^t\ [p]$. Comme $\left(\dfrac{a}{p}\right)$ et $(-1)^t$ sont dans $\{-1,1\}$ et que $p \geqslant 3$, on conclut : $\left(\dfrac{a}{p}\right) = (-1)^t$.

Exemple : $p = 29$, $a = 8$.

j	1	2	3	4	5	6	7	8	9	10	11	12	13	14
ja	8	16	24	32	40	48	56	64	72	80	88	96	104	112
$ja \bmod p$	8	⑯	㉔	3	11	⑲	㉗	6	14	㉒	1	9	⑰	㉕

Ici : $t = 7$, donc $\left(\dfrac{8}{29}\right) = (-1)^7 = -1$.

◇ **Réponse :** $\left(\dfrac{8}{29}\right) = -1$.

d) Avec des notations de *b)* : $a = 2$, $r_1 = 2, \ldots, r_{\frac{p-1}{2}} = p-1$. On a donc $\left(\frac{2}{p}\right) = (-1)^t$, où t est le nombre des entiers de $\{2, 4, \ldots, p-1\}$ qui soient $\geqslant \frac{p}{2}$.

Soit $n \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$. On a : $2n \leqslant \frac{p}{2} \iff n \leqslant \frac{p}{4}$.

Il y a donc exactement $\mathrm{E}\left(\frac{p}{4}\right)$ entiers dans $\{2, 4, \ldots, p-1\}$ qui soient $\leqslant \frac{p}{2}$. Il y en a donc exactement $\frac{p-1}{2} - \mathrm{E}\left(\frac{p}{4}\right)$ qui soient $\geqslant \frac{p}{2}$.

Ainsi : $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} - \mathrm{E}\left(\frac{p}{4}\right)}$.

Séparons en cas suivant le reste de la division de p par 8.

p	$8k+1$	$8k+3$	$8k+5$	$8k+7$
$\frac{p-1}{2} - \mathrm{E}\left(\frac{p}{4}\right)$	$2k$	$2k+1$	$2k+1$	$2k+2$
$\frac{p^2-1}{8}$	$k(8k+2)$	$(2k+1)(4k+1)$	$(2k+1)(4k+3)$	$(8k+6)(k+1)$

Il est clair que, dans chacun des quatre cas ($p = 8k+1$, $p = 8k+3$, $p = 8k+5$, $p = 8k+7$), $\frac{p-1}{2} - \mathrm{E}\left(\frac{p}{4}\right)$ et $\frac{p^2-1}{8}$ ont la même parité. Ainsi : $(-1)^{\frac{p-1}{2} - \mathrm{E}\left(\frac{p}{4}\right)} = (-1)^{\frac{p^2-1}{8}}$.

Exemple : $\left(\frac{8}{31}\right) = \left(\frac{2^3}{31}\right) = \left(\frac{2}{31}\right) = (-1)^{\frac{31^2-1}{8}} = (-1)^{120} = 1$.

◇ **Réponse :** $\left(\frac{8}{31}\right) = 1$.

e) Notons $p = 8n+7$, qui est supposé premier.

D'après *d)* : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{(8n+6)(n+1)} = 1$.

Et, d'après le théorème d'Euler : $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \ [p]$.

D'où : $2^{\frac{p-1}{2}} \equiv 1 \ [p]$, c'est-à-dire : $8n+7 \mid 2^{4n+3} - 1$.

Montrer (par exemple, par récurrence sur n) : $\forall n \in \mathbb{N}^*,\ 8n+7 < 2^{4n+3} - 1$.

II *1) a)* $\mathrm{Card}\left\{\alpha \in \mathbb{N}^*;\ 0 < \alpha < \frac{p}{2}\right\} = \mathrm{Card}\left(\left\{1, \ldots, \frac{p-1}{2}\right\}\right) = \frac{p-1}{2}$ et

$\mathrm{Card}\left\{\beta \in \mathbb{N}^*;\ 0 < \beta < \frac{q}{2}\right\} = \frac{q-1}{2}$, d'où $\mathrm{Card}\left\{(\alpha, \beta) \in (\mathbb{N}^*)^2;\ \begin{cases} 0 < \alpha < \frac{p}{2} \\ 0 < \beta < \frac{p}{2} \end{cases}\right\} = \frac{p-1}{2} \cdot \frac{q-1}{2}$.

b) Supposons qu'il existe $(m, n) \in \left\{1, \ldots, \frac{p-1}{2}\right\} \times \left\{1, \ldots, \frac{q-1}{2}\right\}$ tel que $(m, n) \in OC$. On a alors $\frac{n}{m} = \frac{q}{p}$, d'où $pn = qm$. Comme p et q sont premiers distincts, on déduit $q \mid n$ et $p \mid m$, contradiction.

Ainsi, la diagonale OC du rectangle $OACB$ ne contient aucun point de $(\mathbb{N}^*)^2$.

c) 1) Soit $(j, k) \in \left\{1, \ldots, \frac{p-1}{2}\right\} \times \left\{1, \ldots, \frac{q-1}{2}\right\}$. Pour que (j, k) soit dans le triangle OAC, il faut et il suffit que : $k < \frac{q}{p} j$. Pour j fixé, il y a exactement $\mathrm{E}\left(\frac{jq}{p}\right)$ entiers k dans $\left\{1, \ldots, \frac{q-1}{2}\right\}$ vérifiant $k < \frac{jq}{p}$ (car $\frac{jq}{p} \notin \mathbb{N}$).

Le nombre de points de $(\mathbb{N}^*)^2$ situés dans le triangle OAC (c'est-à-dire dans le rectangle $OACB$ et en dessous de OC) est donc $\sum_{j=1}^{\frac{p-1}{2}} \mathrm{E}\left(\frac{jq}{p}\right)$.

2) De même, pour $k \in \left\{1, \dots, \frac{q-1}{2}\right\}$ fixé, il y a exactement $\mathrm{E}\left(\frac{kp}{q}\right)$ entiers j dans $\left\{1, \dots, \frac{p-1}{2}\right\}$ vérifiant $j < \frac{kp}{q}$. Le nombre de points de $(\mathbb{N}^*)^2$ situés dans le triangle OBC est donc $\sum_{k=1}^{\frac{q-1}{2}} \mathrm{E}\left(\frac{kp}{q}\right)$.

d) Grâce à *a), b), c)*, on obtient : $\sum_{j=1}^{\frac{p-1}{2}} \mathrm{E}\left(\frac{jq}{p}\right) + \sum_{k=1}^{\frac{q-1}{2}} \mathrm{E}\left(\frac{kp}{q}\right) = \frac{p-1}{2}\,\frac{q-1}{2}$.

D'autre part, notons, pour $j \in \left\{1, \dots, \frac{p-1}{2}\right\}$, α_j et r_j les quotient et reste de la division euclidienne de jq par p : $jq = p\alpha_j + r_j$ et $0 \leqslant r_j \leqslant p-1$.

Remarquons : $\alpha_j = \mathrm{E}\left(\frac{jq}{p}\right)$. Notons (avec les notations de *I 4)*) : $u = \sum_{i=1}^{s} u_i$, $v = \sum_{k=1}^{t} v_k$.

On a donc : $u + v = \sum_{i=1}^{s} u_i + \sum_{k=1}^{t} v_k = \sum_{j=1}^{\frac{p-1}{2}} r_j$ et $u + pt - v = \sum_{i=1}^{s} u_i + \sum_{k=1}^{t} (p - v_k) = \sum_{j=1}^{\frac{p-1}{2}} j = \frac{p^2-1}{8}$,

d'où : $t \underset{[2]}{\equiv} pt \underset{[2]}{\equiv} (u+v) + (u+pt-v) = \frac{p^2-1}{8} + \sum_{j=1}^{\frac{p-1}{2}} r_j$.

D'autre part : $\sum_{j=1}^{\frac{p-1}{2}} \mathrm{E}\left(\frac{jq}{p}\right) \underset{[2]}{\equiv} p \sum_{j=1}^{\frac{p-1}{2}} \alpha_j = \sum_{j=1}^{\frac{p-1}{2}} (jq - r_j) = q\,\frac{p^2-1}{8} - \sum_{j=1}^{\frac{p-1}{2}} r_j \underset{[2]}{\equiv} \frac{p^2-1}{8} + \sum_{j=1}^{\frac{p-1}{2}} r_j$.

Il en résulte : $t \underset{[2]}{\equiv} \sum_{j=1}^{\frac{p-1}{2}} \mathrm{E}\left(\frac{jq}{p}\right)$, donc $\left(\frac{q}{p}\right) = (-1)^t = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \mathrm{E}\left(\frac{jq}{p}\right)}$.

De même, en échangeant p et q : $\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{\frac{q-1}{2}} \mathrm{E}\left(\frac{kp}{q}\right)}$.

Finalement : $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \mathrm{E}\left(\frac{jq}{p}\right) + \sum_{k=1}^{\frac{q-1}{2}} \mathrm{E}\left(\frac{kp}{q}\right)} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

2) *a)* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1 \iff \frac{p-1}{2}\cdot\frac{q-1}{2}$ impair $\iff \left(\frac{p-1}{2}$ et $\frac{q-1}{2}$ impairs$\right) \iff \begin{cases} p \equiv 3\ [4] \\ q \equiv 3\ [4] \end{cases}$.

b) On a : $6417 = 3^2 \cdot 23 \cdot 31$, d'où : $\left(\frac{6417}{6607}\right) = \left(\frac{23}{6607}\right)\left(\frac{31}{6607}\right)$.

- Puisque $\left.\begin{cases} 23 \equiv 3\ [4] \\ 6607 \equiv 3\ [4] \end{cases}\right|$, grâce à la loi de réciprocité quadratique :

$\left(\frac{23}{6607}\right) = -\left(\frac{6607}{23}\right) = -\left(\frac{6}{23}\right) = -\left(\frac{2}{23}\right)\left(\frac{3}{23}\right)$.

D'après *I 4) c)* : $\left(\frac{2}{23}\right) = (-1)^{\frac{23^2-1}{8}} = (-1)^{66} = 1$.

Comme $\left.\begin{cases} 3 \equiv 3\ [4] \\ 23 \equiv 3\ [4] \end{cases}\right|$, on a : $\left(\frac{3}{23}\right) = -\left(\frac{23}{3}\right) = -\left(\frac{2}{3}\right) = -(-1)^{\frac{3^2-1}{8}} = 1$.

Donc : $\left(\frac{23}{6607}\right) = -1$.

- $\left\{\begin{array}{l} 31 \equiv 3\ [4] \\ 6607 \equiv 3\ [4] \end{array}\right.$, donc $\left(\frac{31}{6607}\right) = -\left(\frac{6607}{31}\right) = -\left(\frac{4}{31}\right) = -\left(\frac{2^2}{31}\right) = -1$.

◇ **Réponse :** $\left(\frac{6417}{6607}\right) = 1$.

3) 1) Supposons F_n premier. Comme $3 \equiv 3\ [4]$ et $F_n = 2^{2^n} + 1 \equiv 1\ [4]$ (puisque $n \geqslant 1$), on a : $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$.

Modulo 3 : $F_n = 2^{2^n} + 1 \underset{[3]}{\equiv} (-1)^{2^n} + 1 = 2$.

D'où : $\left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1$. Mais, d'après le théorème d'Euler : $\left(\frac{3}{F_n}\right) \underset{[F_n]}{\equiv} 3^{\frac{F_n-1}{2}}$.

Finalement : $3^{\frac{F_n-1}{2}} \equiv -1\ [F_n]$.

1) Réciproquement, supposons $3^{\frac{F_n-1}{2}} \equiv -1\ [F_n]$. Alors : $3^{F_n-1} = \left(3^{\frac{F_n-1}{2}}\right)^2 \equiv 1\ [F_n]$.

Soit p un diviseur premier quelconque de F_n (nécessairement $p \geqslant 5$, puisque $2 \nmid F_n$ et $3 \nmid F_n$).

On a alors : $3^{F_n-1} \equiv 1\ [p]$.

L'ensemble $\{m \in \mathbb{N}^*;\ 3^m \equiv 1\ [p]\}$ est une partie non vide de $\mathbb{N}^*$ (car il contient $F_n - 1$), donc admet un plus petit élément noté α.

Formons la division euclidienne de $F_n - 1$ par α : il existe $q \in \mathbb{N}$ et $r \in \{0, \ldots, \alpha - 1\}$ tels que $F_n - 1 = q\alpha + r$. On a, modulo p : $3^{F_n-1} = (3^\alpha)^q 3^r \equiv 3^r\ [p]$.

Comme $3^{F_n-1} \equiv 1\ [p]$, il en résulte $3^r \equiv 1\ [p]$, puis, par définition de α, $r = 0$.

Ceci montre : $\alpha | F_n - 1 = 2^{2^n}$.

D'autre part : $3^{\frac{F_n-1}{2}} \equiv -1\ [F_n]$, donc $3^{\frac{F_n-1}{2}} \not\equiv 1\ [F_n]$ (car $F_n \neq 2$), d'où $\alpha \nmid \frac{F_n - 1}{2} = 2^{2^n-1}$ (si α divisait $\frac{F_n - 1}{2}$, on aurait $3^{\frac{F_n-1}{2}} \equiv 1\ [F_n]$).

Comme $\alpha | 2^{2^n}$ et $\alpha \nmid 2^{2^n-1}$, il est clair que : $\alpha = 2^{2^n}$.

D'autre part, d'après le petit théorème de Fermat : $3^{p-1} \equiv 1\ [p]$ (car $p \nmid 3$), donc $\alpha \leqslant p - 1$.

Alors : $\alpha = F_n - 1 \leqslant p - 1$, donc $F_n \leqslant p$. Mais $p \mid F_n$, d'où $F_n = p$, F_n est premier.

Exemple : $F_5 = 2^{2^5} + 1 = 4\,294\,967\,297$,

$3^{\frac{F_5-1}{2}} = 3^{2^{31}} \equiv 10\,324\,303 \neq -1\ [4\,294\,967\,297]$, donc F_5 est composé.

On peut «remarquer» : $F_5 = 641 \cdot 6700417$.

4) a) Il nous faut discuter suivant la congruence de p modulo 4 (pour utiliser la loi de réciprocité quadratique), et la congruence de p modulo 3 (pour simplifier $\left(\frac{p}{3}\right)$), d'où une discussion modulo 12.

Traitons, par exemple, le cas $p \equiv -1\ [12]$; il existe $k \in \mathbb{N}^*$ tel que $p = 12k - 1$.

Puisque $\left\{\begin{array}{l} 3 \equiv 3\ [4] \\ p \equiv 3\ [4] \end{array}\right.$, on a : $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$. Puis : $\left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1$.

On déduit : $\left(\frac{3}{p}\right) = 1$.

Les autres cas se traitent de façon analogue.

b) $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$ et utiliser ***I** 2) b)* et ***II** 4) a)*.

Indications et réponses
pour les exercices du chapitre 5

5.1.1 ◇ **Réponse :** $(\lambda,\mu) \in \{(-6,5),\ (6,13)\}$.

5.1.2 Le coefficient du terme en X^{2n} de $(1+X)^{2n}(1-X)^{2n}$ est $\sum_{k=0}^{2n}(-1)^k C_{2n}^k C_{2n}^{2n-k}$ et $C_{2n}^{2n-k} = C_{2n}^k$.

5.1.3
$$\begin{aligned}(P(1))^2 - 2b_{n+1} &= (a_0 + \ldots + a_n)^2 - 2(a_1a_n + a_2a_{n-1} + \ldots + a_na_1)\\ &= a_0^2 + 2a_0(a_1 + \ldots + a_n) - 2(a_1a_n + \ldots + a_na_1) + (a_1 + \ldots + a_n)^2\\ &= a_0^2 + 2\sum_{k=1}^{n} a_k(a_0 - a_{n+1-k}) + (a_1 + \ldots + a_n)^2 \geqslant 0.\end{aligned}$$

5.1.4 Les P_k sont à degrés successifs (cf. 5.1.4 Rem. p. 146).

5.1.5 *a)* Soit $P \in \mathbb{R}_n[X]$; $P(X)P(-X)$ est un polynôme pair, de degré $\leqslant 2n$. Il existe donc $a_0,\ldots,a_n \in \mathbb{R}$ tels que $P(X)P(-X) = \sum_{k=0}^{n} a_k X^{2k}$, d'où l'existence et l'unicité de $\widehat{P}$, et $\widehat{P} = \sum_{k=0}^{n} a_k X^k$.

b) $\widehat{PQ}(X^2) = (PQ)(X)(PQ)(-X) = P(X)Q(X)P(-X)Q(-X) = P(X)P(-X)Q(X)Q(-X)$
$= \widehat{P}(X^2)\widehat{Q}(X^2) = (\widehat{P}\ \widehat{Q})(X^2)$, et donc (unicité des coefficients) : $\widehat{PQ} = \widehat{P}\widehat{Q}$.

c) Il est clair que $\widehat{-1}(X^2) = (-1)^2 = 1$, donc $\varphi(-1) = 1$.

◇ **Réponse :** non.

5.1.6 Considérons $\Delta : \begin{array}{ccc}\mathbb{C}[X] & \longrightarrow & \mathbb{C}[X]\\ A & \longmapsto & A(X+1) - A(X)\end{array}$, appelé *opérateur différence.*

Il est clair que Δ est linéaire, et une récurrence montre :

$$\forall A \in \mathbb{C}[X],\quad \forall k \in \mathbb{N},\quad \Delta^k(A) = (-1)^k \sum_{i=0}^{k}(-1)^i C_k^i A(X+i).$$

En particulier : $(\Delta^n P)(0) = (-1)^n \sum_{k=0}^{n}(-1)^k C_n^k P(k)$.

Mais $\deg(P) < n$, d'où $\deg(\Delta P) < n-1,\ldots,\deg(\Delta^n P) < 0$, donc $\Delta^n P = 0$.

5.1.7 Le cas $A = 0$ étant d'étude immédiate, supposons $A \neq 0$ et notons $n = \deg(A)$. L'application $f : \begin{array}{ccc}\mathbb{C}_n[X] & \longrightarrow & \mathbb{C}_n[X]\\ P & \longmapsto & P(X-\alpha)+P(X-\beta)\end{array}$ est linéaire et bijective car, si on note $e_i = X^i$ $(0 \leqslant i \leqslant n)$, $f(e_i)$ est de degré i.

5.1.8 *1)* Soit f un automorphisme de la K-algèbre $K[X]$. Il existe $A \in K[X] - \{0\}$ tel que $f(A) = X$; notons $A = \sum_{i=0}^{n} a_i X^i$.

On a : $X = f(A) = f\left(\sum_{i=0}^{n} a_i X^i\right) = \sum_{i=0}^{n} a_i (f(X))^i = A \circ (f(X))$.

En comparant les degrés (cf. 5.1.5 Prop. 1 p. 147), on déduit : $\deg(A) = \deg(f(X)) = 1$.

Il existe donc $(\alpha, \beta) \in K^* \times K$ tel que $f(X) = \alpha X + \beta$.

Pour tout polynôme $P = \sum_{k=0}^{p} b_k X^k$ de $K[X]$, on a alors :

$$f(P) = \sum_{k=0}^{p} b_k (\alpha X + \beta)^k = P(\alpha X + \beta) \quad \text{(composée)}.$$

2) Réciproquement, soient $(\alpha, \beta) \in K^* \times K$ et $f : \begin{array}{c} K[X] \longrightarrow K[X] \\ P \longmapsto P(\alpha X + \beta) \end{array}$.

Alors $f(1) = 1$ (où $1 \in K[X]$) et, pour tous λ de K et P, Q de $K[X]$:

- $f(P + Q) = (P + Q)(\alpha X + \beta) = P(\alpha X + \beta) + Q(\alpha X + \beta) = f(P) + f(Q)$
- $f(\lambda P) = (\lambda P)(\alpha X + \beta) = \lambda P(\alpha X + \beta) = \lambda f(P)$
- $f(PQ) = (PQ)(\alpha X + \beta) = P(\alpha X + \beta) Q(\alpha X + \beta) = f(P) f(Q)$.

Enfin, en notant $g : \begin{array}{c} K[X] \longrightarrow K[X] \\ Q \longrightarrow Q\left(\dfrac{X - \beta}{\alpha}\right) \end{array}$, il est clair que $g \circ f = f \circ g = \mathrm{Id}_{K[X]}$, et donc f est bijective.

◇ **Réponse :** $\left\{ \begin{array}{c} K[X] \longrightarrow K[X] \\ P \longmapsto P(\alpha X + \beta) \end{array} ; \quad (\alpha, \beta) \in K^* \times K \right\}$.

5.1.9 *a)* Soient P unitaire convenant tel que $P \neq 0$, et $n = \deg(P)$. Le coefficient du terme en X^n de $X(X + 1)P'' + (X + 2)P' - P$ est $n^2 - 1$, d'où $n = 1$. Noter $P = X + \beta$, et déterminer $\beta \in \mathbb{R}$.

◇ **Réponse :** $\{\alpha(X + 2); \alpha \in \mathbb{R}\}$.

b) Raisonner comme en *a)* en déterminant le degré de P, si P convient.

◇ **Réponse :** $\left\{\frac{4}{9} X^3\right\}$.

5.1.10 Remarquer d'abord que, si P_n convient, alors $\deg(P_n) = n$.

En notant $P_n = \sum_{k=0}^{n} a_k X^k$, on a :

$$P_n - P_n' = X^n \iff (a_n = 1,\ a_{n-1} = n a_n, \ldots, a_0 = a_1)$$
$$\iff (a_n = 1,\ a_{n-1} = n,\ a_{n-2} = n(n-1), \ldots, a_1 = n(n-1)\ldots 2,\ a_0 = n!).$$

◇ **Réponse :** $P_n = n! \sum_{k=0}^{n} \frac{X^k}{k!}$.

5.1.11 *a)* $P_n' = \dfrac{1}{n!}(X+n)^{n-1} + \dfrac{n-1}{n!}X(X+n)^{n-2} = \dfrac{(X+n)^{n-2}}{n!}(X+n+(n-1)X)$

$= \dfrac{1}{(n-1)!}(X+n)^{n-2}(X+1) = P_{n-1}(X+1).$

b) Récurrence sur n

La formule est évidente pour $n = 0$.

Supposons-la vraie pour un n de $\mathbb{N}$. On a :

$$\frac{d}{dx}\left(\sum_{i+j=n+1} P_i(x)P_j(y)\right) = \sum_{i+j=n+1} P_i'(x)P_j(y)$$

$$= \sum_{\substack{i+j=n+1 \\ i\geqslant 1}} P_{i-1}(x+1)P_j(y) = \sum_{k+j=n} P_k(x+1)P_j(y)$$

$$= P_n\big((x+1)+y\big) = P_{n+1}'(x+y) = \frac{d}{dx}\big(P_{n+1}(x+y)\big).$$

Pour $y \in \mathbb{R}$ fixé, il existe donc $C_n(y) \in \mathbb{R}$ tel que :

$$\forall x \in \mathbb{R},\quad \sum_{i+j=n+1} P_i(x)P_j(y) = P_{n+1}(x+y) + C_n(y).$$

Comme de plus : $\displaystyle\sum_{i+j=n+1} P_i(0)P_j(y) = P_{n+1}(y) = P_{n+1}(0+y) + C_n(y)$, on déduit $C_n(y) = 0$, d'où la formule voulue, à l'ordre $n+1$.

c) Remplacer x et y par 1.

5.1.12 *a)* Le polynôme proposé, considéré comme trinôme en X^2, admet $(Y+Z)^2$ et $(Y-Z)^2$ comme «zéros».

◇ **Réponse :** $(X+Y+Z)(X+Y-Z)(Y+Z-X)(Z+X-Y)$.

b) ◇ **Réponse :** $5(X+Y)(X+Z)(Y+Z)(X^2+Y^2+Z^2+XY+XZ+YZ)$.

5.1.13 *1)* La vérification de ce que I et J sont des idéaux est immédiate.

2) Il est clair que X_1X_3, X_1X_4, X_2X_3 sont dans E. Notons $P = X_1X_3 + X_1X_4 + X_2X_3$, et supposons $P \in E$.

Il existe $P_1, P_2, P_3, P_4 \in A$ tels que : $P = (P_1X_1 + P_2X_2)(P_3X_3 + P_4X_4)$.

Pour chaque i de $\{1,\ldots,4\}$, il existe $p_i \in K$ et $Q_i \in A$ tels que : $\begin{cases} P_i = p_i + Q_i \\ \text{val}(Q_i) \geqslant 1 \end{cases}$

(où $\text{val}(Q_i)$ est la «valuation totale» de Q_i).

Alors : $$P = (p_1X_1 + p_2X_2 + Q_1X_1 + Q_2X_2)(p_3X_3 + p_4X_4 + Q_3X_3 + Q_4X_4)$$
$$= p_1p_3X_1X_3 + p_1p_4X_1X_4 + p_2p_3X_2X_3 + p_2p_4X_2X_4 + R,$$

où $R \in A$ est de valuation totale $\geqslant 3$.

On déduit : $p_1p_3 = 1$, $p_1p_4 = 1$, $p_2p_3 = 1$, $p_2p_4 = 0$, contradiction.

Ainsi, $P \notin E$, et E n'est pas un idéal de A.

5.2.1 Pour $n \geqslant 2$: $(X+1)^n - nX - 1 = \displaystyle\sum_{k=2}^{n} C_n^k X^k$.

5.2.2 Notons $A = \sum_{i=0}^{n-1} X^i$, $B = \left(\sum_{i=0}^{n} X^i\right)^p - X^n$.

On a : $B = (A + X^n)^p - X^n = \sum_{k=1}^{p} C_p^k A^k (X^n)^{p-k} + (X^{np} - X^n)$,

et : $X^{np} - X^n = (X^n - 1)\sum_{k=0}^{p-1}(X^n)^k = A(X-1)\sum_{k=0}^{p-1}(X^n)^k$.

5.2.3 Remarquer $B_n = XB_{n-1} + A\sin(n-1)\theta$, d'où, par récurrence :

$$B_n = A\left(\sin(n-1)\theta + X\sin(n-2)\theta + \ldots + X^{n-2}\sin\theta\right).$$

◇ **Réponse :** $C_n = \sum_{k=0}^{n-2} X^k \sin(n-k-1)\theta$.

5.2.4 En effectuant la division euclidienne de $X^4 - X + a$ par $X^2 - aX + 1$, on obtient le reste $R = (a^3 - 2a - 1)X + (-a^2 + a + 1)$. Puis : $R = 0 \iff \begin{cases} a^3 - 2a - 1 = 0 \\ a^2 - a - 1 = 0 \end{cases} \iff a^2 - a - 1 = 0$.

◇ **Réponse :** $\left\{\frac{1-\sqrt{5}}{2}, \frac{1+\sqrt{5}}{2}\right\}$.

5.2.5 Par division euclidienne de $(X\sin\theta + \cos\theta)^n$ par $X^2 + 1$, il existe $Q \in \mathbb{C}[X]$ et $(a,b) \in \mathbb{C}^2$ tels que $(X\sin\theta + \cos\theta)^n = (X^2+1)Q + aX + b$.

En remplaçant X par i et par $-$i : $\begin{cases} ai + b = e^{in\theta} \\ -ai + b = e^{-in\theta} \end{cases}$.

◇ **Réponse :** $X\sin n\theta + \cos n\theta$.

5.2.6 $X^k = (X^{qn} - 1)X^r + X^r = (X^n - 1)\left(\sum_{i=0}^{q-1} X^{in+r}\right) + X^r$, et $\deg(X^r) = r < n = \deg(X^n - 1)$.

5.2.7 En notant Q le quotient de la division euclidienne de P par $X - a$, on a : $P = (X-a)Q + \widetilde{P}(a)$.

En utilisant la formule de Taylor pour les polynômes :

$$(X-a)Q = P - \widetilde{P}(a) = \sum_{k=1}^{n} \frac{\widetilde{P}^{(k)}(a)}{k!}(X-a)^k, \quad \text{où } n = \deg(P).$$

◇ **Réponse :** $\sum_{k=0}^{n-1} \frac{\widetilde{P^{(k+1)}}(a)}{(k+1)!}(X-a)^k$, où $n = \deg(P)$.

5.2.8 *a)* Puisque $\deg(P) \geqslant 1$ et $B \neq 0$, il est clair que : $B(P) \neq 0$.

Comme $\begin{cases} A = BQ + R \\ \deg(R) < \deg(B) \end{cases}$, on a alors : $\begin{cases} A \circ P = (B \circ P)(Q \circ P) + R \circ P \\ \deg(R \circ P) = \deg(R)\deg(P) < \deg(B)\deg(P) = \deg(B \circ P). \end{cases}$

b) Le cas $B = 0$ est d'étude immédiate. Si $B \neq 0$, avec les notations de *a)* :

$$B|A \iff R = 0 \iff R \circ P = 0 \iff B \circ P | A \circ P.$$

5.2.9 Remarquer que le pgcd se calcule par l'algorithme d'Euclide, dans lequel les polynômes intermédiaires sont les mêmes pour les corps K et L.

5.2.10 *a)* Récurrence sur n.

• Cas $n = 0$: $P_0 = 1$, $P_1 = X$, $P_2 = X^2 - 1$, donc $P_1^2 - P_0 P_2 = 1$.

• Supposons la formule vraie pour un n de $\mathbb{N}$. Alors :

$$P_{n+2}^2 - P_{n+1}P_{n+3} = P_{n+2}^2 - P_{n+1}(XP_{n+2} - P_{n+1}) = P_{n+2}(P_{n+2} - XP_{n+1}) + P_{n+1}^2 = -P_{n+2}P_n + P_{n+1}^2 = 1.$$

b) Découle de *a)*, d'après le théorème de Bezout.

5.2.11 Raisonnons par l'absurde : supposons $AB + BC + CA$ et ABC non premiers entre eux. Il existe alors un polynôme irréductible D de $K[X]$ tel que : $D|(AB + BC + CA)$ et $D|(ABC)$. Puisque $D|ABC$ et que D est irréductible, D divise A ou B ou C, par exemple : $D|A$. Comme $D|A$ et $D|(AB + BC + CA)$, $D|BC$, puis (D est irréductible), $D|B$ ou $D|C$. Ainsi, par exemple, $D|A$ et $D|B$, ce qui contredit $A \wedge B = 1$.

5.2.12 **(i) $\Longrightarrow$ (ii) :**

Supposons $A \wedge B \neq 1$ et notons $D = A \wedge B$, $\deg(D) \geqslant 1$.

Il existe $(A_1, B_1) \in (K[X] - \{0\})^2$ tel que : $A = DA_1$ et $B = DB_1$.

En notant $U = B_1$, $V = -A_1$, on a : $AU + BV = 0$, $\deg(U) < \deg(B)$, $\deg(V) < \deg(A)$.

(ii) $\Longrightarrow$ (i) :

Supposons qu'il existe $(U, V) \in (K[X] - \{0\})^2$ tel que : $AU + BV = 0$, $\deg(U) < \deg(B)$, $\deg(V) < \deg(A)$. Notons $D = A \wedge B$. Il existe $(A_1, B_1) \in (K[X] - \{0\})^2$ tel que : $A = DA_1$, $B = DB_1$, $A_1 \wedge B_1 = 1$. Comme $UA_1 + VB_1 = 0$, on déduit $A_1|VB_1$, puis $A_1|V$ (car $A_1 \wedge B_1 = 1$, théorème de Gauss). Il existe donc $P \in K[X] - \{0\}$ tel que $V = PA_1$. Alors : $\deg(A_1) \leqslant \deg(V) < \deg(A)$, donc $\deg(D) \geqslant 1$, $D \neq 1$.

Finalement : $A \wedge B \neq 1$.

5.2.13
$$(b-a)^{2n-1} = \big((X-a) - (X-b)\big)^{2n-1} = \sum_{k=0}^{2n-1} C_{2n-1}^k (-1)^k (X-a)^{2n-1-k}(X-b)^k$$

$$= \left(\sum_{k=0}^{n-1} C_{2n-1}^k (-1)^k (X-a)^{n-1-k}(X-b)^k\right)(X-a)^n$$

$$+ \left(\sum_{k=n}^{2n-1} C_{2n-1}^k (-1)^k (X-a)^{2n-1-k}(X-b)^{k-n}\right)(X-b)^n.$$

◇ **Réponse :** $U = \dfrac{1}{(b-a)^{2n-1}} \displaystyle\sum_{k=0}^{n-1} C_{2n-1}^k (-1)^k (X-a)^{n-1-k}(X-b)^k,$

$$V = \frac{1}{(b-a)^{2n-1}} \sum_{l=0}^{n-1} C_{2n-1}^{n+l} (-1)^{n+l} (X-a)^{n-1-l}(X-b)^l.$$

5.2.14 Une amorce de la division amène la conjecture :

$$1 - abX^2 = \big(1 - (a+b)X + abX^2\big)\left(1 + \sum_{k=1}^{n}(a^k + b^k)X^k\right) + \big(a^{n+1} + b^{n+1} - ab(a^n + b^n)X\big)X^{n+1}.$$

Montrer cette relation par récurrence sur n.

◇ **Réponse :** $Q = 1 + \sum_{k=1}^{n}(a^k + b^k)X^k$, $R = a^{n+1} + b^{n+1} - ab(a^n + b^n)X$.

5.2.15 Notons Q et R les quotient et reste demandés : $A = BQ + X^{n+1}R$ et $\deg(Q) \leqslant n$.

Comme : $(1 - X)A = 1 - X^{n+1}$ et $(1 + X)B = 1 + (-1)^n X^{n+1}$,

on a : $(1 + X)(1 - X^{n+1}) = (1 - X)\left(1 + (-1)^n X^{n+1}\right) Q + (1 - X^2)X^{n+1}R$,

d'où : $1 + X = (1 - X)Q + X^{n+1}S$, où : $S = 1 + X + (-1)^n(1 - X)Q + (1 - X^2)R$.

Comme $(1 + X) - (1 - X)Q = X^{n+1}S$ et que $\deg\big(1 + X - (1 - X)Q\big) \leqslant n + 1$, on déduit $\deg(S) = 0$.
De plus, $\widetilde{S}(1) = 2$. Ainsi $S = 2$, donc $1 + X = (1 - X)Q + 2X^{n+1}$.

Puisque $\deg(Q) \leqslant n$, la relation $1 + X = (1 - X)Q + 2X^{n+1}$ montre que Q est le quotient de la division de $1 + X$ par $1 - X$ suivant les puissances croissantes jusqu'à l'ordre n, d'où : $Q = 1 + 2\sum_{k=1}^{n} X^k$.

Puis : $(1 + X)R = 1 - (-1)^n Q$, d'où l'on déduit l'expression de R, en séparant en deux cas suivant que n est pair ou impair.

◇ **Réponse :** $Q = 1 + 2\sum_{k=1}^{n} X^k$, $R = \begin{cases} 2\sum_{k=0}^{p} X^{2k} & \text{si } n = 2p+1,\ p \in \mathbb{N} \\ -2X\sum_{k=0}^{p-1} X^{2k} & \text{si } n = 2p,\ p \in \mathbb{N}^* \end{cases}$.

5.3.1 Par division euclidienne de A par P, il existe $(Q, R) \in \big(K[X]\big)^2$ tel que :

$$A = PQ + R \text{ et } \deg(R) < n.$$

• Montrons que $(L_i)_{0 \leqslant i \leqslant n}$ est une base de $K_n[X]$. Soit $(\lambda_i)_{0 \leqslant i \leqslant n} \in K^{n+1}$ tel que $\sum_{i=0}^{n} \lambda_i L_i = 0$.

Alors : $\forall j \in \{0, \ldots, n\}$, $\lambda_j = \left(\sum_{i=0}^{n} \lambda_i \widetilde{L_i}\right)(x_j) = 0$. Ceci montre que $(L_i)_{0 \leqslant i \leqslant n}$ est libre.

Comme de plus $\dim(K_n[X]) = n + 1$, on conclut que $(L_i)_{0 \leqslant i \leqslant n}$ est une base de $K_n[X]$.

• Il existe donc $(\alpha_i)_{0 \leqslant i \leqslant n} \in K^{n+1}$ tel que $R = \sum_{i=0}^{n} \alpha_i L_i$. On a, pour tout j de $\{0, \ldots, n\}$:

$$\widetilde{A}(x_j) = \widetilde{P}(x_j)\widetilde{Q}(x_j) + \widetilde{R}(x_j) = \widetilde{R}(x_j) = \left(\sum_{i=0}^{n} \alpha_i \widetilde{L_i}\right)(x_j) = \alpha_j.$$

Finalement : $R = \sum_{i=0}^{n} \widetilde{A}(x_i) L_i$.

5.3.2 Il existe $Q \in \mathbb{R}[X]$ et $(\alpha, \beta) \in \mathbb{R}^2$ tels que : $P_n = (X^2 + 1)Q + \alpha X + \beta$.

En remplaçant X par i, on déduit :

$$\alpha i + \beta = P_n(i) = \prod_{k=1}^{n} (\cos a_k + i \sin a_k) = e^{i\sum_{k=1}^{n} a_k}.$$

◇ **Réponse :** $R = X \sin a + \cos a$, où $a = \sum_{k=1}^{n} a_k$.

5.3.3 *a)* Supposons $X-1 | P(X^n)$. Alors $P(1) = P(1^n) = 0$, et donc il existe $Q \in K[X]$ tel que $P = (X-1)Q$. En remplaçant X par X^{2n}, on obtient :

$$P(X^{2n}) = (X^{2n}-1)Q(X^{2n}) = \left(\sum_{k=0}^{2n-1} X^k\right)\left((X-1)Q(X^{2n})\right).$$

b) Raisonnement analogue à celui de *a)*.

5.3.4 Remarquons d'abord que le reste demandé est le même que celui de la division euclidienne dans $\mathbb{R}[X]$ (cf. 5.2.2 Rem. p. 157).

Il existe $Q \in \mathbb{R}[X]$, $(\alpha,\beta) \in \mathbb{R}^2$ tels que : $X^{2n+1} + (X+1)^{n+2} = (X^2+X+1)Q + \alpha X + \beta$.

En remplaçant X par j, on déduit :

$$\alpha j + \beta = j^{2n+1} + (j+1)^{n+2} = j^{2n+1} + (-j^2)^{n+2}.$$

Séparer en cas suivant la congruence de n modulo 6.

◇ **Réponse :**

$n \equiv \ldots$ [6]	0	1	2	3	4	5
R	$2X$	0	$-2X-2$	0	2	0

5.3.5 En notant $\zeta_k = \exp\left(\dfrac{(2k+1)i\pi}{5}\right)$ $(0 \leqslant k \leqslant 4)$ les racines $5^{\text{èmes}}$ de -1 dans $\mathbb{C}$, on a :

$$X^5 + 1 = \prod_{k=0}^{4}(X - \zeta_k).$$

Alors : $A | P_n \iff \big(\forall k \in \{0,\ldots,4\},\ P_n(\zeta_k) = 0\big)$.

- Il est clair que : $P_n(\zeta_2) = P_n(-1) = 0$.
- Soit $k \in \{0,1,2,3,4\}$. On a alors $\zeta_k^4 - \zeta_k^3 + \zeta_k^2 - \zeta_k + 1 = \dfrac{\zeta_k^5 + 1}{\zeta_k + 1} = 0$, d'où :

$$P_n(\zeta_k) = (\zeta_k^4 - 1)(\zeta_k^4)^n + (\zeta_k+1)\zeta_k^{4n-1} = \zeta_k^{4n-1}\left((\zeta_k^5 - \zeta_k) + (\zeta_k + 1)\right) = 0.$$

5.3.6 Comme $ab = \dfrac{abc}{c} = -\dfrac{1}{c}$ et $a+b = (a+b+c) - c = -3 - c$, on déduit : $a^2b + ab^2 + 3ab = ab(a+b+3) = 1$.

◇ **Réponse :** 1.

5.3.7 *a)* $E = \dfrac{1}{x_1^2} + \dfrac{1}{x_2^2} + \dfrac{1}{x_3^2} = \dfrac{x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2}{x_1^2x_2^2x_3^2} = \dfrac{\sigma_2^2 - 2\sigma_1\sigma_3}{\sigma_3^2}$, et : $\sigma_1 = 0$, $\sigma_2 = p$, $\sigma_3 = -q$.

◇ **Réponse :** $\dfrac{p^2}{q^2}$.

b) $E = (x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2)(x_1 + x_2 + x_3) - (x_1x_2^2x_3^2 + x_1^2x_2x_3^2 + x_1^2x_2^2x_3) = (\sigma_2^2 - 2\sigma_1\sigma_3)\sigma_1 - \sigma_2\sigma_3$, et : $\sigma_1 = 3$, $\sigma_2 = 1$, $\sigma_3 = 1$.

◇ **Réponse :** -16.

c) • $E = 2\sum x_1^3 + 3\sum x_1^2 x_2$.

• $\sum x_1^2 x_2 = \left(\sum x_1 x_2\right)\left(\sum x_3\right) - 3x_1x_2x_3 = \sigma_2\sigma_1 - 3\sigma_3$.

• En sommant les trois égalités $x_k^3 + px_k^2 + qx_k + r = 0$ $(k = 1,2,3)$ on obtient $S_3 + pS_2 + qS_1 + 3r = 0$, d'où l'on déduit la valeur de S_3.

◇ **Réponse :** $-2p^3 + 3pq + 3r$.

d) **1ère méthode**

$E = \left(\sum x_1^2 x_2^2\right)\left(\sum x_1^3\right) - \sum x_1^2 x_2^2 x_3^3 = (\sigma_2^2 - 2\sigma_1\sigma_3)S_3 - \sigma_1\sigma_3^2$, où $S_3 = x_1^3 + x_2^3 + x_3^3$.

On a : $\sigma_1 = 0$, $\sigma_2 = p$, $\sigma_3 = -q$, et $S_3 + pS_1 + 3q = 0$, d'où $S_3 = -3q$.

On déduit la valeur de E.

2ème méthode

$E = S_5S_2 - S_7$, où $S_k = x_1^k + x_2^k + x_3^k$ pour $k \in \mathbb{N}$. On a : $S_0 = 3$, $S_1 = \sigma_1 = 0$, $S_2 = \sigma_1^2 - 2\sigma_2 = -2p$.

Puis, en additionnant les trois égalités $x_i^3 + px_i + q = 0$ $(1 \leqslant i \leqslant 3)$, on obtient $S_3 + pS_1 + 3q = 0$, d'où $S_3 = -3q$.

De même :

$$S_4 + pS_2 + qS_1 = 0, \quad \text{d'où} \quad S_4 = 2p^2$$
$$S_5 + pS_3 + qS_2 = 0, \quad \text{d'où} \quad S_5 = 5pq$$
$$S_7 + pS_5 + qS_4 = 0, \quad \text{d'où} \quad S_7 = -7p^2q.$$

On déduit la valeur de E.

◇ **Réponse :** $-3p^2q$.

e) • $E = \left(\sum x_1x_2\right)\left(\sum x_1^3\right) - \sum x_1^3x_2x_3$, $\sum x_1^3x_2x_3 = \left(\sum x_1x_2x_3\right)\left(\sum x_1^2\right) - \sum x_1^2x_2x_3x_4$, $\sum x_1^2x_2x_3x_4 = \left(\sum x_1x_2x_3x_4\right)\left(\sum x_1\right) - 5\sigma_5$, d'où $E = \sigma_2S_3 - \sigma_3S_2 + \sigma_4S_1 - 5\sigma_5$, en notant $S_k = \sum x_1^k$, $k \in \mathbb{N}$.

• $S_2 = \sigma_1^2 - 2\sigma_2$.

• $S_3 = \left(\sum x_1^2\right)\left(\sum x_1\right) - \sum x_1^2x_2$, $\sum x_1^2x_2 = \left(\sum x_1x_2\right)\left(\sum x_1\right) - 3\sum x_1x_2x_3$.

• $\sigma_1 = -4$, $\sigma_2 = 3$, $\sigma_3 = 0$, $\sigma_4 = 1$, $\sigma_5 = -1$.

◇ **Réponse :** -83.

5.3.8 • $\sigma_1 = \sum z_1z_2 = \tau_2$.

• $\sigma_2 = \sum z_1^2z_2z_3 = \left(\sum z_1z_2z_3\right)\left(\sum z_1\right) - 4\tau_4 = \tau_1\tau_3 - 4\tau_4$.

• $\sigma_3 = \sum z_1^3z_2z_3z_4 + \sum z_1^2z_2^2z_3^2 = \tau_4\left(\sum z_1^2\right) + \left(\left(\sum z_1z_2z_3\right)^2 - 2\left(\sum z_1^2z_2^2z_3z_4\right)\right)$

$= \tau_4(\tau_1^2 - 2\tau_2) + (\tau_3^2 - 2\tau_2\tau_4)$.

◇ **Réponse :** $\sigma_1 = \tau_2$, $\sigma_2 = \tau_1\tau_3 - 4\tau_4$, $\sigma_3 = \tau_1^2\tau_4 + \tau_3^2 - 4\tau_2\tau_4$.

5.3.9 Un triplet (x,y,z) de $\mathbb{C}^3$ est solution du système proposé si et seulement si x,y,z sont les solutions de l'équation algébrique $t^3 - 2t^2 + t - p = 0$, d'inconnue $t \in \mathbb{C}$.

Etudier les variations de

$\varphi : \mathbb{R} \longrightarrow \mathbb{R}$
$t \longmapsto t^3 - 2t^2 + t - p$

t	$-\infty$		$\frac{1}{3}$		1		$+\infty$
$\varphi(t)$	$-\infty$	$\nearrow$		$\searrow$		$\nearrow$	$+\infty$

◇ **Réponse :** $0 \leqslant p \leqslant \frac{4}{27}$.

5.3.10 En notant $\sigma_1,\sigma_2,\sigma_3$ les fse de x,y,z, les complexes x,y,z sont les solutions de l'équation $t^3 - \sigma_1 t^2 + \sigma_2 t - \sigma_3 = 0$, d'inconnue $t \in \mathbb{C}$. On essaiera donc de remplacer le système proposé par un système équivalent portant sur $\sigma_1,\sigma_2,\sigma_3$, et x,y,z seront déterminés comme solutions d'une équation du 3ème degré.

a) En notant $S_k = x^k + y^k + z^k$ $(k \in \mathbb{N})$, on a $S_2 = \sigma_1^2 - 2\sigma_2$ et $S_3 - \sigma_1 S_2 + \sigma_2 S_1 - 3\sigma_3 = 0$.

On en déduit : $\begin{cases} \sigma_1 = 3 \\ \sigma_2 = 2 \\ S_3 = 9 \end{cases} \Longleftrightarrow \begin{cases} \sigma_1 = 3 \\ \sigma_2 = 2 \\ \sigma_3 = 0 \end{cases}$.

◇ **Réponse :** $\{(0,1,2)$ et ses permutés$\}$.

b) Notons $(p,q,r) \in \mathbb{C}^3$ tel que x,y,z soient les solutions de $t^3 - pt^2 + qt - r = 0$ (d'inconnue $t \in \mathbb{C}$), et, pour $k \in \mathbb{N}$: $S_k = x^k + y^k + z^k$.

On a :

- $p = \sigma_1$
- $S_3 = pS_2 - qS_1 + 3r$, donc : $\begin{cases} \sigma_1 = 0 \\ S_3 = 6 \end{cases} \Longleftrightarrow \begin{cases} p = 0 \\ r = 2 \end{cases}$
- $S_2 = \sigma_1^2 - 2\sigma_2 = p^2 - 2q$ et $S_5 = -qS_3 + rS_2$, donc :

$$\begin{cases} \sigma_1 = 0 \\ S_3 = 6 \\ S_5 = 30 \end{cases} \Longleftrightarrow \begin{cases} p = 0 \\ r = 2 \\ -10q = 30 \end{cases} \Longleftrightarrow \begin{cases} p = 0 \\ q = -3 \\ r = 2 \end{cases}.$$

◇ **Réponse :** $\{(-1,-1,2), (-1,2,-1), (2,-1,-1)\}$.

c) ◇ **Réponse :** $\{(1,\mathrm{i},-\mathrm{i})$ et ses permutés$\}$.

d) ◇ **Réponse :** $\{(-1,\mathrm{j},\mathrm{j}^2)$ et ses permutés$\}$.

5.3.11 *a)* En notant $\pi = z_1 z_2$, on a :

$$\text{CNS} \Longleftrightarrow \left(\exists (z_3,\pi) \in \mathbb{C}^2, \begin{cases} -1 + z_3 = -5 \\ -z_3 + \pi = -8 \\ \pi z_3 = -\lambda \end{cases} \right) \Longleftrightarrow \left(\exists (z_3,\pi) \in \mathbb{C}^2, \begin{cases} z_3 = -4 \\ \pi = -12 \\ \lambda = -48 \end{cases} \right) \Longleftrightarrow \lambda = -48.$$

◇ **Réponse :** • CNS : $\lambda = -48$.

• Dans ce cas, les solutions sont -4 (double), 3 (simple).

b) Notons z_1,z_2,z_3 les solutions et $\sigma = z_1+z_2$, $\pi = z_1z_2$. Comme z_1,z_2 jouent des rôles symétriques, on peut remplacer la condition $z_1 - z_2 = 1$ par $(z_1-z_2)^2 = 1$, c'est-à-dire $\sigma^2 - 4\pi = 1$. Puis :

$$\left(\exists(\sigma,\pi,z_3)\in\mathbb{C}^3,\ \begin{cases}\sigma+z_3=0\\ \sigma z_3+\pi=p\\ \pi z_3=-q\\ \sigma^2-4\pi=1\end{cases}\right)\iff\left(\exists(\sigma,\pi,z_3)\in\mathbb{C}^3,\ \begin{cases}z_3=-\sigma\\ \pi=\dfrac{\sigma^2-1}{4}\\ -4\sigma^2+(\sigma^2-1)=4p\\ (\sigma^2-1)\sigma=4q\end{cases}\right)$$

$$\iff\left(\exists\sigma\in\mathbb{C},\ \begin{cases}\sigma^2=-\dfrac{4p+1}{3}\\ (p+1)\sigma=-3q\end{cases}\right).$$

◇ **Réponse :** $(p+1)^2(4p+1)+27q^2=0$.

c) D'après l'exercice 2.3.3 du Tome 1, les points d'affixes z_1,z_2,z_3 forment un triangle équilatéral direct si et seulement si $z_1+jz_2+j^2z_3=0$, puis forment un triangle équilatéral indirect si et ssi $z_1+j^2z_2+jz_3=0$, donc forment un triangle équilatéral si et seulement si $(z_1+jz_2+j^2z_3)(z_1+j^2z_2+jz_3)=0$, c'est-à-dire $z_1^2+z_2^2+z_3^2-(z_1z_2+z_1z_3+z_2z_3)=0$.

◇ **Réponse :** $p^2-3q=0$.

d) $$\left(\exists(z_1,z_2,z_3)\in\mathbb{C}^3,\ \begin{cases}z_2=2z_1\\ z_1+z_2+z_3=0\\ z_1z_2+z_1z_3+z_2z_3=-7\\ z_1z_2z_3=-\lambda\end{cases}\right)\iff\left(\exists(z_1,z_3)\in\mathbb{C}^2,\ \begin{cases}3z_1+z_3=0\\ 2z_1^2+3z_1z_3=-7\\ 2z_1^2z_3=-\lambda\end{cases}\right)$$

$$\iff\left(\exists z_1\in\mathbb{C},\ \begin{cases}z_1^2=1\\ 6z_1^3=\lambda\end{cases}\right).$$

◇ **Réponse :** $\lambda=6$ ou $\lambda=-6$.

e) 1ère méthode :

La CNS s'exprime d'abord par : $\exists(\alpha,\beta)\in\mathbb{C}^2,\ \begin{cases}2(\alpha+\beta)=-a\\ \alpha^2+4\alpha\beta+\beta^2=b\\ 2(\alpha^2\beta+\alpha\beta^2)=-c\\ \alpha^2\beta^2=d\end{cases}$, puis en notant $s=\alpha+\beta$, $p=\alpha\beta$,

par : $\exists(s,p)\in\mathbb{C}^2,\ \begin{cases}2s=-a\\ s^2+2p=b\\ 2sp=-c\\ p^2=d\end{cases}$.

