J.M. Arnaudiès P. Delezoide
H. Fraysse

Exercices résolus d'algèbre du cours de mathématiques - 1

Classes préparatoires
1er cycle universitaire

DUNOD

Exercices résolus d'algèbre

du cours de mathématiques - 1

Exercices résolus d'algèbre du cours de mathématiques - 1

J.M. Arnaudiès
Maître de conférences
Université Paris VI

P. Delezoide
Professeur de Mathématiques supérieures
au Lycée Louis le Grand, Paris

H. Fraysse
Professeur honoraire de Mathématiques spéciales
au lycée Pierre de Fermat, Toulouse

Classes préparatoires
1er cycle universitaire

DUNOD

ISBN 2 10 001470 6

To Donald E. Knuth, for his typesetting system TEX

TABLE DES MATIÈRES

INTRODUCTION

Nous présentons ici le deuxième de la série de quatre livres d'exercices corrigés correspondant au *Cours de Mathématiques* de J. M. Arnaudiès et H. Fraysse, un pour chaque tome.

Dans ces livres de cours, nous avons sélectionné environ un exercice sur cinq, en variant les niveaux, mais surtout en les choisissant aussi représentatifs que possible. Nous avons aussi donné la réponse à un assez grand nombre des exercices les plus ardus. Toutefois, nous n'avons pas classé les questions par ordre de difficulté, car un tel classement comporterait une trop grande part de subjectivité. Chacun sait que bien souvent, les énigmes sont loin d'être résolues par ceux que l'on attend, et qu'inversement, ce ne sont pas toujours ceux que l'on aurait cru qui "sèchent"... donc, au lecteur d'apprécier le prix de son effort !

Pour chaque exercice, nous avons tenu à donner une solution très développée, en l'ouvrant au maximum sur son environnement mathématique ; car il est bien plus bénéfique à tous égards d'étudier un exercice en relation avec cet environnement que l'exercice pour lui-même, isolément. Le rôle de l'association d'idées en mathématiques est bien connu. Le grand mathématicien Hadamard disait que pour résoudre une question épineuse, après avoir bien "séché" sur elle il faut l'abandonner, puis "penser à côté". Les exercices de mathématiques évoquent l'art des illusionnistes : un spectateur passif pourrait s'extasier toute sa vie devant ces tours de magie sans jamais en percer le secret. De même, un "bachoteur" naïf pourrait lire des centaines d'exercices de mathématiques sans augmenter sa capacité à en résoudre de nouveaux, s'il n'essayait de comprendre un peu ce qui se passe dans les coulisses, c'est-à-dire de bien situer la question dans son environnement. L'idéal serait d'apprendre à en composer de nouveaux, ou même plus simplement à en présenter de connus sous un jour original, qui les rende méconnaissables au spectateur passif...

Nous avons voulu la plus grande rigueur dans la rédaction des solutions, au moins autant que pour les livres de cours. Le résultat, nous l'espérons, est un outil de travail de fond, pour les préparations de longue haleine, qui au-delà du souci immédiat de la réussite à tel ou tel concours, préserve le plus large contact avec la science.

Il va de soi que nous remercions d'avance ceux de nos lecteurs qui voudront bien nous faire part de leurs remarques et suggestions.

Nous remercions vivement les Éditions Dunod, et tout particulièrement Gisèle Maïus, d'avoir entrepris la publication de ces ouvrages, qui s'imposaient pour donner leur pleine efficacité aux quatre livres de cours.

Chapitre I

VOCABULAIRE DE THÉORIE DES ENSEMBLES

§ I.1 *UN PEU DE LOGIQUE*

Exercice 1 :

L'implication $(\exists x \mid \forall y, A(x,y)) \Rightarrow (\forall y, (\exists x \mid A(x,y)))$ est vraie. Etudier l'implication réciproque.
Indication : On montrera *à l'aide d'un exemple* que l'implication réciproque est fausse. ■

Supposons que l'assertion $A(x,y)$ soit $(x = y)$. Dans ce cas l'assertion $(\exists x \mid \forall y, A(x,y))$ est fausse (s'il y a au moins deux objets différents). Au contraire, l'assertion $(\forall y, (\exists x \mid A(x,y)))$ est vraie : il suffit de prendre y pour valeur de x. L'implication réciproque de l'implication de l'énoncé ne peut donc être vraie.

Exercice 2 :

Montrer, par disjonction des cas, que l'équation :

$$5\,x^3 + 11\,y^3 + 13\,z^3 = 0\,,$$

n'admet dans $\mathbb{Z}^3$ que la solution $(0,0,0)$. ■

S'il y a une solution $(x,y,z) \neq (0,0,0)$, alors en divisant ces trois nombres par leur pgcd, qui n'est pas nul, on trouve une solution (x',y',z') en nombres premiers entre eux dans leur ensemble. Les nombres x' et y' ne peuvent pas être tous les deux divisibles par 13, sinon z'^3 serait divisible par 13^2, donc z' serait divisible par 13 ; il est de même clair qu'ils ne sont ni l'un ni l'autre divisible par 13. Mais alors comme :

$$5x'^3 + 11y'^3 \equiv 0 \quad [13] \quad \text{soit} \quad 5x'^3 \equiv 2y'^3 \quad [13],$$

soit encore, puisque -6 est l'inverse de 2 modulo 13, et que $-30 \equiv -4$ $[13]$,

$$-4x'^3 \equiv y'^3 \quad [13].$$

Le nombre -4 devrait être un cube modulo 13. Cela est faux comme le montre la table ci-dessous. Nous utiliserons comme ensemble de représentants dans la congruence modulo 13, les entiers entre -6 et $+6$.

x	:	1	2	3	4	5	6
x^2	:	1	4	-4	3	-1	-3
x^3	:	1	-5	1	-1	-5	-5

Les cubes non nuls sont donc $-5, -1, 1, 5$; l'équation $5x^3+11y^3+13z^3 = 0$, n'admet donc pas de solutions entières non nulles.

Exercice 7 :

> Montrer qu'il existe une infinité de nombres premiers de la forme $4n-1$ (resp. $6n-1$). ■

Supposons qu'il y ait un nombre fini k de nombres premiers congrus à -1 modulo 4 ; notons ces nombres $p_1, p_2, \ldots, p_k$. Considérons le nombre $n = 4p_1 \times p_2 \times \ldots \times p_k - 1$. Ce nombre est > 1 (3 est l'un de ces nombres premiers) ; il n'est divisible par aucun des nombres premiers congrus à -1 modulo 4 et il est impair ; sa décomposition en nombres premiers ne comporte donc que des facteurs qui sont congrus à 1 modulo 4, et il est donc congru à 1 modulo 4, ce qui est évidemment contradictoire.

Supposons qu'il y ait un nombre fini k de nombres premiers congrus à -1 modulo 6 ; notons ces nombres $p_1, p_2, \ldots, p_k$. Considérons le nombre $n = 6p_1 \times p_2 \times \ldots \times p_k - 1$. Ce nombre est > 1 (5 est l'un de ces nombres premiers) ; il n'est divisible par aucun des nombres premiers congrus à -1 modulo 6 et il est impair ; sa décomposition en nombres premiers ne comporte donc que des facteurs qui sont congrus à 1 ou 3 modulo 6 ; comme $3^2 \equiv 3$ [6], il est congru à 1 ou 3 modulo 6, ce qui est évidemment contradictoire.

§ I.2 *CONSTRUCTION D'ENSEMBLES*

Exercice 2 :

> Soit Ω un ensemble ; pour toutes parties A, B de Ω, on définit $A * B = (\complement_\Omega A) \cap (\complement_\Omega B)$. Montrer que $\complement_\Omega A$, $A \cup B$, $A \cap B$ s'expriment en utilisant le seul symbole $*$. ■

On vérifie facilement les égalités suivantes :

$$\complement_\Omega(A) = \complement_\Omega(A) \cap \complement_\Omega(\emptyset) = A * \emptyset.$$
$$A \cup B = \complement_\Omega\left(\complement_\Omega(A) \cap \complement_\Omega(B)\right) = (A * B) * \emptyset.$$
$$A \cap B = \complement_\Omega(A) * \complement_\Omega(B) = (A * \emptyset) * (B * \emptyset).$$

Exercice 6 :

Montrer que pour tout ensemble E, on a $\mathcal{P}(E) \not\subset E$. ■

Considérons l'ensemble $A = \{x \in E, \quad x \notin x\}$. Soit $A \in A$, mais alors $A \notin A$, ce qui est contradictoire, soit $A \notin A$, mais alors $A \notin E$ ou $A \in A$, la deuxième possibilité étant exclue, nous en déduisons $A \notin E$. L'ensemble A est une partie de E, donc un élément de $\mathcal{P}(E)$, qui n'est pas élément de E. L'ensemble $\mathcal{P}(E)$ n'est donc pas inclus dans E.

§ I.3 *CORRESPONDANCES ET APPLICATIONS*

Exercice 2 :

Soit $f : E \to F, g : F \to G$, et $h : G \to E$ des applications. On considère les trois applications $h \circ g \circ f$, $g \circ f \circ h$, $f \circ h \circ g$. Montrer que si deux d'entre elles sont injectives (resp. surjectives) et la troisième surjective (resp. injective), alors f, g, et h sont bijectives. ■

Démontrons le lemme suivant :

Lemme :

Soient E, F, G trois ensembles et $f : E \to F$, $g : F \to G$. Si $g \circ f$ est injective, alors f est injective ; si $g \circ f$ est surjective, alors g est surjective. ■

Supposons $g \circ f$ injective ; si x et y sont éléments de E, et que $f(x) = f(y)$, alors $g(f(x)) = g(f(y))$; comme $g \circ f$ est injective, nous pouvons en déduire $x = y$; l'application f est donc injective.
Supposons $g \circ f$ surjective, pour tout élément z de G il existe un élément x de E tel que $z = g(f(x))$; l'application g est donc surjective.
Fin du lemme.