2ème méthode :

$$\left(\exists(\lambda,\mu)\in\mathbb{C}^2,\ X^4+aX^3+bX^2+cX+d=(X^2+\lambda X+\mu)^2\right)$$

$$\iff\left(\exists(\lambda,\mu)\in\mathbb{C}^2,\ 2\lambda=a,\ \lambda^2+2\mu=b,2\lambda\mu=c,\ \mu^2=d\right)$$

$$\iff\begin{vmatrix}a\neq0,\ \left(\dfrac{a}{2}\right)^2+2\dfrac{c}{a}=b,\ \left(\dfrac{c}{a}\right)^2=d\\ \text{ou}\\ a=0,\ c=0,\ \left(\dfrac{b}{2}\right)^2=d.\end{vmatrix}$$

◇ **Réponse :** $\begin{cases}a(4b-a^2)=8c\\ (4b-a^2)^2=64d.\end{cases}$

f) En notant $s=z_1+z_2$, $p=z_1z_2$, $s'=z_3+z_4$, $p'=z_3z_4$, on a :

$$\begin{cases}p=1\\ \sigma_1=0\\ \sigma_2=0\\ \sigma_3=-a\\ \sigma_4=b\end{cases}\iff\begin{cases}p=1\\ s+s'=0\\ ss'+p+p'=0\\ sp'+s'p=-a\\ pp'=b\end{cases}\iff\begin{cases}p=1\\ p'=b\\ s'=-s\\ -s^2+(1+b)=0\\ (b-1)s=-a.\end{cases}$$

L'élimination de s donne : $(b-1)^2(b+1)-a^2=0$.

Application. La condition est bien satisfaite. On a ici : $p = 1$, $s = 3$, $s' = -3$, $p' = 8$. Ainsi, les zéros cherchés sont ceux de $z^2 - 3z + 1 = 0$ et de $z^2 + 3z + 8 = 0$.

◊ **Réponse :** • $(b-1)^2(b+1) - a^2 = 0$

• *Application :* $\left\{\dfrac{3-\sqrt{5}}{2}, \dfrac{3+\sqrt{5}}{2}, \dfrac{-3-\mathrm{i}\sqrt{23}}{2}, \dfrac{-3+\mathrm{i}\sqrt{23}}{2}\right\}$.

g)◊ **Réponse :** $2\lambda + \mu - 8 = 0$.

h)◊ **Réponse :** • $\lambda = -7$

• Les zéros sont alors : $-1-\sqrt{6}$, $1+\sqrt{6}$, $\dfrac{3-\mathrm{i}\sqrt{7}}{2}$, $\dfrac{3+\mathrm{i}\sqrt{7}}{2}$.

i) En notant : $\begin{cases} s, p, \text{ les fse de } z_1, z_2 \\ \sigma_1, \sigma_2, \sigma_3 \text{ les fse de } z_3, z_4, z_5 \end{cases}$, les fse $\tau_1, \ldots, \tau_5$ de $z_1, \ldots, z_5$ sont :

$$\tau_1 = \sigma_1 + s, \quad \tau_2 = \sigma_2 + \sigma_1 s + p, \quad \tau_3 = \sigma_3 + \sigma_2 s + \sigma_1 p, \quad \tau_4 = \sigma_3 s + \sigma_2 p, \quad \tau_5 = \sigma_3 p.$$

La CNS s'exprime par : $\exists (\sigma_1, \sigma_2, \sigma_3, s, p) \in \mathbb{C}^5$, $\begin{cases} p = 1, \sigma_1 = -s, \sigma_2 = s^2 - 1 \\ \sigma_3 = -s^3 + 2s \\ s^4 - 3s^2 - 208 = 0 \\ \lambda = s^3 - 2s. \end{cases}$

◊ **Réponse :** $\lambda = -56$ ou $\lambda = 56$.

5.3.12 *a)* Remarquer d'abord que -1 est solution, et factoriser par $x + 1$. Puis, pour $x \in \mathbb{C}^*$:

$$x^4 + 2x^3 - x^2 + 2x + 1 = 0 \iff \left(x^2 + \frac{1}{x^2}\right) + 2\left(x + \frac{1}{x}\right) - 1 = 0$$
$$\iff y^2 + 2y - 3 = 0 \iff (y = 1 \text{ ou } y = -3).$$

Résoudre $x + \dfrac{1}{x} = 1$, $x + \dfrac{1}{x} = -3$.

◊ **Réponse :** $\left\{-1, \dfrac{-3-\sqrt{5}}{2}, \dfrac{-3+\sqrt{5}}{2}, \dfrac{1-\mathrm{i}\sqrt{3}}{2}, \dfrac{1+\mathrm{i}\sqrt{3}}{2}\right\}$.

b) ◊ **Réponse :**

$$\left\{-\mathrm{j}, -\mathrm{j}^2, \frac{1}{4}\left(3+\sqrt{5}+\varepsilon_1\sqrt{6\sqrt{5}-2}\right), \frac{1}{4}\left(3-\sqrt{5}+\varepsilon_2\mathrm{i}\sqrt{6\sqrt{5}+2}\right); (\varepsilon_1, \varepsilon_2) \in \{-1,1\}^2\right\}.$$

5.3.13 Il existe $z_0 \in \mathbb{C}^*$ tel que z_0 et $-z_0$ soient solutions, d'où par combinaisons :

$$\begin{cases} z_0^6 - 4z_0^3 - 41z_0^2 - 36 = 0 \\ -z_0^4 + 5z_0^2 + 36 = 0 \end{cases}.$$

On remarque alors que : $X^4 - 5X^2 - 36 \,|\, X^6 - 4X^3 - 41X^2 - 36$, ce qui permet de factoriser dans l'équation :

$$(z^2 - z + 1)(z^4 - 5z^2 - 36) = 0.$$

◊ **Réponse :** $\{-3, 3, 2\mathrm{i}, -2\mathrm{i}, -\mathrm{j}, -\mathrm{j}^2\}$.

5.3.14 *a)* En remplaçant x par $z - \dfrac{a}{3}$, on obtient :

$$x^3 + ax^2 + bx + c = z^3 + \left(b - \frac{a^2}{3}\right)z + \left(c - \frac{ab}{3} + \frac{2a^3}{27}\right).$$

b) Soit $(\alpha,\beta) \in \mathbb{C}^2$ tel que ni α ni β ne soit solution de $z^3 + pz + q = 0$ (inconnue $z \in \mathbb{C}$). Le changement d'inconnue $y = \dfrac{\alpha - z}{\beta - z}$ ramène, après quelques lignes de calcul, l'équation $z^3 + pz + q = 0$ (inconnue $z \in \mathbb{C}$) à l'équation :

$$(\beta^3 + p\beta + q)y^3 - \big(3\alpha\beta^2 + p(\alpha + 2\beta) + 3q\big)y^2 + \big(3\alpha^2\beta + p(2\alpha + \beta) + 3q\big)y - (\alpha^3 + p\alpha + q) = 0,$$

d'inconnue $y \in \mathbb{C}$.

Pour que l'équation en y soit de la forme $y^3 + A = 0$, il faut et il suffit que : $\begin{cases} 3\alpha\beta^2 + p(\alpha + 2\beta) + 3q = 0 \\ 3\alpha^2\beta + p(2\alpha + \beta) + 3q = 0 \end{cases}$,

c'est-à-dire (par combinaisons) : $\begin{cases} \alpha\beta(\alpha + \beta) + p(\alpha + \beta) + 2q = 0 \\ 3\alpha\beta + p = 0. \end{cases}$

En notant $\sigma = \alpha + \beta$, $\pi = \alpha\beta$, le système précédent se ramène à : $\pi = -\dfrac{p}{3}$, $\sigma = -3\dfrac{q}{p}$.

Il suffit donc de résoudre une équation du second degré : $t^2 + \dfrac{3q}{p}t - \dfrac{p}{3} = 0$ (inconnue $t \in \mathbb{C}$), pour obtenir α,β, puis de résoudre $(\beta^3 + p\beta + q)y^3 - (\alpha^3 + p\alpha + q) = 0$ (inconnue $y \in \mathbb{C}$) pour obtenir y, et enfin z.

De plus, en notant t pour α ou β, on a :

$$t^3 + pt + q = t\left(-\frac{3q}{p}t + \frac{p}{3}\right) + pt + q = -\frac{3q}{p}\left(-\frac{3q}{p}t + \frac{p}{3}\right) + \frac{4p}{3}t + q = \frac{4p^3 + 27q^2}{3p^2}t.$$

Ainsi, si $4p^3 + 27q^2 \neq 0$ et $\beta \neq 0$, on a : $(\beta^3 + p\beta + q)y^3 - (\alpha^3 + p\alpha + q) = 0 \iff y^3 = \dfrac{\alpha}{\beta}$.

5.3.15 *a)* et *b)* Si $(P,Q) \neq (0,0)$, alors $(X - a)^{\omega_P(a)} | P$ et $(X - a)^{\omega_Q(a)} | Q$, donc $(X - a)^{\mathrm{Min}(\omega_P(a),\omega_Q(a))} | P + Q$ et $(X - a)^{\omega_P(a)+\omega_Q(a)} | PQ$.

Le cas ($P = 0$ ou $Q = 0$) est d'étude immédiate.

c) Les polynômes $(X - a)^{\omega_P(a)}$ ($a \in Z(P)$) sont premiers entre eux deux à deux et divisent P, donc : $\prod_{a\in Z(P)} (X - a)^{\omega_P(a)} | P$, d'où : $\sum_{a\in Z(P)} \omega_P(a) = \deg\left(\prod_{a\in Z(P)} (X - a)^{\omega_P(a)}\right) \leqslant \deg(P)$.

d) De plus : $\sum_{a\in Z(P)} \omega_P(a) = \deg(P) \iff \left(\exists \lambda \in K - \{0\},\ P = \prod_{a\in Z(P)} (X - a)^{\omega_P(a)}\right)$.

5.3.16 Notons $P = \lambda X^n + \mu X^{n-1} + \ldots$, et, pour tout k de $\{0,\ldots,n-1\}$, s_k la somme des zéros de $P^{(k)}$.

Soit $k \in \{0,\ldots,n-1\}$. Comme $P^{(k)} = \lambda \dfrac{n!}{(n-k+1)!} X^{n-k} + \mu \dfrac{(n-1)!}{(n-k)!} X^{n-k-1} + \ldots$, on a :

$$s_k = -\frac{\mu(n-1)!}{(n-k)!} \cdot \frac{(n-k+1)!}{\lambda n!} = -\frac{(n+1)\mu}{n\lambda} + k\frac{\mu}{\lambda n}.$$

5.3.17 En notant $P = X^2 + pX + q$ et $Q = (X-\alpha)(X-\beta)$, on a :

$$\begin{cases} P(\alpha) = \beta \\ P(\beta) = \alpha \end{cases} \iff \begin{cases} \alpha^2 + p\alpha + q = \beta \\ \beta^2 + p\beta + q = \alpha \end{cases} \iff \begin{cases} \alpha^2 + \beta^2 + p(\alpha+\beta) + 2q = \alpha + \beta \\ (\alpha-\beta)(\alpha+\beta+p+1) = 0. \end{cases}$$

En notant $\sigma = \alpha + \beta$, $\pi = \alpha\beta$, le système précédent se ramène à : $\begin{cases} \sigma^2 - 2\pi + (p-1)\sigma + 2q = 0 \\ \sigma + p + 1 = 0 \end{cases}$,

soit encore $\begin{cases} p = -1 - \sigma \\ q = \sigma + \pi. \end{cases}$

Alors : $PQ = (X^2 - \sigma X + \pi)(X^2 + pX + q)$

$= X^4 - (1+2\sigma)X^3 + (\sigma^2 + 2\sigma + 2\pi)X^2 - (\sigma^2 + 2\sigma\pi + \pi)X + \pi(\sigma + \pi)$.

Donc :

$$A = PQ \iff \begin{cases} 1 + 2\sigma = -(2a+1) \\ \sigma^2 + 2\sigma + 2\pi = (a-1)^2 \\ \sigma^2 + 2\sigma\pi + \pi = -b \\ \pi(\sigma + \pi) = 4 \end{cases} \iff \begin{cases} \sigma = -a - 1 \\ \pi = 1 - a \\ b = -3a^2 - a \\ a^2 - a - 2 = 0 \end{cases} \iff \left(\begin{cases} a = -1 \\ \sigma = 0 \\ \pi = 2 \\ b = -2 \end{cases} \text{ ou } \begin{cases} a = 2 \\ \sigma = -3 \\ \pi = -1 \\ b = -14 \end{cases} \right).$$

Enfin : $(\alpha, \beta) \in \mathbb{R}^2 \iff \sigma^2 - 4\pi \geqslant 0$.

◇ **Réponse :** $\{(2, -14)\}$.

5.3.18 • $a^2 - bc = a^2 - (ab+ac+bc) + a(b+c) = a^2 - \sigma_2 + a(\sigma_1 - a) = -\sigma_2 + a\sigma_1 = -(pa+q)$.

• Le changement d'inconnue $y = -(px+q)$ remplace l'équation $x^3 + px^2 + qx + r = 0$ (d'inconnue $x \in \mathbb{C}$) par l'équation :

$$y^3 + (3q - p^2)y^2 + (3q^2 - p^2 q)y + (q^3 - rp^3) = 0.$$

◇ **Réponse :** $y^3 + (3q - p^2)y^2 + (3q^2 - p^2 q)y + (q^3 - rp^3) = 0$.

5.3.19 La condition proposée revient à : $\deg\big(\text{pgcd}(X^4 + 2X^2 + p,\ X^3 + X + q)\big) \geqslant 2$.

◇ **Réponse :** $p = 1$ et $q = 0$.

5.3.20 *1)* $\Longrightarrow$: évident.

2) $\Longleftarrow$:

Les coefficients de $P = \prod_{i=1}^{n}(X + x_i) = X^n + \sum_{k=1}^{n} \sigma_k X^{n-k}$ sont tous $\geqslant 0$, donc P n'a aucun zéro dans $\mathbb{R}_+^*$.

Mais les zéros de P sont les $-x_i$, $1 \leqslant i \leqslant n$; d'où : $\forall i \in \{1, \ldots, n\}$, $x_i \geqslant 0$.

5.3.21 Soit A un diviseur irréductible de P. Comme Q est scindé et que $A | Q$, A est alors de degré 1. Ceci montre que P est scindé.

5.3.22 En notant $x_1, \ldots, x_n$ les zéros de B, on a :

$B | P^2 - A \iff \big(\forall k \in \{1, \ldots, n\}, (\widetilde{P}(x_k))^2 = \widetilde{A}(x_k)\big)$.

Notons, pour $i \in \{1, \ldots, n\}$, $C_i = \prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} (X - x_j)$ (cf. 5.3.1 Exemple p. 169).

Cherchons P sous la forme $P = \sum_{i=1}^{n} \lambda_i C_i$, $(\lambda_1, \ldots, \lambda_n) \in K^n$ à trouver.

On a : $B \mid P^2 - A \iff \left(\forall k \in \{1, \ldots, n\},\ \lambda_k^2 = \dfrac{\widetilde{A}(x_k)}{(\widetilde{C}_k(x_k))^2} \right)$, ce qui montre l'existence des λ_k.

5.2.23 Pour $P \in \mathbb{R}[X]$, par division euclidienne de P par $X^2(X-1)^2$, il existe $A \in \mathbb{R}[X]$ et $(a,b,c,d) \in \mathbb{R}^4$ tels que : $P = X^2(X-1)^2A + aX^3 + bX^2 + cX + d$.

Puis : $\begin{cases} P(0) = 1 \\ P(1) = 0 \\ P'(0) = 0 \\ P'(1) = 1 \end{cases} \iff \begin{cases} d = 1 \\ a+b+c+d = 0 \\ c = 0 \\ 3a+2b+c = 1 \end{cases} \iff \begin{cases} a = 3 \\ b = -4 \\ c = 0 \\ d = 1 \end{cases}$.

◇ **Réponse :** $\{X^2(X-1)^2A + 3X^3 - 4X^2 + 1;\ A \in \mathbb{R}[X]\}$.

5.3.24 *a)* En notant $P_n = \left(\sum_{k=0}^{n-1} X^k\right)^2 - n^2X^{n-1}$, on a $P_n(1) = 0$

et $P_n' = 2\left(\sum_{k=0}^{n-1} X^k\right)\left(\sum_{k=1}^{n-1} kX^{k-1}\right) - n^2(n-1)X^{n-2}$, d'où aussi $P_n'(1) = 2n\,\dfrac{n(n-1)}{2} - n^2(n-1) = 0$.

Il en résulte que 1 est zéro au moins double de P_n, c'est-à-dire : $(X-1)^2 | P_n$.

b) Notons $P_n = nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n$, d'où $P_n' = n(n+2)X^{n+1} - (n+2)(n+1)X^n + n + 2$ et $P_n'' = n(n+1)(n+2)(X^n - X^{n-1})$. On obtient facilement : $P_n(1) = P_n'(1) = P_n''(1) = 0$, donc 1 est zéro au moins triple de P_n, c'est-à-dire : $(X-1)^3 | P_n$.

5.3.25 Notons Q, R les quotient et reste de la division euclidienne de A par B :

$$A = BQ + R \text{ et } \deg(R) \leqslant 3.$$

Comme $\begin{cases} R(a) = A(a) = (a-b)^{2n} \\ R(b) = A(b) = (b-a)^{2n} \end{cases}$, il existe $S \in \mathbb{C}[X]$ tel que :

$$R - (b-a)^{2n} = (X-a)(X-b)S \quad \text{et} \quad \deg(S) \leqslant 1.$$

De plus, en dérivant : $A' = B'Q + BQ' + R'$, d'où : $\begin{cases} 2n(a-b)^{2n-1} = A'(a) = R'(a) = (a-b)S(a) \\ 2n(b-a)^{2n-1} = A'(b) = R'(b) = (b-a)S(b) \end{cases}$

d'où $S(a) = S(b) = 2n(b-a)^{2n-2}$. Comme $\deg(S) \leqslant 1$, on obtient $S = 2n(b-a)^{2n-2}$.

◇ **Réponse :** $R = 2n(b-a)^{2n-2}(X-a)(X-b) + (b-a)^{2n}$.

5.3.26 Eliminer x dans : $\left|\begin{array}{l} x^4 + ax^3 + bx + 1 = 0 \\ 4x^3 + 3ax^2 + b = 0 \\ 12x^2 + 6ax = 0 \end{array}\right|$. On obtient : $b = -\dfrac{a^3}{4}$ et $a^4 = -16$.

◇ **Réponse :** $(a,b) = \left(\sqrt{2}(\varepsilon_1 + \varepsilon_2 i), \sqrt{2}(\varepsilon_1 - \varepsilon_2 i)\right)$, $(\varepsilon_1, \varepsilon_2) \in \{-1,1\}^2$.

5.3.27 Calculer $P_n(1)$, P_n', $P_n'(1)$, P_n'', $P_n''(1)$, ... On obtient :

- $P_n(1) = 0$
- $P_n' = 2nX^{2n-1} - n^2(n+1)X^n + 2n(n^2-1)X^{n-1} - n^2(n-1)X^{n-2}$, $P_n'(1) = 0$
- $P_n'' = 2n(2n-1)X^{2n-2} - n^3(n+1)X^{n-1} + 2n(n^2-1)(n-1)X^{n-2} - n^2(n-1)(n-2)X^{n-3}$, $P_n''(1) = 0$
- $P_n^{(3)} = n(n-1)\big(4(2n-1)X^{2n-3} - n^2(n+1)X^{n-2} + 2(n^2-1)(n-2)X^{n-3} - n(n-2)(n-3)X^{n-4}\big)$, $P_n^{(3)}(1) = 0$
- $P_n^{(4)} = n(n-1)\big(4(2n-1)(2n-3)X^{2n-4} - n^2(n+1)(n-2)X^{n-3} + 2(n^2-1)(n-2)(n-3)X^{n-4} - n(n-2)(n-3)(n-4)X^{n-5}\big)$, $P_n^{(4)} = 2n^2(n-1)(n+1) \neq 0$.

◇ **Réponse :** L'ordre de multiplicité de 1 comme zéro de P_n est : 4.

5.3.28 Puisque $A = (X^p - 1)(X^q - 1)$, les zéros de A sont tous d'ordres $\leqslant 2$, donc $A \wedge A'$ est le produit des $X - z$, où z décrit l'ensemble des zéros doubles de A, c'est-à-dire l'ensemble des racines à la fois $p^{\text{èmes}}$ et $q^{\text{èmes}}$ de 1.

◊ **Réponse :** $A \wedge A' = X^{\text{pgcd}(p,q)} - 1$.

5.2.29 On a : $\begin{cases} (P(a))^2 + \lambda(Q(a))^2 = 0 \\ P(a)P'(a) + \lambda Q(a)Q'(a) = 0 \end{cases}$.

• Si $Q(a) = 0$, alors $P(a) = 0$, et donc $(PQ' - P'Q)(a) = 0$

• Si $Q(a) \neq 0$, alors, comme $\lambda P(a)Q(a)Q'(a) = -(P(a))^2P'(a) = \lambda(Q(a))^2P'(a)$, on déduit : $P(a)Q'(a) - P'(a)Q(a) = 0$.

5.3.30 Soit $P \in \mathbb{C}[X]$ irréductible, tel que $P|A'B - AB'$ et $P|B^2$.

Comme $P|B^2$ et que P est irréductible, $P|B$. Puis ($P|B$ et $P|A'B - AB'$), donc $P|AB'$. Comme $A \wedge B = 1$, on déduit $P|B'$.

Puisque $P|B$ et que B est scindé, P est scindé (cf. exercice 5.3.21 p. 175), donc $\deg(P) = 1$ (car P est irréductible). Alors B et B' ont au moins un zéro commun, contradiction.

Ceci prouve : $(A'B - AB') \wedge B^2 = 1$.

5.3.31 • *Recherche d'un éventuel zéro rationnel*

Soit $(p,q) \in \mathbb{Z}^* \times \mathbb{N}^*$ tel que $p \wedge q = 1$ et que $\dfrac{p}{q}$ soit zéro de $2X^3 - X^2 - X - 3$.

On a alors : $2p^3 - p^2q - pq^2 - 3q^3 = 0$.

On déduit : $\begin{cases} p|3q^3, & \text{donc } p|3 \\ q|2p^3, & \text{donc } q|2. \end{cases}$

D'où : $\dfrac{p}{q} \in \left\{-3,-1,1,3,-\dfrac{3}{2},-\dfrac{1}{2},\dfrac{1}{2},\dfrac{3}{2}\right\}$.

On s'aperçoit que $\dfrac{3}{2}$ est solution.

◊ **Réponse :** $(2X - 3)(X - j)(X - j^2)$.

5.3.32 • En notant $\omega_k = \exp\left(\dfrac{2ik\pi}{n}\right)$, $0 \leqslant k \leqslant n - 1$, on a :

$$\left(\frac{1+iz}{1-iz}\right)^n = a^n \iff \left(\exists k \in \{0,\ldots,n-1\},\ \frac{1+iz}{1-iz} = a\omega_k\right) \iff \left(\exists k \in \{0,\ldots,n-1\},\ z = i\,\frac{1-a\omega_k}{1+a\omega_k}\right).$$

• Pour tout ω de module 1 :

$$i\,\frac{1-a\omega}{1+a\omega} \in \mathbb{R} \iff i\,\frac{1-a\omega}{1+a\omega} = -i\,\frac{1-\dfrac{\overline{a}}{\omega}}{1+\dfrac{\overline{a}}{\omega}} \iff (1-|a|^2)\omega = 0 \iff |a| = 1.$$

◊ **Réponse :** • Si $|a| = 1$ et $a^n \neq (-1)^n$, les solutions sont : $\tan\left(\dfrac{\theta}{2} + \dfrac{k\pi}{n}\right)$, $0 \leqslant k \leqslant n - 1$,

où $\theta = \text{Arg}(a)\ [2\pi]$

• Si $|a| = 1$ et $a^n = (-1)^n$, il existe $k_0 \in \{0,\ldots,n-1\}$ tel que $\text{Arg}(a) = \pi - \dfrac{2k_0\pi}{n}\ [2\pi]$,

et les solutions sont : $\tan\left(\dfrac{\theta}{2} + \dfrac{k\pi}{n}\right)$, $k \in \{0,\ldots,n-1\} - \{k_0\}$.

5.3.33 *a)* Analogue à l'exercice 5.3.32. En notant $\omega_k = \exp\left(\dfrac{2ik\pi}{2n+1}\right)$, $k \in \{1,\dots,2n\}$, on a :

$$(z+\mathrm{i})^{2n+1} - (z-\mathrm{i})^{2n+1} = 0 \iff \left(\exists k \in \{1,\dots,2n\},\quad \frac{z+\mathrm{i}}{z-\mathrm{i}} = \omega_k\right)$$
$$\iff \left(\exists k \in \{1,\dots,2n\},\quad z = \mathrm{i}\,\frac{\omega_k+1}{\omega_k-1} = \operatorname{cotan}\frac{k\pi}{2n+1}\right).$$

D'autre part, en utilisant la formule du binôme de Newton, on voit que le polynôme P_n est de degré $2n$, de coefficient dominant $2\mathrm{i}(2n+1)$.

◇ **Réponse :** $P_n = 2\mathrm{i}(2n+1)\displaystyle\prod_{k=1}^{2n}\left(\mathrm{X} - \operatorname{cotan}\frac{k\pi}{2n+1}\right)$.

b) Comme $\operatorname{cotan}\dfrac{(2n+1-k)\pi}{2n+1} = -\operatorname{cotan}\dfrac{k\pi}{2n+1}$, en regroupant les facteurs deux par deux :

$$P_n = 2\mathrm{i}(2n+1)\prod_{k=1}^{n}\left(\mathrm{X}^2 - \operatorname{cotan}^2\frac{k\pi}{2n+1}\right).$$

En remplaçant X par $a\mathrm{i}$, on obtient : $P_n(a\mathrm{i}) = 2(-1)^n\mathrm{i}(2n+1)\displaystyle\prod_{k=1}^{n}\left(a^2 + \operatorname{cotan}^2\frac{k\pi}{2n+1}\right)$.

D'autre part : $P_n(a\mathrm{i}) = (a\mathrm{i}+\mathrm{i})^{2n+1} - (a\mathrm{i}-\mathrm{i})^{2n+1}$.

◇ **Réponse :** $\displaystyle\prod_{k=1}^{n}\left(a^2 + \operatorname{cotan}^2\frac{k\pi}{2n+1}\right) = \frac{(a+1)^{2n+1} - (a-1)^{2n+1}}{2(2n+1)}$.

Par exemple : $\displaystyle\prod_{k=1}^{n}\left(4 + \operatorname{cotan}^2\frac{k\pi}{2n+1}\right) = \frac{3^{2n+1}-1}{2(2n+1)}$.

5.3.34 *a)* ◇ **Réponse :** $P_n = \displaystyle\prod_{k=1}^{n}(\mathrm{X} - \omega_k)$, où $\omega_k = \exp\left(\dfrac{2ik\pi}{n+1}\right)$.

b) Remplacer X par 1.

◇ **Réponse :** $\displaystyle\prod_{k=1}^{n}\sin\frac{k\pi}{n+1} = \frac{n+1}{2^n}$.

5.3.35 *a)* En notant $P_n = (\mathrm{X}^n+1)^n - \mathrm{X}^n$, on a : $P_n(\mathrm{j}) = (\mathrm{j}^n+1)^n - \mathrm{j}^n$. Séparer en cas suivant la congruence de n modulo 3 :

n	$3p$	$3p+1$	$3p+2$
$P_n(\mathrm{j})$	$2^n - 1$	$(-1)^{p+1}\mathrm{j}^2 - \mathrm{j}$	$(-1)^p\mathrm{j}^2 - \mathrm{j}^2$

◇ **Réponse :** $n \equiv 2\ [6]$.

b) En notant $A = X^3 - X^2 + X - 1 = (X-1)(X-i)(X+i)$, qui est scindé et à zéros simples, et $P_n = (X^2 - X + 1)^n - X^{2n} + X^n - 1$, on a : $A | P_n \iff P_n(1) = P_n(i) = 0$, puisque $P_n \in \mathbb{R}[X]$.

D'abord : $P_n(1) = 0$.

- Si $n = 2p$ $(p \in \mathbb{N})$, alors : $P_n(i) = 2((-1)^p - 1)$
- Si $n = 2p+1$ $(p \in \mathbb{N})$, alors $P_n(i) = 0$.

◇ **Réponse :** $n \not\equiv 2$ [4].

c) En notant $Z = \mathbb{U}_{12} - \mathbb{U}_4$, on a $X^8 + X^4 + 1 = \prod_{\omega \in Z} (X - \omega)$, qui est scindé et à zéros simples. Donc :

$$X^8 + X^4 + 1 \,|\, X^{8n} + pX^{4n} + q \iff (\forall \omega \in Z,\ \omega^{8n} + p\omega^{4n} + q = 0) \iff \begin{cases} j^{2n} + pj^n + q = 0 \\ j^{4n} + pj^{2n} + q = 0 \end{cases}$$

$$\iff j^{2n} + pj^n + q = 0 \quad (\text{car } (p,q) \in \mathbb{R}^2).$$

Séparer en trois cas suivant la classe de congruence de n modulo 3.

◇ **Réponse :** $\begin{cases} n \equiv 0\ [3] \\ 1 + p + q = 0 \end{cases}$ ou $\begin{cases} n \not\equiv 0\ [3] \\ p = q = 1 \end{cases}$.

5.3.36 En notant $P = (X-1)(X^n-1)A(X) = (X^n-1)(X^{p+1}-1)$ et $Q = (X-1)(X^n-1)A(X^n) = (X-1)(X^{n(p+1)}-1)$, on a : $A | A(X^n) \iff P | Q$.

- Si $n \wedge (p+1) = 1$, alors : les zéros de P sont 1 (double) et les éléments de $\mathbb{U}_n \cup \mathbb{U}_{p+1} - \{1\}$ (simples)
  les zéros de Q sont 1 (double) et les éléments de $\mathbb{U}_{n(p+1)} - \{1\}$ (simples),

donc, comme $\mathbb{U}_n \cup \mathbb{U}_{p+1} \subset \mathbb{U}_{n(p+1)}$, $P | Q$.

- Si $n \wedge (p+1) \neq 1$, alors P admet au moins un zéro double autre que 1, alors que Q n'admet, comme zéro double, que 1, donc $P \nmid Q$.

◇ **Réponse :** $n \wedge (p+1) = 1$.

5.3.37 Les ensembles $\mathbb{U}_p - \{1\}, \mathbb{U}_q - \{1\}, \mathbb{U}_r - \{1\}$ sont deux à deux disjoints (car $p \wedge q = p \wedge r = q \wedge r = 1$), inclus dans $\mathbb{U}_{pqr} - \{1\}$, donc :

$$(X^p-1)(X^q-1)(X^r-1) = (X-1)^3 \prod_{z \in \mathbb{U}_p \cup \mathbb{U}_q \cup \mathbb{U}_r - \{1\}} (X-z) \,\Big|\, (X-1)^3 \prod_{z \in \mathbb{U}_{pqr} - \{1\}} (X-z) = (X-1)^2 (X^{pqr}-1).$$

5.3.38 $(X^n-1)(X^p-1)$ est scindé et a pour zéros : les éléments de $\mathbb{U}_n \cap \mathbb{U}_p$ (doubles)
les éléments de $(\mathbb{U}_n \cup \mathbb{U}_p) - (\mathbb{U}_n \cap \mathbb{U}_p)$ (simples).

De plus : $\mathbb{U}_n \cap \mathbb{U}_p = \mathbb{U}_{n \wedge p}$ et $\mathbb{U}_n \cup \mathbb{U}_p \subset \mathbb{U}_{n \vee p}$.

5.3.39 Supposons que P admette au moins un zéro z tel que $|z| < \dfrac{1}{M+1}$. Alors :

$$1 = \left| -\sum_{k=1}^{n} a_k z^k \right| \leqslant \sum_{k=1}^{n} |a_k|\, |z|^k \leqslant M \sum_{k=1}^{n} |z|^k < M \sum_{k=1}^{n} \left(\frac{1}{M+1} \right)^k = \frac{M}{M+1} \, \frac{1 - \dfrac{1}{(M+1)^n}}{1 - \dfrac{1}{M+1}} < 1,$$

contradiction.

5.3.40 *a)* On a : $P^{(n-2)} = \frac{n!}{2}X^2 + (n-1)!\,X + (n-2)! = \frac{(n-2)!}{2}\left(n(n-1)X^2 + 2(n-1)X + 2\right)$, qui est un trinôme réel de discriminant réduit : $\Delta' = (n-1)^2 - 2n(n-1) = 1 - n^2 < 0$.

Raisonnons par l'absurde : supposons que les zéros de P soient tous réels. En appliquant le théorème de Rolle et en tenant compte des ordres de multiplicité, on en déduit que les zéros de P' sont aussi tous réels, puis, de proche en proche, que ceux de $P^{(n-2)}$ sont tous réels, contradiction.

b) Se ramener à *a)* en notant $Y = \frac{1}{X}$.

5.3.41 *a)* On a, pour tout x de $]1; +\infty[$:

$$P(x) = (a_n x^n + \ldots + a_{p+1}x^{p+1}) + (a_p x^p + \ldots + a_0) \geqslant a_n x^n - \sum_{i=0}^{p} |a_i| x^i \geqslant a_n x^n - M\sum_{i=0}^{p} x^i$$

$$= a_n x^n - M\,\frac{x^{p+1} - 1}{x - 1}.$$

b) Raisonnons par l'absurde : supposons que P admette au moins un zéro réel tel que : $x > 1 + \left(\frac{M}{a_n}\right)^{\frac{1}{n-p}}$, et donc $x \in]1; \infty[$.

On a alors : $a_n x^n (x-1) = a_n x^{n-p-1}(x-1)x^{p+1} \geqslant a_n (x-1)^{n-p} x^{p+1} > M x^{p+1}$,

d'où, en utilisant *a)* :

$$0 \geqslant a_n x^n (x-1) - M(x^{p+1} - 1) > M, \quad \text{contradiction.}$$

c) Exemple : $n = 10$, $a_n = 6$, $p = 2$, $M = 7$, d'où, pour tout zéro réel x : $x \leqslant 1 + \left(\frac{7}{6}\right)^{\frac{1}{8}} < 2{,}02$.

5.3.42 Raisonnons par l'absurde : supposons que P admette au moins un zéro z tel que

$$|z| < \frac{\sqrt{5} - 1}{2} \; (< 1).$$

1er cas : $n_1 \geqslant 2$

On a : $0 = |P(z)| = |1 + z^{n_1} + z^{n_2} + \ldots + z^{n_N}| \geqslant 1 - \left(|z|^2 + |z|^3 + \ldots + |z|^{N+1}\right)$

$$= 1 - |z|^2\,\frac{1 - |z|^N}{1 - |z|} \geqslant 1 - \frac{|z|^2}{1 - |z|} = \frac{1 - |z| - |z|^2}{1 - |z|}.$$

Mais clairement : $|z| < \frac{\sqrt{5} - 1}{2} \Longrightarrow 1 - |z| - |z|^2 > 0$, d'où une contradiction.

2ème cas : $n_1 = 1$

Considérer $(1 - X)P(X)$ et remarquer qu'il existe $\varepsilon_2, \ldots, \varepsilon_{n_N+1}$ dans $\{-1, 0, 1\}$ tels que :

$$(1 - X)(1 + X + X^{n_2} + \ldots + X^{n_N}) = 1 + \sum_{k=2}^{n_N+1} \varepsilon_k X^{n_N},$$

et le résultat du 1er cas s'applique aussi à ce polynôme.

5.3.43 L'application φ : $]0;\infty[\longrightarrow \mathbb{R}$ est dérivable sur $]0;+\infty[$ et :

$$x \longmapsto \frac{P(x)}{x^n} = 1 - \sum_{k=0}^{n-1} \frac{a_k}{x^{n-k}}$$

$$\forall x \in]0;+\infty[, \varphi'(x) = \sum_{k=0}^{n-1} \frac{(n-k)a_k}{x^{n+1-k}} > 0.$$

Ainsi, φ est strictement croissante sur $]0;+\infty[$. De plus, φ est continue et : $\lim_{0^+} \varphi = -\infty$, $\lim_{+\infty} \varphi = 1$.

Ainsi : $\exists! x_0 \in]0;+\infty[,\ \varphi(x_0) = 0$.

5.3.44 On a, pour tout x de $\mathbb{R}^*$: $\dfrac{P_n(x)}{x^{2n}} = \displaystyle\sum_{k=0}^{2n} (k+1)\left(-\frac{1}{x}\right)^k$.

Considérons $f : \mathbb{R} \longrightarrow \mathbb{R}$ et $g : \mathbb{R} \longrightarrow \mathbb{R}$.
$t \longmapsto \displaystyle\sum_{k=0}^{2n} (k+1)t^k$ $\quad t \longmapsto \displaystyle\sum_{k=0}^{2n+1} t^k$

Il est clair que g est dérivable sur $\mathbb{R}$ et : $\forall t \in \mathbb{R}, g'(t) = f(t)$. Comme : $\forall t \in \mathbb{R} - \{1\}, g(t) = \dfrac{t^{2n+2} - 1}{t - 1}$,

on déduit : $\forall t \in \mathbb{R} - \{1\}, f(t) = \dfrac{(2n+1)t^{2n+2} - (2n+2)t^{2n+1} + 1}{(t-1)^2}$. D'où, pour tout x de $\mathbb{R} - \{-1,0\}$:

$P_n(x) = x^{2n} f\left(-\dfrac{1}{x}\right) = \dfrac{2n+1+(2n+2)x+x^{2n+2}}{(x+1)^2}$.

Etudier les variations de $h : \mathbb{R} \longrightarrow \mathbb{R}$ définie par : $h(x) = 2n + 1 + (2n+2)x + x^{2n+2}$.

Ceci montre : $\forall x \in \mathbb{R} - \{-1\}, h(x) > 0$, d'où : $\forall x \in \mathbb{R} - \{-1,0\}, P_n(x) > 0$.

Enfin, $P_n(-1) > 0$ et $P_n(0) = 1 > 0$.

x	$-\infty$		-1		$+\infty$
$h'(x)$		$-$	0	$+$	
$h(x)$		$\searrow$	0	$\nearrow$	

5.3.45 *1)* Soit P convenant. Notons Z l'ensemble des zéros de P dans $\mathbb{C}$ et supposons $\deg(P) \geqslant 1$.

• Soit $z \in Z$. On a alors $P(z) = 0$ et $P\big((z-1)+1\big) = 0$, d'où, d'après l'hypothèse : $P(z^2+z+1) = 0$ et $P\big((z-1)^2 + (z-1) + 1\big) = 0$, donc : $z^2 + z + 1 \in Z$ et $z^2 - z + 1 \in Z$.

• D'après le théorème de d'Alembert, Z est une partie finie non vide de $\mathbb{C}$. Il existe donc $u \in Z$ tel que : $\forall z \in Z, |z| \leqslant |u|$. En particulier : $|u^2 + u + 1| \leqslant |u|$ et $|u^2 - u + 1| \leqslant |u|$.

Mais : $2|u| = |(u^2+u+1) - (u^2-u+1)| \leqslant |u^2+u+1| + |u^2-u+1| \leqslant 2|u|$, d'où $|u^2+u+1| = |u^2-u+1| = |u|$ et, d'après l'étude du cas d'égalité dans l'inégalité triangulaire dans $\mathbb{C}$, il existe $\lambda \in \mathbb{R}_+$ tel que $u^2 - u + 1 = -\lambda(u^2+u+1)$ (le cas $u^2+u+1=0$ étant par ailleurs d'étude immédiate).

On déduit alors $\lambda = 1$ (car $|\lambda| = 1$ et $\lambda \in \mathbb{R}_+$), puis $u^2 + 1 = 0$.

Ceci prouve $Z \subset \{-i,i\}$.

Comme $P \in \mathbb{R}[X]$, il existe alors $\alpha \in \mathbb{R}^*$ et $n \in \mathbb{N}^*$ tels que : $P = \alpha(X^2+1)^n$.

2) Pour $(\alpha,n) \in \mathbb{R}^* \times \mathbb{N}^*$, en notant $P = \alpha(X^2+1)^n$, on a :

$$P(X^2+X+1) = \alpha\big((X^2+X+1)^2+1\big)^n = \alpha(X^2+1)^n\big((X+1)^2+1\big)^n.$$

d'où : $P(X)P(X+1) = P(X^2+X+1) \iff \alpha^2 = \alpha$.

◇ **Réponse :** $\big\{(X^2+1)^n ; n \in \mathbb{N}\big\} \cup \{0\}$.

5.3.46 Soit $P \in \mathbb{C}[X]$ convenant, tel que $\deg(P) \geqslant 1$.

Notons Z l'ensemble des zéros de P dans $\mathbb{C}$. D'après le théorème de d'Alembert : $Z \neq \varnothing$.

Soit $z \in Z$. On a : $P(z+1)P(z+2) = P(z)P(z+3) = 0$, donc : $z+1 \in Z$ ou $z+2 \in Z$.

Une récurrence immédiate montre alors que, pour tout n de $\mathbb{N}$:

$$z+n \in Z \quad \text{ou} \quad z+n+1 \in \mathbb{Z} \text{ ou} \ldots \text{ou } z+2n \in Z.$$

En particulier, pour tout k de $\mathbb{N}$: $z+2^k-1 \in Z$ ou $z+2^k \in Z$ ou $\ldots$ ou $z+2^{k+1}-2 \in Z$.

Mais les ensembles $\{z+p;\ p \in \{2^k-1, 2^k, \ldots, 2^{k+1}-2\}\}$, $k \in \mathbb{N}$, sont deux à deux disjoints.

Ainsi, Z serait infini, contradiction.

5.3.47 *a)* En notant $B = aX^2+bX+c$, $(a,b,c) \in \mathbb{Q}^3$, on a :

$$\begin{cases} B(1)=1 \\ B(\alpha)=\beta \\ B(\beta)=\alpha \end{cases} \Longleftrightarrow \begin{cases} a+b+c=1 \\ a\alpha^2+b\alpha+c=\beta \\ a\beta^2+b\beta+c=\alpha \end{cases} \Longleftrightarrow \begin{cases} a+b+c=1 \\ a(\alpha+\beta)+b=-1 \\ a\left((\alpha+\beta)^2-2\alpha\beta\right)+(b-1)(\alpha+\beta)+2c=0 \end{cases}$$

D'autre part, $X^3+X-2=(X-1)(X^2+X+2)$, donc $\alpha+\beta=-1$ et $\alpha\beta=2$.

On se ramène ainsi à la résolution de : $\begin{cases} a+b+c=1 \\ -a+b=-1 \\ -3a+1-b+2c=0 \end{cases}$.

◇ **Réponse :** $B = \frac{3}{4}X^2 - \frac{1}{4}X + \frac{1}{2}$.

b) **1re méthode**

Puisque $A = (X-1)(X-\alpha)(X-\beta)$ est scindé et à zéros tous simples, on a, en notant $C = B \circ B - X$:

$$A \mid C \Longleftrightarrow C(1) = C(\alpha) = C(\beta) = 0.$$

Et : $\begin{cases} C(1) = B(B(1)) - 1 = B(1) - 1 = 0 \\ C(\alpha) = B(B(\alpha)) - \alpha = B(\beta) - \alpha = 0 \\ C(\beta) = B(B(\beta)) - \beta = B(\alpha) - \beta = 0. \end{cases}$

2ème méthode

Comme $B = \frac{3}{4}X^2 - \frac{1}{4}X + \frac{1}{2}$, un calcul direct fournit :

$$B \circ B - X = \frac{9}{64}(3X^4 - 2X^3 + 3X^2 - 8X + 4) = \frac{9}{64}(3X-2)(X^3+X-2).$$

5.3.48 *a)* Notons $P = \sum_{k=0}^{N} \alpha_k X^k$, où $N \in \mathbb{N}$, $\alpha_0, \ldots, \alpha_N \in \mathbb{Q}$.

En utilisant la formule du binôme de Newton :

$$P(a-\sqrt{b}) = P(a+\sqrt{b}) + P(a-\sqrt{b}) = \sum_{k=0}^{N} \alpha_k \left((a+\sqrt{b})^k + (a-\sqrt{b})^k\right) \in \mathbb{Q},$$

$$-P(a-\sqrt{b}) = P(a+\sqrt{b}) - P(a-\sqrt{b}) = \sum_{k=0}^{N} \alpha_k \left((a+\sqrt{b})^k - (a-\sqrt{b})^k\right) \in \sqrt{b}\,\mathbb{Q}.$$

Comme $\sqrt{b} \notin \mathbb{Q}$, on a : $\mathbb{Q} \cap (\sqrt{b}\mathbb{Q}) = \{0\}$, d'où $P(a-\sqrt{b}) = 0$.

b) D'après *a)*, $a+\sqrt{b}$ et $a-\sqrt{b}$ sont des zéros de P dans $\mathbb{R}$, distincts (car $b \neq 0$). En notant $P_2 = \left(X-(a+\sqrt{b})\right)\left(X-(a-\sqrt{b})\right) = (X-a)^2 - b^2$, on a donc : P_2 divise P dans $\mathbb{R}[X]$. Comme P_2 et P sont dans $\mathbb{Q}[X]$, il en résulte que P_2 divise P dans $\mathbb{Q}[X]$ (cf. 5.2.2 Rem. p. 157). Il existe donc $Q \in \mathbb{Q}[X]$ tel que : $P = P_2 Q$.

En appliquant *a)* à Q au lieu de P, on a : $P_2 | Q$ dans $\mathbb{Q}[X]$. Il existe donc $P_1 \in \mathbb{Q}[X]$ tel que $\mathbb{Q} = P_2 P_1$, d'où $P = P_1 P_2^2$.

5.3.49 En remplaçant X par $1, j, j^2$, on obtient : $P(1) + Q(1) = 3R(1)$, $P(1) + jQ(1) = 0$, $P(1) + j^2 Q(1) = 0$, d'où $P(1) = Q(1) = 0$, $R(1) = 0$.

5.3.50 *a)* Notons $P = X^{2p} - X^p + 1$.

Puisque $X^2 - X + 1 = (X + j)(X + j^2)$, qui est scindé et a zéros tous simples, on a, dans $\mathbb{C}[X]$:

$$X^2 - X + 1 | P \iff P(-j) = P(-j^2) = 0 \iff P(-j) = 0, \text{ car } P \in \mathbb{R}[X].$$

Et puisque p est impair et non multiple de 3 : $P(-j) = (-j)^{2p} - (-j)^p + 1 = j^{2p} + j^p + 1 = 0$.

Ceci montre : $X^2 - X + 1 | P$ dans $\mathbb{C}[X]$.

Comme $X^2 - X + 1$ et P sont dans $\mathbb{Q}[X]$, il s'ensuit (cf. 5.2.2 Rem. p. 157) : $X^2 - X + 1 | P$ dans $\mathbb{Q}[X]$.

Enfin, comme le coefficient de plus haut degré de $X^2 - X + 1$ est 1, la division euclidienne de P par $X^2 - X + 1$ montre que les coefficients du quotient A sont dans $\mathbb{Z}$.

b) Soient p premier $\geqslant 5$, $k \in \mathbb{N}^*$, $n = kp$. En remplaçant X par 2^k dans *a)*, et comme $A(2^k) \in \mathbb{Z}$, on déduit :

$$(2^k)^2 - 2^k + 1 \mid (2^k)^{2p} - (2^k)^p + 1 = 2^{2n} - 2^n + 1, \text{ dans } \mathbb{Z}.$$

Enfin : • $2^{2k} - 2^k + 1 \geqslant 2$ car $k \geqslant 1$

• $2^{2k} - 2^k + 1 \neq 2^{2kp} - 2^{kp} + 1$ car $p \geqslant 2$.

Exemple : Pour $N = 2^{168} - 2^{84} + 1$, on a $n = 84$, $p = 7$, $k = 12$, et N est multiple de $m = 2^{24} - 2^{12} + 1 = 16\,773\,121$.

5.3.51 Puisque $a, b, c \in \mathbb{Q}$, $P \in \mathbb{Q}[X]$, et que $P(a) = P(b) = P(c) = 2$, le polynôme $P - 2$ est divisible, dans $\mathbb{Q}[X]$, par $(X-a)(X-b)(X-c)$. Comme de plus $P \in \mathbb{Z}[X]$ et que $(X-a)(X-b)(X-c)$ est unitaire, la division euclidienne de P par $(X-a)(X-b)(X-c)$ montre que le quotient est à coefficients dans $\mathbb{Z}$.

Ainsi, il existe $Q \in \mathbb{Z}[X]$ (c'est-à-dire : $Q \in \mathbb{Q}[X]$ et les coefficients de Q sont dans $\mathbb{Z}$) tel que : $P = (X - a)(X - b)(X - c)Q + 2$.

Supposons qu'il existe $x \in \mathbb{Z}$ tel que $P(x) = 3$. On a alors : $(x - a)(x - b)(x - c)Q(x) = 1$. Comme $x - a, x - b, x - c, Q(x)$ sont dans $\mathbb{Z}$, il en résulte que $x - a, x - b, x - c$ sont dans $\{-1, 1\}$, donc ne sont pas deux à deux distincts, contradiction.

5.3.52 Raisonnons par l'absurde : supposons qu'il existe $a, b, c \in \mathbb{Z}$; deux à deux distincts, et $P \in \mathbb{Z}[X]$, tels que : $P(a) = b$, $P(b) = c$, $P(c) = a$. Puisque $P(a) - b = 0$, il existe $Q \in \mathbb{Q}[X]$ tel que : $P - b = (X - a)Q$. La division euclidienne de $P - b$ par $X - a$ (qui est unitaire) montre alors que les coefficients de Q sont tous dans $\mathbb{Z}$. En remplaçant X par b : $c - b = (b - a)Q(b)$, et $Q(b) \in \mathbb{Z}$, donc : $b - a | c - b$.

En permutant circulairement a, b, c, on obtient : $b - a \mid c - b$, $c - b \mid a - c$, $a - c \mid b - a$, d'où : $|b - a| = |a - c| = |c - b|$.

• Si $b - a = c - a$, alors $b = c$, contradiction.

• Donc, $b - a = a - c$, et de même $a - c = c - b$. On en déduit $a = b = c$, contradiction.

5.3.53 Raisonnons par l'absurde : supposons que $P = X^3 + X + 3$ ne soit pas irréductible dans $\mathbb{Q}[X]$. Il existe alors $A, B \in \mathbb{Q}[X]$ tels que : $P = AB$, $1 \leqslant \deg(A) \leqslant 2$, $1 \leqslant \deg(B) \leqslant 2$. À l'ordre près : $\deg(A) = 1$ et $\deg(B) = 2$.

Donc P admet au moins un zéro dans $\mathbb{Q}$.

Soit $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que : $p \wedge q = 1$ et $P\left(\frac{p}{q}\right) = 0$. On a alors : $p^3 + pq^2 + 3q^3 = 0$, d'où :

$$\begin{cases} p|3q^3, & \text{donc } (p \wedge q = 1) : \ p|3 \\ q|p^3, & \text{donc } (p \wedge q = 1) : \ q = 1. \end{cases}$$

Ainsi : $\frac{p}{q} \in \{-3, -1, 1, 3\}$.

On vérifie aisément que ces quatre rationnels ne sont pas zéros de P.

Finalement : P est irréductible dans $\mathbb{Q}[X]$.

5.3.54 Notons, pour $i \in \{0, \ldots, n\}$, $L_i = \prod_{\substack{0 \leqslant k \leqslant n \\ k \neq i}} \frac{X - k}{i - k}$ (polynômes d'interpolation de Lagrange sur les points 0, 1, ..., n, cf. 5.3.1 Exemple p. 169).

D'après 5.3.1 Exemple p. 169, on a : $P = \sum_{i=0}^{n} P(i) L_i$, d'où : $\forall a \in \mathbb{Z}, \ P(a) = \sum_{i=0}^{n} P(i) L_i(a)$.

Pour $(i,a) \in \{0, \ldots, n\} \times \mathbb{Z}$, notons : $u_{i,a} = \prod_{0 \leqslant k \leqslant i-1} \frac{a-k}{i-k}$ et $v_{i,a} = \prod_{i+1 \leqslant k \leqslant n} \frac{a-k}{i-k}$

(avec la convention : un produit indexé par $\varnothing$ vaut 1); ainsi : $L_i(a) = u_{i,a} v_{i,a}$.

- Si $0 \leqslant a \leqslant n$, alors $L_i(a) = \begin{cases} 0 & \text{si } i \neq a \\ 1 & \text{si } i = a \end{cases}$, donc $L_i(a) \in \mathbb{Z}$.

- Si $a > n$: $u_{i,a} = \frac{a(a-1)\ldots(a-i+1)}{i(i-1)\ldots 1} = C_a^i \in \mathbb{Z}$, et $v_{i,a} = \frac{(a-i-1)(a-i-2)\ldots(a-n)}{(-1)(-2)\ldots(i-n)}$

$$= \frac{(a-n)(a-n-1)\ldots(a-i-1)}{(-1)^{n-i}(n-i)!} = (-1)^{n-i} C_{a-n}^{a-i} \in \mathbb{Z}.$$

- Si $a < 0$: $u_{i,a} = \frac{a(a-1)\ldots(a-i+1)}{i(i-1)\ldots 1} = \frac{(-1)^i |a|(|a|+1)\ldots(|a|+i-1)}{i!} = (-1)^i C_{|a|+i-1}^{i} \in \mathbb{Z}$

et $v_{i,a} = \frac{(a-i-1)(a-i-2)\ldots(a-n)}{(-1)^{n-i}(n-i)!} = \frac{(-1)^i (|a|+i+1)(|a|+i+2)\ldots(|a|+n)}{(-1)^{n-i}(n-i)!}$

$$= (-1)^n C_{|a|+n}^{n-i} \in \mathbb{Z}.$$

Ainsi : $\forall i \in \{0, \ldots, n\}, \ L_i(a) \in \mathbb{Z}$.

Comme $P(a) = \sum_{i=0}^{n} P(i) L_i(a)$, on en déduit $P(a) \in \sum_{i=0}^{n} P(i)\mathbb{Z} = \operatorname{pgcd}\big((P(i))_{0 \leqslant i \leqslant n}\big)\mathbb{Z}$, donc $\operatorname{pgcd}\big((P(i))_{0 \leqslant i \leqslant n}\big) \,|\, P(a)$.

5.3.55 Raisonnons par l'absurde : supposons qu'il existe $A, B \in \mathbb{Z}[X]$ tels que :

$$P = AB, \ 1 \leqslant \deg(A) < n, \ 1 \leqslant \deg(B) < n.$$

On a alors, pour tout k de $\{1, \ldots, n\}$: $A(a_k)B(a_k) = P(a_k) = -1$, d'où, puisque $A(a_k)$ et $B(a_k)$ sont des entiers : $\begin{cases} A(a_k) = 1 \\ B(a_k) = -1 \end{cases}$ ou $\begin{cases} A(a_k) = -1 \\ B(a_k) = 1 \end{cases}$, et donc $A(a_k) + B(a_k) = 0$.

Ceci montre que $A + B$ s'annule en $a_1, \ldots, a_n$ qui sont deux à deux distincts.

Comme d'autre part : $\deg(A+B) \leqslant \operatorname{Max}\big(\deg(A), \deg(B)\big) < n$, il en résulte : $A + B = 0$.

Mais alors $P = AB = -A^2 \leqslant 0$, ce qui contredit : $P(x) \xrightarrow[x \to +\infty]{} +\infty$.

5.3.56 *a)* Remarquer que 3 est zéro.

◇ **Réponse :** $(X-3)^2(X+1)$.

b) Dans $\mathbb{C}[X]$: $(X^2-X+2)^2+(X-2)^2=\big(X^2-X+2+i(X-2)\big)\big(X^2-X+2-i(X-2)\big)$
$=\big(X^2+(-1+i)X+(2-2i)\big)\big(X^2-(1+i)X+(2+2i)\big)$.
Les zéros de $X^2+(-1+i)X+(2-2i)$ sont $-2i$ et $1+i$ (simples). D'où :

$$(X^2-X+2)^2+(X-2)^2=(X-1-i)(X+2i)(X-1+i)(X-2i)=\big((X-1)^2+1\big)(X^2+4).$$

◇ **Réponse :** $(X^2-2X+2)(X^2+4)$.

c) **1re méthode**
Les racines sixièmes de 1 dans $\mathbb{C}$ étant $1, j, j^2, -1, -j, -j^2$, on a, dans $\mathbb{C}[X]$:

$$\begin{aligned}(X+1)^6-X^6&=(X+1-X)(X+1+j^2X)(X+1-jX)(X+1+X)(X+1-j^2X)(X+1+jX)\\&=(2X+1)\big(-jX+1)(-j^2X+1)\big)\big((1-j)X+1\big)\big((1-j^2)X+1\big).\end{aligned}$$

2ème méthode

$$\begin{aligned}&(X+1)^6-X^6=\big((X+1)^3-X^3\big)\big((X+1)^3+X^3\big)\\&=\big((X+1)-X\big)\big((X+1)^2+(X+1)X+X^2\big)\big((X+1)+X\big)\big((X+1)^2)-(X+1)X+X^2\big).\end{aligned}$$

◇ **Réponse :** $(2X+1)(X^2+X+1)(3X^2+3X+1)$.

d) Les éventuels zéros multiples sont les solutions de : $\begin{cases}z^5-7z^3-2z^2+12z+8=0\\5z^4-21z^2-4z+12=0\end{cases}$.

Remarquer que -1 et 2 sont solutions.

◇ **Réponse :** $(X-2)^2(X+1)^2(X+2)$.

e) D'abord : $X^5+1=(X+1)(X^4-X^3+X^2-X+1)$.
L'équation $z^4-z^3+z^2-z+1=0$ (d'inconnue $z\in\mathbb{C}$) est une équation réciproque (cf. exercice 5.3.12 p. 174).

◇ **Réponse :** $(X+1)\left(X^2-\dfrac{1+\sqrt{5}}{2}X+1\right)\left(X^2-\dfrac{1-\sqrt{5}}{2}X+1\right)$.

f) Remarquer que le polynôme proposé est divisible par X^2+3.

◇ **Réponse :** $(X^2+3)\left(X^2-\sqrt{2\sqrt{3}-1}\,X+\sqrt{3}\right)\left(X^2+\sqrt{2\sqrt{3}-1}\,X+\sqrt{3}\right)$.

g) Cf. exercice 5.3.12 p. 174, équations réciproques.

◇ **Réponse :** $(X+1)^2\left(X^2+\dfrac{\sqrt{5}+1}{2}X+1\right)\left(X^2-\dfrac{\sqrt{5}-1}{2}X+1\right)$.

h) $X^8+X^4+1=(X^4+1)^2-X^4=(X^4+X^2+1)(X^4-X^2+1)=\big((X^2+1)^2-X^2\big)\big((X^2+1)^2-3X^2\big)$.

◇ **Réponse :** $(X^2+X+1)(X^2-X+1)(X^2+\sqrt{3}X+1)(X^2-\sqrt{3}X+1)$.

i) $X^{12}+1=(X^4+1)(X^8-X^4+1)$, puis comme en *h)*.

◇ **Réponse :** $(X^2-X\sqrt{2}+1)(X^2+X\sqrt{2}+1)(X^2-\sqrt{2+\sqrt{3}}\,X+1)(X^2+\sqrt{2+\sqrt{3}}\,X+1)$
$(X^2-\sqrt{2-\sqrt{3}}\,X+1)(X^2+\sqrt{2-\sqrt{3}}\,X+1)$.

j) $X^{2n}-2\cos a\,X^n+1=(X^n-e^{ia})(X^n-e^{-ia})=\prod_{k=0}^{n-1}\left(X-\omega_k e^{\frac{ia}{n}}\right)\prod_{k=0}^{n-1}\left(X-\omega_k e^{-\frac{ia}{n}}\right)$,

où $\omega_k=\exp\left(\dfrac{2ik\pi}{n}\right)$, $k\in\mathbb{Z}$.

En groupant les facteurs :

$$X^{2n}-2\cos a\,X^n+1=\prod_{k=0}^{n-1}\left(\left(X-\omega_k e^{\frac{ia}{n}}\right)\left(X-\omega_{n-k}e^{-\frac{ia}{n}}\right)\right)=\prod_{k=0}^{n-1}\left(X^2-2\cos\frac{a+2k\pi}{n}X+1\right),$$

et, pour tout k de $\{0,\dots,n-1\}$, le discriminant du trinôme $X^2-2\cos\dfrac{a+2k\pi}{n}X+1$ vaut $-\sin^2\dfrac{a+2k\pi}{n}$, qui est <0 puisque $a\notin\pi\mathbb{Z}$.

◇ **Réponse :** $\displaystyle\prod_{k=0}^{n-1}\left(X^2-2\cos\frac{a+2k\pi}{n}X+1\right)$.

5.3.57 Les diviseurs irréductibles unitaires de P (dans $\mathbb{R}[X]$) sont :

- les $X-z_k$ pour les k tels que $z_k\in\mathbb{R}$
- les $X^2-2\text{Ré}(z_k)X+|z_k|^2$ pour les k tels que $z_k\in\mathbb{C}-\mathbb{R}$.

Comme $(\forall k,\ \text{Ré}(z_k)\leqslant 0)$, les polynômes $X-z_k$ et $X^2-2\text{Ré}(z_k)X+|z_k|^2$ sont tous à coefficients tous $\geqslant 0$, donc les coefficients de P sont tous du même signe.

5.3.58

- Examiner d'abord le cas où $\deg(P)\leqslant 0$.
- Soit P convenant tel que $\deg(P)\geqslant 1$. Puisque l'application polynomiale P est continue sur l'intervalle $\mathbb{R}$ et non constante, l'ensemble $P(\mathbb{R})$ est un intervalle de $\mathbb{R}$ (théorème des valeurs intermédiaires, Tome 1, 4.3.3 Th.) non vide ni réduit à un point. En particulier, $P(\mathbb{R})$ est infini.

Mais, d'après l'hypothèse : $\forall x\in\mathbb{R},\ P(P(x))=(P(x))^k$, donc : $\forall y\in P(\mathbb{R}),\ P(y)=y^k$.

Ainsi, $P-X^k$ s'annule en une infinité de réels, donc $P-X^k=0$.

Réciproquement, X^k convient à l'évidence.

◇ **Réponse :** $\{(1,\lambda);\ \lambda\in\mathbb{R}\}\cup\{(k,1);\ k\in\mathbb{N}\}\cup\{(k,0);\ k\in\mathbb{N}-\{0,1\}\}\cup\{(k,X^k);\ k\in\mathbb{N}\}$.

5.3.59 Considérons $Q=1+\dfrac{X}{1}+\dfrac{X(X-1)}{2}+\dots+\dfrac{X(X-1)\dots(X-n+1)}{n!}$.

Puisque Q est de degré n et que : $\forall k\in\{0,\dots,n\},\ Q(k)=\displaystyle\sum_{i=0}^{k}C_k^i=2^k$, on a : $Q=P$.

Alors : $P(n+1)=Q(n+1)=\displaystyle\sum_{i=0}^{n}C_{n+1}^i=2^{n+1}-1$.

◇ **Réponse :** $2^{n+1}-1$.

5.3.60 Considérons $Q = XP - 1$.

On a : $\forall k \in \{1,\dots,n+1\},\ Q(k) = kP(k) - 1 = 0$.

Comme $\deg(Q) \leqslant n+1$, il existe $\lambda \in \mathbb{R}$ tel que : $Q = \lambda \prod_{k=1}^{n+1}(X-k)$.

Puisque $Q(0) = -1$, on déduit $\lambda = \dfrac{(-1)^n}{(n+1)!}$. Ainsi : $Q = \dfrac{(-1)^n}{(n+1)!}\prod_{k=1}^{n+1}(X-k)$.

En particulier : $Q(n+2) = \dfrac{(-1)^n}{(n+1)!}(n+1)! = (-1)^n$.

◇ **Réponse :** $\dfrac{1+(-1)^n}{n+2}$.

5.3.61 **1er cas : n pair**

Considérons $Q = P - P(n+1-X)$.

Il est clair que $\deg(Q) \leqslant n-1$ et : $\forall k \in \{1,\dots,n\},\ Q(k) = \dfrac{1}{C_{n+1}^k} - \dfrac{1}{C_{n+1}^{n+1-k}} = 0$.

On en déduit $Q = 0$, d'où : $P(0) - P(n+1) = Q(0) = 0$, $P(n+1) = P(0) = 1$.

2ème cas : n impair

Considérons $Q = (X+1)P - (n+1-X)P(n-X)$.

Il est clair que $\deg(Q) \leqslant n$ et : $\forall k \in \{0,\dots,n\},\ Q(k) = \dfrac{k+1}{C_n^k} - \dfrac{n+1-k}{C_{n+1}^{n-k}} = 0$.

On en déduit $Q = 0$; en particulier $Q(-1) = 0$, d'où $P(n+1) = 0$.

◇ **Réponse :** $\begin{cases} 1 & \text{si } n \text{ est pair} \\ 0 & \text{si } n \text{ est impair.} \end{cases}$

5.3.62 L'application $\varphi : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & P(x) - Q(x) \end{array}$ est continue sur l'intervalle $\mathbb{R}$ et ne s'annule en aucun réel. D'après le théorème des valeurs intermédiaires (Tome 1, 4.3.3 Th.), il en résulte, par exemple : $\forall x \in \mathbb{R},\ P(x) > Q(x)$. Alors : $\forall x \in \mathbb{R},\ P(P(x)) > Q(P(x)) = P(Q(x)) > Q(Q(x))$.

Remarque : le résultat est valable en remplaçant P, Q par des applications continues.

5.3.63 On a : $(C+A)(C-A) = B^2$.

Soit z_0 un zéro de $C + A$.

Si z_0 est zéro de $C - A$, alors $C(z_0) + A(z_0) = C(z_0) - A(z_0) = 0$, donc $C(z_0) = A(z_0) = 0$, puis $(B(z_0))^2 = 0$, et $X - z_0$ divise A, B, C, contradiction.

Ainsi, l'ordre de multiplicité de z_0 dans $C + A$ est le même que dans B^2, donc est pair.

De même pour $C - A$, $C + B$, $C - B$.

5.3.64 Il existe $\lambda \in \mathbb{R}^*$ tel que $P = \lambda \prod_{k=1}^{n}(X - x_k)$. On a : $|P'(x_1)| = |\lambda| \prod_{k=2}^{n} |x_1 - x_k|$, et, pour tout k de $\{1,\dots,n\}$: $|x_1 - x_k| \leqslant |x_1 - x| + |x - x_k| \leqslant 2|x - x_k|$, d'où

$$|P'(x_1)|\,|x - x_1| \leqslant |\lambda| 2^{n-1} \prod_{k=1}^{n} |x - x_k| = 2^{n-1}|P(x)|.$$

5.3.65 D'après le théorème de d'Alembert, P est scindé sur $\mathbb{C}$; en notant $n = \deg(P) \geqslant 2$, il existe $\lambda \in \mathbb{C}^*, z_1, \ldots, z_n \in \mathbb{C}$ tels que : $P = \lambda \prod_{k=1}^{n} (X - z_k)$.

1) Si $z_1, \ldots, z_n$ ne sont pas tous égaux, alors il existe $(k,l) \in \{1, \ldots, n\}^2$ tel que $z_k \neq z_l$, et $P(z_k) = P(z_l) = 0$, donc $\widetilde{P}$ n'est pas injective.

2) Si $z_1 = \ldots = z_n$, considérons $Q = P + 1$, qui est de degré n. Les zéros de Q sont tous simples car, pour tout z de $\mathbb{C}$:

$$Q'(z) = 0 \iff \lambda n (z - z_1)^{n-1} = 0 \iff z = z_1 \implies Q(z) = 1 \neq 0.$$

On peut donc appliquer le *1)* à Q au lieu de P : Q n'est pas injective. Il en résulte, puisque $P = Q - 1$, que P n'est pas injective.

5.3.66 *1)* **Cas $n = 1$**

Notons $Q = a_0 P + a_1 P'$, $\gamma = \dfrac{a_0}{a_1}$, $P = \lambda \prod_{k=1}^{N} (X - x_k)^{\alpha_k}$, où $\lambda \in \mathbb{R}^*$, $N \in \mathbb{N}^*$, $x_1, \ldots, x_N \in \mathbb{R}$, $x_1 < \ldots < x_N$, $\alpha_1, \ldots, \alpha_N \in \mathbb{N}^*$.

L'application $f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \mathrm{e}^{\gamma x} P(x) \end{array}$ est dérivable sur $\mathbb{R}$ et : $\forall x \in \mathbb{R},\ f'(x) = \dfrac{\mathrm{e}^{\gamma x}}{a_1} Q(x)$.

En supposant $\gamma > 0$, par exemple, puisque $\lim_{-\infty} f = f(x_1) = \ldots = f(x_N) = 0$, le théorème de Rolle (généralisé) montre que f' s'annule en au moins N réels $y_1, \ldots, y_N$ tels que :

$$y_1 < x_1 < y_2 < x_2 < \ldots < y_N < x_N.$$

D'autre part, pour tout k de $\{1, \ldots, n\}$ tel que $\alpha_k \geqslant 2$, P' admet x_k pour zéro d'ordre $\alpha_k - 1$, donc Q aussi. Comme : $N + \sum\limits_{\substack{1 \leqslant k \leqslant N \\ \alpha_k \geqslant 2}} (\alpha_k - 1) = N + \sum\limits_{1 \leqslant k \leqslant N} (\alpha_k - 1) = N + (n - N) = n = \deg(Q)$, il en résulte que Q est scindé sur $\mathbb{R}$.

Le cas $\lambda = 0$ (pour lequel $\deg(Q) = n - 1$) se traite de façon analogue.

2) **Cas général**

Notons $u_1, \ldots, u_n$ les zéros de A et, pour $k \in \{1, \ldots, n\}$, $T_k : \begin{array}{ccc} \mathbb{R}[X] & \longrightarrow & \mathbb{R}[X] \\ M & \longmapsto & M' - u_k M \end{array}$.

On a, par exemple, pour tout M de $\mathbb{R}[X]$:

$$T_2 \circ T_1(M) = (M' - u_1 M)' - u_2 (M' - u_1 M) = M'' - (u_1 + u_2) M' + u_1 u_2 M.$$

Il est alors clair (par récurrence) que, en notant $\sigma_1, \ldots, \sigma_n$ les fse de $u_1, \ldots, u_n$:

$$T_n \circ \ldots \circ T_1(M) = M^{(n)} - \sigma_1 M^{(n-1)} + \ldots + (-1)^n \sigma_n M = \frac{1}{a_n} \sum_{k=0}^{n} a_k M^{(k)}.$$

Comme P est scindé sur $\mathbb{R}$, d'après le cas $n = 1$, $T_1(P)$ est scindé sur $\mathbb{R}$, puis, de proche en proche, $T_n \circ \ldots \circ T_1(P)$ est scindé sur $\mathbb{R}$.

5.4.1 On a : $\sum\limits_{k=0}^{n} X^k = \dfrac{1 - X^{n+1}}{1 - X}$, d'où, par dérivation :

$$\sum_{k=0}^{n-1} (k+1) X^k = \frac{nX^{n+1} - (n+1)X^n + 1}{(X-1)^2} = \frac{nX^n \left(X - \left(1 + \dfrac{1}{n}\right)\right) + 1}{(X-1)^2}. \text{ Donc : } P_n\left(1 + \frac{1}{n}\right) = n^2.$$

5.4.2 La fraction 0 n'est pas solution.

Si $F \neq 0$ et $F^2 = X$, alors $\deg(F) \in \mathbb{Z}$ et $2\deg(F) = 1$, contradiction.

5.4.3 D'après le théorème de d'Alembert, P est scindé sur $\mathbb{C}$; il existe $\lambda \in \mathbb{C}^*$, $z_1, \ldots, z_n \in \mathbb{C}$ tels que : $P = \lambda \prod_{k=1}^{n} (X - z_k)$.

On a alors : $\dfrac{P'}{P} = \displaystyle\sum_{k=1}^{n} \frac{1}{X - z_k}$, d'où : $-\dfrac{P'(-1)}{P(-1)} = \displaystyle\sum_{k=1}^{n} \frac{1}{1 + z_k}$.

Ainsi : $\dfrac{n}{2} + \dfrac{P'(-1)}{P(-1)} = \displaystyle\sum_{k=1}^{n} \left(\frac{1}{2} - \frac{1}{1 + z_k} \right) = \frac{1}{2} \sum_{k=1}^{n} \frac{z_k - 1}{z_k + 1}$.

On a, pour tout k de $\{1, \ldots, n\}$: $\dfrac{z_k - 1}{z_k + 1} = \dfrac{(z_k - 1)(\overline{z_k} + 1)}{|z_k + 1|^2}$, d'où $\text{Ré}\left(\dfrac{z_k - 1}{z_k + 1} \right) = \dfrac{|z_k|^2 - 1}{|z_k + 1|^2}$.

Comme $\dfrac{n}{2} + \dfrac{P'(-1)}{P(-1)}$ est réel, on déduit : $\dfrac{1}{2} \displaystyle\sum_{k=1}^{n} \frac{|z_k|^2 - 1}{|z_k + 1|^2} = \frac{n}{2} + \frac{P'(-1)}{P(-1)} \geqslant 0$.

Si $(\forall k \in \{1, \ldots, n\},\ |z_k| < 1)$, alors $\dfrac{1}{2} \displaystyle\sum_{k=1}^{n} \frac{|z_k|^2 - 1}{|z_k + 1|^2} < 0$, contradiction.

Ceci montre que P admet au moins un zéro de module $\geqslant 1$.

5.4.4 ◇ **Réponses :**

a) $\dfrac{1}{X^3} - \dfrac{1}{X} + \dfrac{1}{(X-1)^4} - \dfrac{1}{(X-1)^2} + \dfrac{1}{X-1}$

b) $\dfrac{2}{(X-1)^3} + \dfrac{1}{(X-1)^2} + \dfrac{3}{X-1} - \dfrac{2}{(X+1)^3} + \dfrac{1}{(X+1)^2} - \dfrac{3}{X+1}$

c) $\dfrac{-3}{(X+1)^4} + \dfrac{2}{(X-1)^3}$.

5.4.5 ◇ **Réponses :**

a) $X^2 - 6X + 18 + \dfrac{15}{(X^2 + 2X + 2)^3} + \dfrac{32X}{(X^2 + 2X + 2)^2} + \dfrac{-32X - 40}{X^2 + 2X + 2}$

b) $\dfrac{\frac{1}{2}}{X^2 - \sqrt{2}X + 1} + \dfrac{\frac{1}{2}}{X^2 + \sqrt{2}X + 1}$

c) $\dfrac{\frac{1}{2}X - \frac{\sqrt{2}}{4}}{X^2 - \sqrt{2}X + 1} + \dfrac{\frac{1}{2}X + \frac{\sqrt{2}}{4}}{X^2 + \sqrt{2}X + 1}$.

d) $\dfrac{\frac{1}{2}X + \frac{1}{2}}{X^2 + X + 1} + \dfrac{-\frac{1}{2}X + \frac{1}{2}}{X^2 - X + 1}$

e) $\dfrac{1}{X-1} + \dfrac{-\frac{2\sqrt{3}+3}{6}X + \frac{3+\sqrt{3}}{6}}{X^2 - \sqrt{3}X + 1} + \dfrac{\frac{2\sqrt{3}-3}{6}X + \frac{3-\sqrt{3}}{6}}{X^2 + \sqrt{3}X + 1}$

f) $\dfrac{\frac{1}{3}X}{X^2+2X+3}+\dfrac{-\frac{2}{3}X+\frac{1}{3}}{2X^2+3X+4}$

g) $\dfrac{1}{X^3}-\dfrac{1}{X}+\dfrac{X+1}{(X^2+1)^2}+\dfrac{2X-1}{X^2+1}$

h) $X+3+\dfrac{1}{(X+1)^2}+\dfrac{2}{X+1}+\dfrac{2X+1}{X^2+X+1}$

i) $\dfrac{X-1}{(X^2+1)^2}+\dfrac{1}{X^2+1}+\dfrac{X+1}{(X^2+X+1)^2}+\dfrac{-1}{X^2+X+1}$

j) Remarquer : $\left(\dfrac{X^2}{X^2+1}\right)^n=\left(1-\dfrac{1}{X^2+1}\right)^n$.

◇ **Réponse :** $\displaystyle\sum_{k=0}^{n}(-1)^k C_n^k\frac{1}{(X^2+1)^k}$.

5.4.6 Une DES fournit : $\dfrac{3X^2-1}{(X-1)^2X^2(X+1)^2}=\dfrac{\frac{1}{2}}{(X-1)^2}-\dfrac{1}{X^2}+\dfrac{\frac{1}{2}}{(X+1)^2}$.

D'où, pour tout N de $\mathbb{N}$ tel que $N\geqslant 2$:

$$\begin{aligned}\sum_{n=2}^{N}\frac{3n^2-1}{(n-1)^2n^2(n+1)^2}&=\frac{1}{2}\sum_{n=2}^{N}\frac{1}{(n-1)^2}-\sum_{n=2}^{N}\frac{1}{n^2}+\frac{1}{2}\sum_{n=2}^{N}\frac{1}{(n+1)^2}\\&=\frac{1}{2}\sum_{n=1}^{N-1}\frac{1}{n^2}-\sum_{n=2}^{N}\frac{1}{n^2}+\frac{1}{2}\sum_{n=3}^{N+1}\frac{1}{n^2}\\&=\frac{1}{2}\left(1+\frac{1}{4}\right)-\left(\frac{1}{4}+\frac{1}{N^2}\right)+\frac{1}{2}\left(\frac{1}{N^2}+\frac{1}{(N+1)^2}\right).\end{aligned}$$

◇ **Réponse :** $\dfrac{3}{8}-\dfrac{2N+1}{2N^2(N+1)^2}$.

5.4.7 Une DES fournit : $\dfrac{X^3+2}{(X^2-1)^2}=\dfrac{\frac{3}{4}}{(X-1)^2}+\dfrac{\frac{1}{4}}{(X+1)^2}+\dfrac{1}{X+1}$.

D'où : $\displaystyle\sum_{k=1}^{4}\frac{z_k^3+2}{(z_k^2-1)^2}=\frac{3}{4}u+\frac{1}{4}v+w$, où : $u=\sum_{k=1}^{4}\frac{1}{(z_k-1)^2}$, $v=\sum_{k=1}^{4}\frac{1}{(z_k+1)^2}$, $w=\sum_{k=1}^{4}\frac{1}{z_k+1}$.

Notons $P=X^4-X^3+1$.

• On a : $\dfrac{P'}{P}=\displaystyle\sum_{k=1}^{4}\frac{1}{X-z_k}$, d'où $w=-\dfrac{P'(-1)}{P(-1)}=\dfrac{7}{3}$.

• Puis, en dérivant : $\dfrac{P''P-P'^2}{P^2}=-\displaystyle\sum_{k=1}^{4}\frac{1}{(X-z_k)^2}$,

d'où : $u=\dfrac{(P'(1))^2-P(1)P''(1)}{(P(1))^2}=-5$ et $v=\dfrac{(P'(-1))^2-P(-1)P''(-1)}{(P(-1))^2}=-\dfrac{5}{9}$.

◇ **Réponse :** $-\dfrac{14}{9}$.

5.4.8 *a)* ◇ **Réponse :**

$$\frac{1}{16}\left(\frac{2}{(X-1)^3}-\frac{3}{(X-1)^2}+\frac{3}{X-1}-\frac{2}{(X+1)^3}-\frac{3}{(X+1)^2}-\frac{3}{X+1}\right).$$

b) D'après *a)* : $\dfrac{16}{(X-1)^3(X+1)^3}=\dfrac{2-3(X-1)+3(X-1)^2}{(X-1)^3}+\dfrac{-2-3(X+1)-3(X+1)^2}{(X+1)^3}$.

◇ **Réponse :** $U=\dfrac{1}{16}(8-9X+3X^2)$, $V=-\dfrac{1}{16}(8+9X+3X^2)$.

5.4.9 Une DES fournit, pour $k\in\{0,\dots,n-1\}$:

$$\frac{a^k(X+a^{k+1})}{(X-a^k)(X-a^{k+1})(X-a^{k+2})}=\frac{1}{(1-a)^2}\left(\frac{1}{X-a^k}-\frac{2}{X-a^{k+1}}+\frac{1}{X-a^{k+2}}\right).$$

On déduit :

$$\begin{aligned}(1-a^2)F_n&=\sum_{k=0}^{n-1}\frac{1}{X-a^k}-2\sum_{k=1}^{n}\frac{1}{X-a^k}+\sum_{k=2}^{n+1}\frac{1}{X-a^k}\\&=\left(\frac{1}{X-1}+\frac{1}{X-a}\right)-2\left(\frac{1}{X-a}+\frac{1}{X-a^n}\right)+\left(\frac{1}{X-a^n}+\frac{1}{X-a^{n+1}}\right).\end{aligned}$$

◇ **Réponse :** $\dfrac{1}{(1-a)^2}\left(\dfrac{1}{X-1}-\dfrac{1}{X-a}-\dfrac{1}{X-a^n}+\dfrac{1}{X-a^{n+1}}\right)$.

5.4.10 Notons $Q=\prod_{k=0}^{n-1}(X-\omega_k)=X^n-1$, $F_p=\sum_{k=0}^{n-1}\dfrac{\omega_k^p}{X-\omega_k}$, $P=QF_p$; on a donc :

$$P\in\mathbb{C}[X]\quad\text{et}\quad\deg(P)<n.$$

D'après 5.4.2 *2) a)* Prop. 2 p. 197, pour tout k de $\{0,\dots,n-1\}$: $\omega_k^p=\dfrac{P(\omega_k)}{Q'(\omega_k)}=\dfrac{P(\omega_k)}{n\omega_k^{n-1}}=\dfrac{\omega_k P(\omega_k)}{n}$,

d'où : $\forall k\in\{0,\dots,n-1\}$, $P(\omega_k)=n\omega_k^{p-1}$.

• Si $p\in\{1,\dots,n-1\}$, alors le polynôme $P-nX^{p-1}$, de degré $\leqslant n-1$, s'annule en n complexes deux à deux distincts (les ω_k) donc est nul, d'où $P=nX^{p-1}$.

• Si $p=0$, le même raisonnement s'applique à $P-nX^{n-1}$.

◇ **Réponse :** $\begin{cases}\dfrac{nX^{n-1}}{X^n-1} & \text{si } p=0\\[2mm] \dfrac{nX^{p-1}}{X^n-1} & \text{si } p\in\{1,\dots,n-1\}.\end{cases}$

5.4.11 *a)* Il s'agit de la DES de $\dfrac{P}{(X-a)(X-b)(X-c)}$.

b) Choisir $P=X^2$ dans le résultat de *a)*, puis remplacer X par $\dfrac{a+b+c}{2}$.

◇ **Réponse :** $\dfrac{(a+b+c)^2}{(b+c-a)(c+a-b)(a+b-c)}$.

5.4.12 La détermination des pôles et de la partie entière nécessite la séparation en deux cas suivant la parité de n.

1^er^ cas : n pair

Les pôles de F_n sont les $x_k = \tan\left(\frac{\pi}{2n} + \frac{k\pi}{n}\right)$, $k \in \{0,\dots,n-1\}$, tous simples, et la partie entière est nulle (cf. Tome 1, 2.5.1). Il existe donc $\lambda_0,\dots,\lambda_{n-1} \in \mathbb{R}$ tels que : $F_n = \sum_{k=0}^{n-1} \frac{\lambda_k}{X - x_k}$.

Soit $k \in \{0,\dots,n-1\}$. On a : $\lambda_k = \lim_{x \to x_k} \big((x - x_k)F_n(x)\big)$. Les applications $C_n, S_n : \mathbb{R} \longrightarrow \mathbb{R}$ définies par $\forall x \in \mathbb{R}$, $\big(C_n(x) = \cos(n \operatorname{Arctan} x)$, $S_n(x) = \sin(n \operatorname{Arctan} x)\big)$ sont dérivables sur $\mathbb{R}$ et, pour tout x de $\mathbb{R} - \{x_k;\ 0 \leqslant k \leqslant n-1\}$: $(x - x_k)F_n(x) = S_n(x)\left(\frac{C_n(x) - C_n(x_k)}{x - x_k}\right)^{-1}$,

d'où, puisque $C_n'(x_k) = -\frac{n}{1 + x_k^2} S_n(x_k) \neq 0$: $(x - x_k)F_n(x) \xrightarrow[x \to x_k]{} \frac{S_n(x_k)}{C_n'(x_k)} = -\frac{1 + x_k^2}{n}$.

2^ème^ cas : n impair

Notons $p = \frac{n-1}{2}$, $p \in \mathbb{N}^*$.

Les pôles de F_n sont les $x_k = \tan\left(\frac{\pi}{2n} + \frac{k\pi}{n}\right)$, $k \in \{0,\dots,n-1\} - \{p\}$, tous simples, et la partie entière de F_n vaut $\frac{1}{n}X$. Il existe donc $\lambda_0,\dots,\lambda_{p-1},\lambda_{p+1},\dots,\lambda_{2p} \in \mathbb{C}$ tels que :

$$F = \frac{1}{n}X + \sum_{\substack{0 \leqslant k \leqslant 2p \\ k \neq p}} \frac{\lambda_k}{X - x_k}.$$

On calcule les λ_k comme dans le 1^er^ cas.

◇ **Réponse :**

$$F_n = \begin{cases} -\frac{1}{n}\sum_{k=0}^{n-1} \frac{1 + x_k^2}{X - x_k} & \text{si } n \text{ est pair} \\ \frac{1}{n}X - \frac{1}{n}\sum_{\substack{0 \leqslant k \leqslant n-1 \\ k \neq \frac{n-1}{2}}} \frac{1 + x_k^2}{X - x_k} & \text{si } n \text{ est impair} \end{cases}, \quad \text{où } x_k = \tan\left(\frac{\pi}{2n} + \frac{k\pi}{n}\right).$$

5.4.13 *a)* Il existe $\lambda_1,\dots,\lambda_n \in \mathbb{C}$ tels que $\frac{X^p}{Q} = \sum_{k=1}^{n} \frac{\lambda_k}{X - z_k}$, et (cf. 5.4.2 *2) a)* Prop. 2 p. 197) $\lambda_k = \frac{z_k^p}{Q'(z_k)}$.

◇ **Réponse :** $\frac{X^p}{Q} = \sum_{k=1}^{n} \frac{z_k^p}{Q'(z_k)(X - z_k)}$.

b) En notant, pour $k \in \{1,\dots,n\}$, $Q_k = \frac{Q}{X - z_k} = \prod_{\substack{1 \leqslant i \leqslant n \\ i \neq k}} (X - z_i)$, on a, d'après *a)* : $X^p = \sum_{k=1}^{n} \frac{z_k^p}{Q'(z_k)} Q_k$.

Remarquer que le coefficient de X^{n-1} dans le second membre est $\sum_{k=1}^{n} \frac{z_k^p}{Q'(z_k)}$.

◇ **Réponse :** 0 si $p < n-1$, 1 si $p = n-1$.

5.4.14 On dispose de la DES : $\dfrac{P}{Q} = \displaystyle\sum_{k=1}^{n} \frac{P(z_k)}{Q'(z_k)} \frac{1}{X - z_k}$, d'où $\dfrac{X}{Q} = \displaystyle\sum_{k=1}^{n} \frac{P(z_k)}{Q'(z_k)} \frac{X}{X - z_k}$.

En faisant tendre X vers l'infini, on conclut : $\displaystyle\sum_{k=1}^{n} \frac{P(z_k)}{Q'(z_k)} = 0$.

5.4.15 Notons $Q = \displaystyle\prod_{k=1}^{n}(X - z_k)$ et, pour tout k de $\{1,\ldots,n\}$, $Q_k = \displaystyle\prod_{\substack{1 \leqslant i \leqslant n \\ i \neq k}} (X - z_i)$.

• Soit $k \in \{1,\ldots,n\}$. On a : $Q = (X - z_k)Q_k$, d'où, par dérivation : $Q' = (X - z_k)Q_k' + Q_k$, et donc : $Q'(z_k) = Q_k(z_k) = \displaystyle\prod_{\substack{1 \leqslant i \leqslant n \\ i \neq k}} (z_k - z_i)$.

Ainsi : $\forall k \in \{1,\ldots,n\}$, $u_k = z_k - \dfrac{P(z_k)}{Q'(z_k)}$.

• On dispose de la DES : $\dfrac{P}{Q} = 1 + \displaystyle\sum_{k=1}^{n} \frac{P(z_k)}{Q'(z_k)} \frac{1}{X - z_k}$, où la partie entière vaut 1 puisque $\deg(P) = \deg(Q)$ et que P et Q sont unitaires.

Notons $\alpha_0,\ldots,\alpha_{n-1} \in \mathbb{C}$ tels que $Q = X^N + \alpha_{n-1}X^{n-1} + \ldots + \alpha_0$.

Puisque $\displaystyle\sum_{k=1}^{n} \frac{P(z_k)}{Q'(z_k)} \frac{X}{X - z_k} = \frac{X(P - Q)}{Q}$, on déduit, en faisant tendre X vers l'infini :

$$\sum_{k=1}^{n} \frac{P(z_k)}{Q'(z_k)} = a_{n-1} - \alpha_{n-1}.$$

D'où : $\displaystyle\sum_{k=1}^{n} u_k = \sum_{k=1}^{n} \left(z_k - \frac{P(z_k)}{Q'(z_k)} \right) = \sum_{k=1}^{n} z_k - (a_{n-1} - \alpha_{n-1})$.

D'autre part, puisque $z_1,\ldots,z_n$ sont les zéros de Q, on a : $\displaystyle\sum_{k=1}^{n} z_k = -\alpha_{n-1}$.

Finalement : $\displaystyle\sum_{k=1}^{n} u_k = -a_{n-1}$.

Indications et réponses
pour les exercices du chapitre 6

6.2.1 *a) 1)*

$$\left.\begin{array}{l}\left\{\begin{array}{l}F\cap G\subset F\\ F\cap H\subset F\end{array}\right.\Longrightarrow (F\cap G)+(F\cap H)\subset F\\ \left\{\begin{array}{l}F\cap G\subset G\\ F\cap H\subset H\end{array}\right.\Longrightarrow (F\cap G)+(F\cap H)\subset G+H\end{array}\right|\Longrightarrow (F\cap G)+(F\cap H)\subset F\cap(G+H).$$

2) Puisque G et H jouent des rôles symétriques, on peut supposer, par exemple, $G\subset F$.

Soit $x\in F\cap(G+H)$. Alors $x\in F$ et il existe $(g,h)\in G\times H$ tel que $x=g+h$. On déduit $h=x-g\in F$, car $x\in F$ et $g\in G\subset F$. Puis $x=g+h$, où $g\in G=F\cap G$ et $h\in F\cap H$. Ceci montre : $F\cap(G+H)\subset(F\cap G)+(F\cap H)$, d'où l'égalité, d'après *1)*.

3) ◇ **Réponse :** $K=\mathbb{R}$, $E=\mathbb{R}^2$, $F=\mathbb{R}(1,0)$, $G=\mathbb{R}(0,1)$, $H=\mathbb{R}(1,1)$.

Dans cet exemple : $(F\cap G)+(F\cap H)=\{0\}+\{0\}=\{0\}$ et $F\cap(G+H)=F\cap E=F\neq\{0\}$.

b) 1)
$$\left.\begin{array}{l}\left\{\begin{array}{l}F\subset F+G\\ F\subset F+H\end{array}\right.\Longrightarrow F\subset(F+G)\cap(F+H)\\ \left\{\begin{array}{l}G\subset F+G\\ H\subset F+H\end{array}\right.\Longrightarrow G\cap H\subset(F+G)\cap(F+H)\end{array}\right|\Longrightarrow F+(G\cap H)\subset(F+G)\cap(F+H).$$

2) De même qu'en *a) 2)*, on peut supposer, par exemple, $F\subset G$.

Soit $x\in(F+G)\cap(F+H)$.

Il existe $(f,g)\in F\times G$ et $(f',h)\in F\times H$ tels que : $x=f+g=f'+h$. On déduit $h=f+g-f'\in G$.
Ainsi : $x=f'+h$, $f'\in F$, $h\in G\cap H$, d'où $x\in F+(G\cap H)$.

Ceci montre : $(F+G)\cap(F+H)\subset F+(G\cap H)$, d'où l'égalité d'après *1)*.

3) ◇ **Réponse :** Même exemple qu'en *a) 3)*.

6.2.2 Raisonnons par l'absurde : supposons $F\neq E$ et $G\neq E$. Il existe $x\in E$ tel que $x\notin F$, et $y\in E$ tel que $y\notin G$. Comme $E=F\cup G$, on déduit : $x\in G$ et $y\in F$.

Considérons $x+y$; $x+y\in E=F\cup G$.

Si $x+y\in F$, alors $x=(x+y)+(-y)\in F$, contradiction.

Si $x+y\in G$, alors $y=(x+y)+(-x)\in G$, contradiction.

Ceci montre : $F=E$ ou $G=E$.

6.2.3 Notons $F=\bigcup_{i\in I}F_i$.

1) Puisque $I\neq\varnothing$, il existe $i_0\in I$, puis $F\supset F_{i_0}\supset\{0\}$, donc $F\neq\varnothing$.

2) Soient $x,y\in F$. Il existe $(i,j)\in I^2$ tel que : $x\in F_i$ et $y\in F_j$. Par hypothèse, il existe $k\in I$ tel que $F_i\cup F_j\subset F_k$. On a alors $x\in F_k$ et $y\in F_k$, d'où $x+y\in F_k\subset F$.

3) Soient $\lambda\in K$, $x\in E$. Il existe $i\in I$ tel que $x\in F_i$. On a : $\lambda x\in F_i\subset F$.

Finalement, F est un sev de E

6.2.4 ◇ **Réponse :** $K = \mathbb{Z}/2\mathbb{Z}$, $E = K^2$, $F_1 = \{(0,0), (1,0)\}$, $F_2 = \{(0,0), (0,1)\}$, $F_3 = \{(0,0), (1,1)\}$.

6.2.5 Montrons que E est un sev de $\mathbb{R}^{\mathbb{R}}$ pour les lois usuelles.

1) $E \neq \varnothing$, car $0 \in E$.

2) Soient $f_1, f_2 \in E$. Il existe $A_1, A_2 \in \mathbb{R}_+^*$, $g_1, h_1, g_2, h_2 : \mathbb{R} \longrightarrow \mathbb{R}$ croissantes tels que :

$$\forall x \in \mathbb{R}, \quad \big(|x| \geqslant A_1 \Longrightarrow f_1(x) = g_1(x) - h_1(x)\big)$$
$$\forall x \in \mathbb{R}, \quad \big(|x| \geqslant A_2 \Longrightarrow f_2(x) = g_2(x) - h_2(x)\big).$$

En notant $A = \operatorname{Max}(A_1, A_2)$, $g = g_1 + g_2$, $h = h_1 + h_2$, on a :

$$\left\{\begin{array}{l} A \in \mathbb{R}_+^* \\ g, h \text{ sont croissantes} \\ \forall x \in \mathbb{R}, \ (|x| \geqslant A \Longrightarrow (f_1 + f_2)(x) = g(x) - h(x) \end{array}\right|, \quad \text{d'où } f_1 + f_2 \in E.$$

3) Soient $\lambda \in \mathbb{R}$, $f \in E$. Il existe $A \in \mathbb{R}_+^*$, $g, h : \mathbb{R} \longrightarrow \mathbb{R}$ croissantes telles que :

$$\forall x \in \mathbb{R}, \ \big(|x| \geqslant A \Longrightarrow f(x) = g(x) - h(x)\big).$$

Si $\lambda \geqslant 0$, alors $\lambda g, \lambda h$ sont croissantes et : $\forall x \in \mathbb{R}, \ \big(|x| \geqslant A \Longrightarrow (\lambda f)(x) = (\lambda g)(x) - (\lambda h)(x)\big)$.
Si $\lambda \leqslant 0$, alors $-\lambda h, -\lambda g$ sont croissantes et : $\forall x \in \mathbb{R}, \big(|x| \geqslant A \Longrightarrow (\lambda f)(x) = (-\lambda h)(x) - (-\lambda g)(x)\big)$.
Donc : $\lambda f \in E$.

6.2.6 *1)* • $F \neq \varnothing$ car $0 \in F$.

• Si $(f_1, f_2) \in F^2$, alors : $\forall i \in \{0, \ldots, N\}$, $(f_1 + f_2)(a_i) = f_1(a_i) + f_2(a_i) = 0$, donc $f_1 + f_2 \in F$.

• De même : $\forall \lambda \in \mathbb{R}, \forall f \in F, \lambda f \in F$.

Donc F est un sev de E.

2) Il est clair (cf. 5.1.4 p. 146) que G est un sev de E.

3) Soit $f \in F \cap G$; alors f est un polynôme de degré $\leqslant N$ s'annulant en $N+1$ réels deux à deux distincts, donc $f = 0$.
Ainsi : $F \cap G = \{0\}$.

4) Soit $\varphi \in E$. Il existe $g \in G$ tel que : $\forall i \in \{0, \ldots, N\}$, $g(a_i) = \varphi(a_i)$, cf. polynômes d'interpolation de Lagrange, 5.3.1 Exemple p. 169.
En notant $f = \varphi - g$, on a : $f \in F$, $g \in G$, $\varphi = f + g$.
Ceci montre : $F + G = E$.

6.2.7 *a)* • $X' \subset A$, et $X' \neq \varnothing$ car $0 \in X'$.

• Soit $(y, z) \in X'^2$. On a :

$\forall x \in X, x(y+z) = xy + xz = yx + zx = (y+z)x$, donc $y + z \in X'$.

• Soit $(\lambda, y) \in K \times X'$. On a : $\forall x \in X, x(\lambda y) = \lambda(xy) = \lambda(yx) = (\lambda y)x$, donc $\lambda y \in X'$.

• Soit $(y, z) \in X'^2$. On a : $\forall x \in X, x(yz) = (xy)z = (yx)z = y(xz) = y(zx) = (yz)x$, donc $yz \in X'$.

Ceci montre que X' est une sous-algèbre de A.

b) 1) Supposons $X \subset Y$, et soit $z \in Y'$.

On a : $\forall y \in Y, \quad yz = zy$,

donc : $\forall y \in X, \quad yz = zy$,

d'où $z \in X'$. Ainsi : $Y' \subset X'$.

2) Soit $x \in X$. Par définition de X', on a : $\forall y \in X', xy = yx$, donc $x \in (X')' = X''$.

6.3.1 Pour tout (α,β,γ) de $\mathbb{R}^3$:

$$\alpha u+\beta v+\gamma w = 0 \Longleftrightarrow (\alpha+\gamma)x+(\alpha+\beta)y+(\beta+\gamma)z = 0 \Longleftrightarrow \begin{cases} \alpha+\gamma = 0 \\ \alpha+\beta = 0 \\ \beta+\gamma = 0 \end{cases} \Longleftrightarrow \alpha = \beta = \gamma = 0.$$

6.3.2 Raisonnons par l'absurde : supposons $\sqrt[n]{N} \in \mathbb{Q}$. Il existe $(a,b) \in (\mathbb{N}^*)^2$ tel que :

$\sqrt[n]{N} = \dfrac{a}{b}$ et $a \wedge b = 1$.

Comme $a^n = b^n N$, b divise a^n.

D'autre part, $b \wedge a^n = 1$, car $a \wedge b = 1$ (cf. 4.3.3 Prop. 2, p. 116).

On déduit $b = 1$, $N = a^n$, contradiction.

b) Soit $(\alpha,\beta) \in \mathbb{Q}^2$ tel que $\alpha + \beta\sqrt[n]{N} = 0$. Si $\beta \neq 0$, alors $\sqrt[n]{N} = -\dfrac{\alpha}{\beta} \in \mathbb{Q}$, contradiction. Donc $\beta = 0$, puis $\alpha = 0$.

6.3.3 *Récurrence sur n*

Le cas $n = 0$ est trivial.

Supposons la propriété vraie pour un n de $\mathbb{N}$, et soient $z_0,\ldots,z_{n+1} \in \mathbb{C}$ deux à deux distincts, $\lambda_0,\ldots,\lambda_{n+1} \in \mathbb{C}$ tels que $\displaystyle\sum_{k=0}^{n+1} \lambda_k (X - z_k)^{n+1} = 0$.

En dérivant : $\displaystyle\sum_{k=0}^{n+1} \lambda_k (X - z_k)^n = 0$, puis en multipliant par $(X - z_{n+1})$: $\displaystyle\sum_{k=0}^{n+1} \lambda_k (X - z_{n+1})(X - z_k)^n = 0$,

d'où : $\displaystyle\sum_{k=0}^{n+1} \lambda_k \big((X - z_k) + (z_k - z_{n+1})\big)(X - z_k)^n = 0$.

Comme $\displaystyle\sum_{k=0}^{n+1} \lambda_k (X - z_k)^{n+1} = 0$, on déduit $\displaystyle\sum_{k=0}^{n} \lambda_k (z_k - z_{n+1})(X - z_k)^n = 0$, puis, d'après l'hypothèse de récurrence : $\forall k \in \{0,\ldots,n\}, \lambda_k(z_k - z_{n+1}) = 0$, donc : $\forall k \in \{0,\ldots,n\}, \lambda_k = 0$.

En reportant : $\lambda_{n+1}(X - z_{n+1})^{n+1} = 0$, d'où $\lambda_{n+1} = 0$.

6.3.4 *a)* Soient $n \in \mathbb{N}^*$, $a_1,\ldots,a_n \in]0;1[$ deux à deux distincts, $\lambda_1,\ldots,\lambda_n \in \mathbb{R}$ tels que $\displaystyle\sum_{i=1}^{n} \lambda_i f_i = 0$, c'est-à-dire : $\forall x \in]0;1[, \ \displaystyle\sum_{i=1}^{n} \frac{\lambda_i}{1 - a_i x} = 0$.

Soit $i \in \{1,\ldots,n\}$. On a : $\forall x \in]0;1[, \ \lambda_i = -(1 - a_i x) \displaystyle\sum_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} \frac{\lambda_j}{1 - a_j x}$.

En prenant la limite lorsque x tend vers $\dfrac{1}{a_i}$, on déduit $\lambda_i = 0$.

Remarque : On peut aussi utiliser l'unicité de la décomposition en éléments simples de la fraction rationnelle $\sum_{i=1}^{n} \frac{\lambda_i}{1 - a_i X}$.

b) Utiliser l'unicité de la décomposition en éléments simples (dans $\mathbb{R}(X)$) de la fraction rationnelle 0 dans la relation $\sum_{i=1}^{n} \frac{\lambda_i}{X + a_i^2 + 1} = 0$, pour $n \in \mathbb{N}^*, a_1, \ldots, a_n \in [0; +\infty[$ deux à deux distincts, $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$.

c) Soient $n \in \mathbb{N}^*, a_1, \ldots, a_n \in \mathbb{R}$ tels que $a_1 < \ldots < a_n$, $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ tels que $\sum_{i=1}^{n} \lambda_i f_{a_i} = 0$.

En particulier : $\sum_{i=1}^{n} \lambda_i f_{a_i}(a_1) = 0$. Mais $f_{a_i}(a_1) = \begin{cases} 1 & \text{si } i = 1 \\ 0 & \text{si } i > 1 \end{cases}$, d'où $\lambda_1 = 0$.

En réitérant, on déduit $\lambda_1 = 0, \ldots, \lambda_n = 0$.

d) Soient $n \in \mathbb{N}^*, a_1, \ldots, a_n \in \mathbb{R}$ tels que $a_1 < \ldots < a_n$, $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ tels que $\sum_{i=1}^{n} \lambda_i f_{a_i} = 0$,

c'est-à-dire : $\forall x \in \mathbb{R}, \ \sum_{i=1}^{n} \lambda_i e^{a_i x} = 0$.

Alors : $\forall x \in \mathbb{R}, \lambda_n = -\sum_{i=1}^{n-1} \lambda_i e^{(a_i - a_n)x}$, d'où, en faisant tendre x vers $+\infty$: $\lambda_n = 0$.

En réitérant, on déduit $\lambda_n = 0$, $\lambda_{n-1} = 0, \ldots, \lambda_1 = 0$.

e) Remarquer d'abord que, pour toute famille finie I de $\mathbb{R}^2$, il existe deux familles finies J, K de $\mathbb{R}$ telles que $I \subset J \times K$. La liberté de $(f_{a,b})_{(a,b)\in I}$ résultera de celle de $(f_{a,b})_{(a,b)\in J\times K}$.

Soient donc $(n,p) \in (\mathbb{N}^*)^2$, $a_1, \ldots, a_n \in \mathbb{R}$ deux à deux distincts, $b_1, \ldots, b_p \in \mathbb{R}$ deux à deux distincts, $(\lambda_{ij})_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant p}} \in \mathbb{R}^{np}$ tels que : $\sum_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant p}} \lambda_{ij} f_{a_i, b_j} = 0$.

On a alors : $\forall (x,y) \in \mathbb{R}^2, \ \sum_{j=1}^{p} \left(\sum_{i=1}^{n} \lambda_{ij} e^{a_i x} \right) e^{b_j y} = 0$.

Soit $x \in \mathbb{R}$. D'après *d)*, la famille $\left(\begin{matrix} \mathbb{R} \longrightarrow \mathbb{R} \\ y \longmapsto e^{b_j y} \end{matrix} \right)_{1\leqslant j\leqslant p}$ est libre, d'où : $\forall j \in \{1, \ldots, p\}, \ \sum_{i=1}^{n} \lambda_{ij} e^{a_i x} = 0$.