Une permutation circulaire sur les lettres f, g, h produit une permutation circulaire sur les applications $h \circ g \circ f$, $g \circ f \circ h$, $f \circ h \circ g$. C

supposer, dans la première hypothèse, que les deux premières sont injectives et que la dernière est surjective. Comme $(h\circ g)\circ f$ est injective, nous pouvons en déduire que f est injective (lemme) ; comme $f \circ (h \circ g)$ est surjective, on voit que f est surjective ; l'application f est donc bijective. Comme $f \circ (h \circ g)$ est surjective et que f est bijective, $h \circ g$ est surjective ; donc h est surjective ; comme $(g \circ f) \circ h$ est injective, h est aussi injective, donc bijective. Les applications f et h étant bijectives, il est alors clair que g est bijective.
Supposons maintenant que les deux premières applications sont surjectives et la dernière injective. Comme $g \circ (f \circ h)$ est surjective, nous pouvons en déduire que g est surjective ; comme $(f \circ h) \circ g$ est injective, on voit que g est injective ; l'application g est donc bijective. Comme $(f \circ h) \circ g$ est injective et que g est bijective, $f \circ h$ est injective ; donc h est injective ; comme $h \circ (g \circ f)$ est surjective, h est aussi surjective, donc bijective. Les applications g et h étant bijectives, il est alors clair que f est bijective.

Exercice 6 :

Soit f une application de E dans F, $A \subset E$ et $B \subset F$. Montrer que :

$$f(A \cap f^{-1}(B)) = f(A) \cap B. \blacksquare$$

Il est évident que $f(A\cap f^{-1}(B)) \subset f(A)\cap B$. Montrons l'inclusion opposée. Si $y \in f(A) \cap B$, alors il existe $x \in A$, tel que $y = f(x)$; mais comme $y \in B$, par définition $x \in f^{-1}(B)$, donc $x \in A \cap f^{-1}(B)$; par conséquent, $y \in f(A \cap f^{-1}(B))$, ce qu'il fallait démontrer.

Exercice 8 :

Soit $\mathcal{P}(E)$ l'ensemble des parties d'un ensemble E, non vide, A et B deux de ces parties, et $f : \mathcal{P}(E) \to \mathcal{P}(E)$ l'application définie par $f(X) = (A \cap X) \cup (B \cap \overline{X})$ où $\overline{X}$ désigne $E \setminus X$. Résoudre et discuter l'équation $f(X) = \emptyset$. $\blacksquare$

L'ensemble X est solution si, et seulement si, $A\cap X = \emptyset$ et $B\cap(E\setminus X) = \emptyset$. La première condition s'écrit : $X \subset E \setminus A$, la deuxième $B \subset X$. L'ensemble des solutions est l'ensemble des parties X de E telles que $B \subset X \subset E \setminus A$. L'ensemble des solutions n'est pas vide si, et seulement si, $B \subset E \setminus A$, c'est-à-dire $A \cap B = \emptyset$.

§ I.4 *FAMILLES*

Exercice 2 :

On appelle *recouvrement* d'un ensemble E toute fa

de parties de E telles que : $\bigcup_{i\in I} F_i = E$. Si $(F_i)_{i\in I}$ et $(G_j)_{j\in J}$ sont deux recouvrements de E, le second est dit *plus fin* que le premier ssi $(\forall j \in J)\ \ (\exists i \in I)\ \mid\ G_j \subset F_i$. Montrer qu'étant donnés deux recouvrements quelconques de E il en existe un troisième plus fin que chacun des deux. ■

Soient $(F_i)_{i\in I}$ et $(G_j)_{j\in J}$ deux recouvrements de E. Montrons que la famille $(F_i \cap G_j)_{(i,j)\in I\times J}$ est un recouvrement plus fin que chacun de ces deux recouvrements.
C'est un recouvrement :

$$\bigcup_{(i,j)\in I\times J} F_i \cap G_j = \bigcup_{i\in I}\bigcup_{j\in J} (F_i \cap G_j) = \bigcup_{i\in I}\left(F_i \cap \bigcup_{j\in J} G_j\right) =$$

$$= \bigcup_{i\in I} (F_i \cap E) = \left(\bigcup_{i\in I} F_i\right) \cap E = E \cap E = E.$$

Il est plus fin que les recouvrements $(F_i)_{i\in I}$ et $(G_j)_{j\in J}$ car :

$$\forall (i,j) \in I \times J \quad F_i \cap G_j \subset F_i \quad \text{et} \quad F_i \cap G_j \subset G_j.$$

§ I.5 *RELATIONS D'ÉQUIVALENCE. ENSEMBLE QUOTIENT.*

Exercice 4 :

Soient E et F deux ensembles non vides, munis respectivement de relations d'équivalence $\mathcal{R}$ et $\mathcal{S}$. On définit la relation binaire $\mathcal{T}$ sur $E \times F$ ainsi : $(\forall (x,y) \in E \times F)$, $(\forall (x',y') \in E \times F)$ $(x,y)\ \mathcal{T}\ (x',y')$ ssi $x\ \mathcal{R}\ x'$ et $y\ \mathcal{S}\ y'$. Montrer que $\mathcal{T}$ est une relation d'équivalence. Montrer qu'il existe une bijection naturelle de $(E \times F)/_{\mathcal{T}}$ sur $E/_{\mathcal{R}} \times F/_{\mathcal{S}}$. ■

Soient $\varphi : E \to E/_{\mathcal{R}}$ et $\psi : F \to F/_{\mathcal{S}}$ les projections canoniques sur les quotients. Considérons l'application $\Phi : E \times F \to E/_{\mathcal{R}} \times F/_{\mathcal{S}}$, définie par $\Phi(x,y) = (\varphi(x), \psi(y))$. On voit que si c et c' sont deux éléments de $E \times F$, $c\ \mathcal{T}\ c'$ si, et seulement si, $\Phi(c) = \Phi(c')$; il est donc clair que la relation $\mathcal{T}$ est une relation d'équivalence. Comme l'application Φ est surjective, l'application factorisée $\overline{\Phi}$ est une bijection entre $(E \times F)/_{\mathcal{T}}$ et $E/_{\mathcal{R}} \times F/_{\mathcal{S}}$.

Exercice 5 :

> Soit E un ensemble non vide muni d'une relation d'équivalence $\mathcal{R}$, A une partie non vide de E, et $\mathcal{R}_A$ la relation d'équivalence induite par $\mathcal{R}$ sur A. Condition nécessaire et suffisante pour que l'injection canonique $A/_{\mathcal{R}_A} \to E/_{\mathcal{R}}$ soit bijective ? Appliquer à l'exercice 2. ■

L'application est toujours injective, car deux éléments de A sont équivalents pour la relation $\mathcal{R}_A$ si, et seulement si, ils sont équivalents pour la relation $\mathcal{R}$. Elle est surjective si, et seulement si, toute classe pour la relation $\mathcal{R}$ a un représentant dans A, c'est-à-dire rencontre A.
C'est le cas dans l'exercice 2 : pour tout vecteur x non nul de E, il existe un scalaire $\lambda > 0$ tel que $\lambda x \in S$.

Exercice 11 :

> Soit E un ensemble non vide et $\mathcal{A}$ un ensemble de parties de E. On définit la relation binaire $\mathcal{R}$ dans E par : $x \mathcal{R} y$ ssi $\forall A \in \mathcal{A}$, $\{x, y\} \subset A$ ou $\{x, y\} \subset E \setminus A$. Montrer que $\mathcal{R}$ est une relation d'équivalence. Décrire les classes d'équivalence. ■

Notons χ_A la fonction caractéristique d'une partie A de E. On voit que :

$$(\forall (x, y) \in E \times E) \quad (x \mathcal{R} y) \iff (\forall A \in \mathcal{A} \quad \chi_A(x) = \chi_A(y)).$$

Sous cette forme, il est clair que la relation $\mathcal{R}$ est symétrique, réflexive et transitive ; c'est donc bien une relation d'équivalence.
Soit Φ l'application qui à x élément de E fait correspondre l'application $A \mapsto \chi_A(x)$, $\mathcal{A} \to \{0, 1\}$. On voit que pour tous x et y dans E, $x \mathcal{R} y$ si, et seulement si, $\Phi(x) = \Phi(y)$. L'application factorisée $\overline{\Phi}$ est donc une injection de $E/_{\mathcal{R}}$ dans l'ensemble des applications de $\mathcal{A}$ à valeurs dans l'ensemble $\{0, 1\}$.

Caractérisons maintenant l'image de $\overline{\Phi}$.
Soit $f \in \mathrm{Im}\,(\Phi) = \mathrm{Im}\,(\overline{\Phi})$, la classe correspondante est $\{x \in E \mid \Phi(x) = f\}$, c'est donc aussi $\{x \in E \mid (\forall A \in \mathcal{A}) \ \chi_A(x) = f(A)\}$; cette classe est donc l'ensemble des éléments x de E qui appartiennent à toutes les parties A de $\mathcal{A}$ telles que $f(A) = 1$, et qui n'appartiennent à aucune des parties A telles que $f(A) = 0$, c'est l'intersection de $\bigcap_{f(A)=1} A$ et de $\bigcap_{f(A)=0} E \setminus A$.
Inversement, si $f : \mathcal{A} \to \{0, 1\}$ est telle que l'intersection C de $\bigcap_{f(A)=1} A$ et de $\bigcap_{f(A)=0} E \setminus A$ est non vide, on voit que C est la classe de chacun de ses éléments.