Ainsi : $\forall j \in \{1, \ldots, p\}, \ \forall x \in \mathbb{R}, \ \sum_{i=1}^{n} \lambda_{ij} e^{a_i x} = 0$, d'où, encore d'après *d)* :

$$\forall j \in \{1, \ldots, p\}, \forall i \in \{1, \ldots, n\}, \lambda_{ij} = 0.$$

f) Se ramène à *d)* par le changement de variable $t = \ln x$, puisque $x^a = e^{a \ln x}$.

g) Se ramène à *e)* comme ci-dessus.

h) Soient $N \in \mathbb{N}^*, \lambda_1, \ldots, \lambda_N \in \mathbb{R}$ tels que $\sum_{n=1}^{N} \lambda_n f_n = 0$, c'est-à-dire : $\forall x \in \mathbb{R}, \ \sum_{n=1}^{N} \lambda_n \sin(x^n) = 0$.

En dérivant : $\forall x \in \mathbb{R}, \ \sum_{n=1}^{N} n\lambda_n x^{n-1} \cos(x^n) = 0$.

Supposons $(\lambda_1, \ldots, \lambda_N) \neq (0, \ldots, 0)$ et notons n_0 le plus petit entier $\geqslant 1$ tel que $\lambda_{n_0} \neq 0$. Alors :

$$0 = \sum_{n=1}^{N} n\lambda_n x^{n-1} \cos(x^n) \underset{x \longrightarrow 0}{\sim} n_0 \lambda_{n_0} x^{n_0 - 1}, \quad \text{contradiction.}$$

i) Soit $(\lambda,\mu,\nu) \in \mathbb{R}^3$ tel que : $\lambda f + \mu f \circ f + \nu f \circ f \circ f = 0$. Formons les $DL_5(0)$:

$$f(x) = x - \frac{x^3}{6} + \frac{x^5}{120} + o(x^5), \quad f\circ f(x) = x - \frac{x^3}{3} + \frac{x^5}{10} + o(x^5), \quad f\circ f\circ f(x) = x - \frac{x^3}{2} + \frac{11x^5}{40} + o(x^5).$$

On déduit, par unicité du $DL_5(0)$ de la fonction nulle : $\begin{cases} \lambda + \mu + \nu = 0 \\ -\dfrac{\lambda}{6} - \dfrac{\mu}{3} - \dfrac{\nu}{2} = 0 \\ \dfrac{\lambda}{120} + \dfrac{\mu}{10} + \dfrac{11\nu}{40} = 0 \end{cases}$, d'où, après calculs,

$\lambda = \mu = \nu = 0$.

6.3.5 ◇ **Réponse :** non, car $f_{0,1} + f_{1,2} = 2f_{0,2}$.

6.3.6 *1)* Soit $(f,f',g) \in F \times F' \times (G \cap G')$ tel que $f + f' + g = 0$.

Comme $F' \subset G$, on déduit $f' + g \in G$, d'où, puisque F et G sont supplémentaires dans E : $f = f' + g = 0$.

Puis $f' \in F'$ et $g \in G'$, d'où, puisque F' et G' sont supplémentaires dans E : $f' = g = 0$.

Ceci montre que F, F', $G \cap G'$ ont une somme directe.

2) • $\left.\begin{cases} F' \subset G \\ G \cap G' \subset G \end{cases}\right| \Longrightarrow F' + (G \cap G') \subset G.$

• Soit $x \in G$. Il existe $f' \in F'$, $g' \in G'$ tels que $x = f' + g'$. Comme $F' \subset G$, on a $f' \in G$, d'où $g' = x - f' \in G$, et donc $g' \in G \cap G'$. Ainsi, $x = f' + g'$ où $f' \in F'$ et $g' \in G \cap G'$, ce qui montre : $G \subset F' + (G \cap G')$.

On a obtenu : $F' + (G \cap G') = G$.

3) $F + F' + (G \cap G') = F + (F' + (G \cap G')) = F + G = E$.

6.3.7 *1)* Supposons $(x_1,\ldots,x_n)$ libre.

• Il est clair que : $\forall i \in \{1,\ldots,n\}, x_i \neq 0$.

• Soit $(y_1,\ldots,y_n) \in \prod_{i=1}^{n} Kx_i$ tel que $\sum_{i=1}^{n} y_i = 0$.

Pour chaque i de $\{1,\ldots,n\}$, il existe $\lambda_i \in K$ tel que $y_i = \lambda_i x_i$. Comme $\sum_{i=1}^{n} \lambda_i x_i = 0$ et que $(x_i)_{1\leqslant i\leqslant n}$ est libre, on déduit $(\forall i \in \{1,\ldots,n\}, \lambda_i = 0)$, puis : $(\forall i \in \{1,\ldots n\}, y_i = 0)$.

Ceci montre que $\sum_{i=1}^{n} Kx_i$ est directe.

2) Réciproquement, supposons : $\begin{cases} \forall i \in \{1,\ldots,n\}, \quad x_i \neq 0 \\ \sum_{i=1}^{n} Kx_i \text{ est directe} \end{cases}$.

Soit $(\lambda_1,\ldots,\lambda_n) \in K^n$ tel que $\sum_{i=1}^{n} \lambda_i x_i = 0$. Comme $(\forall i \in \{1,\ldots,n\}, \lambda_i x_i \in Kx_i)$ et que $\sum_{i=1}^{n} Kx_i$ est directe, on déduit : $\big(\forall i \in \{1,\ldots,n\}, \lambda_i x_i = 0\big)$ puis $\big(\forall i \in \{1,\ldots,n\}, \lambda_i = 0\big)$.

Ceci montre que $(x_1,\ldots,x_n)$ est libre.

6.3.8 Soit $(x_1,\dots,x_n) \in \prod_{i=1}^{n} G_i$ tel que $\sum_{i=1}^{n} x_i = 0$. Comme $\big(\forall i \in \{1,\dots,n\},\ G_i \subset F_i\big)$ et que $F_1,\dots,F_n$ sont en somme directe, on déduit : $\forall i \in \{1,\dots,n\},\ x_i = 0$.

6.3.9 *a)* Une sous-famille finie de $\bigcup_{i=1}^{n} \mathcal{L}_i$ peut s'écrire $(x_{ij})_{(i,j)\in\Phi}$

où $\Phi = \{(i,j);\ 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant N_i\}, n, N_1,\dots,N_n \in \mathbb{N}^*$.

Soit $(\lambda_{ij})_{(i,j)\in\Phi}$ tel que $\sum_{(i,j)\in\Phi} \lambda_{ij}x_{ij} = 0$.

Comme $\sum_{i=1}^{n}\left(\sum_{j=1}^{N_i}\lambda_{ij}x_{ij}\right) = 0$, que $\left(\forall i \in \{1,\dots,n\},\ \sum_{j=1}^{N_i}\lambda_{ij}x_{ij} \in F_i\right)$, et que $F_1,\dots,F_n$ sont en somme directe, on déduit : $\forall i \in \{1,\dots,n\},\ \sum_{j=1}^{N_i}\lambda_{ij}x_{ij} = 0$, puis, par liberté des $\mathcal{L}_i$:

$$\forall i \in \{1,\dots,n\},\ \forall j \in \{1,\dots,N_i\},\ \lambda_{ij} = 0.$$

b) $\text{Vect}\left(\bigcup_{i=1}^{n}\mathcal{G}_i\right) = \sum_{i=1}^{n}\text{Vect}(\mathcal{G}_i) = \sum_{i=1}^{n} F_i = E$.

c) Résulte de *a)* et *b)*.

6.4.1 Pour tout (x,y,z) de $\mathbb{C}^3$:

$$\begin{cases} x+y+z=0 \\ x+\mathrm{i}y-z=0 \end{cases} \iff \begin{cases} x=-y-z \\ (\mathrm{i}-1)y=2z \end{cases} \iff \begin{cases} x=\mathrm{i}z \\ y=-(1+\mathrm{i})z \end{cases}.$$

Ainsi, $F = \{z(\mathrm{i},-(1+\mathrm{i}),1));\ z \in \mathbb{C}\}$, donc F est le sev de $\mathbb{C}^3$ engendré par le vecteur $(\mathrm{i},-(1+\mathrm{i}),1)$.

◇ **Réponse :** • Une base de F est $(\mathrm{i},-(1+\mathrm{i}),1)$

• $\dim(F) = 1$.

6.4.2 Notons, pour $\mathrm{i} \in \{1,\dots,4\}$, $g_i : \begin{array}{ccc}]-1;1] & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \sqrt{1-x^2}f_i(x) \end{array}$.

On a ainsi, pour tout x de $]-1;1[$: $g_1(x) = 1-x$, $g_2(x) = 1+x$, $g_3(x) = 1$, $g_4(x) = x$.

Il est clair que (g_3,g_4) est libre et que $g_1 = g_3 - g_4$, $g_2 = g_3 + g_4$; il en résulte que (f_3,f_4) est libre et que $f_1 = f_3 - f_4$, $f_2 = f_3 + f_4$.

◇ **Réponse :** • Une base de F est (f_3,f_4)

• $\dim(F) = 2$.

6.4.3 *1)* Pour tout (α,β,γ) de $\mathbb{R}^3$:

$$\alpha u+\beta v+\gamma w = 0 \iff \left|\begin{array}{l} \alpha+\gamma=0 \\ \beta+\gamma=0 \\ \alpha-\beta+\gamma=0 \\ \gamma=0 \end{array}\right| \iff \alpha=\beta=\gamma=0,$$

donc (u,v,w) est libre, et $\dim(F) = 3$.

2) Il est clair que (x,y) est libre, d'où $\dim(G) = 2$.

3) La famille (u,v,w,x) est libre car, pour tout $(\alpha,\beta,\gamma,\delta)$ de $\mathbb{R}^4$:

$$\alpha u+\beta v+\gamma w+\delta x=0 \Longleftrightarrow \left|\begin{cases}\alpha+\gamma=0\\ \beta+\gamma=0\\ \alpha-\beta+\gamma+\delta=0\\ \gamma=0\end{cases}\right. \Longleftrightarrow \alpha=\beta=\gamma=\delta=0.$$

Il en résulte d'ailleurs que (u,v,w) est libre.
Ainsi, $\dim(F+G)\geqslant 4$, d'où, puisque $F+G\subset\mathbb{R}^4$: $F+G=\mathbb{R}^4$.

4) $\dim(F\cap G)=\dim(F)+\dim(G)-\dim(F+G)=3+2-4$.

◇ **Réponse :** $\dim(F)=3$, $\dim(G)=2$, $\dim(F+G)=4$, $\dim(F\cap G)=1$.

6.4.4 D'après 6.4 Prop. 6, p. 231, F admet au moins un supplémentaire G dans E.
Le sev F (resp. G) de E admet au moins une base $\mathcal{B}=(f_1,\dots,f_p)$, $p\geqslant 1$ (resp. $\mathcal{C}=(g_1,\dots,g_q)$, $q\geqslant 1$). Notons $\mathcal{C}'=(f_1+g_1,g_2,\dots,g_q)$ et $G'=\text{Vect}(\mathcal{C}')$.

1) Montrons : $F\cap G'=\{0\}$.
Soit $x\in F\cap G'$. Il existe $\lambda_1,\dots,\lambda_p,\mu_1,\dots,\mu_q\in K$ tels que : $x=\sum_{i=1}^{p}\lambda_i f_i=\mu_1(f_1+g_1)+\sum_{j=2}^{q}\mu_j g_j$.
Alors : $\sum_{i=1}^{p}\lambda_i f_i-\mu_1 f_1=\sum_{j=1}^{q}\mu_j g_j\in F\cap G=\{0\}$, d'où $\sum_{j=1}^{q}\mu_j g_j=0$, puis, puisque $\mathcal{C}$ est libre : $(\forall j\in\{1,\dots,q\},\ \mu_j=0)$, et donc $x=0$.

2) Montrons : $F+G'=E$.
Soit $x\in E$. Il existe $\lambda_1,\dots,\lambda_p,\mu_1,\dots,\mu_q\in K$ tels que : $x=\sum_{i=1}^{p}\lambda_i f_i+\sum_{j=1}^{q}\mu_j g_j$.
Alors : $x=\left((\lambda_1-\mu_1)f_1+\sum_{i=2}^{p}\lambda_i f_i\right)+\left(\mu_1(f_1+g_1)+\sum_{j=2}^{q}\mu_j g_j\right)\in F+G'$.

3) On a $f_1+g_1\in G'$, et $f_1+g_1\notin G$, car sinon : $f_1=(f_1+g_1)-g_1\in G$, contradiction.
Donc : $G\neq G'$.

6.4.5 Utiliser : $\dim(F)+\dim(G)=\dim(F+G)-\dim(F\cap G)$.

6.4.6 Puisque $E\times F$ est de dimension finie, $E\times F$ admet au moins une famille génératrice finie $(x_i,y_i)_{1\leqslant i\leqslant n}$.
Soit $x\in E$. Comme $(x,0)\in E\times F$, il existe $(\lambda_i)_{1\leqslant i\leqslant n}\in K^n$ tel que $(x,0)=\sum_{i=1}^{n}\lambda_i(x_i,y_i)$,
d'où : $x=\sum_{i=1}^{n}\lambda_i x_i$.
Ceci montre que $(x_i)_{1\leqslant i\leqslant n}$ engendre E, et donc E est de dimension finie.

6.4.7 *1)* En notant $c : \begin{array}{ccc}\mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \cos x\end{array}$, $s : \begin{array}{ccc}\mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \sin x\end{array}$, on a : $\forall i \in \{1,2,3\}$, $f_{a_i} = (\cos a_i)c - (\sin a_i)s$, d'où $\text{Vect}(f_{a_1}, f_{a_2}, f_{a_3}) \subset \text{Vect}(c,s)$, et donc $\text{rg}(f_{a_1}, f_{a_2}, f_{a_3}) \leqslant 2$.

2) Comme $f_{a_1} \neq 0$, on a : $\text{rg}(f_{a_1}, f_{a_2}, f_{a_3}) \geqslant 1$.

3) Le rang de $(f_{a_1}, f_{a_2}, f_{a_3})$ est 1 si et seulement si f_{a_2} et f_{a_3} sont colinéaires à f_{a_1}. Et, en remarquant que (c,s) est libre :

$$(f_{a_1}, f_{a_2}) \text{ lié} \iff \left(\exists \lambda \in \mathbb{R}, \begin{cases} \cos a_2 = \lambda \cos a_1 \\ \sin a_2 = \lambda \sin a_1 \end{cases}\right)$$
$$\iff \cos a_2 \sin a_1 = \sin a_2 \cos a_1 \iff \sin(a_2 - a_1) = 0 \iff a_2 - a_1 \in \pi\mathbb{Z}.$$

◇ **Réponse :** $\begin{cases} 1 & \text{si } (a_2 - a_1, a_3 - a_1) \in (\pi\mathbb{Z})^2 \\ 2 & \text{sinon.} \end{cases}$

6.4.8 *1)* $\Longrightarrow$ *2)*

- Déjà, $\mathcal{F}$ est génératrice de E.
- Soit $\mathcal{G}$ une famille génératrice de E telles que $\mathcal{G} \subset \mathfrak{F}$.

Puisque $\mathcal{F}$ est finie, $\mathcal{G}$ est finie. Comme $\mathcal{G}$ est finie et génératrice de E, d'après 6.4 Prop. 3, *3)*, p. 229 : $\text{Card}(\mathcal{G}) \geqslant \dim(E) = \text{Card}(\mathcal{F})$.

Comme $\left\{\begin{array}{l} \mathcal{G} \subset \mathcal{F} \\ \text{Card}(\mathcal{G}) \geqslant \text{Card}(\mathcal{F}) \end{array}\right.$, on conclut $\mathcal{G} = \mathcal{F}$.

2) $\Longrightarrow$ *1)*

Raisonnons par l'absurde : supposons que $\mathfrak{F}$ soit liée; il existe alors $x \in \mathfrak{F}$ tel que x se décompose linéairement sur $\mathcal{F}' = \mathcal{F} - \{x\}$.

Ainsi, $\mathcal{F}'$ est génératrice de E, $\mathcal{F}' \subset \mathcal{F}$, $\mathcal{F}' \neq \mathcal{F}$, ce qui contredit *2)*.

1) $\Longrightarrow$ *3)*

- Déjà, $\mathcal{F}$ est libre.
- Soit $\mathcal{L}$ une famille libre de E telle que $\mathcal{F} \subset \mathcal{L}$. D'après 6.4 Prop. 3, *1)*, p. 229, $\mathcal{L}$ est finie et $\text{Card}(\mathcal{L}) \leqslant \dim(E) = \text{Card}(\mathcal{F})$.

Comme $\left\{\begin{array}{l} \mathcal{F} \subset \mathcal{L} \\ \text{Card}(\mathcal{L}) \leqslant \text{Card}(\mathcal{F}) \end{array}\right.$, on conclut $\mathcal{L} = \mathcal{F}$.

3) $\Longrightarrow$ *1)*

Raisonnons par l'absurde : supposons que $\mathcal{F}$ ne soit pas génératrice de E; il existe alors $x \in E$ tel que $x \notin \text{Vect}(\mathcal{F})$. Ainsi, la famille $\mathcal{F}'$ définie par $\mathcal{F}' = \mathcal{F} \cup \{x\}$ est libre, $\mathcal{F} \subset \mathcal{F}'$, $\mathcal{F}' \neq \mathcal{F}$, ce qui contredit *3)*.

6.4.9 *a)* Résulte de la preuve de 6.4 Th.-Déf. 1, p. 228.

b) C'est le théorème de la base incomplète, forme faible, 6.4 Th. 2, p. 229.

c) D'après *a)*, il existe une base $\mathcal{B}_1$ de E telle que $\mathcal{B}_1 \subset \mathcal{G}$. D'après le théorème de la base incomplète (forme forte), on peut compléter $\mathcal{L}$ par des vecteurs de $\mathcal{B}_1$ (donc de $\mathcal{G}$) pour obtenir une base $\mathcal{B}_3$ de E. On a bien : $\mathcal{L} \subset \mathcal{B}_3 \subset \mathcal{G}$.

d) Se déduit de *c)* appliqué à $\mathcal{L} \cup \mathcal{G}$ au lieu de $\mathcal{G}$.

6.4.10 *a)* • Par sa définition, A est le sev du $\mathbb{Q}$-ev $\mathbb{R}$ engendré par la famille $\mathcal{F} = (1, \sqrt{2}, \sqrt{3}, \sqrt{6})$.

• Il est clair que : $\forall (\alpha, \beta) \in \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}^2,\ \alpha\beta \in A$.

Par $\mathbb{Q}$-linéarité, il en résulte : $\forall (x, y) \in A^2,\ xy \in A$.

D'après 6.2 Déf. 4, p. 214, A est une sous-algèbre de la $\mathbb{Q}$-algèbre $\mathbb{R}$.

b) Soit $(a,b,c,d) \in \mathbb{Q}^4$ tel que $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$.

On déduit : $\begin{cases} (a + b\sqrt{2})^2 = 3(c + d\sqrt{2})^2 \\ (a + c\sqrt{3})^2 = 2(b + d\sqrt{3})^2 \end{cases}$, puis, d'après l'exercice 6.3.2 p. 218 :

$$\left.\begin{cases} a^2 + 2b^2 - 3c^2 - 6d^2 = 0 \\ ab = 3cd \\ a^2 + 3c^2 - 2b^2 - 6d^2 = 0 \\ ac = 2bd \end{cases}\right|, \quad \text{d'où} \quad \begin{cases} a^2 = 6d^2 \\ 2b^2 = 3c^2 \end{cases}.$$

Comme $\sqrt{6} \notin \mathbb{Q}$ et $\sqrt{\dfrac{3}{2}} \notin \mathbb{Q}$, on obtient (cf. le même exercice) : $a = d = 0$ et $b = c = 0$.

Ceci montre que $\mathcal{F}$ est libre.

Comme, par définition de A, $\mathcal{F}$ engendre A, on conclut que $\mathcal{F}$ est une base de A, et $\dim(A) = 4$.

c) Soit $x \in A - \{0\}$. Puisque $x \in \mathbb{R}^*$, x admet un inverse, noté x^{-1}, dans $\mathbb{R}$. Il reste à montrer $x^{-1} \in A$.

Il existe $(a,b,c,d) \in \mathbb{Q}^4$ tel que $x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$. Nous allons calculer x^{-1} en utilisant des «quantités conjuguées».

Il est clair que $(a,b,c,d) \neq (0,0,0,0)$, donc, d'après *b)*, $(a + b\sqrt{2}) - (c\sqrt{3} + d\sqrt{6}) \neq 0$, d'où $x^{-1} = \dfrac{y}{\alpha + \beta\sqrt{2}}$, en notant $y = (a + b\sqrt{2}) - (c\sqrt{3} + d\sqrt{6})$, $\alpha = a^2 + 2b^2 - 3c^3 - 6d^2$, $\beta = 2ab - 6cd$.

Comme $\alpha + \beta\sqrt{2} \neq 0$, nécessairement $(\alpha, \beta) \neq (0,0)$, et donc, puisque $(1, \sqrt{2})$ est libre, $\alpha - \beta\sqrt{2} \neq 0$.

On obtient : $x^{-1} = \dfrac{y(\alpha - \beta\sqrt{2})}{\alpha^2 - 2\beta^2} \in A$.

◇ **Réponse :** $\dfrac{1}{4} - \dfrac{1}{4}\sqrt{3} + \dfrac{1}{4}\sqrt{6}$.

Indications et réponses
pour les exercices du chapitre 7

7.1.1 *1)* Supposons $f(A) \subset f(B)$, et soit $x \in A + \mathrm{Ker}(f)$. Il existe $a \in A$ et $u \in \mathrm{Ker}(f)$ tels que $x = a + u$. Puisque $f(a) \in f(A) \subset f(B)$, il existe $b \in B$ tel que $f(a) = f(b)$, et donc $a - b \in \mathrm{Ker}(f)$. Alors : $x = b + (a - b + u)$, $b \in B$, $a - b + u \in \mathrm{Ker}(f)$, d'où $x \in B + \mathrm{Ker}(f)$.

On conclut : $A + \mathrm{Ker}(f) \subset B + \mathrm{Ker}(f)$.

2) Réciproquement, supposons $A + \mathrm{Ker}(f) \subset B + \mathrm{Ker}(f)$, et soit $y \in f(A)$. Il existe $a \in A$ tel que $y = f(a)$. Puisque $a \in A \subset A + \mathrm{Ker}(f) \subset B + \mathrm{Ker}(f)$, il existe $b \in B$ et $v \in \mathrm{Ker}(f)$ tels que $a = b + v$. Alors : $y = f(b + v) = f(b) + f(v) = f(b) \in f(B)$. On conclut : $f(A) \subset f(B)$.

7.1.2 Soient $\lambda \in K$, $a, a' \in E$. On a : $\big(a + \lambda a', f(a) + \lambda f(a')\big) = \big(a, f(a)\big) + \lambda\big(a', f(a')\big) \in G$, d'où, par unicité de l'élément c de F tel que $(a + \lambda a', c) \in G$: $f(a) + \lambda f(a') = f(a + \lambda a')$.

7.1.3 La linéarité de f est immédiate.

Pour tout $P = \sum_{k=0}^{n} a_k \mathrm{X}^k$ de $\mathbb{R}[\mathrm{X}]$, on a :

$$f(P) = \sum_{k=0}^{n} a_k \mathrm{X}^k - \mathrm{X} \sum_{k=1}^{n} k a_k \mathrm{X}^{k-1} = \sum_{k=0}^{n} (1 - k) a_k \mathrm{X}^k.$$

• $P \in \mathrm{Ker}(f) \iff (\forall k \in \{0, \ldots, n\},\ (1 - k)a_k = 0) \iff (\forall k \in \{0, \ldots, n\} - \{1\},\ a_k = 0)$, d'où $\mathrm{Ker}(f) = \mathbb{R}\mathrm{X}$.

• $\mathrm{Im}(f) = \mathrm{Vect}\big((\mathrm{X}^k)_{k \in \mathbb{N} - \{1\}}\big)$, puisque : $\forall k \in \mathbb{N}$, $f(\mathrm{X}^k) = (1 - k)\mathrm{X}^k$.

◇ **Réponse :** $\mathrm{Ker}(f) = \mathbb{R}\mathrm{X}$, $\mathrm{Im}(f) = \mathrm{Vect}\big((\mathrm{X}^k)_{k \in \mathbb{N} - \{1\}}\big)$.

7.1.4 D'abord : $\forall P \in E$, $P - P' \in E$.

La linéarité de f est immédiate.

1) Soit $P \in E - \{0\}$; comme $\deg(P) \neq \deg(P')$, on a : $P - P' \neq 0$. Ceci montre : $\mathrm{Ker}(f) = \{0\}$, et donc f est injective.

2) Soit $Q \in E$.

• Supposons qu'il existe $P \in E - \{0\}$ tel que $f(P) = Q$. En notant $n = \deg(P) = \deg(Q)$ et en dérivant : $Q = -P' + P$, $Q' = -P'' + P'$, ..., $Q^{(n)} = -P^{(n+1)} + P^{(n)} = P^{(n)}$, d'où, en additionnant : $Q + Q' + \ldots + Q^{(n)} = P$.

• Considérons donc l'application $g : E \longrightarrow E$ définie par : $\forall Q \in E,\ g(Q) = \sum_{k=0}^{\deg(Q)} Q^{(k)}$ (et $g(0) = 0$);

on peut noter $g(Q) = \sum_{k=0}^{+\infty} Q^{(k)}$. Il est clair que g est linéaire, et :

$$\forall P \in E,\ (g \circ f)(P) = g(P - P') = (P - P') + (P' - P'') + \ldots + (P^{(n)} - 0) = P$$
$$\forall Q \in E,\ (f \circ g)(Q) = f(Q + Q' + \ldots + Q^{(n)})$$
$$= (Q + Q' + \ldots + Q^{(n)}) - (Q' + Q'' + \ldots + Q^{(n+1)}) = Q,$$

où $n = \deg(P) = \deg(Q)$.

Ceci montre que f est un automorphisme de E, et $g = f^{-1}$.

◇ **Réponse :** $\forall Q \in E,\quad f^{-1}(Q) = \sum_{k=0}^{+\infty} Q^{(k)}$.

7.1.5 *a)* Immédiat.

b) La linéarité de ϕ est immédiate.

1) $\forall f \in E,\ \big(f \in \mathrm{Ker}(\phi) \Longleftrightarrow f' = 0 \Longleftrightarrow f \in \mathbb{R}\mathbf{1}\big)$, où $\mathbf{1} : \mathbb{R} \longrightarrow \mathbb{R},\ x \longmapsto 1$.

2) • Soient $g \in \mathrm{Im}(\phi)$, $f \in E$ telle que $g = \phi(f) = f'$.

Par primitivation, il existe $\lambda \in \mathbb{R}$ tel que : $\forall x \in \mathbb{R},\ f(x) = \lambda + \int_0^x g(t)\,\mathrm{d}t$.

Puisque f est T-périodique, en particulier : $f(T) = f(0)$, d'où $\int_0^T g(t)\,\mathrm{d}t = 0$.

• Réciproquement, soit $g \in E$ telle que $\int_0^T g = 0$. Considérons $f : \mathbb{R} \longrightarrow \mathbb{R},\ x \longmapsto \int_0^x g(t)\,\mathrm{d}t$.

Il est connu que f est de classe C^∞ sur $\mathbb{R}$ et $f' = g$ (cf. Tome 1, 6.4.1 Cor. 1). De plus :

$$\forall x \in \mathbb{R},\quad f(x+T) - f(x) = \int_x^{x+T} g(t)\,\mathrm{d}t = \int_x^0 g(t)\,\mathrm{d}t + \int_0^T g(t)\,\mathrm{d}t + \int_T^{x+T} g(t)\,\mathrm{d}t$$
$$\underset{[u = t - T]}{=} -\int_0^x g(t)\,\mathrm{d}t + \int_0^x g(u+T)\mathrm{d}t = 0,$$

ce qui montre : $f \in E$.

◇ **Réponse :** $\mathrm{Ker}(\phi) = \mathbb{R}\mathbf{1}$, $\mathrm{Im}(\phi) = \left\{g \in E;\ \int_0^T g(t)\,\mathrm{d}t = 0\right\}$.

7.1.6 D'après l'hypothèse : $\forall x \in E - \{0\}, \exists! \lambda_x \in K,\ f(x) = \lambda_x x$. Il s'agit de montrer que λ_x ne dépend pas de x. Soit $(x, y) \in (E - \{0\})^2$.

1) Supposons (x, y) libre.

On a : $\left\{\begin{array}{l} f(x+y) = f(x) + f(y) = \lambda_x x + \lambda_y y \\ f(x+y) = \lambda_{x+y}(x+y) \end{array}\right.$, d'où $(\lambda_{x+y} - \lambda_x)x + (\lambda_{x+y} - \lambda_y)y = 0$,

et donc $\lambda_{x+y} - \lambda_x = \lambda_{x+y} - \lambda_y = 0,\ \lambda_x = \lambda_y$.

2) Supposons (x, y) lié.

Il existe $\alpha \in K - \{0\}$ tel que $y = \alpha x$, et on a : $f(y) = \alpha f(x) = \alpha\lambda_x x$ et $f(y) = \lambda_y y = \lambda_y \alpha x$, d'où $\lambda_x = \lambda_y$.

Ceci montre : $\exists \lambda \in K, \forall x \in E - \{0\},\ f(x) = \lambda x$. Enfin : $f(0) = 0 = \lambda 0$.

7.1.7 Récurrence sur n.

Le cas $n = 1$ est trivial.

Supposons la propriété vraie pour un n de $\mathbb{N}^*$, et soient $\lambda_1,\ldots,\lambda_{n+1} \in K$ deux à deux distincts, $N_i = \mathrm{Ker}(f - \lambda_i e)$, $1 \leqslant i \leqslant n+1$.

Soit $(x_1,\ldots,x_{n+1}) \in N_1 \times \ldots \times N_{n+1}$ tel que $\sum_{i=1}^{n+1} x_i = 0$.

En appliquant f : $0 = f(0) = f\left(\sum_{i=1}^{n+1} x_i\right) = \sum_{i=1}^{n+1} f(x_i) = \sum_{i=1}^{n+1} \lambda_i x_i$.

En combinant les deux égalités : $0 = \sum_{i=1}^{n+1} \lambda_i x_i - \lambda_{n+1} \sum_{i=1}^{n+1} x_i = \sum_{i=1}^{n} (\lambda_i - \lambda_{n+1}) x_i$.

Comme $\sum_{i=1}^{n} N_i$ est directe, on déduit : $\forall i \in \{1,\ldots,n\}, (\lambda_i - \lambda_{n+1}) x_i = 0$,

puis, comme $(\forall i \in \{1,\ldots,n\}, \lambda_i \neq \lambda_{n+1})$: $\forall i \in \{1,\ldots,n\}, x_i = 0$, et enfin : $x_{n+1} = -\sum_{i=1}^{n} x_i = 0$.

Ceci montre que $N_1,\ldots,N_{n+1}$ sont linéairement indépendants.

7.2.1 *a)* Immédiat.

b) ◇ **Réponse :** $\psi \circ \varphi : \begin{array}{ccc} E & \longrightarrow & E \\ f & \longmapsto & f - f(0) \end{array}$, $\varphi \circ \psi = \mathrm{Id}_E$.

c) Il est clair que $\psi \circ \varphi$ n'est ni injective (car $\psi \circ \varphi(1) = 0$), ni surjective (car $1 \notin \mathrm{Im}(\psi \circ \varphi)$).

◇ **Réponse :** $\begin{cases} \varphi & \text{est surjective et non injective} \\ \psi & \text{est injective et non surjective} \end{cases}$.

7.2.2 Comme $(\alpha e + g)^n = e$, en développant par la formule du binôme de Newton (e et g commutent), on obtient :

$$(\alpha^n - 1)e + \sum_{k=1}^{n} C_n^k \alpha^{n-k} g^k = 0.$$

En notant $u = \dfrac{1}{1-\alpha^n} \sum_{k=1}^{n} C_n^k \alpha^{n-k} g^{k-1}$, on a donc : $g \circ u = u \circ g = e$, ce qui montre que g est bijective et $g^{-1} = u$.

◇ **Réponse :** $g^{-1} = \dfrac{1}{1-\alpha^n} \sum_{k=1}^{n} C_n^k \alpha^{n-k} g^{k-1}$.

7.2.3 Pour tous (x,y), (X,Y) de $E \times F$:

$$\varphi(x,y) = (X,Y) \Longleftrightarrow \begin{cases} x + g(y) = X \\ y = Y \end{cases} \Longleftrightarrow \begin{cases} x = X - g(Y) \\ y = Y \end{cases}.$$

Comme $\psi : \begin{array}{ccc} E \times F & \longrightarrow & E \times F \\ (X,Y) & \longmapsto & (X - g(Y), Y) \end{array}$ est linéaire et que $\psi \circ \varphi = \varphi \circ \psi = \mathrm{Id}_{E \times F}$, on conclut que φ est un automorphisme de $E \times F$, et $\varphi^{-1} = \psi$.

7.2.4 On a : $f \circ (g \circ f) = (f \circ g) \circ f = e \circ f = f$, d'où : $f \circ (g \circ f - e) = 0$, puis : $f \circ (g \circ f - e + g) = f \circ (g \circ f - e) + f \circ g = f \circ g = e$.

D'après l'hypothèse, on déduit : $g \circ f - e + g = g$, d'où $g \circ f = e$.

7.2.5 Soit $(\lambda_0,\dots,\lambda_{p-1}) \in K^p$ tel que $\sum_{i=0}^{p-1} \lambda_i f^i = 0$.

En composant par f^{p-1}, on déduit $\lambda_0 = 0$.

Puis, en composant par f^{p-2} dans $\sum_{i=1}^{p-1} \lambda_i f^i = 0$, on déduit $\lambda_1 = 0$, etc.

7.2.6 L'application f, qui est linéaire, est injective si et seulement si :

$$\forall (x_1,\dots,x_n) \in E_1 \times \dots \times E_n,\ \left(\sum_{i=1}^{n} x_i = 0 \Longrightarrow \big(\forall i \in \{1,\dots,n\}, x_i = 0\big)\right),$$

c'est-à-dire si et seulement si $E_1,\dots,E_n$ sont linéairement indépendants (cf. 6.3.3 Déf. 2 p. 221).

7.2.7 Il est clair que f est linéaire.

a) Soient $x \in E$, et $(x_1,\dots,x_n) \in E_1 \times \dots \times E_n$ tel que $x = \sum_{i=1}^{n} x_i$. On a :

$$x \in \mathrm{Ker}(f) \Longleftrightarrow \sum_{i=1}^{n} f_i(x_i) = 0 \Longleftrightarrow \big(\forall i \in \{1,\dots,n\},\ f_i(x_i) = 0\big)$$

$$\Longleftrightarrow \big(\forall i \in \{1,\dots,n\},\ x_i \in \mathrm{Ker}(f_i)\big) \Longleftrightarrow x \in \sum_{i=1}^{n} \mathrm{Ker}(f_i),$$

d'où : $\mathrm{Ker}(f) = \sum_{i=1}^{n} \mathrm{Ker}(f_i)$.

De plus, comme $\big(\forall i \in \{1,\dots,n\}, \mathrm{Ker}(f_i) \subset E_i\big)$ et que $\sum_{i=1}^{n} E_i$ est directe, $\sum_{i=1}^{n} \mathrm{Ker}(f_i)$ est directe.

b) Soit $y \in \mathrm{Im}(f)$. Il existe $x \in E$ tel que $y = f(x)$, puis $(x_1,\dots,x_n) \in E_1 \times \dots \times E_n$ tel que $x = \sum_{i=1}^{n} x_i$,

et on a : $y = \sum_{i=1}^{n} f_i(x_i) \in \sum_{i=1}^{n} \mathrm{Im}(f_i)$.

On montre de même la réciproque, d'où : $\mathrm{Im}(f) = \sum_{i=1}^{n} \mathrm{Im}(f_i)$.

De plus, comme $\big(\forall i \in \{1,\dots,n\}, \mathrm{Im}(f_i) \subset E_i\big)$ et que $\sum_{i=1}^{n} E_i$ est directe, $\sum_{i=1}^{n} \mathrm{Im}(f_i)$ est directe.

7.2.8 *1)* Soit $x \in \mathrm{Ker}(f)$. On a : $f\big(g(x)\big) = (f \circ g)(x) = (g \circ f)(x) = g\big(f(x)\big) = g(0) = 0$, donc $g(x) \in \mathrm{Ker}(f)$.

Ceci montre que $\mathrm{Ker}(f)$ est stable par g.

2) Soit $y \in \mathrm{Im}(f)$. Il existe $x \in E$ tel que $y = f(x)$, et on a :

$$g(y) = g\big(f(x)\big) = (g \circ f)(x) = (f \circ g)(x) = f\big(g(x)\big) \in \mathrm{Im}(f).$$

Ceci montre que $\mathrm{Im}(f)$ est stable par g.

7.2.9 *a)* • $\forall x \in E, \big(x \in \mathrm{Ker}(g \circ f) \Longleftrightarrow (g \circ f)(x) = 0 \Longleftrightarrow g\big(f(x)\big) = 0$
$\Longleftrightarrow f(x) \in \mathrm{Ker}(g) \Longleftrightarrow x \in f^{-1}(\mathrm{Ker}(g))\big)$.

• Puisque $\mathrm{Ker}(g) \supset \{0\}$, on a : $\mathrm{Ker}(g \circ f) = f^{-1}\big(\mathrm{Ker}(g)\big) \supset f^{-1}(\{0\}) = \mathrm{Ker}(f)$.

b) • $\mathrm{Im}(g \circ f) = (g \circ f)(E) = g\big(f(E)\big) = g\big(\mathrm{Im}(f)\big)$.

• $\mathrm{Im}(g \circ f) = g\big(\mathrm{Im}(f)\big) \subset g(F) = \mathrm{Im}(g)$.

7.2.10 *1)* Supposons $\mathrm{Ker}(g \circ f) = \mathrm{Ker}(h \circ f)$.

Soit $y \in \mathrm{Im}(f) \cap \mathrm{Ker}(g)$; il existe $x \in E$ tel que $y = f(x)$, et $g(y) = 0$, d'où $g\big(f(x)\big) = 0$.

Ainsi, $x \in \mathrm{Ker}(g \circ f) = \mathrm{Ker}(h \circ f)$, donc $h(y) = h\big(f(x)\big) = 0$, $y \in \mathrm{Ker}(h)$.

Ceci montre : $\mathrm{Im}(f) \cap \mathrm{Ker}(g) \subset \mathrm{Im}(f) \cap \mathrm{Ker}(h)$. Les rôles symétriques de g et h dans l'hypothèse permettent de conclure à l'égalité.

2) Réciproquement, supposons $\mathrm{Im}(f) \cap \mathrm{Ker}(g) = \mathrm{Im}(f) \cap \mathrm{Ker}(h)$.

Soit $x \in \mathrm{Ker}(g \circ f)$. Alors $f(x) \in \mathrm{Im}(f) \cap \mathrm{Ker}(g) = \mathrm{Im}(f) \cap \mathrm{Ker}(h)$, donc $h\big(f(x)\big) = 0$, $x \in \mathrm{Ker}(h \circ f)$.

Ceci montre : $\mathrm{Ker}(g \circ f) \subset \mathrm{Ker}(h \circ f)$, puis, par rôles symétriques de g et h, l'égalité.

7.2.11 *a)* On a, pour tout x de V :

• $(f + g)(x) = f(x) + g(x) \in V$

• $(\lambda f)(x) = \lambda f(x) \in V$

• $(g \circ f)(x) = g\big(f(x)\big) \in V$.

b) Récurrence immédiate sur n, en utilisant *a)* $(g \circ f)$.

c) ◇ **Réponse :** $E = \mathbb{R}^{\mathbb{R}}$ (lois usuelles), $f : \begin{array}{ccc} E & \longrightarrow & E \\ u & \longmapsto & f(u) \end{array}$ où $f(u) : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & u(x-1) \end{array}$,

$V = \{u \in E;\ \forall x \in \mathbb{R}_-,\ u(x) = 0\}$.

7.2.12 Raisonnons par l'absurde : supposons qu'il existe $\alpha \in K - \{0\}$ tel que $q = \alpha p$. Alors : $\alpha p = q = q^2 = (\alpha p)^2 = \alpha^2 p^2 = \alpha^2 p$, d'où $\alpha = \alpha^2$, $\alpha = 1$, $q = p$, contradiction.

7.2.13 Soit $x \in E$. Comme $x - p(x) \in \mathrm{Ker}(p) = \mathrm{Ker}(q)$, on a $q\big(x - p(x)\big) = 0$, d'où $q(x) = (q \circ p)(x)$. Comme p et q jouent des rôles symétriques dans les hypothèses, on a aussi $p(x) = (p \circ q)(x) = (q \circ p)(x)$, d'où $q(x) = p(x)$.

7.2.14 *1)* Si $p \circ q = q \circ p = 0$, alors : $(p + q)^2 = p^2 + p \circ q + q \circ p + q^2 = p^2 + q^2 = p + q$, et donc $p + q$ est un projecteur.

2) Réciproquement, supposons que $p + q$ soit un projecteur. On a :

$$p + q = (p + q)^2 = p^2 + p \circ q + q \circ p + q^2 = p + p \circ q + q \circ p + q,$$

d'où $p \circ q = -q \circ p$, puis : $p \circ q = -p \circ (q \circ p) = -(p \circ q) \circ p = (q \circ p) \circ p = q \circ p$, et donc $2p \circ q = 2q \circ p = 0$, $p \circ q = q \circ p = 0$.

7.2.15 (i) $\Longrightarrow$ (ii) :

On a : $f \circ f = f \circ (g \circ f) = (f \circ g) \circ f = g \circ f = f$, et de même : $g \circ g = g$.

Soit $x \in \mathrm{Im}(f)$. Puisque f est un projecteur : $f(x) = x$.

Puis : $x = f(x) = (g \circ f)(x) = g(f(x)) \in \mathrm{Im}(g)$.

Ainsi : $\mathrm{Im}(f) \subset \mathrm{Im}(g)$.

Les rôles symétriques de f, g dans les hypothèses permettent de conclure à l'égalité.

(ii) $\Longrightarrow$ (i) :

Soit $x \in E$. On a : $f(x) \in \mathrm{Im}(f) = \mathrm{Im}(g)$, d'où, puisque g est un projecteur : $g(f(x)) = f(x)$.

Ainsi $g \circ f = f$, et de même, $f \circ g = g$.

7.2.16 *1)* • $0 \in L$

• Si $\lambda \in K$ et $(f_1, f_2) \in L^2$, il existe $(u_1, u_2) \in \big(\mathcal{L}(E)\big)^2$ tel que $f_1 = u_1 \circ p$ et $f_2 = u_2 \circ p$, d'où $\lambda f_1 + f_2 = (\lambda u_1 + u_2) \circ p \in L$.

Ceci montre que L est un sev de $\mathcal{L}(E)$.

En appliquant ce résultat au projecteur $q = e - p$, on en déduit que M est aussi un sev de $\mathcal{L}(E)$.

2) • Soit $f \in L \cap M$. Il existe $u, v \in \mathcal{L}(E)$ tels que $f = u \circ p = v \circ q$, d'où :

$$f = u \circ p = u \circ p^2 = (u \circ p) \circ p = (v \circ q) \circ p = v \circ (q \circ p) = v \circ 0 = 0.$$

Ceci montre : $L \cap M = \{0\}$.

• $\forall f \in \mathcal{L}(E)$, $f = f \circ (p + q) = f \circ p + f \circ q$, d'où : $L + M = \mathcal{L}(E)$.

7.2.17 *a) 1)* Si $f \circ g = \mathrm{Id}_F$, alors f est surjective puisque : $\forall y \in F$, $y = (f \circ g)(y) = f\big(g(y)\big)$.

2) Réciproquement, supposons f surjective.

Le sev $\mathrm{Ker}(f)$ de E admet au moins un supplémentaire H dans E : $E = \mathrm{Ker}(f) \oplus H$.

L'application $\varphi : H \longrightarrow \mathrm{Im}(f)$, $x \longmapsto f(x)$ est linéaire, surjective à l'évidence, injective car, si $x \in H$ est tel que $\varphi(x) = 0$, alors $x \in H \cap \mathrm{Ker}(f) = \{0\}$, donc $x = 0$.

Considérons l'application linéaire $g : F = \mathrm{Im}(f) \longrightarrow E$ définie par : $\forall y \in F$, $g(y) = \varphi^{-1}(y)$.

On a : $\forall y \in F$, $(f \circ g)(y) = f\left(\varphi^{-1}(y)\right) = \varphi\left(\varphi^{-1}(y)\right) = y$, donc $f \circ g = \mathrm{Id}_F$.

b) 1) Si $h \circ f = \mathrm{Id}_E$, alors f est injective puisque : $\forall x \in \mathrm{Ker}(f)$, $x = (h \circ f)(x) = h(f(x)) = h(0) = 0$.

2) Réciproquement, supposons f injective. Le sev $\mathrm{Im}(f)$ de F admet au moins un supplémentaire L dans F : $F = \mathrm{Im}(f) \oplus L$. Comme f est injective, l'application linéaire $\psi : E \longrightarrow \mathrm{Im}(f)$, $x \longmapsto f(x)$ est clairement bijective.

Considérons l'application linéaire $h : F \longrightarrow E$ définie par le recollement :

$$\begin{cases} \forall y \in \mathrm{Im}(f), & h(y) = \psi^{-1}(y) \\ \forall y \in L, & h(y) = 0 \end{cases}.$$

On a : $\forall x \in E$, $(h \circ f)(x) = h(f(x)) = \psi^{-1}(f(x)) = x$, donc $h \circ f = \mathrm{Id}_E$.

7.2.18 *a) 1)* S'il existe $h \in \mathcal{L}(F, G)$ tel que $g = h \circ f$, alors :
$\forall x \in \mathrm{Ker}(f)$, $g(x) = h(f(x)) = h(0) = 0$, donc $\mathrm{Ker}(f) \subset \mathrm{Ker}(g)$.

2) Réciproquement, supposons $\mathrm{Ker}(f) \subset \mathrm{Ker}(g)$.

Le sev $\mathrm{Im}(f)$ de F admet au moins un supplémentaire L dans F : $F = \mathrm{Im}(f) \oplus L$.

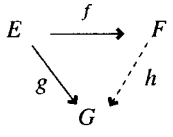
Soit $y \in F$. Il existe $(z,u) \in \mathrm{Im}(f) \times L$ unique tel que $y = z + u$, puis il existe $x \in E$ tel que $z = f(x)$. Si $x_1, x_2 \in E$ sont tels que $z = f(x_1) = f(x_2)$, alors $x_1 - x_2 \in \mathrm{Ker}(f) \subset \mathrm{Ker}(g)$, donc $g(x_1) = g(x_2)$.

Ainsi, l'élément $g(x)$ ne dépend pas du choix de x dans E tel que $z = f(x)$ (pour z fixé).

Considérons l'application $h : \begin{array}{ccc} F & \longrightarrow & G \\ y & \longmapsto & g(x) \end{array}$ ainsi définie.

Si $\lambda \in K$, $y,y' \in F$, $x,x' \in E$, $u,u' \in L$ sont tels que $y = f(x) + u = f(x') + u'$, alors $\lambda y + y' = f(\lambda x + x') + (\lambda u + u')$, donc $h(\lambda y + y') = g(\lambda x + x') = \lambda g(x) + g(x') = \lambda h(y) + h(y')$. Ceci montre que h est linéaire.

Enfin : $\forall x \in E$, $(h \circ f)(x) = h(f(x)) = g(x)$, donc $h \circ f = g$.



b) 1) S'il existe $k \in \mathcal{L}(E,F)$ tel que $g = f \circ k$, alors, pour tout x de E : $g(x) = f(k(x)) \in \mathrm{Im}(f)$, donc $\mathrm{Im}(g) \subset \mathrm{Im}(f)$.

2) Réciproquement, supposons $\mathrm{Im}(g) \subset \mathrm{Im}(f)$. Le sev $\mathrm{Ker}(f)$ de F admet au moins un supplémentaire H dans F : $F = \mathrm{Ker}(f) \oplus H$. Soit $x \in E$. On a : $g(x) \in \mathrm{Im}(g) \subset \mathrm{Im}(f)$. Il existe donc $y \in F$ tel que $g(x) = f(y)$, puis il existe $u \in \mathrm{Ker}(f)$, $z \in H$ tels que $y = u + z$.

Montrons que z ne dépend pas du choix de y dans F. Si $y_1, y_2 \in F$ sont tels que $g(x) = f(y_1) = f(y_2)$, et $u_1, u_2 \in \mathrm{Ker}(f)$, $z_1, z_2 \in H$ sont tels que $y_1 = u_1 + z_1$ et $y_2 = u_2 + z_2$, alors $y_1 - y_2 \in \mathrm{Ker}(f)$, donc : $z_1 - z_2 = (y_1 - y_2) - (u_1 - u_2) \in \mathrm{Ker}(f) \cap H$, donc $z_1 = z_2$.

Considérons l'application $k : \begin{array}{ccc} E & \longrightarrow & F \\ x & \longmapsto & z \end{array}$ ainsi définie.

Si $\lambda \in K, x,x' \in E, y,y' \in F$ sont tels que $g(x) = f(y)$ et $g(x') = f(y')$, puis $u,u' \in \mathrm{Ker}(f), z,z' \in H$ sont tels que $y = u + z$, $y' = u' + z'$, alors :

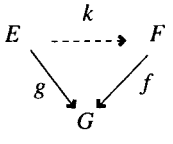
$$g(\lambda x + x') = \lambda g(x) + g(x') = \lambda f(y) + f(y') = f(\lambda y + y'), \text{ et } \lambda y + y' = (\lambda u + u') + (\lambda z + z'),$$

d'où $k(\lambda x + x') = \lambda z + z' = \lambda k(x) + k(x')$.

Ceci montre que k est linéaire.

Enfin, avec les notations précédentes :

$\forall x \in E$, $(f \circ k)(x) = f(k(x)) = f(z) = f(y - u) = f(y) - f(u) = f(y) = g(x)$, donc $f \circ k = g$.



Remarque : L'exercice 7.2.17 est un cas particulier de l'exercice 7.2.18, en prenant $G = E$ et $g = \mathrm{Id}_E$.

7.2.19 Il est clair que :

- $\forall f \in \mathcal{L}(E,F)$, $\forall g \in \mathcal{L}(F,G)$, $g \circ f \in \mathcal{L}(E,G)$
- Pour toute f de $\mathcal{L}(E,F)$, $\phi(f)$ est linéaire, donc $\phi(f) \in \mathcal{L}\big(\mathcal{L}(F,G), \mathcal{L}(E,G)\big)$
- De même : $\forall g \in \mathcal{L}(F,G)$, $\Psi(g) \in \mathcal{L}\big(\mathcal{L}(E,F), \mathcal{L}(E,G)\big)$.

a) 1) Si f est surjective, alors : $\mathrm{Ker}(\phi(f)) = \{g \in \mathcal{L}(E,F),\ F = \mathrm{Im}(f) \subset \mathrm{Ker}(g)\} = \{0\}$, donc $\phi(f)$ est injective.

2) Réciproquement, supposons $\phi(f)$ injective. Le sev $\mathrm{Im}(f)$ de F admet au moins un supplémentaire

L dans F : $F = \text{Im}(f) \oplus L$. Supposons $L \neq \{0\}$; il existe $y_0 \in L - \{0\}$, puis le sev Ky_0 de L admet au moins un supplémentaire L' dans L, de sorte que : $F = \text{Im}(f) \oplus L' \oplus (Ky_0)$.

D'autre part, puisque $G \neq \{0\}$, il existe $z_0 \in G$ tel que $z_0 \neq 0$.

Considérons l'application linéaire $g : F \longrightarrow G$ définie par le recollement : $\begin{cases} \forall y \in \text{Im}(f) \oplus L', \quad g(y) = 0 \\ g(y_0) = z_0. \end{cases}$

On a alors $(\phi(f))(g) = g \circ f = 0$ et $g \neq 0$, contradiction.

Ceci montre $\text{Im}(f) = F$, donc f est surjective.

b) 1) Supposons f injective.

Pour tout h de $\mathcal{L}(E,G)$, on a $\text{Ker}(f) = \{0\} \subset \text{Ker}(h)$, donc (ex. 7.2.18 *a)* p. 252) il existe $g \in \mathcal{L}(F,G)$ tel que $h = g \circ f = (\phi(f))(g)$.