Intuitivement, pour définir une classe, on choisit pour chaque élément A de $\mathscr{A}$ une valeur $f(A)$ qui est 0 ou 1 ; la classe correspondante est l'intersection des parties A telles que $f(A) = 1$, et des complémentaires des parties A telles que $f(A) = 0$; il faut évidemment éliminer les fonctions f qui conduiraient à des classes vides. Si $\mathscr{A}$ est fini de cardinal n, le nombre de classes est au maximum 2^n, et dépend de la configuration des différentes parties A, éléments de $\mathscr{A}$

§ I.6 *RELATIONS D'ORDRE*

Exercice 2 :

> Soit E et F deux ensembles ; on considère l'ensemble $\mathscr{F}_{E,F}$ des couples (X, f) où $X \subset E$ et où $f : X \to F$ est une application. Si $(X, f) \in \mathscr{F}_{E,F}$ et $(Y, g) \in \mathscr{F}_{E,F}$, on écrit $(X, f) \preceq (Y, g)$ ssi on a à la fois $X \subset Y$ et $f = g_{|X}$. Vérifier que $(\mathscr{F}_{E,F}, \preceq)$ est un ensemble ordonné. Quels sont ses éléments maximaux ? ■

On vérifie très facilement les propriétés de réflexivité, antisymétrie et transitivité pour la relation $\preceq$. On pourrait aussi identifier une application de X, partie de E, à valeurs dans l'ensemble F, à son graphe, partie de $E \times F$. On obtient alors un isomorphisme entre $(\mathscr{F}_{E,F}, \preceq)$ et l'ensemble des graphes fonctionnels inclus dans $E \times F$, muni de l'ordre de l'inclusion.
Eliminons le cas très particulier où E ou F seraient vides, et montrons que les éléments maximaux de l'ensemble ordonné $(\mathscr{F}_{E,F}, \preceq)$ sont les couples (E, f), où f est une application $E \to F$.
Ce sont des éléments maximaux :
Si (E, f) et (Y, g) sont deux éléments de $\mathscr{F}_{E,F}$ et que $(E, f) \preceq (Y, g)$, alors $E \subset Y$, donc $E = Y$, et comme $g_{|E} = f$, nécessairement $g = f$; donc $(E, f) = (Y, g)$. L'élément (E, f) est maximal.

Ce sont les seuls :
Si $(X, f) \in \mathscr{F}_{E,F}$ et que X est une partie stricte de E, soit x' un élément de E qui n'est pas dans X, et y un élément quelconque de F ; on peut définir sur $X' = X \cup \{x'\}$, la fonction g par : $g(x) = f(x)$ si $x \in X$, et $g(x') = y$. On obtient ainsi un couple (X', g) élément de $\mathscr{F}_{E,F}$ qui majore strictement (X, f) pour la relation d'ordre $\preceq$. Le couple (X, f) n'est donc pas maximal.

Exercice 3 :

> Dans l'exercice précédent on prend $E = F = \mathbb{C}$. On note Φ le sous-ensemble de $\mathscr{F}_{\mathbb{C},\mathbb{C}}$ formé des (X, f) tels que f soit *rationnelle*, c'est-à-dire telle qu'il existe $\varphi \in \mathbb{C}(X)$ po

ne contient aucun pôle de φ et $\varphi_{|X} = f$. Trouver les éléments maximaux de l'ensemble ordonné $(\Phi, \preceq)$. ■

Notons $D(\varphi)$ le complémentaire de l'ensemble des pôles de la fraction rationnelle φ ($\varphi \in \mathbb{C}(X)$). Nous allons démontrer que les éléments maximaux de Φ sont les couples $(D(\varphi), \varphi)$, où φ est un élément de $\mathbb{C}(X)$ qu'on identifie à une fonction de domaine $D(\varphi)$.
Supposons que le couple (X, f) soit maximal dans Φ ; il existe une fraction rationnelle φ telle que $X \subset D(\varphi)$ et $f = \varphi_{|X}$; comme le couple $(D(\varphi), \varphi)$ majore (X, f) et que (X, f) est supposé maximal, les deux couples sont égaux.
Supposons maintenant que ψ soit une fraction rationnelle et que $(D(\psi), \psi) \preceq (X, f)$; il existe une fraction rationnelle φ telle que $X \subset D(\varphi)$ et $f = \varphi_{|X}$; les deux fractions rationnelles φ et ψ coïncident sur la partie infinie $D(\psi)$ donc sont identiques ; comme $D(\psi) \subset X \subset D(\varphi)$, nous pouvons en déduire que $X = D(\psi)$ et $f = \psi$ (considérée comme fonction de domaine $D(\psi)$). Le couple $(D(\psi), \psi)$ est donc maximal.

Exercice 5 :

Des hussards de tailles variées sont disposés en rectangle. On repère le plus grand de chaque rangée et l'on retient le plus petit de ces plus grands, soit X. Puis on repère le plus petit de chaque colonne et on retient le plus grand de ces plus petits, soit Y. comparer les tailles de X et de Y. ■

Soit Z le hussard qui est sur la même rangée que X et sur la même colonne que Y. La taille du hussard Z est inférieure (ou égale) à celle de X, puisque X est le plus grand de sa rangée ; mais le hussard Z est de taille supérieure (ou égale) à celle du hussard Y, qui est le plus petit de sa colonne ; nous en déduisons que le hussard X est plus grand que le hussard Y.
On peut aussi formaliser ce résultat de la manière suivante. Soient E et F des ensembles non vides et $f : E \times F \to G$ une application, l'ensemble G étant fini et muni d'un ordre total $\geqslant$. Toute partie non vide A de G a donc un plus petit élément que nous noterons $\min(A)$ et un plus grand élément que nous noterons $\max(A)$. Nous pouvons alors écrire :

$$(\forall u \in E,\ \forall y \in F) \quad \max_x f(x, y) \geqslant f(u, y).$$

D'où :

$$(\forall u \in E) \quad \min_y(\max_x f(x, y)) \geqslant \min_y f(u, y),$$

donc :

$$\min_y(\max_x f(x, y)) \geqslant \max_u(\min_y f(u, y)).$$

La variable u étant muette, nous obtenons le résultat attendu :

$$\min_y(\max_x f(x,y)) \geqslant \max_x(\min_y f(x,y)).$$

Exercice 7 :

On munit $\mathbb{R}^n$ (où $n \geqslant 1$) de l' *ordre produit* relatif à l'ordre usuel de $\mathbb{R}$. (Par définition, si $x = (x_1, x_2, \ldots, x_n)$ et $y = (y_1, y_2, \ldots, y_n)$ appartiennent à $\mathbb{R}^n$, on a donc $x \preceq y$ ssi $(\forall i \in \{1, \ldots, n\})\ x_i \leqslant y_i)$.
Soit B le sous-ensemble ordonné de $(\mathbb{R}^n, \preceq)$ défini par :

$$B = \{(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n \mid x_1^2 + x_2^2 + \ldots + x_n^2 \leqslant 1\}\ .$$

Etudier les éléments maximaux de B. ■

Montrons que l'ensemble des éléments maximaux de B est l'ensemble :

$$M = \{(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n \mid x_1^2 + \ldots + x_n^2 = 1 \text{ et } (\forall i \in \{1, 2, \ldots, n\}\ \ x_i \geqslant 0)\}\ .$$

Soit $x = (x_1, x_2, \ldots, x_n)$ un élément de B. Supposons qu'il existe $j \in [\![1, n]\!]$, tel que $x_j < 0$, alors le n-uplet $x' = (x_1, \ldots, x_{j-1}, 0, x_{j+1}, \ldots, x_n)$ est un élément de B qui majore strictement x pour la relation $\preceq$; le n-uplet x n'est donc pas maximal. Supposons maintenant que $x_1^2 + x_2^2 + \ldots + x_n^2 < 1$; posons $x_1' = \sqrt{1 - (x_2^2 + \ldots + x_n^2)}$, on voit que le n-uplet $x' = (x_1', x_2, \ldots, x_n)$ est un élément de B qui majore strictement x pour l'ordre $\preceq$; le n-uplet x n'est donc pas maximal. L'ensemble des éléments maximaux de B est donc inclus dans M.
Soit maintenant un n-uplet $x = (x_1, x_2, \ldots, x_n)$ élément de l'ensemble M. Si le n-uplet $y = (y_1, y_2, \ldots, y_n)$, élément de B, majore x, alors pour tout $i \in [\![1, n]\!]$, $0 \leqslant x_i \leqslant y_i$, donc $y_i^2 \geqslant x_i^2$; comme $y_1^2 + y_2^2 + \ldots + y_n^2 \leqslant 1 = x_1^2 + x_2^2 + \ldots + x_n^2$, on voit que pour tout $i \in [\![1, n]\!]$, $y_i^2 = x_i^2$; comme d'autre part pour tout i, $0 \leqslant x_i \leqslant y_i$, nous pouvons en déduire $x = y$. Le n-uplet x est donc maximal.
L'ensemble des éléments maximaux de B est donc bien M.

Chapitre II

NOMBRES ENTIERS, NOMBRES RATIONNELS

§ II.1 *AXIOMES DE PEANO ; RÉCURRENCE*

Exercice 1 :

Démontrer en détail le corollaire du théorème II.1.2 :
Soit $\mathscr{E}$ et $\mathscr{F}$ deux ensembles non vides, $g : \mathscr{F} \to \mathscr{F}$ et $\psi : \mathscr{E} \to \mathscr{F}$ deux applications. Il existe une, et une seule, application $\varphi : \mathscr{E} \times \mathbb{N} \to \mathscr{F}$ vérifiant :

(I) $\qquad (\forall e \in \mathscr{E}) \qquad \varphi(e, 0) = \psi(e)$

(II) $\qquad (\forall e \in \mathscr{E},\ \forall n \in \mathbb{N}) \quad \varphi(e, S(n)) = g(\varphi(e, n))$. ■

Soit Θ l'application de $(\mathscr{F}^{\mathscr{E}})^{\mathbb{N}}$ dans $\mathscr{F}^{\mathscr{E}\times\mathbb{N}}$ définie par :

$$(\forall \Phi \in (\mathscr{F}^{\mathscr{E}})^{\mathbb{N}} \ \ \forall n \in \mathbb{N} \ \ \forall e \in \mathscr{E}) \quad \Theta(\Phi)(e, n) = \Phi(n)(e).$$

Il est clair qu'il s'agit d'une bijection dont la réciproque est l'application Γ définie par :

$$(\forall u \in \mathscr{F}^{\mathscr{E}\times\mathbb{N}} \ \ \forall n \in \mathbb{N} \ \ \forall e \in \mathscr{E}) \quad \Gamma(u)(n)(e) = u(e, n).$$

Soit maintenant l'application $G : \mathscr{F}^{\mathscr{E}} \to \mathscr{F}^{\mathscr{E}}$ définie par :

$$(\forall f \in \mathscr{F}^{\mathscr{E}}) \quad G(f) = g \circ f.$$

En utilisant le théorème II.1.2 en remplaçant $\mathscr{E}$ par $\mathscr{F}^{\mathscr{E}}$ et g par G, on prouve l'existence (et l'unicité) d'une application $\Phi : \mathbb{N} \to \mathscr{F}^{\mathscr{E}}$ telle que :

(I) $\qquad \Phi(0) = \psi$

(II) $\qquad (\forall n \in \mathbb{N}) \quad \Phi(S(n)) = G(\Phi(n)) = g \circ \Phi(n).$

Ces propriétés s'écrivent aussi :

(I) $\qquad (\forall e \in \mathscr{E}) \quad \Phi(0)(e) = \psi(e)$

(II) $\qquad (\forall n \in \mathbb{N} \ \ \forall e \in \mathscr{E}) \quad \Phi(S(n))(e) = g(\Phi(n)(e)).$

L'application $\varphi = \Theta(\Phi)$ vérifie donc :

$$(I) \qquad (\forall e \in \mathscr{E}) \quad \varphi(e,0) = \psi(e)$$
$$(II) \qquad (\forall e \in \mathscr{E} \ \ \forall n \in \mathbb{N}) \quad \varphi(e,S(n)) = g(\varphi(e,n)).$$

Il est clair que c'est la seule application qui convienne.

Exercice 3 :

On appelle *chaîne simple* tout triplet $\mathscr{C} = (a, \mathscr{E}, f)$ où $\mathscr{E}$ est un ensemble, a un élément de $\mathscr{E}$, et $f : \mathscr{E} \to \mathscr{E}$ une application vérifiant (C_1) $a \notin f(\mathscr{E})$; (C_2) f est injective ; (C_3) la seule partie E de $\mathscr{E}$ telle que $a \in \mathscr{E}$ et $(\forall x \in \mathscr{E})$ $(x \in E) \Rightarrow (f(x) \in E)$ est $E = \mathscr{E}$.

a) Montrer que si $\mathscr{C} = (a, \mathscr{E}, f)$ est une chaîne simple, on a :
$\mathscr{E} = \{a\} \cup f(\mathscr{E})$.

b) Montrer que si $\mathscr{C} = (a, \mathscr{E}, f)$ est une chaîne simple, si $\mathscr{F}$ est un ensemble non vide, b un élément de $\mathscr{F}$, et $g : \mathscr{F} \to \mathscr{F}$ une application, alors il existe une, et une seule, application $\varphi : \mathscr{E} \to \mathscr{F}$ telle que $\varphi(a) = b$ et $\varphi \circ f = g \circ \varphi$ [s'inspirer de la preuve du théorème II.1.2].

c) Montrer que si $\mathscr{C} = (a, \mathscr{E}, f)$ est une chaîne simple, il existe une, et une seule, application $\varphi : \mathbb{N} \to \mathscr{E}$, telle que $\varphi(0) = a$ et $\varphi(n+1) = f(\varphi(n))$ pour tout $n \in \mathbb{N}$, et montrer que cette application φ est bijective. ■

a) Le théorème II.1.2 nous permet d'affirmer l'existence et l'unicité d'une application $\varphi : \mathbb{N} \to \mathscr{E}$ telle que :

$$(I) \qquad \varphi(0) = a$$
$$(II) \qquad (\forall n \in \mathbb{N}) \quad \varphi(S(n)) = f(\varphi(n)).$$

L'ensemble $\varphi(\mathbb{N})$ est stable par l'application f et contient a, c'est donc l'ensemble $\mathscr{E}$. L'application φ est donc surjective. De plus :

$$\mathscr{E} = \varphi(\mathbb{N}) = \varphi(\{0\} \cup S(\mathbb{N})) =$$
$$= \{a\} \cup \varphi(S(\mathbb{N})) = \{a\} \cup f(\varphi(\mathbb{N})) = \{a\} \cup f(\mathscr{E}).$$

b) D'après ce qui précède, si le triplet $(a, \mathscr{E}, f)$ est une chaîne simple, il vérifie les axiomes de Peano. Tous les résultats démontrés pour le triplet $(0, \mathbb{N}, S)$ sont aussi vrais pour le triplet $(a, \mathscr{E}, f)$; en particulier le théorème II.1.2 qui peut s'énoncer sous la forme :

Théorème :

Soit $\mathcal{F}$ un ensemble non vide, $b \in \mathcal{F}$, et $g : \mathcal{F} \to \mathcal{F}$ une application. Il existe une application, et une seule, $\psi : \mathcal{E} \to \mathcal{F}$ telle que : $\psi(a) = b$ et $\psi \circ f = g \circ \psi$. ■

Ce qui est le résultat demandé.

c) L'existence et l'unicité de l'application φ utilisée dans le a) se déduisent facilement du théorème II.1.2. On peut utiliser le résultat du b) avec $\mathcal{F} = \mathbb{N}$ et $g = S$, $b = 0$. Il existe donc une unique application $\psi : \mathcal{E} \to \mathbb{N}$ telle que $\psi(a) = 0$ et $(\forall e \in \mathcal{E})$ $\psi(f(e)) = S(\psi(e))$.
Montrons que φ et ψ sont réciproques l'une de l'autre, et donc bijectives. On vérifie que :

$$\psi(\varphi(0)) = 0 \text{ et } (\psi \circ \varphi) \circ S = \psi \circ f \circ \varphi = S \circ (\psi \circ \varphi) .$$

Par unicité nous en déduisons que $\psi \circ \varphi = \mathrm{Id}_{\mathbb{N}}$.
De même :

$$\varphi(\psi(a)) = a \text{ et } (\varphi \circ \psi) \circ f = \varphi \circ S \circ \psi = f \circ (\varphi \circ \psi) .$$

Par unicité nous en déduisons que $\varphi \circ \psi = \mathrm{Id}_{\mathcal{E}}$.

Exercice 7 :

Montrer que $\forall m \in \mathbb{N}^*$, $\forall n \in \mathbb{N}^*$, $\forall r \in \mathbb{N}$, $m^{2r+1} + n^{2r+1}$ est divisible par $m + n$. ■

Le résultat est évident si $r = 0$; nous supposerons dans la suite $r > 0$.
On peut écrire : $m^{2r+1} + n^{2r+1} = m^{2r+1} - (-n)^{2r+1}$; d'après une identité algébrique bien connue :

$$m^{2r+1} + n^{2r+1} =$$
$$= (m+n)(m^{2r} - m^{2r-1}n + m^{2r-2}n^2 - \ldots + m^2n^{2r-2} - mn^{2r-1} + n^{2r}) .$$

Cela prouve bien le résultat demandé.

Exercice 9 :

Pour quels nombres *complexes* a peut-on définir une suite (u_n) de nombres complexes telle que :

$$u_0 = a \quad \text{et} \quad (\forall n \in \mathbb{N}) \quad u_{n+1} = 1 + \frac{1}{u_n} \quad ? \blacksquare$$

Soit ∞ un élément qui n'est pas dans $\mathbb{C}$. Définissons sur $\mathbb{C} \cup \{\infty\}$ l'application h par :

$$h(0) = \infty, \quad h(\infty) = 1, \quad (\forall z \in \mathbb{C} \setminus \{0\}) \quad h(z) = 1 + \frac{1}{}$$

Il est clair que l'application h est une bijection de $\mathbb{C} \cup \{\infty\}$ vers $\mathbb{C} \cup \{\infty\}$. Pour tout complexe a, il existe une et une seule suite (u_n) d'éléments de $\mathbb{C} \cup \{\infty\}$ telle que $u_0 = a$ et $(\forall n \in \mathbb{N}) \quad u_{n+1} = h(u_n)$. On peut aussi écrire : $(\forall n \in \mathbb{N}) \quad u_n = h^n(a)$. On voit qu'on peut définir une suite de *complexes* vérifiant les conditions de l'énoncé si, et seulement si, pour tout n entier $n > 0$, $h^n(a) \neq \infty$. Comme l'application h est bijective, cette condition s'écrit :

$$(\forall n \in \mathbb{N}^*) \quad a \neq h^{-n}(\infty).$$

On vérifie facilement que $h^{-1}(\infty) = 0$, $h^{-2}(\infty) = -1$, $h^{-3}(\infty) = -1/2$ etc.

Montrons que pour tout entier n, $n > 0$, $h^{-n}(\infty) = -a_{n-1}/a_n$, où (a_n) est la suite de Fibonacci, définie par les conditions : $a_0 = 0$, $a_1 = 1$ et $(\forall p \in \mathbb{N}) \quad a_{p+2} = a_{p+1} + a_p$ (on peut remarquer qu'il s'agit d'une suite d'entiers tous strictement positifs, sauf a_0).

C'est vrai pour $n = 1$, et si c'est vrai pour $n > 0$, alors :

$$h\left(-\frac{a_n}{a_{n+1}}\right) = 1 - \frac{a_{n+1}}{a_n} = \frac{a_n - a_{n+1}}{a_n} = -\frac{a_{n-1}}{a_n} = h^{-n}(\infty),$$

donc :

$$-\frac{a_n}{a_{n+1}} = h^{-(n+1)}(\infty) \ ;$$

l'égalité est donc vraie pour tout entier n, $n > 0$.

L'ensemble des nombres complexes vérifiant les conditions de l'énoncé est donc l'ensemble : $\mathbb{C} \setminus \{-(a_{n-1}/a_n),\ n \in \mathbb{N}^*\}$.