Ceci montre que $\phi(f)$ est surjective.

2) Réciproquement, supposons $\phi(f)$ surjective.

Supposons $\text{Ker}(f) \neq \{0\}$.

Il existe $x_0 \in \text{Ker}(f) - \{0\}$, puis le sev Kx_0 de E admet au moins un supplémentaire H dans E : $E = (Kx_0) \oplus H$. Puisque $G \neq \{0\}$, il existe $z_0 \in G$ tel que $z_0 \neq 0$.

Considérons l'application linéaire $h : E \longrightarrow G$ définie par le recollement : $\begin{cases} h(x_0) = z_0 \\ \forall x \in H, \quad h(x) = 0. \end{cases}$

Puisque $\phi(f)$ est surjective, il existe $g \in \mathcal{L}(F,G)$ tel que $h = (\phi(f))(g) = g \circ f$, d'où : $z_0 = h(x_0) = (g \circ f)(x_0) = g(f(x_0)) = g(0) = 0$, contradiction.

Ceci montre $\text{Ker}(f) = \{0\}$, donc f est injective.

c) 1) Supposons g injective.

Soit $f \in \text{Ker}(\Psi(g))$, c'est-à-dire : $f \in \mathcal{L}(E,F)$ et $(\Psi(g))(f) = g \circ f = 0$.

Alors : $\forall x \in E, g(f(x)) = 0$, d'où, puisque g est injective : $\forall x \in E, f(x) = 0$, et donc $f = 0$.

Ceci montre $\text{Ker}(\Psi(g)) = \{0\}$, $\Psi(g)$ injective.

2) Réciproquement, supposons $\Psi(g)$ injective.

Supposons g non injective. Il existe $y_0 \in \text{Ker}(g)$ tel que $y_0 \neq 0$.

Puisque $E \neq \{0\}$, il existe $x_0 \in E$ tel que $x_0 \neq 0$. Le sev Kx_0 de E admet au moins un supplémentaire H dans E : $E = (Kx_0) \oplus H$.

Considérons l'application linéaire $f : E \longrightarrow F$ définie par le recollement : $\begin{cases} \forall x \in H, \quad f(x) = 0 \\ f(x_0) = y_0. \end{cases}$

On a : $\begin{cases} \forall x \in H, (g \circ f)(x) = g(f(x)) = g(0) = 0 \\ (g \circ f)(x_0) = g(y_0) = 0 \end{cases}$, donc $g \circ f = 0$.

Comme $(\Psi(g))(f) = g \circ f = 0$ et que $\Psi(g)$ est injective, on déduit $f = 0$, contradiction avec $f(x_0) = y_0 \neq 0$.

Ceci montre que g est injective.

d) 1) Supposons g surjective.

Pour tout h de $\mathcal{L}(E,G)$, on a $\text{Im}(h) \subset G = \text{Im}(g)$, donc (ex. 7.2.18 *b)* p. 252) il existe $f \in \mathcal{L}(E,F)$ tel que $h = g \circ f = (\Psi(g))(f)$.

Ceci montre que $\Psi(g)$ est surjective.

2) Réciproquement, supposons $\Psi(g)$ surjective.

Soit $z \in G$.

Puisque $E \neq \{0\}$, il existe $x_0 \in E$ tel que $x_0 \neq 0$, puis le sev Kx_0 de E admet au moins un supplémentaire H dans E : $E = (Kx_0) \oplus H$. Considérons l'application linéaire $h : E \longrightarrow G$ définie par le recollement :

$\begin{cases} \forall x \in H, h(x) = 0 \\ h(x_0) = z_0 \end{cases}$. Puisque $\Psi(g)$ est surjective, il existe $f \in \mathcal{L}(E,F)$ tel que $h = (\Psi(g))(f) = g \circ f$.

On a donc : $z_0 = h(x_0) = (g \circ f)(x_0) = g(f(x_0)) \in \text{Im}(g)$.

Ceci montre : $\forall z_0 \in G, z_0 \in \text{Im}(g)$, et donc g est surjective.

7.2.20 **(i) $\Longrightarrow$ (ii) :**

Supposons qu'il existe $f \in \mathcal{L}(E)$ tel que $\mathrm{Im}(f) = F$ et $\mathrm{Ker}(f) = G$.

Le sev G de E admet au moins un supplémentaire H dans E : $E = G \oplus H$.

Considérons l'application linéaire $\widetilde{f} : \begin{array}{c} H \longrightarrow F \\ x \longmapsto f(x) \end{array}$, restriction de f à H au départ.

• $\widetilde{f}$ est injective car, si $x \in H$ et $\widetilde{f}(x) = 0$, alors $x \in H \cap G = \{0\}$, donc $x = 0$.

• $\widetilde{f}$ est surjective car, pour tout y de F $(= \mathrm{Im}(f))$, il existe $t \in E$ tel que $y = f(t)$, puis il existe $(u,x) \in G \times H$ tel que $t = u + x$, et on a $y = f(t) = f(u) + f(x) = f(x) = \widetilde{f}(x)$.

Ainsi, $\widetilde{f}$ est un isomorphisme de H sur F.

(ii) $\Longrightarrow$ (i) :

Supposons qu'il existe un supplémentaire H de G dans E tel que $H \simeq F$. Il existe donc un isomorphisme $\varphi : H \longrightarrow F$.

Soit $f : E \longrightarrow E$ *l'application linéaire définie par le recollement* : $\begin{cases} \forall x \in G, & f(x) = 0 \\ \forall x \in H, & f(x) = \varphi(x). \end{cases}$

Il est clair que : $\mathrm{Im}(f) = \mathrm{Im}(\varphi) = F$ et $\mathrm{Ker}(f) = G$.

Remarque : Si E est de dimension finie, la condition (ii) est équivalente à : $\dim(F) + \dim(G) = \dim(E)$ (cf. 6.4 Prop. 6 p. 231).

7.2.21 *a)* En notant $i : E' \longrightarrow E$ et $j : F \longrightarrow F'$ les injections canoniques, on a : $\forall f \in \mathcal{L}(E,F)$, $\phi(f) = j \circ f \circ i$, d'où l'on déduit facilement la linéarité de ϕ.

$$\begin{array}{ccc} E' & \xrightarrow{\ i\ } & E \\ {\scriptstyle \phi(f)}\downarrow & & \downarrow{\scriptstyle f} \\ F' & \xleftarrow[\ j\ ]{} & F \end{array}$$

b) • Pour tout f de $\mathcal{L}(E,F)$:

$$f \in \mathrm{Ker}(\phi) \Longleftrightarrow j \circ f \circ i = 0 \Longleftrightarrow f \circ i = 0 \Longleftrightarrow \mathrm{Im}(i) \subset \mathrm{Ker}(f) \Longleftrightarrow E' \subset \mathrm{Ker}(f).$$

• *1)* Soit $f' \in \mathrm{Im}(\phi)$. Il existe $f \in \mathcal{L}(E,F)$ tel que $f' = \phi(f) = j \circ f \circ i$,

d'où : $\forall x' \in E'$, $f'(x') = f(x')$, et donc : $\mathrm{Im}(f') \subset F$.

2) Réciproquement, soit $f' \in \mathcal{L}(E',F')$ tel que $\mathrm{Im}(f') \subset F$.

Le sev E' de E admet au moins un supplémentaire G dans E : $E = E' \oplus G$.

Considérons l'application linéaire $f : E \longrightarrow F$ définie par le recollement : $\begin{cases} \forall x \in E', & f(x) = f'(x) \\ \forall x \in G, & f(x) = 0. \end{cases}$

Alors : $\forall x \in E'$, $(j \circ f \circ i)(x) = f(x) = f'(x)$, donc $f' = j \circ f \circ i = \phi(f)$.

◇ **Réponse :** $\begin{cases} \mathrm{Ker}(\phi) = \{f \in \mathcal{L}(E,F);\ \mathrm{Ker}(f) \supset E'\} \\ \mathrm{Im}(\phi) = \{f' \in \mathcal{L}(E',F');\ \mathrm{Im}(f') \subset F\}. \end{cases}$

7.2.22 Le sev $\mathrm{Ker}(f)$ de E admet au moins un supplémentaire G dans E : $E = \mathrm{Ker}(f) \oplus G$.

Soit $\varphi : \begin{array}{c} G \longrightarrow \mathrm{Im}(f) \\ x \longmapsto f(x) \end{array}$. Montrer que φ est un isomorphisme d'espaces vectoriels (cf. la solution de l'exercice 7.2.17 *a)* p. 522).

Le sev $\mathrm{Im}(f)$ de F admet au moins un supplémentaire L dans F : $F = \mathrm{Im}(f) \oplus L$. Considérons l'application linéaire $g : F \longrightarrow E$ définie par le recollement : $\begin{cases} \forall y \in \mathrm{Im}(f), & g(y) = \varphi^{-1}(y) \\ \forall y \in L, & g(y) = 0. \end{cases}$

On a :

- $\forall x \in E, (f \circ g \circ f)(x) = f\big(g(f(x))\big) = f\big(\varphi^{-1}(f(x))\big) = \varphi\big(\varphi^{-1}(f(x))\big) = f(x)$,

donc $f \circ g \circ f = f$

- $\left.\begin{cases} \forall y \in \mathrm{Im}(f), (g \circ f \circ g)(y) = (g \circ f)(\varphi^{-1}(y)) = g\big(\varphi(\varphi^{-1}(y))\big) = g(y) \\ \forall y \in L, (g \circ f \circ g)(y) = (g \circ f)(g(y)) = (g \circ f)(0) = 0 = g(y) \end{cases}\right|$, donc $g \circ f \circ g = g$.

7.2.23 *a)* On peut remarquer que G n'est pas vide, puisqu'il contient le projecteur sur E_2 parallèlement à E_1.

Soit $f \in G$. Comme $f(E_2) \subset f(E) = E_2$, E_2 est stable par f. Notons $f' : E_2 \longrightarrow E_2$ l'endomorphisme de E_2 induit par f.

1) **f' est injective**

Soit $x \in E_2$ tel que $f'(x) = 0$. On a alors $x \in E_2$ et $x \in \mathrm{Ker}(f) = E_1$, d'où $x = 0$.

Ceci montre que f' est injective.

2) **f' est surjective**

Soit $y \in E_2 = \mathrm{Im}(f)$. Il existe $x \in E$ tel que $y = f(x)$, puis il existe $(x_1,x_2) \in E_1 \times E_2$ tel que $x = x_1 + x_2$.

On a : $y = f(x_1) + f(x_2) = f(x_2) = f'(x_2)$.

Ainsi, f' est surjective.

b) Considérons l'application $\theta : G \longrightarrow \mathcal{GL}(E_2)$, où f' est l'endomorphisme de E_2 induit par f.
$f \longmapsto f'$

1) Montrons que $\circ$ est interne dans G.

Soient $f,g \in G$.

- On a : $(g \circ f)(E_2) = g(f(E_2)) = g(E_2) = E_2$.
- $E_1 = \mathrm{Ker}(f) \subset \mathrm{Ker}(g \circ f)$.
- Soit $x \in \mathrm{Ker}(g \circ f)$. Il existe $(x_1,x_2) \in E_1 \times E_2$ tel que $x = x_1 + x_2$; on a :

$$0 = (g \circ f)(x) = g(f(x_1)) + g(f(x_2)) = g'(f'(x_2)) = (g' \circ f')(x_2).$$

Comme f' et g' sont bijectives, on déduit $x_2 = 0$, puis $x = x_1 \in E_1 = \mathrm{Ker}(f)$.

Ainsi : $\left.\begin{cases} \mathrm{Ker}(g \circ f) = \mathrm{Ker}(f) = E_1 \\ \mathrm{Im}(g \circ f) = E_2 \end{cases}\right|$, et donc $g \circ f \in G$.

2) L'application $\theta : G \longrightarrow \mathcal{GL}(E_2)$ est un morphisme pour la loi $\circ$ car :

$$\forall f,g \in G, \forall x \in E_2, (\theta(g \circ f))(x) = (g \circ f)'(x) = (g \circ f)(x) = (g' \circ f')(x),$$

donc : $\forall f,g \in G, \theta(g \circ f) = \theta(g) \circ \theta(f)$.

3) **Injectivité de θ**

Soit $f \in G$ tel que $f' = \theta(f) = 0$.

Soit $x \in E$. Il existe $(x_1,x_2) \in E_1 \times E_2$ tel que $x = x_1 + x_2$.

On a : $f(x) = f(x_1) + f(x_2) = f(x_2) = f'(x_2) = 0$.

Ceci montre $f = 0$, et donc θ est injective.

4) **Surjectivité de θ**

Soit $\varphi \in \mathcal{GL}(E_2)$. Considérons l'application linéaire $f : E \longrightarrow E$ définie par le recollement :

$$\begin{cases} \forall x \in E_1, f(x) = 0 \\ \forall x \in E_2, f(x) = \varphi(x) \end{cases}.$$

Il est clair que $\mathrm{Ker}(f) = E_1$, $\mathrm{Im}(f) = E_2$, donc $f \in G$, et que : $\theta(f) = f' = \varphi$.

7.3.1 Il est clair que, pour tout P de E_n, $\sum_{i=0}^{n} P^{(i)}\left(\frac{X}{2^i}\right)$ est dans E_n, et que l'application

$f : E_n \longrightarrow E_n$ est linéaire.
$P \longmapsto \sum_{i=0}^{n} P^{(i)}\left(\frac{X}{2^i}\right)$

La famille $(f(X^k))_{0\leqslant k\leqslant n}$ est une famille de polynômes à degrés successifs, donc est une base de E_n (cf. 5.1.4 Rem. p. 146).

Ceci montre que f est bijective, d'où le résultat demandé.

7.3.2 Soient u_1,u_2,u_3 (resp. v_1,v_2,v_3) des vecteurs directeurs de D_1,D_2,D_3 (resp. $\Delta_1,\Delta_2,\Delta_3$).

Soient $(\alpha_1,\alpha_2) \in (K-\{0\})^2$ à choisir ultérieurement, et f l'endomorphisme de E défini par :

$$f(u_1) = \alpha_1 v_1 \quad \text{et} \quad f(u_2) = \alpha_2 v_2.$$

Il est clair que f est un automorphisme de E, et que $f(D_1) = \Delta_1$ et $f(D_2) = \Delta_2$.

Il reste à choisir (α_1,α_2) pour que $f(D_3) = \Delta_3$.

Comme E est de dimension 2, il existe $(a,b,c,d) \in K^4$ tel que : $u_3 = au_1 + bu_2$, $v_3 = cv_1 + dv_2$.
Puisque D_1,D_2,D_3 (resp. $\Delta_1,\Delta_2,\Delta_3$) sont deux à deux distinctes, on a : $(a,b,c,d) \in (K-\{0\})^4$.

On a :

$$f(D_3) = \Delta_3 \iff (\exists \lambda \in K-\{0\}, f(u_3) = \lambda v_3) \iff (\exists \lambda \in K-\{0\}, a\alpha_1 v_1 + b\alpha_2 v_2 = \lambda c v_1 + \lambda d v_2)$$
$$\iff \left(\exists \lambda \in K-\{0\}, \begin{cases} a\alpha_1 = \lambda c \\ b\alpha_2 = \lambda d \end{cases}\right).$$

Il suffit de choisir : $\alpha_1 = bc$, $\alpha_2 = ad$, $\lambda = ab$.

7.3.3 Il existe une base $(e_1,\ldots,e_n)$ de E, où $n = \dim(E)$. Pour chaque i de $\{1,\ldots,n\}$, il existe $p_i \in \mathbb{N}^*$ tel que $f^{p_i}(e_i) = e_i$. Notons $p = \prod_{i=1}^{n} p_i$.

On a : $\forall i \in \{1,\ldots,n\}$, $f^p(e_i) = (f^{p_i})^{\prod_{j\neq i} p_j}(e_i) = e_i$, car e_i est invariant par f^{p_i}, donc par toute puissance de f^{p_i}.

Ceci montre : $f^p = \mathrm{Id}_E$.

7.3.4 Puisque $f \circ (g+h) = f\circ g + f\circ h = e$, f est inversible à droite pour $\circ$ dans $\mathcal{L}(E)$.

Comme E est de dimension finie, d'après 7.3.1 Th. 2 p. 256, on a alors $(g+h)\circ f = e$, d'où :

$$g\circ f = e - h\circ f = e - f\circ h = f\circ g.$$

7.3.5 • Il existe $p_1 \in L_1$ et $p_2 \in L_2$ tels que $e = p_1 + p_2$.

On a : $\begin{cases} p_1 = (p_1+p_2)\circ p_1 = p_1\circ p_1 + p_2\circ p_1 \\ p_1 = p_1\circ(p_1+p_2) = p_1\circ p_1 + p_1\circ p_2 \end{cases}$, d'où $2p_1 = 2p_1\circ p_1 + (p_1\circ p_2 + p_2\circ p_1) = 2p_1\circ p_1$,

et donc $p_1\circ p_1 = p_1$. De même $p_2\circ p_2 = p_2$.

Ainsi, p_1,p_2 sont deux projecteurs associés.

Notons $E_1 = \mathrm{Im}(p_1) = \mathrm{Ker}(p_2)$, $E_2 = \mathrm{Im}(p_2) = \mathrm{Ker}(p_1)$; on a : $E_1 \oplus E_2 = E$.

• Soit $f_1 \in L_1$.

On a : $\forall x \in E_1$, $p_2(f_1(x)) = -(f_1\circ p_2)(x) = -f_1(0) = 0$, donc : $\forall x \in E_1$, $f_1(x) \in \mathrm{Ker}(p_2) = E_1$.

Ceci montre : $f_1(E_1) \subset E_1$.

Soit $x \in E_2$. On a : $f_1(x) = f_1\big(p_2(x)\big) = -p_2 \circ f_1(x)$, puis, en composant par p_2 :
$p_2\big(f_1(x)\big) = -p_2 \circ p_2 \circ f_1(x) = -p_2 \circ f_1(x)$, donc : $p_2 \circ f_1(x) = 0$, d'où $f_1(x) = 0$.
Ceci montre : $f_1(E_2) = \{0\}$.

• On peut donc considérer, pour $f_1 \in L_1$, l'endomorphisme induit $f_1' : \begin{array}{c} E_1 \longrightarrow E_1 \\ x \longmapsto f_1(x) \end{array}$.

Il est clair que l'application $\theta_1 : \begin{array}{c} L_1 \longrightarrow \mathcal{L}(E_1) \\ f_1 \longmapsto f_1' \end{array}$ est linéaire. De plus, pour tout f_1 de $\mathrm{Ker}(\theta_1)$, on a $f_1(E_1) = \{0\}$ et $f_1(E_2) = \{0\}$, donc $f_1 = 0$; ceci montre que θ_1 est injective.

• Il en résulte : $\dim(L_1) \leqslant \dim\big(\mathcal{L}(E_1)\big) = \big(\dim(E_1)\big)^2$.

Puisque L_1 et L_2 jouent des rôles symétriques dans les hypothèses, on a aussi : $\dim(L_2) \leqslant \big(\dim(E_2)\big)^2$.

D'autre part : $\big(\dim(E)\big)^2 = \dim\big(\mathcal{L}(E)\big) = \dim(L_1 \oplus L_2) = \dim(L_1) + \dim(L_2)$.

On obtient : $\big(\dim(E_1) + \dim(E_2)\big)^2 \leqslant \big(\dim(E_1)\big)^2 + \big(\dim(E_2)\big)^2$, d'où : $2\dim(E_1)\dim(E_2) \leqslant 0$, donc : $\dim(E_1) = 0$ ou $\dim(E_2) = 0$, c'est-à-dire : $E_1 = \{0\}$ ou $E_2 = \{0\}$, et finalement :

$$L_1 = \{0\} \text{ ou } L_2 = \{0\}.$$

7.3.6 D'abord, il est clair que : $\mathrm{Ker}(f) \subset \mathrm{Ker}(f^2)$.

En notant $p = \dim\big(\mathrm{Ker}(f)\big)$, $q = \dim\big(\mathrm{Ker}(f^2)\big) - \dim\big(\mathrm{Ker}(f)\big)$, il existe $u_1,\ldots,u_p,v_1,\ldots,v_q \in E$ tels que :

$$\begin{cases} (u_1,\ldots,u_p) \text{ est une base de } \mathrm{Ker}(f) \\ (u_1,\ldots,u_p,v_1,\ldots,v_q) \text{ est une base de } \mathrm{Ker}(f^2). \end{cases}$$

Soit $(\lambda_1,\ldots,\lambda_q) \in K^q$ tel que $\sum_{j=1}^{q} \lambda_j f(v_j) = 0$. Alors $\sum_{j=1}^{q} \lambda_j v_j \in \mathrm{Ker}(f)$ et il existe donc $(\alpha_1,\ldots,\alpha_p) \in K^p$ tel que $\sum_{j=1}^{q} \lambda_j v_j = \sum_{i=1}^{p} \alpha_i u_i$.

Comme $(u_1,\ldots,u_p,v_1,\ldots,v_q)$ est libre, on en déduit : $\lambda_1 = \ldots = \lambda_q = 0$.

Ceci montre que $(f(v_j))_{1 \leqslant j \leqslant q}$ est libre.

Puisque : $\forall j \in \{1,\ldots,q\}$, $f(v_j) \in \mathrm{Ker}(f)$, on a donc : $q \leqslant \dim\big(\mathrm{Ker}(f)\big) = p$, d'où :
$\dim\big(\mathrm{Ker}(f^2)\big) = p + q \leqslant 2p = 2\dim\big(\mathrm{Ker}(f)\big)$.

7.3.7 Supposons $\lambda \neq 0$.

On a, pour tout x de E : $\begin{cases} (\lambda f)(x) = f(\lambda x) \in \mathrm{Im}(f) \\ f(x) = \lambda^{-1}(\lambda f)(x) \in \mathrm{Im}(\lambda f) \end{cases}$, d'où $\mathrm{Im}(\lambda f) = \mathrm{Im}(f)$.

◇ **Réponse :** $\mathrm{rg}(\lambda f) = \begin{cases} 0 & \text{si } \lambda = 0 \\ \mathrm{rg}(f) & \text{si } \lambda \neq 0 \end{cases}$.

7.3.8 • La linéarité de φ est immédiate :

$$\varphi\big(\lambda(x_1,x_2) + (y_1,y_2)\big) = \varphi(\lambda x_1 + y_1, \lambda x_2 + y_2) = \big(f_1(\lambda x_1 + y_1), f_2(\lambda x_2 + y_2)\big) =$$
$$\big(\lambda f_1(x_1) + f_1(y_1), \lambda f_2(x_2) + f_2(y_2)\big) = \lambda\big(f_1(x_1), f_2(x_2)\big) + \big(f_1(y_1), f_2(y_2)\big) = \lambda\varphi(x_1,x_2) + \varphi(y_1,y_2).$$

• $\forall (x_1,x_2) \in E_1 \times E_2, \varphi(x_1,x_2) = \big(f_1(x_1), f_2(x_2)\big) \in \mathrm{Im}(f_1) \times \mathrm{Im}(f_2)$, d'où : $\mathrm{Im}(\varphi) \subset \mathrm{Im}(f_1) \times \mathrm{Im}(f_2)$, et inversement : $\mathrm{Im}(f_1) \times \mathrm{Im}(f_2) \subset \mathrm{Im}(\varphi)$.

Alors : $\mathrm{rg}(\varphi) = \dim\big(\mathrm{Im}(\varphi)\big) = \dim\big(\mathrm{Im}(f_1)\big) + \dim\big(\mathrm{Im}(f_2)\big) = \mathrm{rg}(f_1) + \mathrm{rg}(f_2)$.

7.3.9 • $E = \mathrm{Id}_E(E) = (f+g)(E) \subset f(E) + g(E)$, donc : $E = \mathrm{Im}(f) + \mathrm{Im}(g)$,
puis : $\dim(E) = \mathrm{rg}(f) + \mathrm{rg}(g) - \dim\big(\mathrm{Im}(f) \cap \mathrm{Im}(g)\big)$.
Comme par hypothèse : $\mathrm{rg}(f) + \mathrm{rg}(g) \leqslant \dim(E)$, on déduit : $\dim\big(\mathrm{Im}(f) \cap \mathrm{Im}(g)\big) = 0$, c'est-à-dire : $\mathrm{Im}(f) \cap \mathrm{Im}(g) = \{0\}$.

• Soit $x \in E$. On a $f\big(g(x)\big) \in \mathrm{Im}(f)$ et :

$$f\big(g(x)\big) = \big(f \circ (e-f)\big)(x) = \big((e-f) \circ f\big)(x) = g\big(f(x)\big) \in \mathrm{Im}(g),$$

où $e = \mathrm{Id}_E$.
Donc : $f\big(g(x)\big) = g\big(f(x)\big) = 0$, puis $f(x) = f \circ f(x)$. Ceci montre que f est un projecteur de E.
Enfin, puisque $g = e - f$, g est le projecteur associé à f.

7.3.10 Remarquons d'abord : $\mathrm{Im}(f+g) \subset \mathrm{Im}(f) + \mathrm{Im}(g)$, d'où :
$\mathrm{rg}(f+g) \leqslant \dim\big(\mathrm{Im}(f) + \mathrm{Im}(g)\big) = \mathrm{rg}(f) + \mathrm{rg}(g) - \dim\big(\mathrm{Im}(f) \cap \mathrm{Im}(g)\big)$.

1) Supposons : $\mathrm{rg}(f+g) = \mathrm{rg}(f) + \mathrm{rg}(g)$.
On a alors : $\mathrm{Im}(f) \cap \mathrm{Im}(g) = \{0\}$, et : $\dim\big(\mathrm{Im}(f+g)\big) = \dim\big(\mathrm{Im}(f)\big) + \dim\big(\mathrm{Im}(g)\big)$, d'où : $\mathrm{Im}(f+g) = \mathrm{Im}(f) + \mathrm{Im}(g)$.
Soit $x \in E$. Comme $\mathrm{Im}(f) \subset \mathrm{Im}(f+g)$, il existe $t \in E$ tel que $f(x) = (f+g)(t)$.
Alors : $g(t) = f(x-t) \in \mathrm{Im}(f) \cap \mathrm{Im}(g) = \{0\}$, donc : $t \in \mathrm{Ker}(g)$ et $x - t \in \mathrm{Ker}(f)$.
Ainsi : $x = (x-t) + t \in \mathrm{Ker}(f) + \mathrm{Ker}(g)$, et donc : $\mathrm{Ker}(f) + \mathrm{Ker}(g) = E$.

2) Réciproquement, supposons $\begin{cases} \mathrm{Im}(f) \cap \mathrm{Im}(g) = \{0\} \\ \mathrm{Ker}(f) + \mathrm{Ker}(g) = E \end{cases}$.
Soit $y \in \mathrm{Im}(f)$. Il existe $x \in E$ tel que $y = f(x)$, puis il existe $(u,v) \in \mathrm{Ker}(f) \times \mathrm{Ker}(g)$ tel que $x = u + v$. On a : $y = f(u) + f(v) = f(v) = f(v) + g(v) = (f+g)(v) \in \mathrm{Im}(f+g)$.
Ceci montre : $\mathrm{Im}(f) \subset \mathrm{Im}(f+g)$.
Les rôles symétriques de f et g dans les hypothèses permettent de déduire : $\mathrm{Im}\, g \subset \mathrm{Im}(f+g)$, et donc : $\mathrm{Im}(f) \oplus \mathrm{Im}(g) \subset \mathrm{Im}(f+g)$.
L'autre inclusion étant déjà acquise, on obtient : $\mathrm{Im}(f+g) = \mathrm{Im}(f) \oplus \mathrm{Im}(g)$, d'où :

$$\mathrm{rg}(f+g) = \mathrm{rg}(f) + \mathrm{rg}(g).$$

7.3.11 *a)* • Pour tout y de $\mathrm{Ker}(g|_{\mathrm{Im}(f)})$, on a : $y \in \mathrm{Im}(f)$ et $g(y) = 0$, donc $y \in \mathrm{Ker}(g) \cap \mathrm{Im}(f)$.

• Réciproquement, pour tout y de $\mathrm{Ker}(g) \cap \mathrm{Im}(f)$, on a : $y \in \mathrm{Ker}(g|_{\mathrm{Im}(f)})$.

b) Le théorème du rang, appliqué à $g|_{\mathrm{Im}(f)} : \mathrm{Im}(f) \longrightarrow G$, donne :

$$\dim\big(\mathrm{Im}(g|_{\mathrm{Im}(f)})\big) = \dim\big(\mathrm{Im}(f)\big) - \dim\big(\mathrm{Ker}(g|_{\mathrm{Im}(f)})\big).$$

Comme $\mathrm{Im}\big(g|_{\mathrm{Im}(f)}\big) = g\big(\mathrm{Im}(f)\big) = (g \circ f)(E) = \mathrm{Im}(g \circ f)$, et d'après *a)*, on obtient :

$$\mathrm{rg}(g \circ f) = \mathrm{rg}(f) - \dim\big(\mathrm{Ker}(g) \cap \mathrm{Im}(f)\big).$$

c) $\mathrm{Ker}(g) \cap \mathrm{Im}(f) \subset \mathrm{Ker}(g) \implies \big(\mathrm{Ker}(g) \cap \mathrm{Im}(f)\big) \leqslant \dim\big(\mathrm{Ker}(g)\big) = \dim(F) - \mathrm{rg}(g)$
$\implies \mathrm{rg}(f) - \mathrm{rg}(g \circ f) \leqslant \dim(F) - \mathrm{rg}(g) \implies \mathrm{rg}(g \circ f) \geqslant \mathrm{rg}(f) + \mathrm{rg}(g) - \dim(F)$.

C 7.1 *1)* • $\forall \sigma \mathfrak{S}_n$, $f_\sigma(s) = f_\sigma\left(\sum_{i=1}^{n} e_i\right) = \sum_{i=1}^{n} f_\sigma(e_i) = \sum_{i=1}^{n} e_{\sigma(i)} = s$,

donc : $\forall \sigma \in \mathfrak{S}_n$, $f_\sigma(D) \subset D$, d'où : $D \in \mathfrak{F}$.

• Soient $x = \sum_{i=1}^{n} x_i e_i \in H$, $\sigma \in \mathfrak{S}_n$; on a : $f_\sigma(x) = \sum_{i=1}^{n} x_i e_{\sigma(i)} = \sum_{k=1}^{n} x_{\sigma^{-1}(k)} e_k$

et $\sum_{k=1}^{n} x_{\sigma^{-1}(k)} = \sum_{i=1}^{n} x_i = 0$, donc $f_\sigma(x) \in H$.

Ainsi : $(\forall \sigma \in \mathfrak{S}_n, f_\sigma(H) \subset H)$, donc : $H \in \mathfrak{F}$.

2) • Soit $x = \sum_{i=1}^{n} x_i e_i \in D \cap H$. Alors $\begin{cases} x_1 = \ldots = x_n \\ x_1 + \ldots + x_n = 0 \end{cases}$, d'où $x_1 = \ldots = x_n = 0, x = 0$.

Ainsi $D \cap H = \{0\}$.

• $\dim(D \oplus H) = \dim(D) + \dim(H) = 1 + (n-1) = n$, donc $D \oplus H = E$.

• Soit $x = \sum_{i=1}^{n} x_i e_i \in E$. On a :

$$\left(\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} f_\sigma\right)(x) = \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}\sum_{i=1}^{n} x_i e_{\sigma(i)} = \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}\sum_{k=1}^{n} x_{\sigma^{-1}(k)} e_k = \frac{1}{n!}\sum_{k=1}^{n}\left(\sum_{\sigma\in\mathfrak{S}_n} x_{\sigma^{-1}(k)}\right) e_k$$

$$= \frac{1}{n!}\sum_{k=1}^{n}\left((n-1)!\sum_{i=1}^{n} x_i\right) e_k = \sum_{k=1}^{n}\left(\frac{1}{n}\sum_{i=1}^{n} x_i\right) e_k,$$

donc $\left(\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} f_\sigma\right)(x) \in D$.

Et, comme $\sum_{i=1}^{n}\left(x_i - \frac{1}{n}\sum_{i=1}^{n} x_i\right) = 0$, on a : $x - \left(\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} f_\sigma\right)(x) \in H$.

Ainsi, $p = \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} f_\sigma$ est le projecteur sur D parallèlement à H.

3) Puisque $F \not\subset D$, il existe $x = \sum_{k=1}^{n} x_k e_k \in F$ tel que $x \notin D$. Il existe donc $(i,j) \in \{1,\ldots,n\}^2$ tel que $i < j$ et $x_i \neq x_j$.

Soit $q \in \{2,\ldots,n\}$. Il existe $\sigma \in \mathfrak{S}_n$ telle que $\sigma(i) = 1$ et $\sigma(j) = q$. Puisque $F \in \mathfrak{F}$ et $x \in F$, en notant $x' = \sum_{k=1}^{n} x'_k e_k = f_{\sigma^{-1}}(x)$, on a $x' \in F$, $x'_1 = x_i \neq x_j = x'_q$.

Comme $\tau_{1q} \in \mathfrak{S}_n$, on a aussi $x'_q e_1 + x'_1 e_q + \sum_{\substack{2\leqslant k\leqslant n \\ k\neq q}} x'_k e_k \in F$, et donc, par différence avec x', F étant un sev : $(x'_q - x'_1)(e_1 - e_q) \in F$.

Enfin, F étant un sev et $x'_q - x'_1 \neq 0$: $e_1 - e_q \in F$.

Puisque $(e_1 - e_2, \ldots, e_1 - e_n)$ est une base de H, on conclut : $H \subset F$.

4) • $\{0\}, D, H, E \in \mathfrak{F}$, cf. *1)*

• Soit $F \in \mathfrak{F}$.

Si $F \subset D$, alors $F = \{0\}$ ou $F = D$.

Si $F \not\subset D$, alors (cf. *3)*) $H \subset F$, donc $F = H$ ou $F = E$.

Finalement : $\mathfrak{F} = \{\{0\}, D, H, E\}$.

Indications et réponses
pour les exercices du chapitre 8

8.1.1 On a : $E_{ij} = (\delta_{ui}\delta_{vj})_{u,v}$, $E_{kl} = (\delta_{vk}\delta_{wl})_{v,w}$, donc $E_{ij}E_{kl} = (a_{uw})_{u,w}$ où :

$$a_{uw} = \sum_{v=1}^{p} \delta_{ui}\delta_{vj}\delta_{vk}\delta_{wl} = \delta_{ui}\delta_{jk}\delta_{wl} = \delta_{jk}(\delta_{ui}\delta_{wl}).$$

Comme $E_{il} = (\delta_{ui}\delta_{wl})_{u,w}$, on conclut : $E_{ij}E_{kl} = \delta_{jk}E_{il}$.

8.1.2 Pour $(i,j) \in \{1,\dots,n\}^2$, on a, en notant $A = (a_{kl})_{kl}$:

$$E_{ij}A = \begin{pmatrix} & & \\ & 1 & \\ & & \end{pmatrix}\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} = \begin{pmatrix} 0 & & 0 \\ a_{j1} & \dots & a_{jn} \\ 0 & & 0 \end{pmatrix} \longleftarrow i^{ème} \text{ ligne,}$$

donc : $(E_{ij}A)^2 = \begin{pmatrix} 0 & & 0 \\ a_{ji}a_{j1} & \dots & a_{ji}a_{jn} \\ 0 & & 0 \end{pmatrix} \longleftarrow i^{\text{ème}}$ ligne.

Ainsi : $\forall i,j,k \in \{1,\dots,n\},\ a_{ji}a_{jk} = 0.$

En particulier : $\forall (i,j) \in \{1,\dots,n\}^2, a_{ji}^2 = 0$, et donc $A = 0$.

8.1.3 En notant $I = I_n$, on a : $0 = AB + \alpha A + \beta B = (A + \beta I)(B + \alpha I) - \alpha\beta I$, d'où : $\dfrac{1}{\alpha\beta}(A + \beta I)(B + \alpha I) = I$.

Ceci montre que $B + \alpha I$ est inversible à gauche, donc inversible (cf. 8.1.5 Th. p. 273) et a pour inverse $\dfrac{1}{\alpha\beta}(A + \beta I)$.

Ainsi : $\dfrac{1}{\alpha\beta}(B + \alpha I)(A + \beta I) = I$, donc : $BA + \alpha A + \beta B = 0$, et finalement : $AB = BA$.

8.1.4 En notant $Y = X - I_2$, on a : $X^2 - 2X = \begin{pmatrix} -1 & 0 \\ 6 & 3 \end{pmatrix} \iff Y^2 = \begin{pmatrix} 0 & 0 \\ 6 & 4 \end{pmatrix}$.

Puis, en notant $Y = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$: $Y^2 = \begin{pmatrix} 0 & 0 \\ 6 & 4 \end{pmatrix} \iff \begin{cases} a^2 + bc = 0 \\ b(a+d) = 0 \\ c(a+d) = 6 \\ bc + d^2 = 4 \end{cases} \iff \begin{cases} a = 0 \\ b = 0 \\ cd = 6 \\ d^2 = 4 \end{cases}$.

◇ **Réponse :** $\left\{\begin{pmatrix} 1 & 0 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -3 & -1 \end{pmatrix}\right\}$.

8.1.5 Comme $(XYX)Y = X(YXY)$, on a : $\begin{cases} XYX = I_2 \\ YXY = I_2 \end{cases} \iff \begin{cases} Y = X \\ X^3 = I_2 \end{cases}$.

En notant $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on obtient : $X^3 = I_2 \iff \begin{cases} a^3 + 2abc + bcd = 1 \\ b(a^2 + ad + bc + d^2) = 0 \\ c(a^2 + ad + bc + d^2) = 0 \\ abc + 2bcd + d^3 = 1 \end{cases}$.

Le cas $b = c = 0$ est d'étude immédiate.

Et : $\begin{cases} a^3 + 2abc + bcd = 1 \\ a^2 + ad + bc + d^2 = 0 \\ abc + 2bcd + d^3 = 1 \end{cases} \iff \begin{cases} bc = -(a^2 + ad + d^2) \\ a^3 - (2a + d)(a^2 + ad + d^2) = 1 \\ -(a + 2d)(a^2 + ad + d^2) + d^3 = 1 \end{cases}$

$\iff \begin{cases} bc = -(a^2 + ad + d^2) \\ (a + d)^3 = -1 \end{cases} \iff \begin{cases} d = -1 - a \\ bc = -1 - a - a^2. \end{cases}$

◇ **Réponse :** $\{I_2\} \cup \left\{ \begin{pmatrix} a & b \\ c & -1 - a \end{pmatrix} ; (a,b,c) \in \mathbb{R}^3, bc = -1 - a - a^2 \right\}$.

8.1.6 Remarquer $U^2 = nU$, d'où, pour tout (a,b) de $\mathbb{C}^2$: $(aU)(bU) = (nab)U$.

Il est clair que l'application $\theta : \begin{array}{ccc} \mathbb{C} & \longrightarrow & E \\ a & \longmapsto & aU \end{array}$ est bijective et : $\begin{cases} \theta(1) = U \\ \forall (a,b) \in \mathbb{C}^2, \begin{cases} \theta(a + b) = \theta(a) + \theta(b) \\ \theta(ab) = \theta(a)\theta(b) \end{cases} \end{cases}$.

Par transport de structure, comme $\mathbb{C}$ est un corps, E est aussi un corps isomorphe à $\mathbb{C}$.

Si $n \geqslant 2$, comme $I_n \notin E$, E n'est pas un sous-corps de l'anneau $\mathbf{M}_n(\mathbb{C})$. Ceci revient à remarquer que les neutres de la multiplication dans E et dans $\mathbf{M}_n(\mathbb{C})$ sont différents : ce sont respectivement $\frac{1}{n}U$ et I_n.

8.1.7 *a)* Il est clair que l'addition et la multiplication sont internes dans E et que : $\forall A \in E, -A \in E$.

b) $I_2 \notin E$. Les neutres de la multiplication dans E et $\mathbf{M}_2(K)$ sont différents : $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ et I_2.

◇ **Réponse :** non.

8.1.8 *a)* • E est le sev de $\mathbf{M}_4(\mathbb{C})$ engendré par $\{I, J, K\}$, où

$I = I_4$, $J = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$, $K = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$. De plus, (I, J, K) est à l'évidence libre.

• Calculer : $J^2 = 2I + 2K$, $JK = K$, $KJ = K$, $K^2 = I$. Il en résulte que la multiplication est interne dans E, commutative dans E, et que I est neutre.

b) En notant $X = aI + bJ + cK$, $(a,b,c) \in \mathbb{C}^3$, on a :

$$X^2 = I \iff a^2 I + b^2(2I + 2K) + c^2 I + 2abJ + 2acK + 2bcK = I$$

$$\iff \begin{cases} a^2 + 2b^2 + c^2 = 1 \\ 2ab = 0 \\ 2b^2 + 2ac + 2bc = 0 \end{cases} \iff \left(\begin{cases} a = 0 \\ 2b^2 + c^2 = 1 \\ b(b + c) = 0 \end{cases} \text{ ou } \begin{cases} b = 0 \\ a^2 + c^2 = 1 \\ ac = 0 \end{cases} \right)$$

$$\iff \left(\begin{cases} a = 0 \\ b = 0 \\ c^2 = 1 \end{cases} \text{ ou } \begin{cases} a = 0 \\ 3b^2 = 1 \\ c = -b \end{cases} \text{ ou } \begin{cases} b = 0 \\ c = 0 \\ a^2 = 1 \end{cases} \right).$$

◇ **Réponse :** $\left\{ K, -K, \frac{1}{\sqrt{3}}(J - K), -\frac{1}{\sqrt{3}}(J - K), I, -I \right\}$.

8.1.9 En notant $U = \begin{pmatrix} 1 & & 1 \\ & \ddots & \\ 1 & & 1 \end{pmatrix} \in \mathbf{M}_n(\mathbb{C})$, on a : $M_{a,b} = (a-b)\mathrm{I}_n + bU$.

Comme I_n et U commutent, d'après la formule du binôme de Newton : $M_{a,b}^k = \sum_{i=0}^{k} \mathrm{C}_k^i (a-b)^{k-i} b^i U^i$.

D'autre part, $U^2 = nU$, d'où, par récurrence immédiate : $\forall i \in \mathbb{N}^*,\ U^i = n^{i-1}U$.

Donc : $M_{a,b}^k = (a-b)^k \mathrm{I}_n + \sum_{i=1}^{k} \mathrm{C}_k^i (a-b)^{k-i} b^i n^{i-1} U = (a-b)^k \mathrm{I}_n + \frac{1}{n}\left(\sum_{i=1}^{k} \mathrm{C}_k^i (a-b)^{k-i} (nb)^i\right) U$

$= (a-b)^k \mathrm{I}_n + \frac{1}{n}\big((a-b+nb)^k - (a-b)^k\big)U.$

◇ **Réponse :** $M_{a,b}^k = (a-b)^k \mathrm{I}_n + \frac{1}{n}\big((a+(n-1)b)^k - (a-b)^k\big)U$, où $U = \begin{pmatrix} 1 & & 1 \\ & \ddots & \\ 1 & & 1 \end{pmatrix}$.

8.1.10 On obtient d'abord : $A^2 = \begin{pmatrix} 1 & 2 & \cdots & n \\ & \ddots & \ddots & \vdots \\ & & \ddots & 2 \\ 0 & & & 1 \end{pmatrix}$, $A^3 = \begin{pmatrix} 1 & 3 & 6 & \cdots & \frac{n(n+1)}{2} \\ & \ddots & \ddots & \ddots & \vdots \\ & & \ddots & \ddots & 6 \\ & & & \ddots & 3 \\ 0 & & & & 1 \end{pmatrix}$.

Montrons, par récurrence sur k : $A^k = (a_{k;i,j})_{1 \leqslant i,j \leqslant n}$ où $a_{k;i,j} = \begin{cases} \mathrm{C}_{j-i+k-1}^{k-1} & \text{si } i \leqslant j \\ 0 & \text{si } i > j \end{cases}$.

La formule est évidente pour $k = 1$. Supposons-la vraie pour k, et notons $A^{k+1} = (a_{k+1;i,j})_{ij}$.

Il est clair que, pour $i > j$, $a_{k+1;i,j} = 0$ (cf. aussi 8.3.2 Prop. 2 p. 296).

Soit $(i,j) \in \{1,\dots,n\}^2$ tel que $i \leqslant j$. On a :

$$a_{k+1;i,j} = \sum_{q=1}^{n} a_{k;i,q} a_{1;q,j} = \sum_{q=i}^{j} \mathrm{C}_{q-i+k-1}^{k-1} = \sum_{r=0}^{j-i} \mathrm{C}_{r+k-1}^{k-1}.$$

Montrer, par récurrence sur s : $\forall s \in \mathbb{N},\ \sum_{r=0}^{s} \mathrm{C}_{r+k-1}^{k-1} = \mathrm{C}_{s+k}^{k}$.

On conclut : $a_{k+1;i,j} = \mathrm{C}_{j-i+k}^{k}$.

◇ **Réponse :** $A^k = \begin{pmatrix} 1 & \mathrm{C}_k^{k-1} & \cdots & \mathrm{C}_{n+k-2}^{k-1} \\ & \ddots & \ddots & \vdots \\ & & \ddots & \mathrm{C}_k^{k-1} \\ 0 & & & 1 \end{pmatrix}$.

8.1.11 *1)* Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ convenant.

De $A^2 = \begin{pmatrix} a^2 & b^2 \\ c^2 & d^2 \end{pmatrix}$, déduire : $\begin{cases} bc = 0 \\ (a+d-b)b = 0 \\ (a+d-c)c = 0 \end{cases}$.

- Supposons $c \neq 0$.

Alors $b = 0$ et $a + d = c$. De $A^3 = \begin{pmatrix} a^3 & 0 \\ c^3 & d^3 \end{pmatrix}$, déduire $c(a^2 + ad + d^2) = c^3$, puis $ad = 0$.

Donc A est de la forme $\begin{pmatrix} 0 & 0 \\ c & c \end{pmatrix}$ ou $\begin{pmatrix} a & 0 \\ a & 0 \end{pmatrix}$.

- De même, si $b \neq 0$, A est de la forme $\begin{pmatrix} 0 & b \\ 0 & b \end{pmatrix}$ ou $\begin{pmatrix} a & a \\ 0 & 0 \end{pmatrix}$.

- Si $b = c = 0$, $A = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$.

2) Examiner la réciproque.

◇ **Réponse :**

$$\left\{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} ; (a,d) \in \mathbb{R}^2\right\} \cup \mathbb{R}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \cup \mathbb{R}\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \cup \mathbb{R}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \cup \mathbb{R}\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

8.1.12 *1)* • E est le sev de $\mathbf{M}_2(\mathbb{R})$ engendré par $\mathrm{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $J = \begin{pmatrix} 1 & 3 \\ -1 & -1 \end{pmatrix}$. Et il est clair que (I, J) est $\mathbb{R}$-libre.

- $J^2 = \begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix} = -2\mathrm{I}$, d'où :

$$\forall x,y,x',y' \in \mathbb{R}, \quad (x\mathrm{I} + yJ)(x'\mathrm{I} + y'J) = (xx' - 2yy')\mathrm{I} + (xy' + yx')J \in E.$$

- $\mathrm{I}_2 \in E$.

- Soit $M \in E - \{0\}$. Il existe $(x,y) \in \mathbb{R}^2 - \{(0,0)\}$ unique tel que $M = x\mathrm{I} + yJ$.

Soient $x',y' \in \mathbb{R}$, $M' = x'\mathrm{I} + y'J$. On a : $MM' = \mathrm{I}_2 \iff \begin{cases} xx' - 2yy' = 1 \\ yx' + xy' = 0 \end{cases} \iff \begin{cases} x' = \dfrac{x}{x^2 + 2y^2} \\ y' = \dfrac{-y}{x^2 + 2y^2} \end{cases}$,

car $x^2 + 2y^2 > 0$. Ainsi, M admet un inverse dans E.

Ceci prouve que E est un sous-corps de l'anneau $\mathbf{M}_2(\mathbb{R})$.

2) L'application $\theta : \begin{array}{ccc} E & \longrightarrow & \mathbb{C} \\ x\mathrm{I} + yJ & \longmapsto & x + y\sqrt{2}\,\mathrm{i} \end{array}$, $(x,y) \in \mathbb{R}^2$, est un isomorphisme de corps :

- $\theta\big((x\mathrm{I} + yJ) + (x'\mathrm{I} + y'J)\big) = (x + x') + (y + y')\sqrt{2}\,\mathrm{i} = (x + y\sqrt{2}\,\mathrm{i}) + (x' + y'\sqrt{2}\,\mathrm{i}) = \theta(x\mathrm{I} + yJ) + \theta(x'\mathrm{I} + y'J)$

- $\theta\big((x\mathrm{I} + yJ)(x'\mathrm{I} + y'J)\big) = xx' - 2yy' + (xy' + yx')\mathrm{i} = (x + y\sqrt{2}\,\mathrm{i})(x' + y'\sqrt{2}\,\mathrm{i}) = \theta(x\mathrm{I} + yJ)\theta(x'\mathrm{I} + y'J)$

- $\theta(\mathrm{I}) = 1$

- θ est bijective.

8.1.13 *a)* • E est le sev de $\mathbf{M}_2(\mathbb{R})$ engendré par $\mathrm{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $J = \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix}$.

- Comme $J^2 = \alpha\mathrm{I}$, on a :

$$\forall x,y,x',y' \in \mathbb{R}, \quad (x\mathrm{I} + yJ)(x'\mathrm{I} + y'J) = (xx' + \alpha yy')\mathrm{I} + (xy' + yx')J \in E_\alpha.$$

- La formule précédente montre que la multiplication est commutative dans E_α.

- $I_2 \in E$.

b) • Si $\alpha < 0$, l'application $\theta : \begin{array}{ccc} E & \longrightarrow & \mathbb{C} \\ xI + yJ & \longmapsto & x + y\sqrt{-\alpha}\,\mathrm{i} \end{array}$, $(x,y) \in \mathbb{R}^2$, est un isomorphisme pour les lois $+$ et $\times$, donc, par transport de structure, E_α est un corps, isomorphe à $\mathbb{C}$.

• Si $\alpha \geqslant 0$, E_α est un anneau (cf. *a)*) non intègre car : $\begin{cases} \sqrt{\alpha}\,I + J \neq 0, & \sqrt{\alpha}\,I - J \neq 0 \\ (\sqrt{\alpha}\,I + J)(\sqrt{\alpha}\,I - J) = 0. \end{cases}$

8.1.14 *a)* Soient $(e_1,\dots,e_n)$ la base canonique de $\mathbf{M}_{n,1}(\mathbb{R})$, et $(f_1,\dots,f_n)$ la famille de vecteurs de $\mathbf{M}_{n,1}(\mathbb{R})$ définie par : $A = \mathrm{Mat}_{(e_1,\dots,e_n)}(f_1,\dots,f_n)$.

Le système d'équations

$$\begin{cases} f_1 = e_1 \\ f_2 = e_2 + e_1 = e_2 + f_1 \\ f_3 = e_3 + e_2 = e_3 + f_2 - f_1 \\ \vdots \\ f_n = e_n + e_{n-1} = e_n + f_{n-1} - f_{n-2} + \dots + (-1)^n f_1 \end{cases} \quad \text{donne} \quad \begin{cases} e_1 = f_1 \\ e_2 = f_2 - f_1 \\ \vdots \\ e_n = f_n - f_{n-1} + \dots + (-1)^{n-1} f_1. \end{cases}$$

◇ **Réponse :** $A^{-1} = \begin{pmatrix} 1 & -1 & \dots & (-1)^{n-1} \\ & \ddots & \ddots & \vdots \\ & & \ddots & -1 \\ 0 & & & 1 \end{pmatrix}$.

b) Analogue à *a)*.

◇ **Réponse :** $A^{-1} = \begin{pmatrix} 1 & -1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & -1 \\ 0 & & & 1 \end{pmatrix}$.

c) Analogue à *a)*. On peut aussi remarquer qu'il s'agit du carré de la matrice A de *a)*.

◇ **Réponse :** $A^{-1} = \begin{pmatrix} 1 & -2 & 1 & 0 \\ & \ddots & \ddots & 1 \\ & & \ddots & -2 \\ 0 & & & 1 \end{pmatrix}$.