§ II.2 *ORDRE NATUREL DANS* $\mathbb{N}$

Exercice 1 :

Soit $(E, \leqslant)$ un ensemble totalement ordonné non vide tel que (I) $(E, \leqslant)$ est bien ordonné ; (II) E n'a pas de plus grand élément ; (III) toute partie de E non vide et majorée admet un plus grand élément . Montrer qu'il existe une, et une seule, bijection croissante ψ de $(\mathbb{N}, \leqslant)$ sur $(E, \leqslant)$. ■

Montrons qu'un ensemble bien ordonné $(E, \leqslant)$ n'a pas d'automorphismes autres que l'identité. En effet si f était une bijection strictement croissante de $(E, \leqslant)$ vers $(E, \leqslant)$, de réciproque strictement croissante, et différente de l'identité, l'ensemble $D = \{x \in E, \quad f(x) \neq x\}$ ne serait pas vide et aurait un plus petit élément m. Si on suppose $f(m) < m$, alors $f(f(m)) = f(m)$, d'où $f(m) = m$, il y a contradiction. Si on suppose $f(m) > m$, alors $m > f^{-1}(m)$, donc $f(f^{-1}(m)) = f^{-1}(m)$, c'est-à-dire $m = f^{-1}(m)$, ce qui est la même contradiction.

Il est alors clair qu'il ne peut exister entre deux ensembles bien ordonnés qu'au plus un isomorphisme, car si f_1 et f_2 sont deux isomorphismes, $f_1 \circ f_2^{-1}$ est un automorphisme de l'un des ensembles bien ordonnés, et est donc égal à l'identité de cet ensemble.
Dans le problème posé ici, les deux ensembles sont bien ordonnés, donc totalement ordonnés et par conséquent toute bijection croissante de l'un vers l'autre est un isomorphisme d'ensembles ordonnés. Le lecteur évitera d'étendre indûment ce résultat. Par exemple on peut numéroter les parties d'un ensemble fini E de cardinal n, de telle sorte que l'application ainsi obtenue, de $\mathcal{P}(E)$ muni de l'ordre de l'inclusion vers l'intervalle des entiers $[\![1, 2^n]\!]$ muni de son ordre naturel, soit bijective croissante ; il suffit de numéroter la partie vide, puis les singletons, les paires etc., et terminer par l'ensemble entier ; cette bijection croissante n'est évidemment pas un isomorphisme d'ensembles ordonnés.

Montrons maintenant l'existence de cet isomorphisme.
Soit $\mathcal{S}$ l'ensemble des parties non vides de E qui n'ont pas de plus grand élément ; cet ensemble n'est pas vide puisque $E \in \mathcal{S}$. Soit $\varphi : \mathcal{S} \to \mathcal{S}$, $A \mapsto A \setminus \{\mathrm{Min}\,(A)\}$. L'élément $\mathrm{Min}\,(A)$ existe puisque l'ensemble E est bien ordonné et que la partie A n'est pas vide ; la partie $A \setminus \{\mathrm{Min}\,(A)\}$, n'est pas vide, sinon on aurait $A = \{\mathrm{Min}\,(A)\}$ et A aurait un plus grand élément, et elle n'a pas de plus grand élément, sinon la partie A aurait le même plus grand élément. On a donc bien défini une application de $\mathcal{S}$ vers $\mathcal{S}$. Posons pour n entier $E_n = \varphi^n(E)$, $(E_0 = E)$, et $\psi(n) = \mathrm{Min}\,(E_n)$.
Montrons que l'application ψ est une bijection croissante entre $(\mathbb{N}, \leqslant)$ et $(E, \leqslant)$, donc un isomorphisme entre ces deux ensembles ordonnés.
Comme pour tout entier n, $E_{n+1} \subset E_n$, nous pouvons en déduire que pour tout entier n, $\psi(n+1) = \mathrm{Min}\,(E_{n+1}) \geqslant \psi(n) = \mathrm{Min}\,(E_n)$, et il n'y a pas égalité car $\mathrm{Min}\,(E_n) \notin E_{n+1}$. L'application ψ est donc strictement croissante.
Montrons maintenant que l'application ψ est surjective. Comme l'ensemble $\mathrm{Im}\,(\psi) = \{\psi(n),\ \ n \in \mathbb{N}\}$ n'admet pas de plus grand élément (puisque $\psi(n)$ est majoré strictement par $\psi(n+1)$), il n'est pas majoré. Soit x un élément de E, ce n'est pas un majorant de $\mathrm{Im}\,(\psi)$, il existe donc un entier N tel que $x < \psi(N)$, donc $x \notin E_N$; l'ensemble des entiers n tels que $x \in E_n$ n'est pas vide car $x \in E_0 = E$, et est majoré par N, puisque la suite (E_n) est décroissante pour l'inclusion, cet ensemble a donc un plus grand élément p ; mais alors $x \in E_p$ et $x \notin E_{p+1}$, comme $E_{p+1} = E_p \setminus \{\psi(p)\}$, nous pouvons en déduire $x = \psi(p)$. L'application ψ est donc surjective.
Nous avons bien établi que l'application ψ était un isomorphisme d'ensembles ordonnés.

Exercice 3 :

a) Soit $(E, \leqslant)$ un ensemble bien ordonné non vide sans plus grand élément. Montrer que l'application $S : E$

$\text{Min}(\{y \in E \mid y > x\})$ est bien définie (c'est l'application *successeur*). Si 0 désigne le plus petit élément de E, montrer qu'en général $\text{Im}(S) \neq E \setminus \{0\}$ (cf. exercice 2) .

b) On note $E' = (E \setminus \{0\}) \setminus \text{Im}(S)$. En remarquant que tout sous-ensemble ordonné d'un ensemble bien ordonné est bien ordonné, étudier si on peut définir E'', ..., $E^{(k)} = (E^{(k-1)})'$, pour $k \in \mathbb{N}^*$.

c) Donner un exemple d'ensemble bien ordonné E tel que tous les $E^{(k)}$ soient définis pour $k \in \mathbb{N}^*$. ■

a) Soit $x \in E$, comme x n'est pas le plus grand élément de E, l'ensemble $\{y \in E,\ y > x\}$ n'est pas vide et a donc un plus petit élément, c'est le successeur de x, $S(x)$.
Soit (u_n) la suite vérifiant les conditions $u_0 = 0_E$ et $(\forall n \in \mathbb{N})\ u_{n+1} = S(u_n)$. Cette suite est strictement croissante et donc injective. Montrons que si $\text{Im}(S) = E \setminus \{0_E\}$, la suite (u_n) est surjective ; nous pourrons en déduire que dans ce cas les ensembles bien ordonnés $(\mathbb{N}, \leqslant)$ et $(E, \leqslant)$ sont isomorphes.
Si on suppose que la suite (u_n) n'est pas surjective, soit a le plus petit élément de E qui n'est pas l'un des termes de cette suite ; ce n'est pas 0_E car $u_0 = 0_E$, et comme nous supposons $\text{Im}(S) = E \setminus \{0_E\}$, l'élément a a un prédécesseur b, c'est-à-dire $a = S(b)$; l'élément b est l'un des termes de la suite : $\exists n \in \mathbb{N} \mid b = u_n$, donc $a = S(u_n) = u_{n+1}$, l'élément a est donc l'un des termes de la suite, ce qui est contradictoire.
L'égalité : $\text{Im}(S) = E \setminus \{0_E\}$ n'est donc vraie que dans le cas où les ensembles ordonnés $(\mathbb{N}, \leqslant)$ et $(E, \leqslant)$ sont isomorphes, ce qui n'est pas le cas général.

b) On peut définir l'ensemble E'' si l'ensemble E' est non vide et n'a pas de plus grand élément ; de même pour les ensembles suivants. Etudions le problème dans l'exemple ci-dessous.
Munissons l'ensemble $\mathbb{N} \times \mathbb{N}$ de l'ordre lexicographique, c'est-à-dire posons $(n, m) \leqslant (n', m')$ si $n < n'$, ou $n = n'$ et $m \leqslant m'$. On vérifie facilement qu'on définit ainsi un ordre total sur l'ensemble $\mathbb{N} \times \mathbb{N}$. Montrons que c'est un bon ordre.
Soit A une partie non vide de $\mathbb{N} \times \mathbb{N}$.
Considérons l'ensemble $\{n \in \mathbb{N} \mid \exists m \in \mathbb{N}\ \ (n, m) \in A\}$; c'est une partie non vide de $\mathbb{N}$ puisque A n'est pas vide, et elle a donc un plus petit élément n_0 ; l'ensemble $\{m \in \mathbb{N} \mid (n_0, m) \in A\}$ n'est alors pas vide et a donc un plus petit élément m_0 ; le couple (n_0, m_0) est le plus petit élément de A, en effet, c'est un élément de A, et si (n, m) est élément de A, alors $n_0 \leqslant n$ et si $n_0 = n$, alors $m_0 \leqslant m$. Toute partie non vide A de $\mathbb{N} \times \mathbb{N}$ a donc un plus petit élément ; l'ensemble $\mathbb{N} \times \mathbb{N}$ est donc bien ordonné]

lexicographique.
Il est clair que le successeur du couple (n, m) est le couple $(n, m+1)$; par conséquent les éléments qui n'ont pas de prédécesseurs sont les couples de la forme $(n, 0)$. Le plus petit élément de l'ensemble est le couple $(0, 0)$; l'ensemble E' est donc ici l'ensemble des couples $(n, 0)$ où $n \in \mathbb{N}^*$, c'est un ensemble ordonné isomorphe à $(\mathbb{N}, \leqslant)$. On peut donc définir l'ensemble E'', mais il est vide.
L'exercice 2 donne d'autres exemples d'ensembles bien ordonnés. On peut aussi étudier l'ordre lexicographique sur $\mathbb{N}^p$, où $p \in \mathbb{N}^*$, qui est un bon ordre.

c) Soit E l'ensemble des polynômes non nuls à coefficients entiers $\geqslant 0$; si P et Q sont des éléments de E, nous dirons que $P \leqslant Q$ si, et seulement si, $P = Q$ ou si le coefficient dominant du polynôme $Q - P$ est > 0. On vérifie facilement qu'on définit ainsi un ordre total ; cela tient principalement au fait que l'ensemble des polynômes, nul ou de coefficient dominant $\geqslant 0$, est stable par l'addition. Observons que si P et Q sont deux éléments de E et que $\deg(P) < \deg(Q)$, alors $P < Q$. Montrons qu'il s'agit d'un bon ordre.
Soit A une partie non vide de E. L'ensemble D des degrés des polynômes éléments de A est une partie non vide de $\mathbb{N}$ et a donc un plus petit élément d. L'ensemble $A_1 = \{P \in A \mid \deg(P) = d\}$ n'est pas vide et d'après la remarque ci-dessus, si l'ensemble A_1 a un plus petit élément, c'est aussi le plus petit élément de A. On obtiendra le plus petit élément de A_1 en prenant le polynôme élément de A_1 dont le coefficient de puissance d est (non nul) le plus petit possible, puis, ce coefficient étant fixé, le coefficient de puissance $d-1$ le plus petit possible etc., jusqu'au coefficient de puissance 0.
Le plus petit élément de E est le polynôme constant 1. On vérifie facilement que le successeur d'un polynôme non nul P est le polynôme $P+1$. L'image de la fonction successeur est donc l'ensemble des éléments de E différents de 1, dont la valeur en 0 est > 0. L'ensemble E' est donc ici l'ensemble des éléments P de E tels que $P(0) = 0$, c'est-à-dire l'ensemble des polynômes non nuls à coefficients entiers $\geqslant 0$, qui sont divisibles par X. Il est clair que l'ensemble ordonné E' est ici isomorphe à l'ensemble ordonné E ; on peut donc définir les ensembles $E^{(k)}$ pour tout entier k, $k > 0$, et ils sont tous isomorphes entre eux.

Exercice 5 :

Soit $f : \mathbb{N}^* \to \mathbb{N}^*$ une application qui vérifie la propriété $(\forall n \in \mathbb{N}^*)\ \ f(n+1) > f(f(n))$. Montrer que $(\forall n \in \mathbb{N}^*)\ \ f(n) = n$. [*Olympiades 1977.*] ■

Montrons d'abord par récurrence sur l'entier p que : $(\forall n > p)$

La propriété est vraie si $p = 0$ puisque l'application f est à valeurs dans $\mathbb{N}^*$. Supposons que la propriété soit vraie pour p. Si $n > p+1$, alors $n-1 > p$, donc $f(n-1) > p$ et $f(f(n-1)) > p$ (récurrence) ; nous déduisons alors de l'hypothèse : $f(n) = f(n-1+1) > f(f(n-1)) > p$, donc $f(n) > p+1$. La propriété est donc vraie pour $p+1$. Cette propriété est donc vraie pour tout entier p.
En particulier nous en déduisons : $(\forall n \in \mathbb{N}^*)\ f(n) > n-1$, soit encore $f(n) \geqslant n$; d'où $(\forall n \in \mathbb{N}^*)\ f(n+1) > f(f(n)) \geqslant f(n)$; l'application f est donc strictement croissante et comme $(\forall n \in \mathbb{N}^*)\ f(n+1) > f(f(n))$, on en déduit que $(\forall n \in \mathbb{N}^*)\ n+1 > f(n)$; pour terminer $(\forall n \in \mathbb{N}^*)\ n+1 > f(n) \geqslant n$, soit $f(n) = n$, ce qu'il fallait démontrer.

§ II.3 *ENSEMBLES FINIS, ENSEMBLES INFINIS ; ENSEMBLES DÉNOMBRABLES*

Exercice 1 :

Montrer que, pour qu'un ensemble E soit fini, il faut et il suffit que toute partie non vide de $\mathcal{P}(E)$ possède un élément maximal pour l'inclusion. ■

Si E est fini et $P \subset \mathcal{P}(E)$, un élément de P de cardinal maximum est maximal dans P, pour l'ordre de l'inclusion.
Supposons que toute partie non vide de $\mathcal{P}(E)$ possède un élément maximal pour l'inclusion. C'est vrai en particulier pour l'ensemble F des parties finies de E (F n'est pas vide, car $\emptyset$ est fini) ; il existe donc une partie finie A de E, maximale pour l'ordre de l'inclusion parmi les parties finies de E. Si x est un élément quelconque de E la partie $A \cup \{x\}$ est finie et contient A, par conséquent c'est A et $x \in A$. Donc $A = E$ et E est fini.

Exercice 4 :

a) $\mathbb{Z} = \mathbb{N} \cup \mathbb{Z}_-$ est évidemment dénombrable. Construire une bijection *explicite* de $\mathbb{Z}$ sur $\mathbb{N}$.

b) Soit $(p_n)_{n\in\mathbb{N}^*}$ la suite croissante des nombres premiers dans $\mathbb{N}^*$ $(p_1 = 2, p_2 = 3, \text{etc.})$. On note I l'ensemble $\mathbb{N}^{(\mathbb{N}^*)}$ des suites $(a_n)_{n\in\mathbb{N}^*}$ d'éléments de $\mathbb{N}$, *à support fini*, c'est-à-dire telles que l'ensemble $\{n \in \mathbb{N}^* \mid a_n \neq 0\}$ soit fini. De même on note J l'ensemble des suites $(\alpha_n)_{n\in\mathbb{N}^*}$ d'éléments de $\mathbb{Z}$ à support fini. On démontrera au chapitre sur les nombres premiers que l'application $\varphi : I \to \mathbb{N}^*$, $(a_n)_{n\geqslant 1} \mapsto \prod_{n\geqslant 1} p_n^{a_n}$ est bijective.
De même, l'application $\psi : J \to \mathbb{Q}_+^*$, $(\alpha_n)_{n\geqslant 1} \mapsto$

bijective. En déduire une bijection *explicite* de $\mathbb{N}^*$ sur $\mathbb{Q}_+^*$, à l'aide du a).

c) Construire une bijection explicite de $\mathbb{N}$ sur $\mathbb{Q}$. ■

a) Posons $f(n) = -2n$ si n est entier relatif $\leqslant 0$ et $f(n) = 2n - 1$ si n est entier > 0. On voit que f induit une bijection entre $\mathbb{Z}_-$ et l'ensemble des entiers naturels pairs, et une bijection entre $\mathbb{N}^*$ et l'ensemble des entiers naturels impairs. C'est donc une bijection entre $\mathbb{Z} = \mathbb{Z}_- \sqcup \mathbb{N}^*$ et $\mathbb{N}$.

b) Remarquons que $f(0) = 0$, et que par conséquent si la suite $(\alpha_n)_{n\geqslant 1}$ est élément de J, la suite $(f(\alpha_n))_{n\geqslant 1}$ est élément de I. Soit Φ l'application de J dans I définie par $\Phi((\alpha_n)_{n\geqslant 1}) = (f(\alpha_n))_{n\geqslant 1}$; il est clair que cette application est une bijection de J sur I. L'application $\theta = \psi \circ \Phi^{-1} \circ \varphi^{-1}$ est donc une bijection de $\mathbb{N}^*$ sur $\mathbb{Q}_+^*$.

c) Définissons l'application Θ de $\mathbb{Z}$ vers $\mathbb{Q}$ de la manière suivante : $\Theta(n) = -\theta(-n)$ si $n < 0$, $\Theta(0) = 0$, et $\Theta(n) = \theta(n)$ si $n > 0$. L'application Θ induit une bijection entre $\mathbb{N}_-^*$ et $\mathbb{Q}_-^*$ et induit aussi une bijection entre $\mathbb{N}_+^*$ et $\mathbb{Q}_+^*$; comme de plus $\Theta(0) = 0$, il est clair que l'application Θ est une bijection. L'application $\Theta \circ f^{-1}$ est alors une bijection de $\mathbb{N}$ vers $\mathbb{Q}$.

Exercice 5 :

Utiliser les théorèmes II.3.8 et II.3.10 pour prouver : si E est une ensemble infini et si $a \in E$, alors $E \setminus \{a\}$ est équipotent à E. Construire une bijection explicite de $[0,1]$ sur $[0,1[$. ■

Si A et B sont des ensembles disjoints, leur union sera notée ici $A \sqcup B$.
L'ensemble $E \setminus \{a\}$ étant infini, il existe une injection $\varphi : \mathbb{N} \to E \setminus \{a\}$. Notons $F = (E \setminus \{a\}) \setminus \varphi(\mathbb{N})$. Nous pouvons écrire :

$$E \setminus \{a\} = F \sqcup \varphi(\mathbb{N}) \quad \text{et} \quad E = F \sqcup \{a\} \sqcup \varphi(\mathbb{N}).$$

L'ensemble $\varphi(\mathbb{N})$ est équipotent à $\mathbb{N}$ et donc à $\mathbb{N}^*$; l'ensemble $\{a\} \sqcup \varphi(\mathbb{N})$ est par conséquent équipotent à $\{0\} \sqcup \mathbb{N}^* = \mathbb{N}$. Les deux ensembles $\varphi(\mathbb{N})$ et $\{a\} \sqcup \varphi(\mathbb{N})$ sont donc équipotents entre eux, et à l'ensemble $\mathbb{N}$. Les ensembles E et $E \setminus \{a\}$ sont donc équipotents.
Il suffit dans le cas particulier d'appliquer la méthode générale avec une injection explicite $\varphi : \mathbb{N} \to [0,1[$. Prenons par exemple $\varphi(n) = 1/(n+2)$. On obtient une bijection de $\theta : [0,1] \to [0,1[$ en posant :

$x \in [0,1]$ et x n'est pas l'inverse d'un entier, et si $x = 1/n$, n entier > 0, $\theta(x) = 1/(n+1)$.