8.1.15 Notons $\gamma_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$ le terme général de AB. Il est clair que, si $i > j$, alors $\gamma_{ij} = 0$ (cf. aussi 8.3.2 Prop. 2 p. 296). Supposons $i \leqslant j$. On a :

$$\begin{aligned} \gamma_{ij} &= \sum_{k=i}^{j} t^{k-i} \mathrm{C}_k^i (-1)^{j+k} t^{j-k} \mathrm{C}_j^k = (-1)^j t^{j-i} \sum_{k=i}^{j} (-1)^k \mathrm{C}_k^i \mathrm{C}_j^k \\ &= (-1)^j t^{j-i} \sum_{k=i}^{j} (-1)^k \frac{j!}{i!(k-i)!(j-k)!} = (-1)^j t^{j-i} \frac{j!}{i!(j-i)!} \sum_{k=i}^{j} (-1)^k \frac{(j-i)!}{(k-i)!(j-k)!} \\ &= (-1)^{j+i} t^{j-i} \mathrm{C}_j^i \sum_{p=0}^{j-i} (-1)^p \mathrm{C}_{j-i}^p = (-1)^{j+i} t^{j-i} \mathrm{C}_j^i (1 + (-1))^{j-i} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i < j \end{cases}. \end{aligned}$$

8.1.16 $\begin{cases} AX + BY = 0 \\ BX - AY = \mathrm{I}_n \end{cases} \iff \begin{cases} Y = -B^{-1}AX \\ (B - AB^{-1}A)X = \mathrm{I}_n \end{cases}$.

◇ **Réponse :** $\{(B - AB^{-1}A)^{-1}, -B^{-1}A(B - AB^{-1}A)^{-1})\}$.

8.1.17 Notons $A = \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix}$, $C = \begin{pmatrix} 2 & 0 \\ 2 & 0 \end{pmatrix}$.

Si (X,Y,Z) convient, alors : $AC = (XY)(ZX) = X(YZ)X = XBX$.

En notant $X = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$, on a

$$AC = XBX \iff \begin{cases} (2x + y)(x + z) = 2 \\ (2x + y)(y + t) = 0 \\ (2z + t)(x + z) = 6 \\ (2z + t)(y + t) = 0 \end{cases} \iff \begin{cases} y + t = 0 \\ (2x + y)(x + z) = 2 \\ (2z + t)(x + z) = 6 \end{cases}$$

$$\iff \begin{cases} y + t = 0 \\ (2x + y)(x + z) = 2 \\ 2(x + z)^2 = 8 \end{cases} \iff \begin{cases} t = -y \\ x + z = 2\varepsilon \\ 2x + y = \varepsilon \end{cases},$$

où $\varepsilon = 1$ ou -1.

Ainsi : $X = \begin{pmatrix} x & \varepsilon - 2x \\ 2\varepsilon - x & -\varepsilon + 2x \end{pmatrix}$.

Montrer que X est inversible si et seulement si $4\varepsilon x - 2 \neq 0$ et que, lorsque $4\varepsilon x - 2 \neq 0$:

$$X^{-1} = \frac{1}{4\varepsilon x - 2} \begin{pmatrix} -\varepsilon + 2x & -\varepsilon + 2x \\ -2\varepsilon + 2x & x \end{pmatrix}.$$

◇ **Réponse :** $\left\{ \left(\begin{pmatrix} x & \varepsilon - 2x \\ 2\varepsilon - x & -\varepsilon + 2x \end{pmatrix}, \frac{1}{2\varepsilon x - 1} \begin{pmatrix} -\varepsilon + 2x & -\varepsilon + 2x \\ -\varepsilon + x & x \end{pmatrix}, \begin{pmatrix} \varepsilon & \varepsilon \\ \varepsilon & \varepsilon \end{pmatrix} \right); \right.$

$\left. (\varepsilon, x) \in \{-1, 1\} \times \mathbb{R} \text{ et } 2\varepsilon x - 1 \neq 0 \right\}$.

8.1.18 *a)* L'application $f : \begin{array}{ccc} \mathbf{M}_n(K) & \longrightarrow & \mathbf{M}_n(K) \\ M & \longmapsto & MS \end{array}$ est clairement linéaire, et $E = \mathrm{Ker}(f)$, donc E est un sev de $\mathbf{M}_n(K)$.

b) α) Remarquer : $\forall A \in \mathbf{M}_n(K)$, $(A \in F \iff AS = S)$.

Soit $(A, B) \in F^2$. Alors $AS = S$ et $BS = S$, d'où : $(AB)S = A(BS) = AS = S$, et donc $AB \in F$.

β) Soit $A \in F \cap \mathbf{GL}_n(K)$. On a : $A^{-1}S = A^{-1}(AS) = (A^{-1}A)S = S$, donc $A^{-1} \in F$.

8.1.19 *a)* $(\mathrm{I}_n + \mathrm{E}_{ij})(\mathrm{I}_n - \mathrm{E}_{ij}) = \mathrm{I}_n - \mathrm{E}_{ij}^2 = \mathrm{I}_n$, cf. exercice 8.1.1 p. 271. Donc $\mathrm{I}_n + \mathrm{E}_{ij}$ est inversible, et $(\mathrm{I}_n + \mathrm{E}_{ij})^{-1} = \mathrm{I}_n - \mathrm{E}_{ij}$. Cf. aussi 8.1.7 p. 279.

b) • Soit $A \in \mathbf{M}_n(K)$ telle que : $\forall X \in \mathbf{GL}_n(K)$, $AX = XA$.

En particulier, pour tout (i, j) de $\{1, \ldots, n\}^2$ tel que $i \neq j$: $A(\mathrm{I}_n + \mathrm{E}_{ij}) = (\mathrm{I}_n + \mathrm{E}_{ij})A$,

et donc : $A\mathrm{E}_{ij} = \mathrm{E}_{ij}A$.

En notant $A = (a_{kl})_{kl}$, on a :

$$AE_{ij} = \begin{pmatrix} & a_{1i} & \\ 0 & \vdots & 0 \\ & a_{ni} & \end{pmatrix} \quad , \quad E_{ij}A = \begin{pmatrix} a_{j1} & \cdots & a_{jn} \\ & 0 & \end{pmatrix} \longleftarrow i^{\text{ème}} \text{ ligne.}$$

$\uparrow$
$j^{\text{ème}}$ colonne

D'où : $a_{ii} = a_{jj}$ et $a_{ji} = 0$, et donc $A = a_{11}\mathrm{I}_n$.

- Réciproque immédiate.

◇ **Réponse :** $K\mathrm{I}_n$.

8.1.20 Déterminons $\mathrm{Ker}(M_{a,b})$. Soit $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in Mg_{n,1}(\mathbb{C})$. On a :

$$X \in \mathrm{Ker}(M_{a,b}) \Longleftrightarrow \begin{cases} ax_1 + bx_2 + \ldots + bx_n = 0 \\ \vdots \\ bx_1 + \ldots + bx_{n-1} + ax_n = 0 \end{cases} \Longleftrightarrow \begin{cases} (a-b)x_1 + b(x_1 + \ldots + x_n) = 0 \\ \vdots \\ (a-b)x_n + b(x_1 + \ldots + x_n) = 0 \end{cases}.$$

Le cas $a = b$ est d'étude immédiate.

Supposons $a \neq b$. On a : $X \in \mathrm{Ker}(M_{a,b}) \Longleftrightarrow \begin{cases} x_1 = \ldots = x_n \\ (a - b + nb)(x_1 + \ldots + x_n) = 0 \end{cases}$.

- Si $a + (n-1)b \neq 0$, alors : $X \in \mathrm{Ker}(M_{a,b}) \Longleftrightarrow \begin{cases} x_1 = \ldots = x_n \\ x_1 + \ldots + x_n = 0 \end{cases} \Longleftrightarrow x_1 = \ldots = x_n = 0$,

et donc $\mathrm{Ker}(M_{a,b}) = \{0\}$, d'où $\mathrm{rg}(M_{a,b}) = n$.

- Si $a + (n-1)b = 0$, alors : $X \in \mathrm{Ker}(M_{a,b}) \Longleftrightarrow x_1 = \ldots = x_n$, et donc $\dim\big(\mathrm{Ker}(M_{a,b})\big) = 1$, d'où (théorème du rang) : $\mathrm{rg}(M_{a,b}) = n - 1$.

◇ **Réponse :** $\mathrm{rg}(M_{a,b}) = \begin{cases} n & \text{si } a \neq b \text{ et } a + (n-1)b \neq 0 \\ n-1 & \text{si } a \neq b \text{ et } a + (n-1)b = 0 \\ 1 & \text{si } a = b \neq 0 \\ 0 & \text{si } a = b = 0. \end{cases}$

8.1.21 *a)* $\mathrm{rg}(A) = n \Longleftrightarrow \mathrm{rg}(C_1, \ldots, C_p) = \dim\big(\mathbf{M}_{n,1}(K)\big)$
$\Longleftrightarrow \mathrm{Vect}(C_1, \ldots, C_p) = \mathbf{M}_{n,1}(K) \Longleftrightarrow \big((C_1, \ldots, C_p) \text{ engendre } \mathbf{M}_{n,1}(K)\big)$.

b) $\mathrm{rg}(A) = p \Longleftrightarrow \mathrm{rg}(C_1, \ldots, C_p) = p \Longleftrightarrow \big((C_1, \ldots, C_p) \text{ est libre}\big)$.

8.1.22 *a)* $\mathrm{rg}(A) = n \Longleftrightarrow \mathrm{rg}(f) = n \Longleftrightarrow \dim\big(\mathrm{Im}(f)\big) = \dim(F)$
$\Longleftrightarrow \mathrm{Im}(f) = F \Longleftrightarrow f$ surjective.

b) $\mathrm{rg}(A) = p \Longleftrightarrow \mathrm{rg}(f) = p \Longleftrightarrow \dim\big(\mathrm{Ker}(f)\big) = 0 \Longleftrightarrow \mathrm{Ker}(f) = \{0\} \Longleftrightarrow f$ injective.

On peut aussi utiliser l'exercice 8.1.21.

8.1.23 *1)* Notons $r = \text{rg}(A)$ et supposons $r \leqslant s$.

D'après le théorème du rang, $\dim(\text{Ker}(A)) \geqslant p - s$. Si $s = p$, alors on peut choisir $q = 1$ et $B = 0$.

Supposons $s < p$. Il existe une base $V_1, \ldots, V_{p-r}$ de $\text{Ker}(A)$. En notant $q = p - r$ et B la matrice de $\mathbf{M}_{p,q}(K)$ dont les colonnes sont $V_1, \ldots, V_{p-r}$, on a $\text{rg}(B) = p - r \geqslant p - s$, et $AB = 0$ puisque $AV_1 = \ldots = AV_{p-r} = 0$.

2) Réciproquement, supposons qu'il existe $q \in \mathbb{N}^*$, $B \in \mathbf{M}_{p,q}(K)$ tels que : $AB = 0$ et $\text{rg}(B) \geqslant p - s$. Il existe alors $p - s$ colonnes de B formant une famille libre, et ces colonnes sont dans $\text{Ker}(A)$ (puisque $AB = 0$). Donc $\dim(\text{Ker}(A)) \geqslant p - s$, d'où, d'après le théorème du rang, $\text{rg}(A) \leqslant s$.

8.1.24 • $\text{Ker}(B) \subset \text{Ker}(AB)$ puisque : $\forall X \in \mathbf{M}_{n,1}(K)$, $\big(BX = 0 \Longrightarrow (AB)X = A(BX) = 0\big)$.

• D'autre part, d'après le théorème du rang : $\dim(\text{Ker}(B)) = q - \text{rg}(B) = q - \text{rg}(AB) = \dim\big(\text{Ker}(AB)\big)$. On déduit : $\text{Ker}(B) = \text{Ker}(AB)$.

• Comme plus haut : $\text{Ker}(BC) \subset \text{Ker}(ABC)$.

• Et, pour tout X de $\mathbf{M}_{r,1}(K)$:

$X \in \text{Ker}(ABC) \Longleftrightarrow CX \in \text{Ker}(AB) \Longleftrightarrow CX \in \text{Ker}(B) \Longrightarrow X \in \text{Ker}(BC)$.

Ainsi : $\text{Ker}(ABC) = \text{Ker}(BC)$, d'où, par le théorème du rang :

$\text{rg}(ABC) = r - \dim\big(\text{Ker}(ABC)\big) = r - \dim\big(\text{Ker}(BC)\big) = \text{rg}(BC)$.

8.1.25 En notant $M = \begin{pmatrix} 0 & -1 & -1 \\ -1 & 0 & -1 \\ 1 & 1 & 2 \end{pmatrix}$, vérifier $M^2 = M$.

On déduit : $ABC = M = M^2 = (ABC)^2$.

Montrer $\text{rg}(M) = 2$, d'où : $2 = \text{rg}(ABC) = \text{rg}\big((ABC)^2\big) = \text{rg}\big(AB(CAB)C\big) \leqslant \text{rg}(CAB)$

(cf. 8.1.6 Rem. p. 277).

Mais $CAB \in \mathbf{M}_2(\mathbb{R})$, donc $\text{rg}(CAB) \leqslant 2$.

On obtient $\text{rg}(CAB) = 2$, c'est-à-dire $CAB \in \mathbf{GL}_2(\mathbb{R})$.

Puis : $(CAB)^2 = C(ABC)AB = C(ABC)^2AB = (CAB)^3$, d'où, puisque CAB est inversible :

$CAB = \text{I}_2$.

Enfin : $(BCA)^2 = B(CAB)CA = B\text{I}_2CA = BCA$.

8.1.26 *a)* Remarquer d'abord $\text{Im}(BA) \subset \text{Im}(B)$, et, d'autre part, par une récurrence immédiate :

$$\forall k \in \mathbb{N}^*,\ A^kB = BA^k.$$

Supposons $\text{Im}(BA) = \text{Im}(B)$.

• Montrons, par récurrence sur k : $\forall k \in \mathbb{N}^*$, $\text{Im}(BA^k) = \text{Im}(B)$.

La propriété est acquise, par hypothèse, pour $k = 1$. Supposons-la vraie pour un k de $\mathbb{N}^*$.

En notant $E = \mathbf{M}_{n,1}(K)$, on a alors :

$$\text{Im}(BA^{k+1}) = (BA^{k+1})(E) = (A^{k+1}B)(E) = A\big((A^kB)(E)\big) = A\big(B(E)\big) = (AB)(E) = (BA)(E)$$
$$= \text{Im}(BA) = \text{Im}(B).$$

• Comme A est nilpotente, il existe $k \in \mathbb{N}^*$ tel que $A^k = 0$. On a alors : $\text{Im}(B) = \text{Im}(BA^k) = \{0\}$, d'où $B = 0$, exclu.

Ceci montre : $\text{Im}(BA) \subsetneq \text{Im}(B)$, et donc $\text{rg}(AB) = \text{rg}(BA) < \text{rg}(B)$.

b) Récurrence sur p.

La propriété est vraie pour $p = 1$ puisque A_1 est nilpotente, donc non inversible,

d'où $\operatorname{rg}(A_1) \leqslant n - 1 = (n-1)^+$.

Supposons la propriété vraie pour un p de $\mathbb{N}^*$, et soient $A_1, \dots, A_{p+1} \in \mathbf{M}_n(K)$ nilpotentes et commutant deux à deux. Notons $B = \prod_{i=1}^{p} A_i$.

Montrer que B est nilpotente et commute avec A. Si $B = 0$, la propriété est triviale. Supposons $B \neq 0$. D'après *a)* : $\operatorname{rg}(A_{p+1}B) \leqslant \operatorname{rg}(B) - 1$, d'où $A_{p+1}B = 0$ ou $\operatorname{rg}(A_{p+1}B) \leqslant (n-p) - 1 = n - (p+1)$.

c) $\operatorname{rg}\left(\prod_{i=1}^{n} A_i\right) \leqslant (n-n)^+ = 0$, donc : $\prod_{i=1}^{n} A_i = 0$.

8.1.27 En notant $H = U\,{}^tV = \begin{pmatrix} 1 \\ \frac{1}{a} \\ \vdots \\ \frac{1}{a^{n-1}} \end{pmatrix} (1\ a\ \dots\ a^{n-1}) = \begin{pmatrix} 1 & a & \dots & a^{n-1} \\ \frac{1}{a} & & \iddots & \vdots \\ \vdots & \iddots & \iddots & a \\ \frac{1}{a^{n-1}} & \dots & \frac{1}{a} & 1 \end{pmatrix}$,

il est clair que : $A = H - \mathrm{I}_n$.

a) Puisque H et I_n commutent, on a, d'après la formule du binôme de Newton : $A^k = \sum_{i=0}^{k} \mathrm{C}_k^i (-1)^{k-i} H^i$.

Comme : $H^2 = (U\,{}^tV)(U\,{}^tV) = U({}^tVU)\,{}^tV = ({}^tVU)U\,{}^tV = nH$ (car ${}^tVU \in \mathbb{R}$), on obtient :

$$A^k = (-1)^k \mathrm{I}_n + \sum_{i=1}^{k} \mathrm{C}_k^i (-1)^{k-i} n^{i-1} H = (-1)^k \mathrm{I}_n + \frac{1}{n}\left((n-1)^k - (-1)^k\right) H.$$

◇ **Réponse :** $A^k = \begin{pmatrix} (-1)^k + \alpha_k & \alpha_k a & \dots & \alpha_k a^{n-1} \\ \frac{\alpha_k}{a} & & \iddots & \vdots \\ \vdots & \iddots & \iddots & \alpha_k a \\ \frac{\alpha_k}{a^{n-1}} & \dots & \frac{\alpha_k}{a} & (-1)^k + \alpha_k \end{pmatrix}$,

où $\alpha_k = \frac{1}{n}\left((n-1)^k - (-1)^k\right)$.

b) D'après *a)* : $A^2 = \mathrm{I}_n + (n-2)H = (n-2)A + (n-1)\mathrm{I}_n$, d'où : $A\left(\frac{1}{n-1}(A - (n-2)\mathrm{I}_n)\right) = \mathrm{I}_n$.

Ceci montre que A est inversible et donne A^{-1}.

◇ **Réponse :** $A^{-1} = \frac{1}{n-1}(A - (n-2)\mathrm{I}_n) = \frac{1}{n-1} \begin{pmatrix} -(n-2) & a & \dots & a^{n-1} \\ \frac{1}{a} & & \iddots & \vdots \\ \vdots & \iddots & \iddots & a \\ \frac{1}{a^{n-1}} & \dots & \frac{1}{a} & -(n-2) \end{pmatrix}$.

c) En prolongeant la notation $\alpha_k = \frac{1}{n}\big((n-1)^k - (-1)^k\big)$, proposée dans la solution de *a)*, au cas $k \in \mathbb{Z}_-^*$, on a $\alpha_{-1} = \dfrac{1}{n-1}$, et la formule du *a)* sur A^k est alors vraie pour $k = -1$.

Supposons, pour un k de $\mathbb{Z}_-$: $A^k = (-1)^k \mathrm{I}_n + \alpha_k H$.

Alors : $A^{k-1} = \big((-1)^k \mathrm{I}_n + \alpha_k H\big)\big(-\mathrm{I}_n + \dfrac{1}{n-1} H\big) = (-1)^{k+1}\mathrm{I}_n + \big(\dfrac{(-1)^k}{n-1} - \alpha_k + \dfrac{n\alpha_k}{n-1}\big)H$

Vérifier : $\alpha_{k+1} = \dfrac{(-1)^k}{n-1} - \alpha_k + \dfrac{n\alpha_k}{n-1}$.

◇ **Réponse :** La même formule qu'en *a)*.

8.1.28 Soit $(A,B,C) \in (\mathbf{M}_2(K))^3$.

Puisque $\mathrm{tr}(AB - BA) = \mathrm{tr}(AB) - \mathrm{tr}(BA) = 0$, il existe $(\alpha,\beta,\gamma) \in K^3$ tel que : $AB - BA = \begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix}$.

On a alors : $(AB - BA)^2 = \begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix}^2 = \begin{pmatrix} \alpha^2 + \beta\gamma & 0 \\ 0 & \alpha^2 + \beta\gamma \end{pmatrix} = (\alpha^2 + \beta\gamma)\mathrm{I}_2$.

Comme I_2 commute avec C, on conclut à la formule voulue.

8.1.29 Supposons qu'il existe (A,B,C,D) convenant. Alors :

$$\begin{cases} n = \mathrm{tr}(\mathrm{I}_n) = \mathrm{tr}(AC + DB) = \mathrm{tr}(AC) + \mathrm{tr}(DB) \\ 0 = \mathrm{tr}(CA + BD) = \mathrm{tr}(CA) + \mathrm{tr}(BD) = \mathrm{tr}(AC) + \mathrm{tr}(DB), \quad \text{contradiction.} \end{cases}$$

8.1.30 Si (X,Y) convient, alors : $\mathrm{tr}\big(\mathrm{tr}(X)Y + \mathrm{tr}(Y)X\big) = \mathrm{tr}\begin{pmatrix} 4 & 8 \\ 4 & -4 \end{pmatrix} = 0$, d'où $\mathrm{tr}(X)\mathrm{tr}(Y) = 0$.

1) Supposons $\mathrm{tr}(X) = 0$.

Il existe alors $\lambda \in \mathbb{R}^*$ tel que $\mathrm{X} = \lambda \begin{pmatrix} 4 & 8 \\ 4 & -4 \end{pmatrix}$. Alors :

$$(S) \iff \begin{cases} \mathrm{tr}(Y) = \dfrac{1}{\lambda} \\ 4\lambda \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix} Y = \begin{pmatrix} 1 & 1 \\ 4 & -2 \end{pmatrix} \end{cases} \iff \begin{cases} \mathrm{tr}(Y) = \dfrac{1}{\lambda} \\ Y = \dfrac{1}{4\lambda} \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ 4 & -2 \end{pmatrix} \end{cases}$$

$$\iff Y = \frac{1}{4\lambda} \begin{pmatrix} 3 & -1 \\ -1 & 1 \end{pmatrix}.$$

2) Supposons $\mathrm{tr}(Y) = 0$.

Il existe alors $\mu \in \mathbb{R}^*$ tel que $Y = \mu \begin{pmatrix} 4 & 8 \\ 4 & -4 \end{pmatrix}$. Alors :

$$(S) \iff \begin{cases} \mathrm{tr}(X) = \dfrac{1}{\mu} \\ 4\mu X \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 4 & -2 \end{pmatrix} \end{cases} \iff \begin{cases} \mathrm{tr}(X) = \dfrac{1}{\mu} \\ X = \dfrac{1}{4\mu} \begin{pmatrix} 1 & 1 \\ 4 & -2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}^{-1} \end{cases}$$

$$\iff X = \frac{1}{12\mu} \begin{pmatrix} 2 & 1 \\ 2 & 10 \end{pmatrix}.$$

◇ **Réponse :**

$$\left\{ \left(\alpha \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}, \frac{1}{\alpha} \begin{pmatrix} 3 & -1 \\ -1 & 1 \end{pmatrix} \right) ; \alpha \in \mathbb{R}^* \right\} \cup \left\{ \left(\frac{1}{3\beta} \begin{pmatrix} 2 & 1 \\ 2 & 10 \end{pmatrix}, \beta \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix} \right) ; \beta \in \mathbb{R}^* \right\}.$$

8.1.31 *a)* Puisque $\mathrm{rg}(H) \leqslant 1$, il existe $U = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} \in \mathbf{M}_{n,1}(K)$ tel que les colonnes de H soient colinéaires à U ; il existe donc $v_1, \ldots, v_n \in K$ tels que les colonnes de H soient $v_1 U, \ldots, v_n U$, d'où :

$$H = \begin{pmatrix} u_1 v_1 & \ldots & u_1 v_n \\ \vdots & & \vdots \\ u_n v_1 & \ldots & u_n v_n \end{pmatrix} = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} (v_1 \ldots v_n) = U\,{}^t V, \quad \text{en notant } V = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}.$$

De plus : $\mathrm{tr}(H) = \sum_{i=1}^{n} u_i v_i = (u_1 \ldots u_n) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = {}^t U V.$

b) $H^2 = (U\,{}^t V)(U\,{}^t V) = U({}^t V U)\,{}^t V = ({}^t V U) U\,{}^t V = \mathrm{tr}(H) H$ $\quad (\text{car } {}^t V U \in \mathbb{R}).$

8.1.32 *1)* Supposons $A^2 = 0$. Alors $\mathrm{Im}(A) \subset \mathrm{Ker}(A)$, d'où $\mathrm{rg}(A) \leqslant \dim \mathrm{Ker}(A) = 3 - \mathrm{rg}(A)$, donc $\mathrm{rg}(A) \leqslant 1$. D'après l'exercice 8.1.31, $A^2 = \mathrm{tr}(A) A$, d'où $\mathrm{tr}(A) = 0$ ou $A = 0$, donc $\mathrm{tr}(A) = 0$.

2) Réciproquement, si $\mathrm{rg}(A) \leqslant 1$ et $\mathrm{tr}(A) = 0$, alors, d'après l'exercice 8.1.31 : $A^2 = \mathrm{tr}(A) A = 0$.

8.1.33 Remarquer d'abord : $\forall X \in \mathbf{M}_{p,q}(K)$, $\mathrm{tr}(AXB) = \mathrm{tr}(XBA)$.

1) L'implication $\Longleftarrow$ est immédiate.

2) Supposons : $\forall X \in \mathbf{M}_{p,q}(K)$, $\mathrm{tr}(XBA) = 0$.
En particulier, pour $X = \mathrm{E}_{ij}$, $(i,j) \in \{1,\ldots,p\} \times \{1,\ldots,q\}$, on obtient, en notant $BA = (c_{vw})_{vw}$:

$$0 = \mathrm{tr}(X B A) = \sum_{u=1}^{p} \sum_{v=1}^{q} \delta_{ui} \delta_{vj} c_{vu} = c_{ji},$$

et donc $BA = 0$.

8.1.34 *a) 1)* Soit f convenant. On a, pour tous i,j,k,l de $\{1,\ldots,n\}$: $f(\mathrm{E}_{ij}\mathrm{E}_{kl}) = f(\mathrm{E}_{kl}\mathrm{E}_{ij})$, donc (cf. exercice 8.1.1 p. 271) : $\delta_{jk} f(\mathrm{E}_{il}) = \delta_{li} f(\mathrm{E}_{kj})$.
Pour (i,l) fixé, en choisissant $k = j = 1$, on obtient : $f(\mathrm{E}_{il}) = \delta_{li} f(\mathrm{E}_{11})$.
On a alors, pour toute $A = (a_{ij})_{ij}$ de $\mathbf{M}_n(K)$:

$$f(A) = f\left(\sum_{i,j} a_{ij} \mathrm{E}_{ij}\right) = \sum_{i,j} a_{ij} \delta_{ji} f(\mathrm{E}_{11}) = \left(\sum_{i=1}^{n} a_{ii}\right) f(\mathrm{E}_{11}) = \mathrm{tr}(A) f(\mathrm{E}_{11}).$$

Ceci montre qu'il existe $F \in \mathbf{M}_n(K)$ telle que : $\forall A \in \mathbf{M}_n(K)$, $f(A) = \mathrm{tr}(A)F$.

2) Réciproquement, soient $F \in \mathbf{M}_n(K)$ et $f : \begin{array}{ccc} \mathbf{M}_n(K) & \longrightarrow & \mathbf{M}_n(K) \\ A & \longmapsto & \mathrm{tr}(A)F \end{array}$.

Il est clair que f est linéaire et, pour tout (A,B) de $(\mathbf{M}_n(K))^2$:
$f(AB) = \mathrm{tr}(AB)F = \mathrm{tr}(BA)F = f(BA)$.

◇ **Réponse :** $\left\{ \begin{array}{ccc} \mathbf{M}_n(K) & \longrightarrow & \mathbf{M}_n(K) \\ A & \longmapsto & \mathrm{tr}(A)F \end{array} ;\ F \in \mathbf{M}_n(K) \right\}$.

b) 1) Soit f convenant. D'après *a)*, il existe $F \in \mathbf{M}_n(K)$ telle que : $\forall A \in \mathbf{M}_n(K),\ f(A) = \mathrm{tr}(A)F$.
On a donc : $\forall A,B,C \in \mathbf{M}_n(K),\ \mathrm{tr}(ABC)F = \mathrm{tr}(BAC)F$.
Si $F \neq 0$, on déduit en particulier (si $n \geqslant 2$) : $1 = \mathrm{tr}(E_{11}E_{12}E_{21}) = \mathrm{tr}(E_{12}E_{11}E_{21}) = 0$, contradiction.

2) Réciproque immédiate.

◇ **Réponse :** • $\{0\}$ si $n \geqslant 2$
• $\mathcal{L}(\mathbf{M}_1(K))$ si $n = 1$.

8.2.1 D'après 8.2.3 *2)* Prop. 2 p. 288, il existe $P \in \mathbf{GL}_p(K)$, $Q \in \mathbf{GL}_n(K)$ telles que : $A = Q^{-1}J_{n,p,r}P$.

En notant $A_k = Q^{-1}E_{kk}P$ pour $k \in \{1,\dots,r\}$, on a : $\begin{cases} A = Q^{-1}\left(\sum_{k=1}^{r} E_{kk}\right)P = \sum_{k=1}^{r} A_k \\ \forall k \in \{1,\dots,r\},\quad \mathrm{rg}(A_k) = 1. \end{cases}$

8.2.2 Soit $A \in \mathbf{M}_n(\mathbb{C})$; notons $r = \mathrm{rg}(A)$.
D'après 8.2.3 *2)* Prop. 2 p. 288, il existe $P,Q \in \mathbf{GL}_n(\mathbb{C})$ telles que $A = Q^{-1}J_{n,n,r}P$.

Soient $U = \frac{1}{2}I_n$, $V = J_{n,n,r} - U = \begin{pmatrix} \frac{1}{2} & & & & & \\ & \ddots & & & 0 & \\ & & \frac{1}{2} & & & \\ & 0 & & -\frac{1}{2} & & \\ & & & & \ddots & \\ & & & & & -\frac{1}{2} \end{pmatrix}$, $B = Q^{-1}UP$, $C = Q^{-1}VP$.

On a : $\begin{cases} A = Q^{-1}(U+V)P = B + C \\ (B,C) \in (\mathbf{GL}_n(\mathbb{C}))^2 \end{cases}$.

8.2.3 *1)* Notons $s = \mathrm{rg}(A)$ et supposons $s \leqslant r$. D'après 8.2.3 *2)* Prop. 2 p. 288, il existe $P \in \mathbf{GL}_p(K)$, $Q \in \mathbf{GL}_n(K)$ telles que : $A = Q^{-1}J_{n,p,s}P$.
Remarquer $J_{n,r,s}J_{r,p,s} = J_{n,p,s}$, d'où, en notant $B = Q^{-1}J_{n,r,s}$ et $C = J_{r,p,s}P$:
$B \in \mathbf{M}_{n,r}(K)$, $C \in \mathbf{M}_{r,p}(K)$, $A = BC$.

2) Réciproquement, supposons qu'il existe $(B,C) \in \mathbf{M}_{n,r}(K) \times \mathbf{M}_{r,p}(K)$ tel que $A = BC$.
Alors $\mathrm{Im}(A) = \mathrm{Im}(BC) \subset \mathrm{Im}(B)$, d'où $\mathrm{rg}(A) \leqslant \mathrm{rg}(B) \leqslant r$.

8.2.4 *a)* Si $A = 0$, la propriété est évidente.
Supposons $A \neq 0$. En permutant les lignes et en permutant les colonnes, on se ramène à une matrice $(\alpha_{ij})_{ij}$ telle que $\alpha_{11} \neq 0$.
En multipliant la 1ère colonne par α_{11}^{-1}, puis en remplaçant chaque colonne C_j $(2 \leqslant j \leqslant p)$ par $C_j - \alpha_{11}^{-1}C_1$, on se ramène à une matrice de la forme : $\begin{pmatrix} 1 & 0 & \dots & 0 \\ . & & & \\ \vdots & & A_1 & \end{pmatrix}$, où $A_1 \in \mathbf{M}_{n-1,p-1}(K)$ et $\mathrm{rg}(A_1) = r - 1$.
On réitère sur A_1.

Il existe donc une suite finie d'opérations élémentaires sur les lignes et les colonnes ramenant A à une matrice T de la forme $T = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ & & 1 \\ 0 & & 0 \end{pmatrix}$.

Par des opérations élémentaires sur les lignes ($C_2 \longleftarrow C_2 - t_{21}C_1, \ldots$), on se ramène à

$$J_{n,p,r} = \begin{pmatrix} 1 & & 0 & \\ & \ddots & & 0 \\ 0 & & 1 & \\ & 0 & & 0 \end{pmatrix}.$$

En particulier, on retrouve ainsi la Prop. 2 de 8.2.3 *2)* p. 288.

b) (i) $\Longrightarrow$ (ii) :

Si $\mathrm{rg}(A) = \mathrm{rg}(B)$, d'après *a)*, on peut passer de A et de B à $J_{n,p,r}$ par des opérations élémentaires, donc on peut passer de A à B par des opérations élémentaires.

(ii) $\Longrightarrow$ (i) : cf. 8.1.7 Prop. p. 281.

c) Soit $A \in \mathbf{GL}_n(K)$. Puisque $\mathrm{rg}(A) = n$, d'après *b)*, on peut passer de A à $J_{n,n,n} = I_n$ par des opérations élémentaires, donc A est un produit de matrices d'opérations élémentaires (et des inverses, qui en sont encore).

8.2.5 Notons $p = \dim(E)$, $n = \dim(F)$, $r = \mathrm{rg}(f)$, $r' = \mathrm{rg}(g)$.

a) D'après 8.2.3 2) Prop. 2 p. 288, il existe des bases $\mathcal{B},\mathcal{B}'$ de E, et $\mathcal{C},\mathcal{C}'$ de F telles que :

$$\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f) = J_{n,p,r},\ \mathrm{Mat}_{\mathcal{B}',\mathcal{C}'} = J_{n,p,r'}.$$

α) Considérons $h \in \mathcal{L}(F)$, $k \in \mathcal{L}(E)$ définis par : $\mathrm{Mat}_{\mathcal{B}',\mathcal{B}}(k) = J_{p,p,r'}$, $\mathrm{Mat}_{\mathcal{C}',\mathcal{C}}(h) = I_n$.

On a : $\mathrm{Mat}_{\mathcal{B}',\mathcal{C}}(h \circ g) = (\mathrm{Mat}_{\mathcal{C}',\mathcal{C}}(h))(\mathrm{Mat}_{\mathcal{B}',\mathcal{C}'}(g)) = I_n J_{n,p,r'} = J_{n,p,r'}$.

$\mathrm{Mat}_{\mathcal{B}',\mathcal{C}}(f \circ k) = (\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f))(\mathrm{Mat}_{\mathcal{B}',\mathcal{B}}(k)) = J_{n,p,r}J_{n,p,r'}$.

Comme $r' \leqslant r$, on a $J_{n,p,r}J_{n,p,r'} = J_{n,p,r'}$, d'où $\mathrm{Mat}_{\mathcal{B}',\mathcal{C}}(h \circ g) = \mathrm{Mat}_{\mathcal{B}',\mathcal{C}}(f \circ k)$, et donc $h \circ g = f \circ k$.

De plus, clairement : $h \in \mathcal{GL}(F)$.

β) Analogue à α).

b) Même méthode que dans la résolution de *a)* α), en prenant : $\mathrm{Mat}_{\mathcal{B}',\mathcal{B}}(k) = I_p$, $\mathrm{Mat}_{\mathcal{C}',\mathcal{C}}(h) = I_n$.

8.2.6 Remarquer $S(A) = \mathrm{tr}(A^2)$, d'où :

$S(P^{-1}AP) = \mathrm{tr}\big((P^{-1}AP)(P^{-1}AP)\big) = \mathrm{tr}(P^{-1}A^2P) = \mathrm{tr}(A^2) = S(A)$.

8.2.7 Remarquer : $A^2 \neq 0$ et $B^2 = 0$.

◇ **Réponse :** non.

8.3.1 Il est clair que : $\forall P \in \mathbb{C}_n[X]$, $P(X) + P'\left(\frac{X}{2}\right) + \ldots + P^{(n)}\left(\frac{X}{2^n}\right) \in \mathbb{C}_n[X]$, et que l'application $f : \mathbb{C}_n[X] \longrightarrow \mathbb{C}_n[X]$ définie par : $\forall P \in \mathbb{C}_n[X]$, $f(P) = P(X) + \ldots + P^{(n)}\left(\frac{X}{2^n}\right)$ est linéaire.

De plus, $\mathrm{Mat}_{(1,X,\ldots,X^n)}(f) = \begin{pmatrix} 1 & & \cdots \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$, qui est triangulaire supérieure à termes diagonaux non nuls, et inversible.

Ainsi, f est bijectif, d'où le résultat voulu.

Cf. aussi exercice 7.3.1 p. 259.

8.3.2 • Supposons A nilpotente. Il existe $k \in \mathbb{N}^*$ tel que $A^k = 0$. Comme les termes diagonaux de A^k sont les a_{ii}^k $(1 \leqslant i \leqslant n)$, cf. 8.3.2 Rem. 2 p. 296, on déduit : $\forall i \in \{1,\ldots,n\}$, $a_{ii} = 0$.

• Réciproquement, supposons : $\forall i \in \{1,\ldots,n\}$, $a_{ii} = 0$. Alors :

$$A = \begin{pmatrix} 0 & & \cdots \\ & \ddots & \\ 0 & & 0 \end{pmatrix}, A^2 = \begin{pmatrix} 0 & 0 & & \cdots \\ & \ddots & \ddots & \\ & & \ddots & 0 \\ 0 & & & 0 \end{pmatrix}, \ldots, A^{n-1} = \begin{pmatrix} 0 & \cdots & 0 & \cdot \\ & \ddots & & 0 \\ & & \ddots & \vdots \\ 0 & & & 0 \end{pmatrix},$$

$$A^n = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & 0 & \vdots \\ 0 & \cdots & 0 \end{pmatrix} = 0.$$

8.3.3 *a) 1)* $\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+x & b+cx+y \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix} \in G.$

2) $I_3 \in G$.

3) $\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$ est inversible et son inverse est de la forme $\begin{pmatrix} 1 & \cdot & \cdot \\ 0 & 1 & \cdot \\ 0 & 0 & 1 \end{pmatrix}$, cf. 8.3.2 Prop. 4 p. 297, donc est dans G.

b) Soit $A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in G$. On a :

$$(\forall M \in G, AM = MA) \Longleftrightarrow \left(\forall (x,y,z) \in K^3,\ b + cx + y = y + za + b\right)$$
$$\Longleftrightarrow \left(\forall (x,y,z) \in K^3,\ cx = za\right) \Longleftrightarrow a = c = 0.$$

◇ **Réponse :** $\left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} ;\ b \in K \right\}$.

8.3.4 *1)* Soit A convenant. En particulier : $\forall (i,j) \in \{1,\dots,n\}^2$, $(i \leqslant j \Longrightarrow AE_{ij} = E_{ij}A)$.

Notons $A = (a_{kl})_{kl}$. On a pour tous i,j,u,v tels que $i \leqslant j$:

$$\sum_{l=1}^{n} a_{ul}\delta_{li}\delta_{vj} = \sum_{l=1}^{n} \delta_{ui}\delta_{lj}a_{lv},$$

c'est-à-dire : $a_{ui}\delta_{vj} = \delta_{ui}a_{jv}$.

Soit $(u,v) \in \{1,\dots,n\}^2$ tel que $u \neq v$.

En prenant $i = j = v$, on déduit $a_{u,v} = 0$. Si $u < v$, en prenant $i = u$, $j = v$, on déduit $a_{un} = a_{vv}$.

Il existe donc $\alpha \in K$ tel que $A = \alpha I_n$.

2) Réciproque immédiate.

◇ **Réponse :** $K\,I_n$.

8.3.5 *1)* Soit A convenant. En particulier : $\forall i \in \{1,\dots,n\}$, $AE_{ii} = E_{ii}A$.

Notons $A = (a_{kl})_{kl}$. On a, pour tous i,u,v de $\{1,\dots,n\}$: $\displaystyle\sum_{l=1}^{n} a_{ul}\delta_{li}\delta_{vi} = \sum_{l=1}^{n} \delta_{ui}\delta_{li}a_{lv}$,

c'est-à-dire : $a_{ui}\delta_{vi} = \delta_{ui}a_{iv}$.

Soit $(u,v) \in \{1,\dots,n\}^2$ tel que $u \neq v$.

En choisissant $i = v$, on déduit $a_{uv} = 0$.

2) Réciproquement, si A est diagonale, alors A commute avec toute matrice diagonale (cf. 8.3.3 Prop. 1 p. 299).

◇ **Réponse :** $D_n(K)$.

8.3.6 *1)* Soit $A = (a_{ij})_{ij}$ convenant. On a donc :

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix},$$

c'est-à-dire : $\begin{pmatrix} a_{11}\lambda_1 & \dots & a_{1n}\lambda_n \\ \vdots & & \vdots \\ a_{n1}\lambda_1 & \dots & a_{nn}\lambda_n \end{pmatrix} = \begin{pmatrix} \lambda_1 a_{11} & \dots & \lambda_1 a_{1n} \\ \vdots & & \vdots \\ \lambda_n a_{n1} & \dots & \lambda_n a_{nn} \end{pmatrix}$,

ou encore : $\forall (i,j) \in \{1,\dots,n\}^2$, $(\lambda_i - \lambda_j)a_{ij} = 0$.

Comme $\lambda_1,\dots,\lambda_n$ sont deux à deux distincts, on déduit : $\forall (i,j) \in \{1,\dots,n\}^2$, $(i \neq j \Longrightarrow a_{ij} = 0)$, et donc A est diagonale.

2) Réciproquement, toute matrice diagonale commute avec D (cf. 8.3.3 Prop. 1 p. 299).

◇ **Réponse :** $D_n(K)$.

C.8.1 **I** Soit $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbf{M}_{n,1}(\mathbb{R})$ telle que $AX = 0$, c'est-à-dire :

$$\begin{cases} \alpha_1 x_1 + \beta x_2 + \ldots + \beta x_n = 0 \\ \qquad\qquad\qquad\qquad \vdots \\ \beta x_1 + \ldots + \beta x_{n-1} + \alpha_n x_n = 0 \end{cases}.$$

En notant $S = x_1 + \ldots + x_n$, on déduit : $\beta S = (\beta - \alpha_1)x_1 = \ldots = (\beta - \alpha_n)x_n$.

• S'il n'existe aucun i de $\{1,\ldots,n\}$ tel que $\alpha_i = \beta$, alors : $\forall i \in \{1,\ldots,n\}$, $\beta - \alpha_i < 0$, et donc $x_1,\ldots,x_n$ sont du même signe au sens large, c'est-à-dire : $(x_1,\ldots,x_n) \in (\mathbb{R}_+)^n$ ou $(x_1,\ldots,x_n) \in (\mathbb{R}_-)^n$.

Mais alors, dans le premier cas, on a $S \geqslant 0$, puis $x_1 = \dfrac{\beta S}{\beta - \alpha_1} \leqslant 0, \ldots, x_n = \dfrac{\beta S}{\beta - \alpha_n} \leqslant 0$, d'où $x_1 = \ldots = x_n = 0$, $X = 0$. De même pour le second cas.

• S'il existe un et un seul indice i_0 de $\{1,\ldots,n\}$ tel que $\alpha_{i_0} = \beta$, alors $S = \dfrac{\beta - \alpha_{i_0}}{\beta} x_{i_0} = 0$, d'où :

$$\forall i \in \{1,\ldots,n\} - \{i_0\}, \quad x_i = \frac{\beta S}{\beta - \alpha_i} = 0,$$

puis $x_{i_0} = S - \displaystyle\sum_{\substack{1 \leqslant i \leqslant n \\ i \neq i_0}} x_i = 0$, et donc $X = 0$.

Ceci montre : $\forall X \in \mathbf{M}_{n,1}(\mathbb{R})$, $(AX = 0 \Longrightarrow X = 0)$, et donc : $A \in \mathbf{GL}_n(\mathbb{R})$.

II *1)* • Notons $A = (a_{ij})_{ij}$. On a, pour tout (i,j) de $\{1,\ldots,n\}^2$:

$$\begin{aligned} a_{ij} = \sum_{k=1}^{p} b_{ki} b_{kj} &= \operatorname{Card}\{k \in \{1,\ldots,p\};\ b_{ki} = b_{kj} = 1\} \\ &= \operatorname{Card}\{k \in \{1,\ldots,p\};\ u_k \in A_i \text{ et } u_k \in A_j\} \\ &= \operatorname{Card}(A_i \cap A_j). \end{aligned}$$

• D'après l'hypothèse : $\begin{cases} \forall (i,j) \in \{1,\ldots,n\}^2,\ \big(i \neq j \Longrightarrow a_{ij} = \operatorname{Card}(A_i \cap A_j) = \beta\big) \\ \forall (i,j) \in \{1,\ldots,n\}^2,\ a_{ii} = \operatorname{Card}(A_i) \geqslant \operatorname{Card}(A_i \cap A_j) = \beta \end{cases}$.

Supposons qu'il existe au moins deux indices i_1, i_2 de $\{1,\ldots,n\}$, distincts, tels que $a_{i_1 i_1} = a_{i_2 i_2} = \beta$.

On a alors : $\operatorname{Card}(A_{i_1}) = \operatorname{Card}(A_{i_2}) = \operatorname{Card}(A_{i_1} \cap A_{i_2})$, d'où, puisque A_{i_1} et A_{i_2} sont finis, $A_{i_1} = A_{i_2}$, contradiction.

Ainsi, A satisfait les hypothèses de I, donc $A \in \mathbf{GL}_n(\mathbb{R})$.

2) Puisque $A \in \mathbf{GL}_n(\mathbb{R})$: $n = \operatorname{rg}(A)$.

D'autre part, comme $\operatorname{Im}(A) = \operatorname{Im}({}^t B B) \subset \operatorname{Im}({}^t B)$ (cf. aussi ex. 7.2.9 *b)* p. 251), on a :

$$\operatorname{rg}(A) = \dim\big(\operatorname{Im}(A)\big) \leqslant \dim\big(\operatorname{Im}({}^t B)\big) = \operatorname{rg}({}^t B).$$

Et, comme ${}^t B \in \mathbf{M}_{n,p}(\mathbb{R})$: $\operatorname{rg}({}^t B) \leqslant p$.

Finalement : $n \leqslant p$.

Indications et réponses
pour les exercices du chapitre 9

9.4.1 $$|\det(A)| = \left|\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1}\dots a_{\sigma(n)n}\right| \leqslant \sum_{\sigma\in\mathfrak{S}_n} |a_{\sigma(1)1}|\dots|a_{\sigma(n)n}|$$
$$\leqslant \sum_{(i_1,\dots,i_n)\in\{1,\dots,n\}^n} |a_{i_1 1}|\dots|a_{i_n n}| = \prod_{j=1}^{n}\left(\sum_{i=1}^{n}|a_{ij}|\right),$$
en reconnaissant le développement du produit de n sommes de n termes.

9.4.2 *a)* $AB = -BA \Longrightarrow \det(AB) = (-1)^n\det(BA) \Longleftrightarrow \det(A)\det(B) = (-1)^n\det(B)\det(A)$
$\Longleftrightarrow 1 = (-1)^n \Longleftrightarrow n$ pair.

b) ◇ **Réponse :** $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

9.4.3 *a)* • $\mathbf{SL}_n(K) \subset \mathbf{GL}_n(K)$, car $\det(A) = 1 \Longrightarrow \det(A) \neq 0$.

- Si $A, B \in \mathbf{SL}_n(K)$, alors $\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$, donc $AB \in \mathbf{SL}_n(K)$.
- $\mathrm{I}_n \in \mathbf{SL}_n(K)$ car $\det(\mathrm{I}_n) = 1$.
- Si $A \in \mathbf{SL}_n(K)$, alors $\det(A^{-1}) = \big(\det(A)\big)^{-1} = 1^{-1} = 1$, donc $A^{-1} \in \mathbf{SL}_n(K)$.

b) Soit $A \in \mathbf{GL}_n(\mathbb{C})$. Il existe $\alpha \in \mathbb{C}^*$ tel que $\alpha^n = \det(A)$; en notant $B = \dfrac{1}{\alpha}A$, on a alors : $\det(B) = \dfrac{1}{\alpha^n}\det(A) = 1$, donc $B \in \mathbf{SL}_n(\mathbb{C})$.

9.4.4 Soit A convenant.

• En prenant $M = A$, on obtient $2^n\det(A) = 2\det(A)$, d'où, puisque $n \geqslant 2$, $\det(A) = 0$.

On a donc : $\forall M \in \mathbf{M}_n(\mathbb{C})$, $\det(A + M) = \det(M)$.

• Notons $C_1, \dots, C_n$ les colonnes de A.

Supposons $A \neq 0$; il existe $j \in \{1,\dots,n\}$ tel que $C_j \neq 0$. D'après le théorème de la base incomplète, il existe des colonnes $V_1, \dots, V_{j-1}, V_{j+1}, \dots, V_n$ de $\mathbf{M}_{n,1}(\mathbb{C})$ telles que $(V_1, \dots, V_{j-1}, C_j, V_{j+1}, \dots, V_n)$ soit une base de $\mathbf{M}_{n,1}(\mathbb{C})$.

En notant M la matrice dont les colonnes sont $V_1, \dots, V_{j-1}, -C_j, V_{j+1}, \dots, V_n$, on a alors :

$\left\{\begin{array}{l} \det(A + M) = 0 \quad (\text{car la } j^{\text{ème}} \text{ colonne est nulle}) \\ \det(M) \neq 0 \end{array}\right.$, contradiction.

Donc $A = 0$.

Réciproque évidente.

◇ **Réponse :** $\{0\}$.

9.4.5 *a)* Puisque $AB = BA$, on a : $A^2 + B^2 = (A + iB)(A - iB)$, d'où :
$\det(A^2 + B^2) = \det(A + iB)\det(A - iB) = \det(A + iB)\overline{\det(A + iB)} = |\det(A + iB)|^2 \geqslant 0$.

b) ◇ **Réponse :** • oui, si $n = 1$

• non, si $n \geqslant 2$; exemple : $A = \begin{pmatrix} 0 & -2 \\ 2 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$.

9.4.6 L'application $P : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \det(A + xB) \end{array}$ est polynomiale, donc continue.

Puisque $P(x) \underset{x \to 0}{\longrightarrow} P(0) = \det(A) \neq 0$, il existe $\varepsilon > 0$ tel que :

$\forall x \in \mathbb{R}, \big(|x| < \varepsilon \Longrightarrow P(x) \neq 0 \Longrightarrow A + xB \in \mathbf{GL}_n(\mathbb{R})\big)$.

9.4.7 *a)* Récurrence sur k.

• Evident pour $k = 0$.

• Si $AB^k = B^k(A + kI_n)$, alors :

$$AB^{k+1} = AB^k B = B^k(A + kI_n)B = B^k(AB + kB) = B^k(BA + B + kB) = B^{k+1}\big(A + (k+1)I_n\big).$$

b) Raisonnons par l'absurde : supposons $\det(B) \neq 0$. On déduit alors de *a)* :

$$\forall k \in \mathbb{N}, \det(A) = \det(A + kI_n).$$

Mais $\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \det(A + xI_n) \end{array}$ est, par développement, un polynôme de degré n et de coefficient dominant 1 (le seul terme en x^n provient du développement du déterminant faisant intervenir la permutation identité).
Donc $\det(A + kI_n) \underset{k \infty}{\longrightarrow} +\infty$, contradiction.

9.5.1 ◇ **Réponse :** $\operatorname{com}(A) = \begin{pmatrix} \det(M) & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & 0 & \\ 0 & & & \end{pmatrix}$.

9.5.2 Puisque $A^p = I_n$ et $p \in \mathbb{N}^*$, A est inversible, d'où :
$\big(\operatorname{com}(A)\big)^p = \big(\det(A)\,{}^tA^{-1}\big)^p = \big(\det(A)\big)^p\,{}^t(A^{-1})^p = \det(A^p)\,{}^t(A^p)^{-1} = I_n$.

9.5.3 Puisque A est inversible :
$\operatorname{com}(A^{-1}) = \det(A^{-1})\,{}^t(A^{-1})^{-1} = \big(\det(A)\,{}^tA^{-1}\big)^{-1} = \big(\operatorname{com}(A)\big)^{-1}$.

9.6.1 *a)*
$$\begin{vmatrix} 1^2 & 2^2 & 3^2 & \dots & n^2 \\ 2^2 & 3^2 & 4^2 & \dots & (n+1)^2 \\ \vdots & \vdots & \vdots & & \vdots \\ n^2 & (n+1)^2 & (n+2)^2 & \dots & (2n-1)^2 \end{vmatrix} = \begin{vmatrix} 1^2 & 3 & 5 & \dots & 2n-1 \\ 2^2 & 5 & 7 & \dots & 2n+1 \\ \vdots & \vdots & \vdots & & \vdots \\ n^2 & 2n+1 & 2n+3 & \dots & 4n-3 \end{vmatrix}$$

par $C_j \longleftarrow C_j - C_{j-1}$ pour $j \geqslant 2$

$$= \begin{vmatrix} 1^2 & 3 & 2 & \cdots & 2 \\ 2^2 & 5 & 2 & \cdots & 2 \\ \vdots & \vdots & | & & | \\ n^2 & 2n+1 & 2 & \cdots & 2 \end{vmatrix} \text{ par } C_j \longleftarrow C_j - C_{j-1} \text{ pour } j \geqslant 3.$$

◇ **Réponse :** $\begin{cases} 0 & \text{si } n \geqslant 3 \\ -7 & \text{si } n = 2 \\ 1 & \text{si } n = 1 \end{cases}$.

b) Opérer simultanément : $C_2 \longleftarrow C_2 - C_1, C_3 \longleftarrow C_3 - C_2, \dots, C_n \longleftarrow C_n - C_{n-1}$ (ce qui revient à opérer *successivement* : $C_n \longleftarrow C_n - C_{n-1}, \dots, C_3 \longleftarrow C_3 - C_2, C_2 \longleftarrow C_2 - C_1$) :

$$\begin{vmatrix} S_1 & S_1 & S_1 & \cdots & S_1 \\ S_1 & S_2 & S_2 & \cdots & S_2 \\ S_1 & S_2 & S_3 & \cdots & S_3 \\ | & | & | & \ddots & \vdots \\ S_1 & S_2 & S_3 & \dots & S_n \end{vmatrix} = \begin{vmatrix} S_1 & 0 & \cdots & 0 \\ | & S_2 - S_1 & & \\ | & | & \ddots & 0 \\ S_1 & S_2 - S_1 & \dots & S_n - S_{n-1} \end{vmatrix}$$

◇ **Réponse :** $n!$.

c) Opérer simultanément $C_2 \longleftarrow C_2 - C_1, C_3 \longleftarrow C_3 - C_2, \dots, C_n \longleftarrow C_n - C_{n-1}$, puis développer par rapport à la dernière ligne.

◇ **Réponse :** $(-1)^{n+1} a_1 (a_2 - a_1)^{n-1}$.

d) En développant par multilinéarité et alternance :

$$\begin{vmatrix} a_1 + b_1 & a_1 & \dots & a_1 \\ a_2 & a_2 + b_2 & \dots & a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_n & a_n & \dots & a_n + b_n \end{vmatrix} = \begin{vmatrix} b_1 & & & 0 \\ & \ddots & & \\ & & & \\ 0 & & & b_n \end{vmatrix} + \begin{vmatrix} a_1 & 0 & & \\ a_2 & b_2 & 0 & \\ \vdots & & \ddots & \\ a_n & 0 & & b_n \end{vmatrix} + \begin{vmatrix} b_1 & a_1 & 0 & \\ 0 & a_2 & 0 & \\ | & \vdots & b_3 & 0 \\ | & \vdots & & \ddots \\ 0 & a_n & 0 & b_n \end{vmatrix}$$

$$+ \dots + \begin{vmatrix} b_1 & & & a_1 \\ & \ddots & 0 & \vdots \\ & & b_{n-1} & \vdots \\ 0 & & & a_n \end{vmatrix}$$

◇ **Réponse :** $b_1 \dots b_n + a_1 b_2 \dots b_n + b_1 a_2 b_3 \dots b_n + \dots + b_1 \dots b_{n-1} a_n$.

Si $b_1 \dots b_n \neq 0$, on peut écrire le résultat sous la forme : $b_1 \dots b_n \left(1 + \dfrac{a_1}{b_1} + \dots + \dfrac{a_n}{b_n}\right)$.

e) En notant Δ_n le déterminant proposé, et en remplaçant C_n par $C_1 + \ldots + C_n$, on obtient :

$$\Delta_n = \begin{vmatrix} a_1 & -a_1 & & & 0 \\ -a_1 & a_1+a_2 & \ddots & & \\ & \ddots & \ddots & -a_{n+2} & \\ & 0 & -a_{n-2} & a_{n-2}+a_{n-1} & 0 \\ & & 0 & -a_{n-1} & a_n \end{vmatrix} = a_n \Delta_{n-1}.$$

◇ **Réponse :** $\prod_{k=1}^{n} a_k$.

f) Notons $\Delta_n = \begin{vmatrix} a & b & & & 0 \\ c & \ddots & \ddots & & \\ & \ddots & \ddots & b & \\ & & c & a & \\ 0 & & & & \end{vmatrix}_{[n]}$.

Pour $n \geqslant 3$, on obtient en développant d'abord par rapport à la 1ère ligne :

$$\Delta_n = a\Delta_{n-1} - b \begin{vmatrix} c & b & & & \\ 0 & a & b & 0 & \\ & c & \ddots & \ddots & \\ & & \ddots & \ddots & b \\ 0 & & 0 & c & a \end{vmatrix}_{[n-1]} = a\Delta_{n-1} - bc\Delta_{n-2}.$$

Utiliser l'étude des suites récurrences linéaires du 2nd ordre à coefficients constants (Tome 1, 3.4.2).

L'équation caractéristique est $r^2 - ar + bc = 0$, de discriminant $\delta = a^2 - 4bc$.

1er cas : $\delta \neq 0$

L'équation caractéristique admet deux solutions distinctes r_1, r_2, et il existe $(\lambda_1, \lambda_2) \in \mathbb{C}^2$ tel que :

$$\forall n \in \mathbb{N}^*,\ \Delta_n = \lambda_1 r_1^n + \lambda_2 r_2^n.$$

Remarquons qu'on peut poser $\Delta_0 = 1$ pour que la relation $\Delta_n = a\Delta_{n-1} - bc\Delta_{n-2}$ soit aussi vraie pour $n = 2$. Alors : $\begin{cases} \Delta_0 = 1 \\ \Delta_1 = a \end{cases} \iff \begin{cases} \lambda_1 + \lambda_2 = 1 \\ \lambda_1 r_1 + \lambda_2 r_2 = a \end{cases} \iff \begin{cases} \lambda_1 = \dfrac{r_1}{r_1 - r_2} \\ \lambda_2 = \dfrac{r_2}{r_2 - r_1} \end{cases}$.

D'où : $\Delta_n = \dfrac{1}{r_1 - r_2}(r_1^{n+1} - r_2^{n+1})$.

2ème cas : $\delta = 0$

L'équation caractéristique admet une solution «double» valant $\dfrac{a}{2}$, et il existe $(\lambda, \mu) \in \mathbb{C}^2$ tel que :

$$\forall n \in \mathbb{N},\ \Delta_n = (\lambda n + \mu)\left(\frac{a}{2}\right)^n.$$

Alors : $\begin{cases} \Delta_0 = 1 \\ \Delta_1 = a \end{cases} \iff \begin{cases} \mu = 1 \\ (\lambda + \mu)\dfrac{a}{2} = a \end{cases} \iff \lambda = \mu = 1.$

◇ **Réponse :** • Si $a^2 - 4bc \neq 0$, en notant r_1, r_2 les deux zéros de $X^2 - aX + bc$ dans $\mathbb{C}$, on a :

$$\forall n \in \mathbb{N},\quad \Delta_n = \frac{1}{r_1 - r_2}(r_1^{n+1} - r_2^{n+1}).$$

• Si $a^2 - 4bc = 0$, alors : $\forall n \in \mathbb{N},\ \Delta_n = (n+1)\left(\dfrac{a}{2}\right)^n$.

On peut réunir les réponses de ces deux cas sous la forme : $\Delta_n = \sum_{k=0}^{n} r_1^k r_2^{n-k}$.

g) En notant Δ_n le déterminant proposé :

$$\Delta_n = \begin{vmatrix} C_0^0 & 0 & \cdots & 0 \\ C_1^0 & C_1^1 & \cdots & C_n^n \\ C_2^0 & C_2^1 & \cdots & C_{n+1}^n \\ \vdots & \vdots & & \vdots \\ C_n^0 & C_n^1 & \cdots & C_{2n-1}^n \end{vmatrix} \quad \text{par } C_j \longleftarrow C_j - C_{j-1} \text{ pour } j \geqslant 2$$

$$= \begin{vmatrix} C_0^0 & 0 & \cdots & 0 \\ 0 & C_1^1 & \cdots & C_n^n \\ \vdots & C_1^0 & \cdots & C_n^{n-1} \\ & \vdots & & \vdots \\ 0 & C_{n-1}^0 & \cdots & C_{2n-2}^{n-1} \end{vmatrix} \quad \text{par } L_i \longleftarrow L_i - L_{i-1} \text{ pour } i \geqslant 2$$

$= \Delta_{n-1}$.

◇ **Réponse :** 1.

h) Notons Δ_n le déterminant proposé. En développant par rapport à la dernière ligne :

$$\Delta_n = \alpha\, \Delta_{n-1} + (-1)^{n+1} a_n \begin{vmatrix} -1 & & & \\ \alpha & \ddots & 0 & \\ & \ddots & \ddots & \\ 0 & & \alpha & -1 \end{vmatrix} = \alpha \Delta_{n-1} + a_n.$$

◇ **Réponse :** $\displaystyle\sum_{k=0}^{n} \alpha^k a_{n-k}$ (en notant $a_0 = 1$).

i) Notons Δ_n le déterminant proposé. On a, en développant par rapport à la dernière ligne :

$$\Delta_n = b_n \Delta_{n-1} + (-1)^{n+2} a_n \begin{vmatrix} -a_1 & \cdots & \cdots & -a_n \\ b_1 & \ddots & 0 & \\ & \ddots & \ddots & \\ 0 & & b_{n-1} & 0 \end{vmatrix}_{[n]}$$

$$= b_n \Delta_{n-1} + (-1)^{n+2} a_n (-1)^{n+1} (-a_n) b_1 \ldots b_{n-1} = b_n \Delta_{n-1} + b_1 \ldots b_{n-1} a_n^2.$$

Sommer, après multiplication par les coefficients :

$$\begin{array}{ll} \Delta_n = b_n \Delta_{n-1} + b_1 \ldots b_{n-1} a_n^2 & 1 \\ \Delta_{n-1} = b_{n-1} \Delta_{n-2} + b_1 \ldots b_{n-2} a_{n-2}^2 & b_n \\ \Delta_{n-2} = b_{n-2} \Delta_{n-3} + b_1 \ldots b_{n-3} a_{n-2}^2 & b_{n-1} b_n \\ \quad \vdots & \quad \vdots \\ \Delta_1 = b_1 + a_1^2 & b_2 \ldots b_n \end{array}$$

◇ **Réponse :** $b_1 \ldots b_{n-1} a_n^2 + b_1 \ldots b_{n-2} a_{n-1}^2 b_n + \ldots + a_1^2 b_2 \ldots b_n$.

Si $b_1 \ldots b_n \neq 0$, on peut écrire le résultat sous la forme : $b_1 \ldots b_n \left(1 + \dfrac{a_1^2}{b_1} + \ldots + \dfrac{a_n^2}{b_n}\right)$.

j) Montrer la relation $\Delta_n = z\Delta_{n-1} - xyz^{n-2}$.

◇ **Réponse :** $az^{n-1} - (n-1)xyz^{n-2}$.

k) En notant Δ_n le déterminant proposé, on a :

$$\Delta_n = \begin{vmatrix} -(a+1) & 1 & & 0 & -a \\ a & & \ddots & & 0 \\ & \ddots & & n-2 & \vdots \\ 0 & & a & -(a+n-1) & 0 \\ 0 & \cdots & 0 & a & -n \end{vmatrix} \quad \text{par } C_n \leftarrow C_1 + \ldots + C_n$$

$= (-1)^{n+1}(-a)a^{n-1} - n\Delta_{n-1}$ par développement par rapport à la dernière colonne.

En notant $D_n = \dfrac{(-1)^n}{n!}\Delta_n$, on obtient : $\forall n \in \mathbb{N} - \{0,1\}$, $D_n = \dfrac{a^n}{n!} + D_{n-1}$ (et $D_1 = -(a+1)$).

◇ **Réponse :** $(-1)^n n! \displaystyle\sum_{k=0}^{n} \frac{a^k}{k!}$.

9.6.2 Notons $I = \mathrm{I}_3$, $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix}$. Comme $A^2 = \begin{pmatrix} 0 & 0 & 1 \\ 2 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}$, on a :

$$E = \{xI + yA + zA^2 ; (x,y,z) \in \mathbb{Q}^3\}.$$

Il est clair alors que E est le sev de $\mathbf{M}_3(\mathbb{Q})$ engendré par (I, A, A^2).

D'autre part, comme $A^3 = 2I$, le produit de deux éléments de E se décompose $\mathbb{Q}$-linéairement sur I, A, A^2. On en déduit que E est un sous-anneau de $\mathbf{M}_3(\mathbb{Q})$.

Il reste à montrer que tout élément de E autre que 0 admet un inverse dans E.

Nous allons d'abord établir : $\forall M \in E$, $\big(\det(M) = 0 \Longrightarrow M = 0\big)$.

Soient $(x,y,z) \in \mathbb{Q}^3$, $M = xI + yA + zA^2$, et supposons $\det(M) = 0$, c'est-à-dire après développement :

$$x^3 + 2y^3 + 4z^3 - 6xyz = 0.$$

Il existe $(\alpha,\beta,\gamma) \in \mathbb{Z}^3$ et $q \in \mathbb{N}^*$ tels que $x = \dfrac{\alpha}{q}$, $y = \dfrac{\beta}{q}$, $z = \dfrac{\gamma}{q}$, d'où :

$$\alpha^3 + 2\beta^3 + 4\gamma^3 - 6\alpha\beta\gamma = 0.$$

Nous allons montrer, par la méthode de descente infinie, que cette équation d'inconnue $(\alpha,\beta,\gamma) \in \mathbb{Z}^3$, n'admet que $(0,0,0)$ pour solution.

Soit (α,β,γ) une solution.

Alors $2|\alpha^3$, donc $2|\alpha$, et il existe donc $\alpha' \in \mathbb{Z}$ tel que $\alpha = 2\alpha'$, d'où :

$$4\alpha'^3 + \beta^3 + 2\gamma^3 - 6\alpha'\beta\gamma = 0.$$

De même, $2|\beta$ et il existe donc $\beta' \in \mathbb{Z}$ tel que $\beta = 2\beta'$, d'où :

$$2\alpha'^3 + 4\beta'^3 + \gamma^3 - 6\alpha'\beta'\gamma = 0.$$

Encore, $2|\gamma$ et il existe donc $\gamma' \in \mathbb{Z}$ tel que $\gamma = 2\gamma'$, d'où :

$$\alpha'^3 + 2\beta'^3 + 4\gamma'^3 - 6\alpha'\beta'\gamma' = 0,$$

c'est-à-dire que (α',β',γ') est solution.

Ainsi, pour tout solution (α,β,γ), les trois entiers α,β,γ sont divisibles par 2. En réitérant, on en déduit que α,β,γ sont divisibles par toute puissance 2^n ($n \in \mathbb{N}^*$), et donc $\alpha = \beta = \gamma = 0$.

Soit $M \in E - \{0\}$. D'après l'étude précédente, $\det(M) \neq 0$, et donc $M \in \mathbf{GL}_3(\mathbb{Q})$.

L'application $f : \begin{array}{ccc} E & \longrightarrow & E \\ N & \longmapsto & MN \end{array}$ est linéaire, injective (puisque M est inversible dans $\mathbf{GL}_3(\mathbb{Q})$), et E est de dimension finie, donc f est bijective. Comme $I_3 \in E$, il existe donc $N \in E$ telle que $MN = I_3$, c'est-à-dire : $M^{-1} \in E$.

9.6.3 *a)* $\begin{cases} abc < 0 \\ def < 0 \\ ghk < 0 \end{cases} \Longrightarrow abcdefghk < 0$, et $\begin{cases} adg > 0 \\ beh > 0 \\ cfk > 0 \end{cases} \Longrightarrow abcdefghk > 0.$

b) $\begin{cases} aeh > 0 \\ bfg > 0 \\ cdh > 0 \end{cases} \Longrightarrow abcdefghk > 0$, et $\begin{cases} -ceg > 0 \\ -afh > 0 \\ -bdk > 0 \end{cases} \Longrightarrow abcdefghk < 0.$

9.6.4 Remarquer d'abord que f est linéaire.

Rappelons que $\mathbf{S}_n(\mathbb{R})$ (ensemble des matrices symétriques réelles d'ordre n) et $\mathbf{A}_n(\mathbb{R})$ (ensemble des matrices antisymétriques réelles d'ordre n) sont deux sev supplémentaires dans $\mathbf{M}_n(\mathbb{R})$ (cf. 8.3.1 Prop. 2 p. 295).

Dans une base de $\mathbf{M}_n(\mathbb{R})$ formée d'une base de $\mathbf{S}_n(\mathbb{R})$ suivie d'une base de $\mathbf{A}_n(\mathbb{R})$, la matrice de f est :

$$\begin{pmatrix} 1 & & & & \\ & \ddots & & 0 & \\ & & 1 & & \\ & & & -1 & \\ & 0 & & & \ddots \\ & & & & -1 \end{pmatrix}, \text{ d'où : } \det(f) = (-1)^{\dim(\mathbf{A}_n(\mathbb{R}))} = (-1)^{\frac{n(n-1)}{2}}.$$

On pouvait remarquer au départ que, puisque f est une involution : $\big(\det(f)\big)^2 = \det(f^2) = 1$.

◇ **Réponse :** $(-1)^{\frac{n(n-1)}{2}}$.

9.6.5 *a)*

$$\varphi_p(x+1) - \varphi_p(x) = \begin{vmatrix} 1 & 0 & 0 & \dots & \dots & (1+x)-x \\ & 2 & 0 & \ddots & \dots & (1+x)^2 - x^2 \\ & & 3 & \ddots & \ddots & \vdots \\ & & \vdots & \ddots & C_p^{p-1} & (1+x)^p - x^p \\ 1 & C_{p+1}^1 & C_{p+1}^2 & \dots & C_{p+1}^{p-1} & (1+x)^{p+1} - x^{p+1} \end{vmatrix}.$$

La dernière colonne se décompose :

$$\begin{pmatrix} (1+x)-x \\ (1+x)^2-x^2 \\ \vdots \\ (1+x)^p-x^p \\ (1+x)^{p+1}-x^{p+1} \end{pmatrix} = \begin{pmatrix} 1 \\ 1+2x \\ 1+3x+3x^2 \\ \vdots \\ \sum_{k=0}^{p} C_{p+1}^k x^k \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} + x \begin{pmatrix} 0 \\ 2 \\ 3 \\ \vdots \\ C_{p+1}^1 \end{pmatrix} + \ldots + x^{p-1} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ C_p^{p-1} \\ C_{p+1}^{p-1} \end{pmatrix} + x^p \begin{pmatrix} 0 \\ \vdots \\ 0 \\ C_{p+1}^p \end{pmatrix},$$

d'où, par multilinéarité et alternance :

$$\varphi_p(x+1)-\varphi_p(x) = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 2 & 0 & & \vdots \\ 1 & 3 & 3 & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & C_p^{p-1} \\ 1 & C_{p+1}^1 & C_{p+1}^2 & \cdots & C_{p+1}^{p-1} \end{vmatrix} \begin{matrix} \\ \\ \\ \\ 0 \\ 0 \\ C_{p+1}^p x^p \end{matrix} = 1 \cdot 2 \cdot 3 \ldots p(p+1)x^p.$$

◇ **Réponse :** $(p+1)!x^p$.

b)
$$\begin{array}{lll} \varphi_p(n+1)-\varphi_p(n) & = & (p+1)!n^p \\ \varphi_p(n)-\varphi_p(n-1) & = & (p+1)!(n-1)^p \\ \vdots & & \\ \varphi_p(2)-\varphi_p(1) & = & (p+1)!1^p \\ \varphi_p(1) & = & 0 \\ \hline \varphi_p(n+1) & = & (p+1)!\sum_{k=1}^{n} k^p. \end{array}$$

c) 1) $$\sum_{k=1}^{n} k = \frac{1}{2!}\varphi_1(n+1) = \frac{1}{2}\begin{vmatrix} 1 & n+1 \\ 1 & (n+1)^2 \end{vmatrix} = \frac{n(n+1)}{2}.$$

2) $$\sum_{k=1}^{n} k^2 = \frac{1}{3!}\varphi_2(n+1) = \frac{1}{6}\begin{vmatrix} 1 & 0 & n+1 \\ 1 & 2 & (n+1)^2 \\ 1 & 3 & (n+1)^3 \end{vmatrix} = \frac{n+1}{6}\begin{vmatrix} 1 & 0 & 0 \\ 1 & 2 & n \\ 1 & 3 & n^2+2n \end{vmatrix} = \frac{n(n+1)(2n+1)}{6}.$$

3) $$\sum_{k=1}^{n} k^3 = \frac{1}{4!}\varphi_3(n+1) = \frac{1}{24}\begin{vmatrix} 1 & 0 & 0 & n+1 \\ 1 & 2 & 0 & (n+1)^2 \\ 1 & 3 & 3 & (n+1)^3 \\ 1 & 4 & 6 & (n+1)^4 \end{vmatrix}$$

$$= \frac{n+1}{24}\begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & n \\ 1 & 3 & 3 & n^2+2n \\ 1 & 4 & 6 & n^3+3n^2+3n \end{vmatrix} = \frac{n(n+1)}{24}\begin{vmatrix} 2 & 0 & 1 \\ 3 & 3 & n+2 \\ 4 & 6 & n^2+3n+3 \end{vmatrix} = \frac{n^2(n+1)^2}{4}.$$

◇ **Réponse :** $\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$, $\displaystyle\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$, $\displaystyle\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$.

9.6.6 En développant par multilinéarité et alternance (comme dans la solution de l'exercice 9.6.1 *d)* p. 549), on obtient :

$$\det(A) = x_1 \dots x_n + x_2 \dots x_n + x_1 x_3 \dots x_n + \dots + x_1 \dots x_{n-1} = \sigma_n + \sigma_{n-1},$$

où $\sigma_1, \dots, \sigma_n$ sont les fonctions symétriques élémentaires de $x_1, \dots, x_n$ (cf. 5.3.2 Déf. 2 p. 172). Comme $x_1, \dots, x_n$ sont les zéros de $X^n - X + 1$, on a (cf. 5.3.2 Prop. p. 173) : $\sigma_{n-1} = (-1)^n$ et $\sigma_n = (-1)^n$.

◇ **Réponse :** $2(-1)^n$.

9.6.7 L'application $\varphi : E^n \longrightarrow K$ définie par :

$$\forall (V_1, \dots, V_n) \in E^n, \quad \varphi(V_1, \dots, V_n) = \sum_{j=1}^{n} \det_{\mathcal{B}}(V_1, \dots, f(V_j), \dots, V_n)$$

est clairement une forme n-linéaire alternée.

D'après 9.2.2 Prop. 1 p. 306, on a : $\forall (V_1, \dots, V_n) \in E^n, \quad \varphi(V_1, \dots, V_n) = \det_{\mathcal{B}}(V_1, \dots, V_n)\varphi(\mathcal{B})$.

D'autre part, en notant $A = (a_{ij})_{ij}$ la matrice de f dans $\mathcal{B}$, on a :

$$\varphi(\mathcal{B}) = \sum_{j=1}^{n} \begin{vmatrix} 1 & & 0 & a_{1j} & & \\ & \ddots & & \vdots & & 0 \\ & & 1 & a_{jj} & & \\ & & & \vdots & 1 & \\ 0 & & & a_{nj} & 0 & \ddots \\ & & & & & 1 \end{vmatrix} = \sum_{j=1}^{n} a_{jj} = \operatorname{tr}(A) = \operatorname{tr}(f).$$

9.6.8 Puisque $\det(A)$ s'exprime comme somme de produits d'éléments de A, on obtient, en passant modulo 2 : $\det(A) \equiv \begin{vmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{vmatrix} = 1$, et donc $\det(A) \neq 0$.

9.6.9 De même que dans la solution de l'exercice 9.6.8, on obtient, modulo 2 :

$$\det(A) \equiv \begin{vmatrix} 0 & & 1 \\ & \ddots & \\ 1 & & 0 \end{vmatrix}_{[n]}$$

$$\text{Et : } \begin{vmatrix} 0 & & 1 \\ & \ddots & \\ 1 & & 0 \end{vmatrix}_{[n]} = (n-1) \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \vdots & 0 & \ddots & \\ 1 & & 1 & 0 \end{vmatrix} \quad \text{par } C_1 \longleftarrow C_1 + \dots + C_n$$

$$= (n-1) \begin{vmatrix} 1 & \cdots & \cdots & 1 \\ 0 & -1 & & \\ \vdots & & \ddots & \\ 0 & & & -1 \end{vmatrix} \quad \text{par } L_i \longleftarrow L_i - L_1 \text{ pour } i \geqslant 2$$

$$= (n-1)(-1)^{n-1}.$$

Comme n est pair : $(n-1)(-1)^{n-1} \equiv 1$ [2].

Autre méthode : montrer qu'on peut appliquer l'exercice 9.6.8 à A^2, d'où $\det(A^2) \neq 0$, puis $\det(A) \neq 0$.

9.8.1 *1)* Si $\operatorname{rg}(A) \leqslant n-2$, alors tous les cofacteurs de A sont nuls, puisque ce sont des déterminants de matrices carrées d'ordre $n-1$ extraites de A, cf. 9.8 Th. p. 330.

2) Si $\operatorname{rg}(A) = n$, alors $\det(A) \neq 0$ et, comme $\left(\frac{1}{\det(A)}\,{}^tA\right)\operatorname{com}(A) = I_n$, $\operatorname{com}(A)$ est inversible, donc $\operatorname{rg}\big(\operatorname{com}(A)\big) = n$.

3) Supposons $\operatorname{rg}(A) = n-1$.

Puisque $A\,{}^t\operatorname{com}(A) = \det(A)I_n = 0$, on a $\operatorname{Im}\big({}^t\operatorname{com}(A)\big) \subset \operatorname{Ker}(A)$ et donc :

$\operatorname{rg}\big(\operatorname{com}(A)\big) = \operatorname{rg}\big({}^t\operatorname{com}(A)\big) \leqslant \dim\big(\operatorname{Ker}(A)\big)$.

Mais, d'après le théorème du rang, $\dim\big(\operatorname{Ker}(A)\big) = n - \operatorname{rg}(A) = 1$.

D'autre part, d'après 9.8 Th. p. 330, il existe une matrice carrée d'ordre $n-1$ extraite de A et inversible, et donc au moins un des cofacteurs de A est $\neq 0$, d'où $\operatorname{com}(A) \neq 0$.

On conclut : $\operatorname{rg}\big(\operatorname{com}(A)\big) = 1$.

9.8.2 Pour $p \in \mathbb{N}^*$, notons $\operatorname{com}_p(A) = \operatorname{com}(\ldots(\operatorname{com}(A))\ldots)$, où com est itéré p fois.

a) Commençons par déterminer $\operatorname{com}_2(A)$.

1) Si $\operatorname{rg}(A) \leqslant n-2$, d'après l'exercice 9.8.1, $\operatorname{com}(A) = 0$, donc $\operatorname{com}_2(A) = 0$.

2) Supposons $\operatorname{rg}(A) = n$. Alors : $\operatorname{com}(A) = \det(A)\,{}^tA^{-1}$, d'où :

$\det\big(\operatorname{com}(A)\big) = \big(\det(A)\big)^n\big(\det(A)\big)^{-1} = \big(\det(A)\big)^{n-1} \neq 0$,

et donc $\operatorname{com}(A)$ est inversible (cf. aussi exercice 9.5.3 p. 317). Puis :

$$\begin{aligned}\operatorname{com}_2(A) &= \operatorname{com}\big(\operatorname{com}(A)\big) = \det\big(\operatorname{com}(A)\big)\,{}^t\big(\operatorname{com}(A)\big)^{-1}\\ &= \big(\det(A)\big)^{n-1}\,{}^t\big(\det(A)\,{}^tA^{-1}\big)^{-1} = \big(\det(A)\big)^{n-2}A.\end{aligned}$$

3) Supposons $\operatorname{rg}(A) = n-1$.

D'après l'exercice 9.8.1, $\operatorname{rg}\big(\operatorname{com}(A)\big) = 1$, donc si $n \geqslant 3$, en appliquant l'exercice 9.8.1 à $\operatorname{com}(A)$ au lieu de A : $\operatorname{com}_2(A) = 0$.

Si $n = 2$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\det(A) = 0$, $\operatorname{com}(A) = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$, $\operatorname{com}_2(A) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = A = \big(\det(A)\big)^{n-2}A$, puisque $0^0 = 1$.

On a ainsi prouvé : $\forall A \in \mathbf{M}_n(K)$, $\operatorname{com}_2(A) = \big(\det(A)\big)^{n-2}A$.

b) On déduit : $\operatorname{com}_3(A) = \operatorname{com}\big(\big(\det(A)\big)^{n-2}A\big) = \big(\det(A)\big)^{(n-2)(n-1)}\operatorname{com}(A)$, grâce à la formule évidente :

$$\forall \lambda \in K,\ \operatorname{com}(\lambda A) = \lambda^{n-1}\operatorname{com}(A).$$

Puis $\operatorname{com}_4(A) = \big(\det(A)\big)^{(n-2)(n-1)^2}\operatorname{com}_2(A) = \big(\det(A)\big)^{(n-2)(1+(n-1)^2)}A$.

Montrer le résultat par récurrence.

◇ **Réponse :**

$\big(\det(A)\big)^{(n-2)(n-1)(1+(n-1)^2+\ldots+(n-1)^{2k-2})}\operatorname{com}(A)$ si p est impair $\geqslant 3$, $p = 2k+1$, $k \in \mathbb{N}^*$

$\big(\det(A)\big)^{(n-2)(1+(n-1)^2+\ldots+(n-1)^{2k-2})}A$ si p est pair, $p = 2k$, $k \in \mathbb{N}^*$.

9.8.3 On a : $AB = 0 \Longrightarrow \mathrm{Im}(B) \subset \mathrm{Ker}(A) \Longrightarrow \mathrm{rg}(B) \leqslant \dim\big(\mathrm{Ker}(A)\big) = n - \mathrm{rg}(A) = 1$.

Si $B = 0$, alors $\gamma = 0$ convient.

Supposons $B \neq 0$. Comme $\mathrm{rg}(B) = 1$, d'après l'exercice 8.1.31 *a)* p. 285, il existe $U, V \in \mathbf{M}_{n,1}(K)$ tels que $B = U\,{}^tV$. Alors : $\begin{cases} AB = 0 \\ BA = 0 \end{cases} \iff \begin{cases} (AU)\,{}^tV = 0 \\ U({}^tVA) = 0 \end{cases}$.

Si l'un des éléments de la colonne AU était $\neq 0$, comme la ligne ${}^tV$ est $\neq 0$ (sinon : $B = 0$), l'un au moins des éléments de la matrice carrée $(AU)\,{}^tV$ serait non nul, contradiction.

Donc $AU = 0$; de même ${}^tVA = 0$, donc ${}^tAV = 0$.

Comme $\dim\big(\mathrm{Ker}(A)\big) = 1$ et $\dim\big(\mathrm{Ker}({}^tA)\big) = n - \mathrm{rg}({}^tA) = n - \mathrm{rg}(A) = 1$, on déduit que U (resp. V) engendre $\mathrm{Ker}(A)$ (resp. $\mathrm{Ker}({}^tA)$).

Le même raisonnement est applicable à ${}^t\mathrm{com}(A)$ au lieu de B.

Il existe donc $U_0, V_0 \in \mathbf{M}_{n,1}(K)$, $\alpha, \beta \in K - \{0\}$ tels que : ${}^t\mathrm{com}(A) = U_0\,{}^tV_0$, $U = \alpha U_0$, $V = \beta V_0$, et donc $B = \alpha\beta U_0\,{}^tV_0 = \alpha\beta\,{}^t\mathrm{com}(A)$.

9.8.4 *1)* Déterminons $\mathrm{rg}(A)$.

On peut d'abord remarquer que la somme des colonnes de A est nulle, donc $\det(A) = 0$.

Pour tout $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ de $\mathbf{M}_{n,1}(K)$:

$$X \in \mathrm{Ker}(A) \iff \begin{cases} (1-n)x_1 + x_2 + \ldots + x_n = 0 \\ \vdots \\ x_1 + \ldots + x_{n-1} + (1-n)x_n = 0 \end{cases} \iff \begin{cases} x_1 + \ldots + x_n = nx_1 \\ \vdots \\ x_1 + \ldots + x_n = nx_n \end{cases} \iff x_1 = \ldots = x_n.$$

Donc $\dim(\mathrm{Ker}(A)) = 1$, $\mathrm{rg}(A) = n - 1$.

2) D'après l'exercice 9.8.1 p. 556, on a donc $\mathrm{rg}\big(\mathrm{com}(A)\big) = 1$.

En notant $B = \begin{pmatrix} 1 & & 1 \\ & \ddots & \\ 1 & & 1 \end{pmatrix} \in \mathbf{M}_n(K)$, on a clairement $AB = BA = 0$.

D'après l'exercice 9.8.3, il existe $\delta \in K$ tel que ${}^t\mathrm{com}(A) = \delta B$. Autrement dit, tous les termes de $\mathrm{com}(A)$ sont égaux. Le $(1,1)^{\text{ème}}$ terme de $\mathrm{com}(A)$ est :

$$\begin{vmatrix} 1-n & 1 & & \\ & \ddots & & \\ 1 & & 1-n & \\ & & & \end{vmatrix}_{[n-1]} = \begin{vmatrix} -1 & 1 & & 1 \\ & 1-n & & \\ & & \ddots & \\ -1 & & 1 & 1-n \end{vmatrix}_{[n-1]} \quad \text{par } C_1 \longleftarrow C_1 + \ldots + C_{n-1}$$

$$= \begin{vmatrix} -1 & 1 & & 1 \\ 0 & -n & & \\ & & \ddots & \\ 0 & & & -n \end{vmatrix}_{[n-1]} \quad \text{par } L_i \longleftarrow L_i - L_1 \text{ pour } i \geqslant 2$$

$$= (-1)^{n-1}n^{n-2}$$

◇ **Réponse :** $\mathrm{com}(A) = (-1)^{n-1}n^{n-2}\begin{pmatrix} 1 & & 1 \\ & \ddots & \\ 1 & & 1 \end{pmatrix}$.

9.8.5 Par développement par rapport à la 1ère ligne, on a :

$$\begin{vmatrix} A_{11} & 0 & \cdots & 0 & A_{1n} \\ A_{21} & 1 & \ddots & & A_{2n} \\ \vdots & & \ddots & 0 & \vdots \\ A_{n-11} & & 0 & 1 & A_{n-1n} \\ A_{n1} & 0 & \cdots & 0 & A_{nn} \end{vmatrix}$$

$$= A_{11}\begin{vmatrix} 1 & & & A_{2n} \\ & \ddots & 0 & \vdots \\ & 0 & 1 & A_{n-1n} \\ 0 & \cdots & 0 & A_{nn} \end{vmatrix} + (-1)^{n+1}A_{1n}\begin{vmatrix} A_{21} & 1 & & \\ \vdots & & \ddots & \\ A_{n-11} & & 0 & 1 \\ A_{n1} & 0 & \cdots & 0 \end{vmatrix}$$

$$= A_{11}A_{nn} + (-1)^{n+1}A_{1n}(-1)^{n}A_{n1} = A_{11}A_{nn} - A_{1n}A_{n1}.$$

D'autre part :

$$\det\left(\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}\begin{pmatrix} A_{11} & & & A_{1n} \\ \vdots & 1 & \ddots & \vdots \\ & & 0 & \\ A_{n1} & 0 & 1 & A_{nn} \end{pmatrix}\right)$$

$$= \begin{vmatrix} \sum_{i=1}^{n} a_{1i}A_{i1} & a_{12} & \cdots & a_{1n-1} & \sum_{i=1}^{n} a_{1i}A_{in} \\ \vdots & \vdots & & \vdots & \vdots \\ \sum_{i=1}^{n} a_{ni}A_{i1} & a_{n2} & \cdots & a_{nn-1} & \sum_{i=1}^{n} a_{ni}A_{in} \end{vmatrix} = \begin{vmatrix} \det A & a_{12} & \cdots & a_{1n-1} & 0 \\ 0 & a_{22} & \cdots & a_{2n-1} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & a_{n-12} & \cdots & a_{n-1n-1} & 0 \\ 0 & a_{n2} & \cdots & a_{nn-1} & \det(A) \end{vmatrix}$$

$$= \det(A)\det(B)\det(A).$$

On obtient ainsi : $\det(A) \cdot (A_{11}A_{nn} - A_{1n}A_{n1}) = \big(\det(A)\big)^2\det(B)$.

- Si $\det(A) \neq 0$, on déduit $\begin{vmatrix} A_{11} & A_{1n} \\ A_{n1} & A_{nn} \end{vmatrix} = \det(A)\det(B)$.
- Si $\det(A) = 0$, alors $\operatorname{rg}\big(\operatorname{com}(A)\big) \leqslant 1$ (cf. exercice 9.8.1 p. 232), et donc $\begin{vmatrix} A_{11} & A_{1n} \\ A_{n1} & A_{nn} \end{vmatrix} = 0$.

9.9.1 *a)* Par exemple, en tirant z de la 1ère équation et en reportant, le système équivaut à :

$$\begin{cases} z = 2x + 3y + 1 \\ 7x + 11y + 1 = 0 \end{cases}.$$

◇ **Réponse :** $\left\{\left(x, -\dfrac{7x+1}{11}, \dfrac{x+8}{11}\right) ; x \in \mathbb{C}\right\}$.

b) En tirant z de la 2ème équation, le système se ramène à :

$$\begin{cases} z = -mx - y + 1 \\ (m-1)\big((2m+1)x + 2(m-1)y - 2(m-1)\big) = 0. \\ (1-m)x + (m-1)y - 3m - 2 = 0 \end{cases}$$

Si $m \neq 1$, tirer $y = \dfrac{(-2m-1)x+2}{2}$ et reporter dans la 3ème équation.

◇ **Réponse :**
$$\begin{cases} \left\{\left(-\dfrac{2}{m-1}, \dfrac{3m}{m-1}, -\dfrac{1}{m-1}\right)\right\} & \text{si } m \neq -\dfrac{3}{2} \text{ et } m \neq 1 \\ \left\{\left(x, x+1, \dfrac{x}{2}\right) ; x \in \mathbb{C}\right\} & \text{si } m = -\dfrac{3}{2} \\ \varnothing & \text{si } m = 1. \end{cases}$$

c) Par différence entre les 1ère et 3ème équations, déduire : $m(x+2y+z) = 0$.

Si $m \neq 0$, le système se ramène à : $\begin{cases} z = -x-2y \\ (2m+5)x + (m+3)y = m-1 \\ x + y = -m-1. \end{cases}$

Tirer y et reporter.

◇ **Réponse :**
$$\begin{cases} \left\{\left(\dfrac{m^2+5m+2}{m+2}, -\dfrac{2m^2+8m+4}{m+2}, \dfrac{3m^2+11m+6}{m+2}\right)\right\} & \text{si } m \neq 0 \text{ et } m \neq -2 \\ \varnothing & \text{si } m = -2 \\ \left\{\left(x, -x-1, \dfrac{7x+8}{5}\right) ; x \in \mathbb{C}\right\} & \text{si } m = 0. \end{cases}$$

d) ◇ **Réponse :**
$$\begin{cases} \left\{\left(m, 1, \dfrac{1}{m}\right)\right\} & \text{si } m \notin \{-1, 0, 1, -\mathrm{i}, \mathrm{i}\} \\ \{(-1, y, -y) ; y \in \mathbb{C}\} & \text{si } m = -1 \\ \varnothing & \text{si } m = 0 \\ \{(1, y, y) ; y \in \mathbb{C}\} & \text{si } m = 1 \\ \{(x, -\mathrm{i}x, -\mathrm{i}) ; x \in \mathbb{C}\} & \text{si } m = \mathrm{i} \\ \{(x, \mathrm{i}x, \mathrm{i}) ; x \in \mathbb{C}\} & \text{si } m = -\mathrm{i}. \end{cases}$$

e) ◇ **Réponse :**
$$\begin{cases} \varnothing & \text{si } a + b \neq 3 \\ \{(2-a, y, y+5-3a) ; y \in \mathbb{C}\} & \text{si } a + b = 3. \end{cases}$$

f) Par soustraction d'équations, le système se ramène à : $\begin{cases} ax + (b-1)y + 2z = 1 \\ (b-2)y + z = 0 \\ bz = 2b-4 \end{cases}$.

◇ **Réponse :**
$$\begin{cases} \left\{\left(-\dfrac{b-6}{ab}, -\dfrac{2}{b}, \dfrac{2b-4}{b}\right)\right\} & \text{si } b \neq 0, b \neq 2, a \neq 0 \\ \{(x, 1-ax, 0) ; x \in \mathbb{C}\} & \text{si } b = 2 \\ \left\{\left(x, -\dfrac{1}{3}, \dfrac{4}{3}\right) ; x \in \mathbb{C}\right\} & \text{si } a = 0, b = 6 \\ \varnothing & \text{sinon.} \end{cases}$$

g) Le système formé par les 3 premières équations admet une solution et une seule, $(2, 2a-2, 2a)$. Reporter dans la 4ème.

◇ **Réponse :**
$$\begin{cases} \varnothing & \text{si } a \neq b \\ \{(2, 2a-2, 2a)\} & \text{si } a = b. \end{cases}$$

9.9.2 Les trois plans considérés contiennent une même droite vectorielle si et seulement si le système linéaire $\begin{cases} (1-m)x - 2y + z = 0 \\ 3x - (1+m)y - 2z = 0 \\ 3x - 2y - (1+m)z = 0 \end{cases}$ admet au moins une solution autre que $(0,0,0)$, ce qui (cf. 9.9.2 *4)* Prop. p. 337) équivaut à : $\begin{vmatrix} 1-m & -2 & 1 \\ 3 & -1-m & -2 \\ 3 & -2 & -1-m \end{vmatrix} = 0.$

◇ **Réponse :** $m \in \{-2, 0, 1\}$.

9.9.3 *a)* $\begin{cases} 3x+4y+z+2t=3 \\ 2(3x+4y+z)+6t=7 \\ 3(3x+4y+z)+10t=0 \end{cases} \iff \begin{cases} 3x+4y+z=2 \\ 2t=1 \\ 11=0 \end{cases}$.

◇ **Réponse :** $\varnothing$.

b) ◇ **Réponse :**
$$\begin{cases} \left\{\left(x, y, \dfrac{-7x+6y+2}{5}, \dfrac{-3x-y+3}{5}\right);\ (x,y)\in\mathbb{C}^2\right\} & \text{si } m=5 \\ \varnothing & \text{si } m\neq 5 \end{cases}$$

c) ◇ **Réponse :**
$$\begin{cases} \left\{\left(x, x+1, x+\dfrac{m}{m-1}, -(m+2)x-\dfrac{m}{m-1}\right);\ x\in\mathbb{C}\right\} & \text{si } m\neq 1 \\ \varnothing & \text{si } m=1. \end{cases}$$

d) Par addition des quatre premières équations : $x+y+z+t=2$. Ainsi, le système formé par les quatre premières équations admet une solution et une seule : $x=1, y=-1, z=0, t=2$.

◇ **Réponse :**
$$\begin{cases} \{1,-1,0,2)\} & \text{si } a=b=-1 \\ \varnothing & \text{sinon.} \end{cases}$$

e) Par addition, on déduit : $(a+3)(x+y+z+t)=1+b+b^2+b^3$.

◇ **Réponse :**
$$\begin{cases} \left\{\left(\dfrac{1}{a-1}(1-c), \dfrac{1}{a-1}(b-c), \dfrac{1}{a-1}(b^2-c), \dfrac{1}{a-1}(b^3-c)\right)\right\} & \text{si } a\neq 1 \text{ et } a\neq 3, \text{ en notant } c=\dfrac{1+b+b^2+b^3}{a+3} \\ \{(x,y,z,1-x-y-z);\ (x,y,z)\in\mathbb{C}^3\} & \text{si } a=b=1 \\ \left\{\left(x, x+\dfrac{1-b}{4}, x+\dfrac{1-b^2}{4}, x+\dfrac{1-b^3}{4}\right);\ x\in\mathbb{C}\right\} & \text{si } a=-3 \text{ et } 1+b+b^2+b^3=0 \\ \varnothing & \text{sinon.} \end{cases}$$

9.9.4 Déduire successivement $x_2, x_3, \ldots, x_n$ en fonction de x_1, et reporter dans la dernière équation; séparer en cas suivant la parité de n.

◇ **Réponse :**

1) Si n est pair, $n=2p$ $(p\in\mathbb{N}^*)$:

- $\mathcal{S}=\varnothing$ si $a_{2p}-a_{2p-1}+\ldots+a_2-a_1\neq 0$
- $\mathcal{S}=\{(x_1, 2a_1-x_1, 2a_2-2a_1+x_1, \ldots, 2a_{2p-1}-2a_{2p-2}+\ldots+2a_1-x_1;\ x_1\in\mathbb{C}\}$ si $a_{2p}-a_{2p-1}+\ldots+a_2-a_1=0$

2) Si n est impair, $n=2p+1$ $(p\in\mathbb{N}^*)$: $\mathcal{S}=\{(x_1,x_2,\ldots,x_{2p+1})\}$ où :
$$x_1=a_{2p+1}-a_{2p}+\ldots-a_2+a_1,$$
$$x_{2k+1}=a_{2p+1}-a_{2p}+\ldots-a_{2k+2}+a_{2k+1}+a_{2k}-a_{2k-1}+\ldots-a_1,\ k\in\{1,\ldots,p\}$$
$$x_{2k}=-a_{2p+1}+a_{2p}-\ldots+a_{2k}+a_{2k-1}-a_{2k-2}+\ldots-a_2+a_1,\ k\in\{1,\ldots,p\}.$$

Par exemple, pour $p=2$ $(n=5)$, on a :
$$\begin{cases} x_1=a_5-a_4+a_3-a_2+a_1 \\ x_2=-a_5+a_4-a_3+a_2+a_1 \\ x_3=a_5-a_4+a_3+a_2-a_1 \\ x_4=-a_5+a_4+a_3-a_2+a_1 \\ x_5=a_5+a_4-a_3+a_2-a_1 \end{cases}.$$

Indications et réponses
pour les exercices du chapitre 10

10.1.1 En développant à l'aide du produit scalaire, tous les termes se simplifient.

Variante

Notons $u = b - a$, $v = c - a$, $w = d - a$. En utilisant l'égalité du parallélogramme :

$$2\big(||u||^2 + ||v-u||^2 + ||w-v||^2 + ||w||^2\big) = 2\big(||u||^2 + ||w-v||^2\big) + 2\big(||v-u||^2 + ||w||^2\big)$$
$$= ||u+w-v||^2 + ||u-w+v||^2 + ||v-u+w||^2 + ||v-u-w||^2$$

et $2\big(||v||^2 + ||w-u||^2 + ||v-w-u||^2\big) = ||v+w-u||^2 + ||v-w+u||^2 + 2||v-w-u||^2$,

d'où l'égalité demandée.

10.1.2 Soit $X \in \mathbf{M}_{n,1}(\mathbb{R})$ tel que $(I_n + A)X = 0$, c'est-à-dire $AX = -X$. En transposant, et puisque A est antisymétrique, on obtient ${}^tXA = X$. D'où : $\begin{cases} {}^tXAX = {}^tX(AX) = -{}^tXX \\ {}^tXAX = ({}^tXA)X = {}^tXX \end{cases}$,

donc ${}^tXX = 0$, et enfin $X = 0$.

10.1.3 En utilisant l'inégalité triangulaire dans E, puis l'inégalité de Cauchy-Schwarz dans $\mathbb{R}^n$ usuel appliquée à $(1,\dots,1)$ et $(||x_1||,\dots,||x_n||)$, on obtient :

$$\left\|\sum_{k=1}^{n} x_k\right\|^2 \leqslant \left(\sum_{k=1}^{n} ||x_k||\right)^2 \leqslant \left(\sum_{k=1}^{n} 1^2\right)\left(\sum_{k=1}^{n} ||x_k||^2\right) = n\sum_{k=1}^{n} ||x_k||^2.$$

10.1.4 D'après l'égalité du parallélogramme :

$2\big(||x-y||^2 + ||y-z||^2\big) = ||x-z||^2 + ||x-2y+z||^2 \geqslant ||x-z||^2$.

Remarque : l'inégalité est plus généralement vraie dans un evn car

$$||x-z||^2 \leqslant ||x-y||^2 + ||y-z||^2 + 2||x-y||\,||y-z|| \leqslant \big(2||x-y||^2 + ||y-z||^2\big),$$

vu que : $\forall (\alpha,\beta) \in (\mathbb{R}_+^2),\ 2\alpha\beta \leqslant \alpha^2 + \beta^2$.

10.1.5 D'après l'inégalité de Cauchy-Schwarz, appliquée à $(1,1,1,1)$ et $(1-x, x-y, y-z, z)$ dans $\mathbb{R}^4$ usuel :

$$1^2 = \big((1-x) + (x-y) + (y-z) + z\big)^2 \leqslant 4\big((1-x)^2 + (x-y)^2 + (y-z)^2 + z^2\big).$$

D'après 10.1.2 Prop. 1 p. 342, il y a égalité si et seulement si $(1-x, x-y, y-z, z)$ est colinéaire à $(1,1,1,1)$, c'est-à-dire : $1 - x = x - y = y - z = z$.

◇ **Réponse :** $\left\{\left(\frac{3}{4}, \frac{1}{2}, \frac{1}{4}\right)\right\}$.

10.1.6 L'inégalité demandée résulte de l'inégalité de Cauchy-Schwarz dans $\mathbb{R}^n$ usuel, appliquée à $u = (\sqrt{x_1}, \ldots, \sqrt{x_n})$ et $v = \left(\frac{1}{\sqrt{x_1}}, \ldots, \frac{1}{\sqrt{x_n}}\right)$.

D'après 10.1.2 Prop. 1 p. 342, il y a égalité si et seulement si (u, v) est lié.

◇ **Réponse :** Il y a égalité si et seulement si : $x_1 = \ldots = x_n = \frac{1}{n}$.

10.1.7 Supposons $\sum_{i \neq j} a_i b_j = 0$, donc $\left(\sum_i a_i\right)\left(\sum_i b_i\right) = \sum_i a_i b_i$.

Comme les a_i sont > 0, on déduit : $\sum_i b_i = \dfrac{\sum_i a_i b_i}{\sum_i a_i}$.

D'après l'inégalité de Cauchy-Schwarz : $\left(\sum_i a_i b_i\right)^2 \leqslant \left(\sum_i a_i^2\right)\left(\sum_i b_i^2\right)$,

et comme les a_i sont > 0 : $\sum_i a_i^2 \leqslant \left(\sum_i a_i\right)^2$.

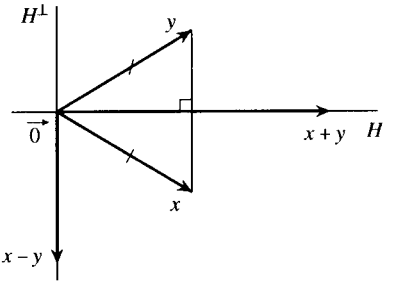
On déduit :
$$\sum_{i \neq j} b_i b_j = \left(\sum_i b_i\right)^2 - \sum_i b_i^2 = \left(\frac{\sum_i a_i b_i}{\sum_i a_i}\right)^2 - \sum_i b_i^2$$
$$= \frac{1}{\left(\sum_i a_i\right)^2}\left(\left(\sum_i a_i b_i\right)^2 - \left(\sum_i a_i\right)^2 \left(\sum_i b_i^2\right)\right) \leqslant 0.$$

10.2.1 L'étude du cas $x = y$ est immédiate.

a) Notons $H = (x - y)^\perp$.

Comme $< x + y, x - y > = ||x||^2 - ||y||^2 = 0$, on a : $x + y \in H$.

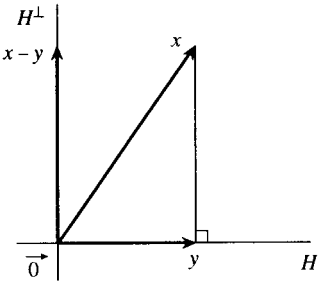
Puisque $\begin{cases} y + x \in H \\ y - x \in H^\perp \end{cases}$, on déduit $y = s_H(x)$.



b) Notons $H = (x - y)^\perp$.

Comme $< x - y, y > = < x, y > - ||y||^2 = 0$, on a : $y \in H$.

Puisque $\begin{cases} y \in H \\ y - x \in H^\perp \end{cases}$, on déduit $y = p_H(x)$.