§ II.4 *LOIS DE COMPOSITION. STRUCTURE DE GROUPE*

Exercice 4 :

Soit n et $p \in \mathbb{N}^*$, $n \neq p$. Démontrer que les monoïdes $(\mathbb{N}^n, +)$ et $(\mathbb{N}^p, +)$ ne sont pas isomorphes. Montrer également que $(\mathbb{N}^n, +)$ et $(\mathbb{N}^*, \times)$ ne sont pas isomorphes. ■

Pour p entier > 0 donné, notons $\mathcal{R}_p$ la relation binaire sur $\mathbb{N}^p$ définie par : $(x_1, x_2, \ldots, x_p)\,\mathcal{R}_p\,(y_1, y_2, \ldots, y_p)$ si, et seulement si, pour tout i dans $[\![1, p]\!]$, x_i et y_i ont la même parité. Il est clair qu'il s'agit d'une relation d'équivalence. L'ensemble quotient a 2^p éléments, nous le noterons E_p.
Supposons que Φ soit un isomorphisme de monoïde entre $(\mathbb{N}^n, +)$ et $(\mathbb{N}^p, +)$. Si $(x_1, x_2, \ldots, x_n)$ et $(y_1, y_2, \ldots, y_n)$ sont deux éléments de $\mathbb{N}^n$ équivalents pour la relation $\mathcal{R}_n$, alors pour tout i dans $[\![1, n]\!]$ l'entier $x_i + y_i$ est pair, notons le $2z_i$. Nous pouvons alors écrire :

$$\begin{aligned}\Phi((x_1, x_2, \ldots, x_n)) + \Phi((y_1, y_2, \ldots, y_n)) &= \\ = \Phi((x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)) &= \\ = \Phi((2z_1, 2z_2, \ldots, 2z_n)) = 2\,\Phi((z_1, z_2, \ldots, z_n))\ ;&\end{aligned}$$

cet élément de $\mathbb{N}^p$ est donc un p-uplet constitué de nombres pairs. Notons $\Phi((x_1, x_2, \ldots, x_n)) = (a_1, a_2, \ldots, a_p)$ et $\Phi((y_1, y_2, \ldots, y_n)) = (b_1, b_2, \ldots, b_p)$; nous avons montré que pour tout j dans $[\![1, p]\!]$, $a_j + b_j$ est pair, donc a_j et b_j ont la même parité. Les p-uplets $(a_1, a_2, \ldots, a_p)$ et $(b_1, b_2, \ldots, b_p)$ sont donc équivalents pour la relation $\mathcal{R}_p$. On peut donc définir une application de l'ensemble quotient E_n vers l'ensemble quotient E_p qui est surjective puisque Φ l'est. Nous en déduisons $2^n \geqslant 2^p$.
On démontrerait de manière analogue $2^p \geqslant 2^n$ en utilisant l'isomorphisme Φ^{-1}. Les monoïdes $(\mathbb{N}^n, +)$ et $(\mathbb{N}^p, +)$ ne sont donc isomorphes que si $n = p$.

Soit ε_i le n-uplet dont toutes les composantes sont nulles, sauf celle d'indice i qui vaut 1. Soit, s'il en existe, φ un homomorphisme de $(\mathbb{N}^n, +)$ vers $(\mathbb{N}^*, \times)$; posons pour tout i dans $[\![1, p]\!]$, $k_i = \varphi(\varepsilon_i)$. On voit facilement que :

$$(\forall (a_1, a_2, \ldots, a_n) \in \mathbb{N}^n) \quad \varphi((a_1, a_2, \ldots, a_n)) = k_1^{a_1} k_2^{a_2} \ldots k_n^{a_n}\ .$$

On peut alors prouver de multiples façons que φ ne peut pas être surjective. Par exemple un entier différent de 1 qui n'est divisible par aucun des nombres $k_1, k_2, \ldots, k_n$ (c'est le cas de l'entier $k_1 k_2 \ldots k_n + 1$) ne p

l'image. Il ne peut donc pas exister d'homomorphisme surjectif du monoïde $(\mathbb{N}^n, +)$ vers le monoïde $(\mathbb{N}^*, \times)$; a fortiori pas d'isomorphisme.

Exercice 7 :

‖ Montrer qu'un monoïde fini et régulier est un groupe. ■

Notons $(M, \star)$ le monoïde, et e son élément neutre. Pour un élément x de M donné, l'application $M \to M$, $y \mapsto x \star y$ est par hypothèse injective . Comme l'ensemble M est fini, cette application est aussi surjective. Nous pouvons en déduire en particulier que l'élément x a un inverse à droite x'_{d}. De même cet élément a un inverse à gauche que nous noterons x'_{g}. Ces deux inverses sont nécessairement identiques, en effet :

$$\begin{aligned}(x'_{\mathrm{g}} \star x) \star x'_{\mathrm{d}} &= e \star x'_{\mathrm{d}} = x'_{\mathrm{d}} \\ &= x'_{\mathrm{g}} \star (x \star x'_{\mathrm{d}}) = x'_{\mathrm{g}} \star e = x'_{\mathrm{g}} \ .\end{aligned}$$

Tout élément x de M est donc inversible. Le monoïde $(M, \star)$ est donc un groupe.

N.B. : si $(M, \star)$ est un ensemble fini non vide muni d'une loi de composition associative et régulière, alors $(M, \star)$ possède un élément neutre (c'est donc, d'après ce qui précède, un groupe). En effet, soit x un élément de M (qui est non vide), l'application $y \mapsto y \star x$ de M vers M est injective, donc surjective ; il existe donc un élément e dans M tel que $e \star x = x$; pour tout élément y de M, $y \star e \star x = y \star x$, d'où par régularité de la loi, $y \star e = y$; en particulier $x \star e = x$, donc pour tout y dans M, $x \star e \star y = x \star y$; nous en déduisons que pour tout y dans M, $e \star y = y$. L'élément e de M est donc l'élément neutre bilatère de $(M, \star)$.

Exercice 9 :

‖ Si G est un groupe et si $k \in \mathbb{Z}$, l'application $f_k : G \to G$, $x \mapsto x^k$ est-elle un homomorphisme de groupes ? ■

Nous noterons $\star$ la loi du groupe G. Si l'entier k est 0 ou 1, l'application f_k est évidemment un homomorphisme de groupes. Dans le cas général, c'est homomorphisme de groupes si, et seulement si :

$$(\forall (x, y) \in G \times G) \quad x^k y^k = (xy)^k.$$

Cette condition est réalisée si le groupe G est abélien.
Pour $k = 2$ la condition s'écrit :

$$(\forall (x, y) \in G \times G) \quad x \star x \star y \star y = x \star y \star x \star y.$$

En simplifiant nous obtenons :

$$(\forall (x,y) \in G \times G) \quad x \star y = y \star x.$$

L'application f_2 est donc un homomorphisme de groupes si, et seulement si, le groupe est abélien.
Pour $k = -1$ la condition s'écrit :

$$(\forall (x,y) \in G \times G) \quad x^{-1} \star y^{-1} = (x \star y)^{-1} = y^{-1} \star x^{-1} .$$

Il est donc clair que f_{-1} est un homomorphisme de groupes si, et seulement si, le groupe est abélien.

Exercice 11 :

> Soit G un groupe. On suppose qu'il existe $k \in \mathbb{N}^*$ tel que, pour tous $a \in G$ et $b \in G$: $(ab)^i = a^i b^i$ pour $i \in \{k-1, k, k+1\}$.
> Démontrer que G est abélien. ■

Pour $k = 1$ la seule condition est $(\forall (a,b) \in G \times G)$ $(ab)^2 = a^2 b^2$. Nous avons déjà vu dans la résolution de l'exercice 9 que cette condition est réalisée si, et seulement si, le groupe est abélien. Nous supposerons dans la suite $k > 1$.

Si a et b sont des éléments quelconques de G , comme $a^{k-1}b^{k-1} = (ab)^{k-1}$, et $(ab)^k = a^k b^k$, nous en déduisons :

$$a^k b^k = (ab)^k = (ab)^{k-1} ab = a^{k-1} b^{k-1} ab,$$

donc en simplifiant à gauche par a^{k-1} et à droite par b , nous obtenons $ab^{k-1} = b^{k-1}a$. En remplaçant dans le raisonnement ci-dessus k par $k+1$, nous obtenons de manière analogue $ab^k = b^k a$; donc $ab^k = bb^{k-1}a = bab^{k-1}$, soit encore $abb^{k-1} = bab^{k-1}$; en simplifiant par b^{k-1} à droite, nous obtenons finalement $ab = ba$.
Le groupe G est donc abélien.

§ II.5 *L'ANNEAU DES ENTIERS RELATIFS, LA STRUCTURE D'ANNEAU*

Exercice 5 :

> Pour $n \in \mathbb{N}^*$ trouver les homomorphismes d'anneaux de $\mathbb{Z}^n$ dans $\mathbb{Z}$. ■

Pour i dans $[\![1, n]\!]$ notons ε_i le n-uplet élément de $\mathbb{Z}^n$ dont toutes les composantes sont 0 , sauf celle d'indice i qui vaut 1 ; la multip

$\mathbb{Z}^n$ est telle que $\varepsilon_i \times \varepsilon_i = \varepsilon_i$, et si j est un indice différent de i, $\varepsilon_i \times \varepsilon_j = 0$. Soit $\varphi : \mathbb{Z}^n \to \mathbb{Z}$ un homomorphisme d'anneau ; posons pour tout i dans $[\![1, n]\!]$, $\varphi(\varepsilon_i) = k_i$. Nous pouvons déduire de ce qui précède que pour tout i dans $[\![1, n]\!]$, $k_i^2 = k_i$, donc $k_i = 0$, ou $k_i = 1$, et si j est un indice différent de i, $k_i k_j = 0$. On voit alors que soit tous les nombres k_i sont nuls, soit un seul d'entre eux n'est pas nul, et vaut 1.
D'autre part :

$$\forall (a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n \quad (a_1, a_2, \ldots, a_n) = \sum_{i=1}^{n} a_i \cdot \varepsilon_i.$$

Comme φ est un homomorphisme pour l'addition, on voit que :

$$\forall (a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n \quad \varphi((a_1, a_2, \ldots, a_n)) = \sum_{i=1}^{n} a_i \cdot \varphi(\varepsilon_i) = \sum_{i=1}^{n} a_i \cdot k_i.$$

Il est impossible que tous les nombres k_i soient nuls, car l'application φ serait nulle, ce qui contredit $\varphi((1, 1, \ldots, 1)) = 1$; donc un et un seul des k_i n'est pas nul et vaut 1. L'homomorphisme $\varphi : \mathbb{Z}^n \to \mathbb{Z}$ est donc nécessairement la projection sur l'une des composantes. Ces n applications étant bien des homomorphismes d'anneaux, ce sont les homomorphismes d'anneaux de $\mathbb{Z}^n$ dans $\mathbb{Z}$.