10.3.1 En notant $A = (a_{ij})_{ij}$, on a, pour tout j de $\{1,\dots,n\}$: $C_j\,{}^tC_j = (a_{ij}a_{kj})_{i,k}$,

d'où : $\displaystyle\sum_{j=1}^{n} C_j\,{}^tC_j = \left(\sum_{j=1}^{n} a_{ij}a_{kj}\right)_{i,k} = A\,{}^tA.$

10.3.2 • $\displaystyle{}^tS = \mathrm{I}_n - \frac{2}{{}^tCC}\,{}^t(C\,{}^tC) = I_n - \frac{2}{{}^tCC}\,C\,{}^tC = S$

• $\displaystyle{}^tSS = S^2 = I_n - \frac{4}{{}^tCC}\,C\,{}^tC + \frac{4}{({}^tCC)^2}\,C\,{}^tCC\,{}^tC = I_n - \frac{4}{{}^tCC}\,C\,{}^tC + \frac{4}{({}^tCC)^2}({}^tCC)C\,{}^tC = S$

• $\displaystyle SC = C - \frac{2}{{}^tCC}\,C\,{}^tCC = C - 2C = -C$

• $\forall X \in C^{\perp},\ \displaystyle SX = X - \frac{2}{{}^tCC}C\,{}^tCX = X.$

10.3.3 En notant $\displaystyle U = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \in \mathbf{M}_{n,1}(\mathbb{R})$, on a : $\displaystyle AU = \begin{pmatrix} \sum_{j=1}^{n} a_{1j} \\ \vdots \\ \sum_{j=1}^{n} a_{nj} \end{pmatrix}$.

D'après l'inégalité de Cauchy-Schwarz dans $\mathbf{M}_{n,1}(\mathbb{R})$ muni du produit scalaire canonique :

$|< AU,U >| \leqslant ||AU||\,||U||$, et $||AU|| = ||U||$ car $A \in \mathbf{O}_n(\mathbb{R})$, donc

$$\left|\sum_{1\leqslant i,j\leqslant n} a_{ij}\right| = \left|\sum_{i=1}^{n}\left(\sum_{j=1}^{n} a_{ij}\right)\right| \leqslant ||U||^2 = n.$$

Etude du cas d'égalité

D'après 10.1.2 Prop. 1 p. 342, il y a égalité si et seulement si (AU,U) est lié.

◇ **Réponse :** Il y a égalité si et seulement si $AU = U$ ou $AU = -U$, où $\displaystyle U = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$.

10.3.4 Si $(V_1,\dots,V_n)$ est lié, l'inégalité est évidente.

Supposons $(V_1,\dots,V_n)$ libre.

D'après le procédé d'orthogonalisation de Schmidt, il existe $W_1,\dots,W_n \in E$ tels que :

$$\begin{cases} (W_1,\dots,W_n) & \text{est une famille orthogonale} \\ \forall i \in \{1,\dots,n\}, & W_i \neq 0 \\ \forall i \in \{2,\dots,n\}, & W_i \in \mathrm{Vect}(V_i,W_1,\dots,W_{i-1}). \end{cases}$$

Notons, pour $i \in \{1,\dots,n\}$, $\displaystyle e_i = \frac{W_i}{||W_i||}$.

D'après 9.2.2 Cor. p. 306 (relation de Chasles pour les déterminants) :

$$|\det_{\mathcal{B}}(V_1,\dots,V_n)| = |\det_{\mathcal{B}}(e_1,\dots,e_n)|\,|\det_{(e_1,\dots,e_n)}(W_1,\dots,W_n)|\,|\det_{(W_1,\dots,W_n)}(V_1,\dots,V_n)|.$$

• $|\det_{\mathcal{B}}(e_1,\dots,e_n)| = 1$, puisque $\mathcal{B}$ et $(e_1,\dots,e_n)$ sont des b.o.n. de E (cf. 10.3.2 Prop. 3 et 4 p. 359)

• $\displaystyle|\det_{(e_1,\dots,e_n)}(W_1,\dots,W_n)| = \prod_{i=1}^{n} ||W_i||$, d'après la définition des e_i.

• $\det_{(W_1,\dots,W_n)}(V_1,\dots,V_n) = 1$, car la matrice de passage de $(V_1,\dots,V_n)$ à $(W_1,\dots,W_n)$ est triangulaire supérieure à termes diagonaux égaux à 1.

On obtient : $|\det_{\mathcal{B}}(V_1,\dots,V_n)| = \prod_{i=1}^{n} ||W_i||$.

Enfin, comme $W_i = V_i + U_i$, où $U_i \in \text{Vect}(V_1,\dots,V_{i-1}) = \text{Vect}(W_1,\dots,W_{i-1})$ donc $U_i \perp W_i$, on a, d'après le théorème de Pythagore : $||V_i||^2 = ||W_i||^2 + ||U_i||^2 \geqslant ||W_i||^2$.

On conclut : $|\det_{\mathcal{B}}(V_1,\dots,V_n)| \leqslant \prod_{i=1}^{n} ||V_i||$.

b) Etude du cas d'égalité, lorsque $(V_1,\dots,V_n)$ est libre.

Supposons qu'il y ait égalité : $|\det_{\mathcal{B}}(V_1,\dots,V_n)| = \prod_{i=1}^{n} ||V_i||$.

Comme $\begin{cases} \prod_{i=1}^{n} ||W_i|| = \prod_{i=1}^{n} ||V_i|| \\ \forall i \in \{1,\dots,n\},\ 0 < ||W_i|| \leqslant ||V_i|| \end{cases}$, on déduit : $\forall i \in \{1,\dots,n\},\ ||W_i|| = ||V_i||$,

puis, avec les notations précédentes : $\forall i \in \{1,\dots,n\},\ U_i = 0$, c'est-à-dire : $\forall i \in \{1,\dots,n\},\ W_i = V_i$.

Il en résulte que $(V_1,\dots,V_n)$ est une famille orthogonale.

◇ **Réponse :** Il y a égalité si et seulement si : $\left|\begin{array}{l} (V_1,\dots,V_n) \text{ est orthogonale} \\ \text{ou} \\ (\exists i \in \{1,\dots,n\},\ V_i = 0) \end{array}\right.$.

10.3.5 • Puisque f est bijectif, $\dim(f(F)) = \dim(F)$. De l'inclusion $f(F) \subset F$, on déduit alors l'égalité $f(F) = F$. De plus : $f^{-1}(F) = f^{-1}\big(f(F)\big) = F$.

• Soit $y \in f(F^\perp)$; il existe $x \in F^\perp$ tel que $y = f(x)$.

On a, pour tout z de F : $< y,z > = < f(x),z > = < x,f^{-1}(z) > = 0$, puisque $f^{-1}(z) \in F$.

D'où $y \in F^\perp$, et ainsi $f(F^\perp) \subset F^\perp$.

• Comme au début, on obtient $f(F^\perp) = F^\perp$.

Les propriétés $f|_F \in \mathcal{O}(F)$ et $f|_{F^\perp} \in \mathcal{O}(F^\perp)$ sont ensuite immédiates.

10.3.6 • Il est clair que f est linéaire.

• Soit $x \in E$. Comme $u\big(p_F(x)\big) \in F$ et $v\big(p_{F^\perp}(x)\big) \in F^\perp$, on a :

$$||f(x)||^2 = \big\|u\big(p_F(x)\big)\big\|^2 + \big\|v\big(p_{F^\perp}(x)\big)\big\|^2 = ||p_F(x)||^2 + ||p_{F^\perp}(x)||^2 = ||x||^2.$$

Ceci montre : $f \in \mathcal{O}(E)$.

10.3.7 Récurrence sur n.

Si $n = 1$, alors f est l'identité ou la réflexion $-\text{Id}_E$.

Supposons la propriété vraie pour tout ev euclidien de dimension n, et soient E un ev euclidien de dimension $n+1$ et $f \in \mathcal{O}(E)$.

L'ev euclidien E admet au moins une b.o.n $(e_1,\dots,e_{n+1})$. D'après l'ex 10.2.1 *a)* p. 355, il existe une réflexion s de E telle que $s\big(f(e_{n+1})\big) = e_{n+1}$.

Puisque l'endomorphisme orthogonal $s \circ f$ laisse stable la droite vectorielle $\mathbb{R}e_{n+1}$, d'après l'ex. 10.3.5, $s \circ f$ laisse aussi stable $(\mathbb{R}e_{n+1})^\perp$, c'est-à-dire $\text{Vect}(e_1,\dots,e_n)$.

Notons $F = \text{Vect}(e_1,\ldots,e_n)$ et f' l'endomorphisme induit par $s \circ f$ sur F. Comme $f' \in \mathcal{O}(F)$ (cf. ex. 10.3.5 p. 361), d'après l'hypothèse de récurrence, il existe $s'_2,\ldots,s'_{n+1}$ (réflexions ou identité de F) telles que $f' = s'_2 \circ \ldots \circ s'_{n+1}$. En notant, pour $2 \leqslant i \leqslant n+1$, s_i l'endomorphisme orthogonal obtenu par recollement de s'_i sur F et de l'identité sur $\mathbb{R}e_{n+1}$ (cf. ex. 10.3.6 p. 361), il est clair que $s_2,\ldots,s_{n+1}$ sont des réflexions ou l'identité, et que $s \circ f = s_2 \circ \ldots \circ s_{n+1}$, d'où $f = s \circ s_2 \circ \ldots \circ s_{n+1}$.

On pourra comparer cette solution avec la preuve de 3.4.2 Th. 1 p. 85 relative à la décomposition d'une permutation en un produit de transpositions.

10.4.1 ◇ **Réponse :** $R_\theta R_{\theta'} = R_{\theta+\theta'}$, $R_\theta S_\varphi = S_{\theta+\varphi}$, $S_\varphi R_\theta = S_{\varphi-\theta}$, $S_\varphi S_{\varphi'} = R_{\varphi-\varphi'}$.

10.4.2 *1ère méthode*

Puisque $r \circ s$ est un endomorphisme orthogonal indirect de E_2, c'est une réflexion, donc $(r \circ s)^2 = e$ (où $e = \text{Id}_E$), c'est-à-dire $r \circ s \circ r \circ s = e$, d'où $s \circ r \circ s = r^{-1}$ et $r \circ s \circ r = s^{-1} = s$.

2ème méthode

En utilisant les résultats de l'exercice 10.4.1 :

$S_\varphi R_\theta S_\varphi = S_{\varphi-\theta} S_\varphi = R_{-\theta} = R_\theta^{-1}$ et $R_\theta S_\varphi R_\theta = S_{\theta+\varphi} R_\theta = S_\varphi$.

◇ **Réponse :** $s \circ r \circ s = r^{-1}$, $r \circ s \circ r = s$.

10.4.3 Utiliser $u \bullet v = ||u||\,||v|| \cos(\widehat{u,v})$ et $\det_{(i,j)}(u,v) = \begin{vmatrix} -2 & 1 \\ 1 & 3 \end{vmatrix} = -7 < 0$.

◇ **Réponse :** $-\text{Arccos}\left(\dfrac{\sqrt{2}}{10}\right)\ [2\pi]$.

10.4.4 *a)* • Si $b^2 - ac < 0$: $ax^2 + 2bxy + cy^2 = 0 \iff x = y = 0$

• Si $b^2 - ac \geqslant 0$ et $c \neq 0$, le trinôme réel $a + 2b\text{X} + c\text{X}^2$ admet deux zéros réels (éventuellement confondus) m,m' et : $ax^2 + 2bxy + cy^2 = 0 \iff (y = mx \text{ ou } y = m'x)$.

• Si $c = 0$: $ax^2 + 2bxy + cy^2 = 0 \iff (x = 0 \text{ ou } ax + 2by = 0)$.

◇ **Réponse :** $b^2 - ac \geqslant 0$.

b) Supposons $b^2 - ac \geqslant 0$ et $c \neq 0$.

Soient $V\begin{pmatrix} 1 \\ m \end{pmatrix}$, $V'\begin{pmatrix} 1 \\ m' \end{pmatrix}$ des vecteurs directeurs de D, D' respectivement, où m,m' sont les zéros réels de $a + 2b\text{X} + c\text{X}^2$. On a :

$$\cos(\widehat{V,V'}) = \frac{V \cdot V'}{||V|| \cdot ||V'||} = \frac{1 + mm'}{\sqrt{(1+m^2)(1+m'^2)}}.$$

Comme $m + m' = -\dfrac{2b}{c}$ et $mm' = \dfrac{a}{c}$, on obtient :

$$\cos(\widehat{V,V'}) = \frac{a+c}{\sqrt{(a-c)^2 + 4b^2}}.$$

Si $c = 0$, alors on prend $V\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $V'\begin{pmatrix} -2b \\ a \end{pmatrix}$, d'où $\cos(\widehat{V,V'}) = \dfrac{a}{\sqrt{a^2 + 4b^2}}$.

◇ **Réponse :** $|(\widehat{D,D'})| = \text{Arccos}\dfrac{|a+c|}{\sqrt{(a-c)^2 + 4b^2}}$.

c) La gerbe quadratique des bissectrices de D et D', qui est la réunion des deux bissectrices de D, D', est l'ensemble des $W\begin{pmatrix} x \\ y \end{pmatrix}$ de E_2 tels que $d(W,D) = d(W,D')$.

• Supposons $c \neq 0$. Comme $d(W,D) = \dfrac{|y - mx|}{\sqrt{1+m^2}}$ et $d(W,D') = \dfrac{|y - m'x|}{\sqrt{1+m'^2}}$, on a :

$d(W,D) = d(W,D') \iff (1+m'^2)(y-mx)^2 - (1+m^2)(y-m'x)^2 = 0$

$\iff (m+m')x^2 - 2(1-mm')xy - (m+m')y^2 = 0$ si $m \neq m'$

$\iff -\dfrac{2b}{c}x^2 - 2\left(1 - \dfrac{a}{c}\right)xy + \dfrac{2b}{c}y^2 = 0.$

• Examiner le cas $c = 0$.

◇ **Réponse :** $bx^2 + (c-a)xy - by^2 = 0$.

10.5.1 *a)* ◇ **Réponse :** f est la rotation d'axe dirigé et orienté par $7i + 7j - 3k$ et d'angle $\text{Arccos}\left(-\dfrac{53}{54}\right)$ $[2\pi]$.

b) ◇ **Réponse :** f est le retournement autour de la droite vectorielle engendrée par $i + 2j - 2k$.

c) ◇ **Réponse :** f est la réflexion par rapport au plan d'équation $x - 2y - 2z = 0$.

d) ◇ **Réponse :** f est la composée commutative de la rotation d'axe dirigé et orienté par $i - 4k$ et d'angle $-\text{Arccos}\left(\dfrac{8}{9}\right)$ $[2\pi]$ et de la réflexion par rapport au plan d'équation $x - 4z = 0$.

e) En notant $u = ai + bj + ck$, remarquer : $\forall x \in E_3,\ f(x) = (u \cdot x)u + u \wedge x$.

◇ **Réponse :** f est la rotation d'axe dirigé et orienté par $ai + bj + ck$ et d'angle $\dfrac{\pi}{2}$ $[\pi]$.

10.5.2 Notons $u = \dfrac{1}{\sqrt{3}}(i + j + k)$, $v = \dfrac{1}{\sqrt{2}}(i - j)$ qui est normé et orthogonal à u, $w = u \wedge v = \dfrac{1}{\sqrt{6}}(i + j - 2k)$, $\mathcal{B}' = (u,v,w)$ qui est une b.o.n.d, $\Omega_1 = \text{Mat}_{\mathcal{B}'}(f) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$,

$P = \text{Pass}(\mathcal{B},\mathcal{B}') = \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & 0 & -\frac{2}{\sqrt{6}} \end{pmatrix}$.

Calculer alors : $\Omega = P\Omega_1 P^{-1} = P\Omega_1\,{}^tP$

◇ **Réponse :** $\Omega = \dfrac{1}{3}\begin{pmatrix} 2 & -1 & 2 \\ 2 & 2 & -1 \\ -1 & 2 & 2 \end{pmatrix}$.

10.5.3 Notons $\overrightarrow{\Delta}$ l'axe de f, u le vecteur normé dirigeant et orientant $\overrightarrow{\Delta}$, θ l'angle de f, et $\overrightarrow{\Delta'}, u', \theta'$ de même pour g.

1) Supposons $f \circ g = g \circ f$.

On a : $f\big(g(u)\big) = g\big(f(u)\big) = g(u)$.

Comme f est une rotation autre que Id_{E_3}, on déduit $g(u) \in \mathbb{R}u$.

De plus, $||g(u)|| = ||u||$, donc $g(u) = u$ ou $g(u) = -u$.

De même : $f(u') = u'$ ou $f(u') = -u'$.

1er cas : $g(u) = u$ ou $f(u') = u'$.

Alors $u' = u$ ou $u' = -u$, donc f et g ont le même (support d') axe.

2ème cas : $g(u) = -u$ et $f(u') = -u'$.

Alors : $u \cdot u' = f(u) \cdot f(u') = u \cdot (-u')$, donc $u \perp u'$. En notant $w = u \wedge u'$, $\mathcal{B}' = (u, u', w)$ est donc une b.o.n.d. de E_3. La matrice de f dans $\mathcal{B}'$ est de la forme : $\begin{pmatrix} 1 & 0 & \alpha \\ 0 & -1 & \beta \\ 0 & 0 & \gamma \end{pmatrix}$, $(\alpha, \beta, \gamma) \in \mathbb{R}^3$.

Comme $f \in \mathcal{O}(E_3)$, on a $\gamma^2 = 1$, puis $\alpha = \beta = 0$, et enfin, comme $f \in \mathcal{SO}(E_3)$, $\gamma = -1$.

De même : $\mathrm{Mat}_{\mathcal{B}'}(g) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$.

Ainsi, f et g sont deux retournements par rapport à deux droites orthogonales.

2) Réciproque

α) Si $\overrightarrow{\Delta'} = \overrightarrow{\Delta}$, il est clair que : $f \circ g = g \circ f = \mathrm{Rot}_{\overrightarrow{\Delta}, \theta+\theta'}$.

β) Si f et g sont deux retournements tels que $\Delta \perp \Delta'$, alors, dans la b.o.n.d. $(u, u', u \wedge u')$, les matrices de f et g sont $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ et $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$, qui commutent car elles sont toutes deux diagonales.

10.5.4 Soient f une rotation de E_3, $\overrightarrow{\Delta}$ l'axe de f, θ l'angle de f, I le vecteur normé dirigeant et orientant $\overrightarrow{\Delta}$, J un vecteur normé orthogonal à I (il en existe au moins un), $K = I \wedge J$. Alors $\mathcal{B} = (I, J, K)$ est une b.o.n.d. de E_3 et : $\Omega = \mathrm{Mat}_{\mathcal{B}}(f) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$.

Il est clair que $\Omega = \Omega_1 \Omega_2$, où : $\Omega_1 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$, $\Omega_2 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & -\sin\theta & -\cos\theta \end{pmatrix}$.

Comme Ω_1, Ω_2 sont orthogonales, symétriques, de déterminant 1, distinctes de I_3, on en déduit que Ω_1, Ω_2 sont les matrices dans $\mathcal{B}$ de deux retournements.

On peut remarquer ainsi que, pour toute droite D_1 orthogonale à Δ, il existe une droite D_2 unique telle que $f = \mathrm{Ret}_{D_1} \circ \mathrm{Ret}_{D_2}$, où Ret_{D_1} (resp. Ret_{D_2}) est le retournement autour de D_1 (resp. D_2).

10.5.5 Puisque : $\forall x \in E_3,\ a \wedge x \perp a$, si $a \cdot b \neq 0$, l'équation (1) $a \wedge x = b$ n'a pas de solution $x \in E_3$.

Supposons donc $a \cdot b = 0$.

Si ($a = 0$ et $b \neq 0$), (1) n'a pas de solution.

Si ($a \neq 0$ et $b = 0$), l'ensemble des solutions de (1) est $\mathbb{R}a$.

Supposons $a \neq 0$ et $b \neq 0$.

Alors $(a,b,a \wedge b)$ est une base de E_3 ; en notant (α,β,γ) les composantes de x dans cette base, on a :

$$a \wedge x = b \iff \beta a \wedge b + \gamma a \wedge (a \wedge b) = b \iff \beta a \wedge b - \gamma ||a||^2 b = b \iff \left(\beta = 0 \text{ et } \gamma = -\frac{1}{||a||^2}\right).$$

◇ **Réponse :**
$$\begin{cases} \varnothing & \text{si } a \cdot b \neq 0 \\ \left\{-\dfrac{1}{||a||^2} a \wedge b + \alpha a ;\ \alpha \in \mathbb{R}\right\} & \text{si } (a \cdot b = 0 \text{ et } a \neq 0) \\ \varnothing & \text{si } (a = 0 \text{ et } b \neq 0) \\ E_3 & \text{si } a = b = 0. \end{cases}$$

10.5.6 Raisonnons par l'absurde : supposons qu'il existe $c \in E_3$ tel que :

$$\forall x \in E_3,\ a \wedge (b \wedge x) = c \wedge x.$$

En particulier, en remplaçant x par b : $c \wedge b = 0$. Il existe donc $\alpha \in \mathbb{R}$ tel que $c = \alpha b$. Puis, en remplaçant x par a : $a \wedge (b \wedge a) = \alpha b \wedge a$. Mais $a \wedge (b \wedge a)$ est non nul et orthogonal à $b \wedge a$, d'où une contradiction.

10.5.7 Déduire : $a - x = a \wedge y = a \wedge (a - a \wedge c) = -a \wedge (a \wedge x) = -(a \cdot x)a + ||a||^2 x$, d'où : $(1 + ||a||^2)x = (1 + a \cdot x)a$.

Il existe donc $\lambda \in \mathbb{R}$ tel que $x = \lambda a$. Alors : $\begin{cases} a \wedge x + y = a \\ a \wedge y + x = a \end{cases} \iff \begin{cases} y = a \\ x = a \end{cases}$.

◇ **Réponse :** $\{(a,a)\}$.

10.5.8 $(a \wedge x) \wedge b = a \wedge (x \wedge b) \iff -(b \cdot x)a + (b \cdot a)x = (a \cdot b)x - (a \cdot x)b \iff a \cdot x = b \cdot x = 0$

◇ **Réponse :** $\mathbb{R}(a \wedge b)$.

10.5.9 $(S) \iff \begin{cases} a \wedge (x - y) = b \wedge (y - x) \\ a \wedge (x + y) = b \wedge (y + x) \end{cases} \implies \begin{cases} (a + b) \wedge (x - y) = 0 \\ (a - b) \wedge (x + y) = 0 \end{cases}$.

Il existe donc $(\alpha,\beta) \in \mathbb{R}^2$ tel que : $\begin{cases} x - y = 2\alpha(a + b) \\ x + y = 2\beta(a - b) \end{cases}$, d'où : $\begin{cases} x = (\alpha + \beta)a + (\alpha - \beta)b \\ y = (\beta - \alpha)a - (\alpha + \beta)b \end{cases}$.

Alors : $(S) \iff -(\alpha + \beta)^2 a \wedge b - (\alpha - \beta)^2 b \wedge a = a \wedge b \iff -(\alpha + \beta)^2 b + (\alpha - \beta)^2 = 1$.

◇ **Réponse :** $\left\{\left((\alpha + \beta)a + (\alpha - \beta)b,\ (\beta - \alpha)a - (\alpha + \beta)b\right);\ (\alpha,\beta) \in \mathbb{R}^2,\ -4\alpha\beta = 1\right\}$.

10.5.10 • $[x\wedge u, y\wedge v, z\wedge w] = (x\wedge u)\cdot\big((y\wedge v)\wedge(z\wedge w)\big)$
$= (x\wedge u)\cdot\big(\big((y\wedge v)\cdot w\big)z - \big((y\wedge v)\cdot z\big)w\big) = [x,u,z][y,v,w] - [x,u,w][y,v,z]$

• $[x\wedge v, y\wedge w, z\wedge u] = [y\wedge w, z\wedge u, x\wedge v] = (y\wedge w)\cdot\big((z\wedge u)\wedge(x\wedge v)\big)$
$= (y\wedge w)\cdot\big(\big((z\wedge u)\cdot v\big)x - \big((z\wedge u)\cdot x\big)v\big) = [y,w,x][z,u,v] - [y,w,v][z,u,x]$

• $[x\wedge w, y\wedge u, z\wedge v] = [z\wedge v, x\wedge w, y\wedge u] = (z\wedge v)\cdot\big((x\wedge w)\wedge(y\wedge u)\big)$
$= (z\wedge v)\cdot\big(\big((x\wedge w)\cdot u\big)y - \big((x\wedge w)\cdot y\big)u\big) = [z,v,y][x,w,u] - [z,v,u][x,w,y]$.

10.5.11 *a)* Les formules voulues sont immédiates.

b) Supposons $x\cdot y = 0$. On a alors : $f_a(x,y) = -(y\cdot x)a + (y\cdot a)x - (x\cdot y)a + (x\cdot a)y = (y\cdot a)x + (x\cdot a)y$.
Comme ($x\neq 0$, $y\neq 0$, $x\cdot y = 0$), (x,y) est libre, et donc :

$$f_a(x,y) = 0 \Longleftrightarrow x\cdot a = y\cdot a = 0 \Longleftrightarrow a\in\mathbb{R}(x\wedge y).$$

10.5.12 $f^2(x) = (x\wedge u)\wedge u = -x + (u\cdot x)u$, $f^3(x) = \big(-x + (u\cdot x)u\big)\wedge u = -x\wedge u = -f(x)$.

10.5.13 *1)* Cherchons d'abord une CNS pour que f soit un endomorphisme orthogonal.
D'abord, f est clairement linéaire.
On a, pour tout x de E_3 :

$$\begin{aligned}||f(x)||^2 &= \alpha^2||x||^2 + \beta^2(u\cdot x)^2 + \gamma^2||u\wedge x||^2 + 2\alpha\beta(u\cdot x)^2\\ &= (\alpha^2+\gamma^2)||x||^2 + (2\alpha\beta+\beta^2-\gamma^2)(u\cdot x)^2.\end{aligned}$$

Puis : $\forall x\in E_3,\ ||f(x)|| = ||x|| \Longleftrightarrow \forall x\in E_3,\ (\alpha^2+\gamma^2-1)||x||^2 + (2\alpha\beta+\beta^2-\gamma^2)(u\cdot x)^2 = 0$
$$\Longleftrightarrow \begin{cases}\alpha^2+\gamma^2-1=0\\ 2\alpha\beta+\beta^2-\gamma^2=0\end{cases} \Longleftrightarrow \begin{cases}\alpha^2+\gamma^2=1\\ \alpha+\beta\in\{-1,1\}\end{cases}.$$
On peut aussi remarquer $f(u) = (\alpha+\beta)u$ et, pour tout y normé et orthogonal à u, $||f(y)||^2 = \alpha^2+\gamma^2$.

2) Supposons cette dernière condition réalisée. En particulier, il existe $\theta\in\mathbb{R}$ tel que :

$$\alpha = \cos\theta \text{ et } \gamma = \sin\theta.$$

Il existe $v,w\in E_3$ tels que (u,v,w) soit une b.o.n.d. de E_3. On a : $\begin{cases} f(u) = \alpha u + \beta u = (\alpha+\beta)u\\ f(v) = \alpha v + \gamma u\wedge v = \alpha v + \gamma w\\ f(w) = \alpha w + \gamma u\wedge w = -\gamma v + \alpha w\end{cases}$.

Ainsi : $\mathrm{Mat}_{(u,v,w)}(f) = \begin{pmatrix}\alpha+\beta & 0 & 0\\ 0 & \cos\theta & -\sin\theta\\ 0 & \sin\theta & \cos\theta\end{pmatrix}$.

Il en résulte que f est une rotation si et seulement si $\alpha+\beta = 1$.

◇ **Réponse :** • $\alpha^2+\gamma^2 = 1$ et $\alpha+\beta = 1$.

• Dans ce cas, f est la rotation d'axe dirigé et orienté par u, d'angle θ défini par :
$$\begin{cases}\cos\theta = \alpha\\ \sin\theta = \gamma\end{cases}.$$

C 10.1 *I* *1)* • Cf. 10.1.1 Exemple 3) p. 340.

• $< PQ,R >= \int_{-1}^{1} (P(x)Q(x))R(x)\,dx = \int_{-1}^{1} P(x)(Q(x)R(x))\,dx =< P,QR >$.

2) **Existence**

Récurrence forte sur n.

Notons $P_0 = \dfrac{1}{\sqrt{2}}$; ainsi, P_0 est de degré 0, à coefficient dominant > 0, et $||P_0||^2 = \int_{-1}^{1} \left(\dfrac{1}{\sqrt{2}}\right)^2 dx = 1$.

Supposons définis $P_0,\dots,P_n$ convenant, c'est-à-dire tels que :

$$\begin{cases} \forall (k,l) \in \{0,\dots,n\}^2,\ < P_k,P_l >= \begin{cases} 1 & \text{si } k = l \\ 0 & \text{si } k \neq l \end{cases} \\ \text{Pour tout } k \text{ de } \{0,\dots,n\},\ P_k \text{ est de degré } k \text{ et à coefficient dominant } > 0. \end{cases}$$

Comme : $\forall k \in \{0,\dots,n\}$, $\deg(P_k) = k$, $(P_0,\dots,P_n)$ est une base de E_n (cf. 5.1.4 Rem. p. 146).

D'autre part, E_n est un sev de E_{n+1} et $\dim(E_{n+1}) = n+2 = \dim(E_n)+1$. Donc l'orthogonal de E_n dans E_{n+1} est une droite vectorielle. Il existe $V_{n+1} \in E_{n+1} - \{0\}$ tel que : $\forall P \in E_n,\ < P,V_{n+1} > = 0$.

Il est clair que $V_{n+1} \notin E_n$ (sinon : $||V_{n+1}||^2 = 0$), donc $\deg(V_{n+1}) = n+1$.

Quitte à remplacer éventuellement V_{n+1} par $-V_{n+1}$, on peut supposer que le coefficient dominant de V_{n+1} est > 0.

Il est alors clair que le polynôme P_{n+1} défini par $P_{n+1} = \dfrac{1}{||V_{n+1}||} V_{n+1}$ convient.

Remarque : On peut aussi construire $(P_n)_{n\in\mathbb{N}}$ par orthogonalisation (puis normalisation) de $(X^n)_{n\in\mathbb{N}}$ en utilisant le procédé de Schmidt (cf. 10.2.1 p. 348), adapté au cas d'une famille indexée par $\mathbb{N}$.

Unicité

Supposons que deux suites $(P_n)_{n\in\mathbb{N}}$, $(Q_n)_{n\in\mathbb{N}}$ conviennent.

Il est d'abord clair que : $P_0 = Q_0 = \dfrac{1}{\sqrt{2}}$.

Soit $n \in \mathbb{N}^*$. Notons p_n (resp. q_n) le coefficient dominant de P_n (resp. Q_n), et remarquons que $p_nQ_n - q_nP_n$ est de degré $\leqslant n-1$ (les termes de degré n s'éliminent).

D'autre part, P_n et Q_n sont orthogonaux à E_{n-1}, puisque $(P_0,\dots,P_{n-1})$ engendre E_{n-1} et $(Q_0,\dots,Q_{n-1})$ aussi. Donc $p_nQ_n - q_nP_n$ est orthogonal à E_{n-1}.

Il en résulte : $p_nQ_n - q_nP_n = 0$.

Comme $||P_n|| = ||Q_n|| = 1$ et que $p_n > 0$ et $q_n > 0$, on déduit $p_n = q_n$, $P_n = Q_n$.

3) Soit $n \in \mathbb{N}^*$. Puisque : $\forall k \in \{0,\dots,n-1\}$, $\deg(P_k) = k$, $(P_0,\dots,P_{n-1})$ est une base de E_{n-1}. Comme P_n est orthogonal à $P_0,\dots,P_{n-1}$, on obtient : $P_n \in E_{n-1}^{\perp}$. Cette propriété est d'ailleurs apparue dans solution ci-dessus de *2)*.

II *1) a)* Soit $n \in \mathbb{N}$. Puisque $(X^2-1)^n$ est pair, il est clair que sa dérivée $n^{\text{ème}}$ est paire si n est pair, impaire si n est impair.

b) Soit $n \in \mathbb{N}$. On a : $\deg(U_n) = \deg((X^2-1)^n) - n = 2n - n = n$.

De plus, le terme en X^n de U_n est $(X^{2n})^{(n)}$, c'est-à-dire $\dfrac{(2n)!}{n!}X^n$.

◇ **Réponse :** Le coefficient dominant de U_n est $\dfrac{(2n)!}{n!}$.

2) a) Pour $(p,q) \in \mathbb{N}^2$, notons $H_{p,q} = ((X^2-1)^p)^{(q)}$. Il est clair que :

$$\begin{cases} \forall p \in \mathbb{N},\quad H_{p,p} = U_p \\ \forall (p,q) \in \mathbb{N}^2,\quad H'_{p,q} = H_{p,q+1} \\ \forall (p,q) \in \mathbb{N}^2,\quad \big(p > q \Longrightarrow H_{p,q}(1) = H_{p,q}(-1) = 0\big). \end{cases}$$

Soit $(m,n) \in \mathbb{N}^2$ tel que $m \neq n$; on peut supposer, par exemple, $m > n$. Grâce à une intégration par parties :

$$< U_m, U_n > = \int_{-1}^{1} H_{m,m}(x) H_{n,n}(x)\, dx = \left[H_{m,m-1}(x) H_{n,n}(x)\right]_{-1}^{1} - \int_{-1}^{1} H_{m,m-1}(x) H_{n,n+1}(x)\, dx$$
$$= - < H_{m,m-1}, H_{n,n+1} > .$$

On obtient en réitirant (ou par récurrence) :

$$< U_m, U_n > = - < H_{m,m-1}, H_{n,n+1} > = < H_{m,m-2}, H_{n,n+2} > = \ldots = (-1)^m < H_{m,0}, H_{n,n+m} > .$$

Comme $n + m > 2n$, on a $H_{n,n+m} = 0$, et donc $< U_m, U_n > = 0$.

b) • Avec les mêmes notations qu'en *a)* : $||U_n||^2 = < U_n, U_n > = (-1)^n < H_{n,0}, H_{n,2n} >$.

Mais $H_{n,0} = (X^2 - 1)^n$ et $H_{n,2n} = ((X^2 - 1)^n)^{(2n)} = (2n)!$, d'où : $||U_n||^2 = (2n)! \int_{-1}^{1} (1 - x^2)^n\, dx$.

• Pour $(p,q) \in \mathbb{N}^2$, notons $I_{p,q} = \int_{-1}^{1} (1 - x)^p (1 + x)^q\, dx$, de sorte que : $||U_n||^2 = (2n)! I_{n,n}$.

Une intégration par parties fournit (pour $q \geqslant 1$) :

$$I_{p,q} = \left[-\frac{(1-x)^{p+1}}{p+1}(1+x)^q\right]_{-1}^{1} + \int_{-1}^{1} \frac{(1-x)^{p+1}}{p+1} q (1+x)^{q-1}\, dx = \frac{q}{p+1} I_{p+1,q-1},$$

d'où, par une récurrence immédiate : $I_{p,q} = \frac{q}{p+1} \frac{q-1}{p+2} \cdots \frac{1}{p+q} I_{p+q,0}$.

Et : $I_{p+q,0} = \int_{-1}^{1} (1 - x)^{p+q}\, dx = \frac{2^{p+q+1}}{p+q+1}$. D'où : $I_{p,q} = \frac{p!q!}{(p+q+1)!} 2^{p+q+1}$.

On déduit : $||U_n||^2 = \frac{(n!)^2}{2n+1} 2^{2n+1}$.

◇ **Réponse :** $\forall n \in \mathbb{N}, ||U_n|| = \sqrt{\frac{2}{2n+1}}\, 2^n n!$.

c) D'après ***II 2) a)*** et *b)*, la suite $\left(\frac{1}{2^n n!}\sqrt{\frac{2n+1}{2}} U_n\right)_{n \in \mathbb{N}}$ satisfait les conditions de ***I 2)***.

Par unicité de $(P_n)_{n \in \mathbb{N}}$, on déduit : $\forall n \in \mathbb{N}, P_n = \frac{1}{2^n n!}\sqrt{\frac{2n+1}{2}}\, U_n$.

d) Utiliser ***II 1) b)*** et ***II 2) c)***.

◇ **Réponse :** Le coefficient dominant de P_n est $\frac{(2n)!}{2^n (n!)^2}\sqrt{\frac{2n+1}{2}}$, ou encore : $\frac{C_{2n}^n}{2}\sqrt{\frac{2n+1}{2}}$.

3) Soit $n \in \mathbb{N}$. Il est clair que : $(X^2 - 1) M_n' = 2nX(X^2 - 1)^n = 2nXM_n$.

En prenant les dérivées $(n + 1)$èmes et en utilisant la formule de Leibniz, on obtient :

$$(X^2 - 1) M_n^{(n+2)} + C_{n+1}^1 2X M_n^{(n+1)} + 2C_{n+1}^2 M_n^{(n)} = 2n\left(XM_n^{(n+1)} + C_{n+1}^1 M_n^{(n)}\right),$$

d'où, puisque $M_n^{(n)} = U_n$:

$$(X^2 - 1) U_n'' + \left(2C_{n+1}^1 - 2n\right) X U_n' + \left(2C_{n+1}^2 - 2nC_{n+1}^1\right) U_n = 0,$$

c'est-à-dire : $(X^2 - 1) U_n'' + 2XU_n' - n(n+1) U_n = 0$.

Comme, pour n fixé, L_n est colinéaire à U_n, on conclut : $(1 - X^2) L_n'' - 2XL_n' + n(n+1) L_n = 0$.

4) a) Pour tout k de $\mathbb{N}$, notons c_k le coefficient dominant de L_k.

Soit $n \in \mathbb{N}^*$. Le polynôme $D_n = c_n L_{n+1} - c_{n+1} X L_n$ est de degré $\leqslant n$ (les termes en X^{n+1} s'éliminent), et donc $D_n \in \text{Vect}(L_0, \ldots, L_n)$.

• Pour tout k de $\{0, \ldots, n-2\}$, on a : $< D_n, L_k > = c_n < L_{n+1}, L_k > - c_{n+1} < L_n, XL_k > = 0$, car $< L_{n+1}, L_k > = 0$ $(n+1 \neq k)$ et $< L_n, XL_k > = 0$ $(L_n \in E_{n-1}^{\perp}$ et $XL_k \in E_{n-1})$.

Et : $< D_n, L_n > = c_n < L_{n+1}, L_n > - c_{n+1} < XL_n, L_n > = 0$,

car $< L_{n+1}, L_n > = 0$ et $< XL_n, L_n > = \displaystyle\int_{-1}^{1} x(L_n(x))^2 \, dx = 0$ par imparité de XL_n^2.

Ceci montre que D_n est orthogonal à $L_0, \ldots, L_{n-2}, L_n$, donc est colinéaire à L_{n-1} ; il existe $\gamma_n \in \mathbb{R}$ tel que $D_n = \gamma_n L_{n-1}$.

• Il existe $R_{n-1}, R_{n-2} \in \mathbb{R}[X]$ tels que : $\begin{cases} L_n = c_n X^n + R_{n-1} \text{ et } \deg(R_{n-1}) \leqslant n-1 \\ L_{n-1} = c_{n-1} X^{n-1} + R_{n-2} \text{ et } \deg(R_{n-2}) \leqslant n-2 \end{cases}$.

Comme $L_{n-1} = \sqrt{\dfrac{2}{2n-1}} P_{n-1}$ (cf. *2) c)*) et $||P_{n-1}|| = 1$, on a : $||L_{n-1}|| = \sqrt{\dfrac{2}{2n-1}}$. D'où :

$$\frac{2}{2n-1} \gamma_n = \gamma_n ||L_{n-1}||^2 = < \gamma_n L_{n-1}, L_{n-1} > = < c_n L_{n+1} - c_{n+1} X L_n, L_{n-1} > = -c_{n+1} < L_n, XL_{n-1} >$$

$$= -c_{n+1} < L_n, c_{n-1} X^n + XR_{n-2} > = -c_{n+1} c_{n-1} < L_n, X^n > ,$$

car $L_n \in E_{n-1}^{\perp}$ et $XR_{n-2} \in E_{n-1}$. Puis : $< L_n, c_n X^n > = < L_n, L_n - R_{n-1} > = ||L_n||^2 = \dfrac{2}{2n+1}$.

D'où : $\gamma_n = -\dfrac{(2n-1)c_{n+1}c_{n-1}}{(2n+1)c_n}$, et donc : $c_n L_{n+1} - c_{n+1} X L_n + \dfrac{(2n-1)c_{n+1}c_{n-1}}{(2n+1)c_n} L_{n-1} = 0$.

On a vu *(1) b)* : $\forall k \in \mathbb{N}$, $c_k = \dfrac{(2k)!}{2^k (k!)^2}$.

Un calcul élémentaire permet d'obtenir : $(n+1)L_{n+1} - (2n+1)XL_n + nL_{n-1} = 0$.

• On a $\begin{cases} U_0 = 1, \text{ donc } L_0 = 1 \\ U_1 = (X^2 - 1)' = 2X, \text{ donc } L_1 = X. \end{cases}$

Puis, par application de la formule de récurrence précédente, on déduit $L_2, L_3, \ldots, L_6$.

b) ◇ **Réponse :**

$$L_0 = 1$$

$$L_1 = X$$

$$L_2 = \frac{1}{2}(3X^2 - 1)$$

$$L_3 = \frac{1}{2}(5X^3 - 3X)$$

$$L_4 = \frac{1}{8}(35X^4 - 30X^2 + 3)$$

$$L_5 = \frac{1}{8}(63X^5 - 70X^3 + 15X)$$

$$L_6 = \frac{1}{16}(231X^6 - 315X^4 + 105X^2 - 5).$$

c) • *Calcul de* $L_n(1)$

Récurrence sur n (à deux pas) :

• $L_0(1) = L_1(1) = 1$

• Si, pour n fixé $(n \geqslant 1)$, $L_{n-1}(1) = L_n(1) = 1$, alors :

$(n+1)L_{n+1}(1) = (2n+1)L_n(1) - nL_{n-1}(1) = n+1$, donc $L_{n+1}(1) = 1$.

• *Calcul de* $L_n'(1)$

Utiliser *3)*.

◇ **Réponse :** Pour tout n de $\mathbb{N}$: $L_n(1) = 1$, $L_n'(1) = \dfrac{n(n+1)}{2}$.

III 1) Soient $n \in \mathbb{N}$, $(x,y) \in \mathbb{R}^2$.

- D'après ***II 4)***, on a, pour tout k de $\{0,\dots,n\}$ (en notant aussi $L_{-1} = 0$) :

$$(k+1)L_{k+1} = (2k+1)XL_k - kL_{k-1},$$

d'où : $(k+1)\big(L_{k+1}(x)L_k(y) - L_k(x)L_{k+1}(y)\big)$

$$= \big((2k+1)xL_k(x) - kL_{k-1}(x)\big)L_k(y) - L_k(x)\big((2k+1)yL_k(y) - kL_{k-1}(y)\big)$$

$$= (2k+1)(x-y)L_k(x)L_k(y) + k\big(L_k(x)L_{k-1}(y) - L_{k-1}(x)L_k(y)\big),$$

c'est-à-dire :

$$(x-y)(2k+1)L_k(x)L_k(y) = (k+1)\big(L_{k+1}(x)L_k(y) - L_k(x)L_{k+1}(y)\big) - k\big(L_k(x)L_{k-1}(y) - L_{k-1}(x)L_k(y)\big).$$

- En sommant ces égalités de $k = 0$ à $k = n$, on obtient :

$$(x-y)\sum_{k=0}^{n}(2k+1)L_k(x)L_k(y) = (n+1)\big(L_{n+1}(x)L_n(y) - L_n(x)L_{n+1}(y)\big),$$

puisque $L_{-1} = 0$.

2) Soit $n \in \mathbb{N}^*$. Notons $\alpha_1,\dots,\alpha_p$ ceux des zéros de L_n qui sont d'ordre impair et situés dans $]-1;1[$, rangés de façon que : $-1 < \alpha_1 < \dots < \alpha_p < 1$ (on a donc : $0 \leqslant p \leqslant n$).

Supposons $p < n$ et considérons le polynôme $V = \prod_{i=1}^{p}(X - \alpha_i)$. Alors $V \in E_{n-1}$, donc $< L_n, V > = 0$, c'est-à-dire $\displaystyle\int_{-1}^{1} L_n(x)V(x)\,dx = 0$.

Mais, d'après le choix de V, le polynôme L_nV est de signe fixe (au sens large) sur $]-1;1[$. Comme de plus L_nV est continu, il en résulte : $\forall x \in [-1;1]$, $(L_nV)(x) = 0$, d'où $L_nV = 0$ (polynôme), $L_n = 0$ ou $V = 0$, contradiction.

Ceci montre $p \geqslant n$, et donc $p = n$ (car $\deg(L_n) = n$).

Ainsi, dans $]-1;1[$, L_n admet exactement n zéros.

Comme $\deg(L_n) = n$, on conclut que L_n est scindé sur $\mathbb{R}$, à zéros tous simples et tous situés dans $]-1;1[$.

3) a) Soient $n \in \mathbb{N}$, $x \in \mathbb{R}$. D'après *1)* :

$$\forall y \in \mathbb{R} - \{x\}, \quad \frac{1}{n+1}\sum_{k=0}^{n}(2k+1)L_k(x)L_k(y) = \frac{L_{n+1}(x)L_n(y) - L_n(x)L_{n+1}(y)}{x-y}$$

$$= \frac{L_{n+1}(x) - L_{n+1}(y)}{x-y}\,L_n(y) - \frac{L_n(x) - L_n(y)}{x-y}\,L_{n+1}(y).$$

En faisant tendre y vers x et puisque L_n et L_{n+1} sont dérivables (donc continues), on obtient :

$$\frac{1}{n+1}\sum_{k=0}^{n}(2k+1)(L_k(x))^2 = L'_{n+1}(x)L_n(x) - L'_n(x)L_{n+1}(x).$$

b) D'après *2)*, L_{n+1} est scindé sur $\mathbb{R}$ et à zéros tous simples, notés ici $\xi_1,\dots,\xi_{n+1}$. De plus, $\deg(L_n) < \deg(L_{n+1})$. D'après la théorie de la décomposition en éléments simples, il existe $\lambda_1,\dots,\lambda_{n+1} \in \mathbb{R}$ tels que : $F_n = \dfrac{L_n}{L_{n+1}} = \displaystyle\sum_{i=1}^{n+1}\frac{\lambda_i}{X - \xi_i}$.

On sait (cf. 5.4.2 *2) a)* Prop. 2 p. 197) : $\forall i \in \{1,\dots,n+1\},\quad \lambda_i = \dfrac{L_n(\xi_i)}{L'_{n+1}(\xi_i)}$.

D'autre part, d'après *a)* appliqué en $x = \xi_i$: $\dfrac{1}{n+1}\displaystyle\sum_{k=0}^{n}(2k+1)(L_k(\xi_i))^2 = L'_{n+1}(\xi_i)L_n(\xi_i)$.

Comme $L_0 = 1$ et $n \in \mathbb{N}^*$, il est clair que $\displaystyle\sum_{k=0}^{n}(2k+1)(L_k(\xi_i))^2 \geqslant 1 > 0$, et donc : $\lambda_i > 0$.

4) Gardons les notations de *3) b)* : $F_n = \dfrac{L_n}{L_{n+1}} = \displaystyle\sum_{i=1}^{n+1}\frac{\lambda_i}{X-\xi_{n+1,i}}$, d'où : $F'_n = -\displaystyle\sum_{i=1}^{n+1}\frac{\lambda_i}{(X-\xi_{n+1,i})^2}$.

On en déduit les variations de la fonction rationnelle F_n sur $\mathbb{R}$:

x	$-\infty$	$\xi_{n+1,1}$	$\cdots$	$\xi_{n+1,i}$	$\xi_{n+1,i+1}$	$\cdots$	$\xi_{n+1,n+1}$	$+\infty$
$F_n(x)$	0 ↘	$-\infty$ || $+\infty$	$\cdots$	$-\infty$ || $+\infty$ ↘ $-\infty$	|| $+\infty$	$\cdots$	|| $+\infty$ ↘ 0	

D'après le théorème des valeurs intermédiaires, F_n admet au moins n zéros réels $x_1,\dots,x_n$ tels que :

$$\xi_{n+1,1} < x_1 < \xi_{n+1,2} < \dots < \xi_{n+1,i} < x_i < \xi_{n+1,i+1} < \dots < \xi_{n+1,n} < x_n < \xi_{n+1,n+1}.$$

Comme $F_n = \dfrac{L_n}{L_{n+1}}$, il est clair que : $\forall i \in \{1,\dots,n\},\ \xi_{n,i} = x_i$.

5) Le cas $c = 0$ est déjà vu *(2)*. Supposons $c \neq 0$, et notons $A_n = L_n + cL_{n-1}$.

Soit $i \in \{1,\dots,n-1\}$.

D'après *4)* : $L_{n-1}(\xi_{n,i})L_{n-1}(\xi_{n,i+1}) < 0$, car L_{n-1} admet dans $]\xi_{n,i};\xi_{n,i+1}[$ un zéro et un seul et celui-ci est simple.

D'où : $A_n(\xi_{n,i})A_n(\xi_{n,i+1}) = c^2L_{n-1}(\xi_{n,i})L_{n-1}(\xi_{n,i+1}) < 0$.

D'après le théorème des valeurs intermédiaires, A_n admet au moins un zéro, noté u_i, dans $]\xi_{n,i};\xi_{n,i+1}[$.

Montrons que u_i est zéro simple de A_n. Raisonnons par l'absurde : supposons que u_i soit zéro au moins double de A_n.

Alors : $A_n(u_i) = A'_n(u_i) = 0$, d'où : $L_n(u_i) = -cL_{n-1}(u_i)$ et $L'_n(u_i) = -cL'_{n-1}(u_i)$, et donc :

$$L'_n(u_i)L_{n-1}(u_i) - L'_{n-1}(u_i)L_n(u_i) = 0.$$

Mais alors (cf. *3) a)*) : $\displaystyle\sum_{k=0}^{n-1}(2k+1)(L_k(u_i))^2 = 0$;

contradiction, car $\displaystyle\sum_{k=0}^{n-1}(2k+1)(L_k(u_i))^2 \geqslant (L_0(u_i))^2 = 1$.

Ainsi, A_n admet au moins $n-1$ zéros $u_1,\dots,u_{n-1}$ tous simples et situés dans $]-1;1[$. Comme $\deg(A_n) = n$, il est alors clair que A_n admet exactement n zéros réels et que ceux-ci sont tous simples ($n-1$ d'entre eux sont dans $]-1;1[$).

Index des notations du tome 5

Index alphabétique du tome 5

D

E

F

G

H

I

J K

L

M

N

O

P

Q

R

S

T

U

V

W X Y Z

Imprimé en France. - JOUVE, 18, rue Saint-Denis, 75001 PARIS
N° 235337X. - Dépôt légal : Avril 1996

L'objectif de ce cours de mathématiques est de devenir l'outil de travail familier, efficace et adapté des élèves des classes préparatoires, des étudiants du 1er cycle universitaire scientifique et des candidats aux concours externes et internes de recrutement de professeurs.

Accompagné d'exercices corrigés nombreux et variés couvrant tout le **nouveau programme**, il s'adresse à ceux qui souhaitent confronter les théories enseignées à leur pratique.

Ce premier volume contient l'étude des **structures algébriques, nombres entiers, nombres rationnels, l'arithmétique, les polynômes et fractions rationnelles, les espaces vectoriels et applications linéaires, matrices, déterminants** et **les espaces euclidiens** ce qui correspond à la partie de l'algèbre enseignée en 1re année.

Jean-Marie Monier est professeur en classe de Spéciales au Lycée la Martinière-Monplaisir à Lyon. Il est l'auteur, chez Dunod, de cinq recueils d'excercices résolus de mathématiques.

J'intègre c'est un objectif qui a donné son nom à une collection d'ouvrages pour les classes préparatoires aux grandes écoles.
Cette collection qui se décline pour les prépas commerciales, les prépas scientifiques et les langues comprend trois types de livres : des *manuels* pour l'acquisition des connaissances fondamentales, des livres *d'exercices et d'annales* régulièrement mis à jour pour la maîtrise des connaissances, et des séries de *QCM* pour l'évaluation et l'entraînement individuels.

Couverture : L'atelier Cerce

9 782100 029747

Code 042974
ISBN 2 10 002974 6

DUNOD
EDITEUR