Exercice 7 :

> Dans un anneau A, on suppose $(\forall x \in A)\ x^2 = x$. Montrer que A est commutatif. Si A contient au moins 3 éléments distincts montrer qu'il a nécessairement des diviseurs de zéro. Montrer qu'en fait A ne peut avoir exactement 3 éléments. *Nota* : A est appelé un *anneau de Boole*. ■

Soit n un entier relatif, nous noterons aussi n, l'élément $n \cdot 1_A$ de l'anneau A. De l'égalité $4 = 2^2 = 2$, nous déduisons $2 = 0$; l'anneau A est donc de caractéristique 2. D'autre part, pour tous x et y éléments de A nous pouvons écrire :

$$(x + y)^2 = xx + xy + yx + yy = x + xy + yx + y = x + y.$$

Donc $(\forall (x, y) \in A \times A)\ xy = -yx = yx$; l'anneau A est par conséquent commutatif, et de caractéristique 2.
Si A a au moins trois éléments distincts, ce n'est pas l'anneau nul, donc $1 \neq 0$, et il a au moins un élément x, distinct de 0 et de 1. De l'égalité $xx = x = x \times 1$, nous déduisons $x(x - 1) = 0$; comme les éléments x et $x - 1$ ne sont pas nuls, l'anneau A a des diviseurs de zéro.
Supposons que l'anneau A ait au moins 3 éléments, alors $0 \neq$

un élément c différent de 0 et de 1. L'élément $c-1$ de A ne peut être ni 0, ni c, ni $1=-1$. L'anneau A a donc au moins 4 éléments. L'anneau $\left(\mathbb{Z}/_{2\mathbb{Z}}\right)^2$ est un anneau de Boole à 4 éléments (voir chapitre IV).

Exercice 8 :

Dans un anneau A, on suppose $(\forall x \in A)\ x^3 = x$. Montrer que A est commutatif. ■

Soit n un entier relatif, nous noterons aussi n, l'élément $n \cdot 1_A$ de l'anneau A. De l'égalité $8 = 2^3 = 2$, nous déduisons $6 = 0$ ou encore $3 = -3$. Pour tout x dans A nous obtenons :

$$(x-1)^3 = x^3 - 3x^2 + 3x - 1 = x - 3x^2 + 3x - 1 = x - 1 \quad \text{soit} \quad 3x^2 = 3x.$$

D'où, pour tous x et y éléments de A :

$$3(x+y)^2 = 3x^2 + 3(xy+yx) + 3y^2 = 3x + 3(xy+yx) + 3y = 3(x+y)$$
$$\text{soit} \quad 3xy = -3yx = 3yx.$$

Nous obtenons aussi :

$$(x+y)^3 = x^3 + xyx + yx^2 + y^2x + x^2y + xy^2 + yxy + y^3 = x + y$$

et

$$(x-y)^3 = x^3 - xyx - yx^2 + y^2x - x^2y + xy^2 + yxy - y^3 = x - y,$$

d'où par différence :

$$(x+y)^3-(x-y)^3 = 2(xyx+yx^2+x^2y+y^3) = 2y \quad \text{soit} \quad 2(xyx+yx^2+x^2y) = 0.$$

Posons $z = xyx + yx^2 + x^2y$. On voit que :

$$xz - zx = x^2yx + xyx^2 + x^3y - xyx^2 - yx^3 - x^2yx = xy - yx.$$

Comme $2z = 0$, nous en déduisons $2xy = 2yx$. Nous avions démontré plus haut que $3xy = 3yx$, donc par différence $xy = yx$. Ceci étant vrai pour tous x et y éléments de l'anneau A, cet anneau est nécessairement commutatif.

Exercice 10 :

Soit $\mathcal{S}_t$ le sous-ensemble de l'anneau $\mathbb{Z}^{\mathbb{N}}$ formé des suites stationnaires d'entiers relatifs.
a) Vérifier que $\mathcal{S}_t$ est un sous-anneau de $\mathbb{Z}^{\mathbb{N}}$.

‖ *b*) Trouver tous les homomorphismes d'anneaux : $\mathcal{S}_t \to \mathbb{Z}$. ■

a) La suite constante égale à 1, élément neutre pour la multiplication dans l'anneau $\mathbb{Z}^{\mathbb{N}}$, est stationnaire ; si (u_n) est une suite d'entiers relatifs stationnaire à partir du rang p, et que (v_n) est une suite d'entiers relatifs stationnaire à partir du rang q, alors les suites $(u_n - v_n)$ et $(u_n v_n)$ sont stationnaires à partir de rangs $\leqslant \sup(p, q)$. Le sous-ensemble des suites stationnaires est donc un sous-anneau de $\mathbb{Z}^{\mathbb{N}}$.

b) Pour tout entier naturel i notons ε_i la suite dont tous les termes sont nuls, sauf le terme d'indice i qui vaut 1 ; ces suites sont stationnaires. Soit $\varphi : \mathcal{S}_t \to \mathbb{Z}$ un homomorphisme d'anneaux ; posons pour tout $i \in \mathbb{N}$, $\varphi(\varepsilon_i) = k_i$. On vérifie comme dans l'exercice 5 que les nombres k_i sont tous 0 ou 1 et que soit tous les k_i sont nuls, soit un et un seul d'entre eux n'est pas nul. Notons aussi I la suite constante égale à 1 ; c'est l'élément neutre multiplicatif de l'anneau, donc $\varphi(I) = 1$. Si la suite u est stationnaire au moins à partir du rang p, de valeur stationnaire a, nous pouvons écrire :

$$u = \sum_{i=1}^{p-1} (u_i - a)\varepsilon_i + a \cdot I.$$

Donc :

$$\varphi(u) = \sum_{i=1}^{p-1} (u_i - a)k_i + a \ .$$

Si tous les k_i sont nuls, l'application φ est nécessairement l'application qui à une suite stationnaire fait correspondre sa valeur stationnaire ; cette application est effectivement un homomorphisme d'anneau.
Si l'un des k_i n'est pas nul, posons $k_q = 1$; on peut supposer $q < p$, donc :

$$\varphi(u) = (u_q - a) + a = u_q.$$

Dans ce cas l'application φ est nécessairement l'application $u \mapsto u_q$. Il est clair que pour toute valeur de l'entier q, on obtient bien ainsi un homomorphisme d'anneaux de $\mathbb{Z}^{\mathbb{N}}$ vers $\mathbb{Z}$.

En conclusion, les homomorphismes cherchés sont les applications coordonnées et l'application qui à une suite stationnaire fait correspondre sa valeur stationnaire.

Exercice 13 :

‖ Soit A un anneau. On suppose, pour tout couple (

$\|$: $(ab)^2 = a^2b^2$. Démontrer que A est commutatif. ■

Pour tous x et y éléments de A :

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

D'où par différence $xy^2 = yxy$.
En appliquant cette égalité à x et $y+1$, nous obtenons :

$$x(y+1)^2 = xy^2 + 2xy + x = yxy + 2xy + x$$
$$= (y+1)x(y+1) = yxy + yx + xy + x.$$

Par différence nous obtenons : $xy - yx = 0$. L'anneau A est donc néces sairement commutatif.

§ II.6 *LES NOMBRES RATIONNELS, LA STRUCTURE DE CORPS*

Exercice 4 :

$\|$ Trouver tous les triplets $(x, y, z) \in (\mathbb{N}^*)^3$ tels que :
$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1 \,.$$ ■

Nous pouvons supposer $x \leqslant y \leqslant z$. Comme $1/x < 1$, nous en déduisons $x > 1$, donc $x \geqslant 2$.
Supposons $x = 2$. La condition devient :

$$\frac{1}{y} + \frac{1}{z} = \frac{1}{2} \quad \text{soit} \quad 2(y+z) = yz.$$

Nous pouvons encore écrire cela sous la forme : $(y-2)(z-2) = 4$. Les solutions (y, z) , en nombres entiers $\geqslant 1$, telles que $y \leqslant z$, sont $(y, z) = (3, 6)$ et $(y, z) = (4, 4)$; ce qui correspond aux égalités :

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1 \quad \text{et} \quad \frac{1}{2} + \frac{1}{4} + \frac{1}{4} = 1.$$

Supposons $3 \leqslant x \leqslant y \leqslant z$.
Nous observons que :

$$\frac{1}{y} + \frac{1}{z} = 1 - \frac{1}{x} \geqslant 1 - \frac{1}{3} = \frac{2}{3} \quad \text{soit} \quad 3(y+z) \geqslant 2yz$$

Posons $y' = y - 3$ et $z' = z - 3$, on peut écrire la condition ci-dessus sous la forme :

$$3(y' + z' + 6) \geqslant 2(y' + 3)(z' + 3) \quad \text{soit} \quad 0 \geqslant 2y'z' + 3y' + 3z'.$$

La seule solution possible en nombres $\geqslant 0$ est $x' = 0$ et $y' = 0$, d'où $y = 3$ et $z = 3$, ce qui implique $x = 3$. On vérifie facilement que le triplet $(3, 3, 3)$ est solution puisque :

$$\frac{1}{3} + \frac{1}{3} + \frac{1}{3} = 1.$$

En conclusion, les triplets croissants vérifiant la condition de l'énoncé, sont les triplets $(1, 3, 6)$, $(2, 4, 4)$ et $(3, 3, 3)$.

Exercice 5 :

Trouver tous les triplets $(x, y, z) \in (\mathbb{N}^*)^3$ tels que $xyz = 1 + x + y + z$. ■

Nous pouvons supposer $1 \leqslant x \leqslant y \leqslant z$. La condition équivaut à :

$$xyxz = x + x^2 + xy + xz \quad \text{soit} \quad (xy - 1)(xz - 1) = 1 + x + x^2.$$

En minorant y et z par x nous obtenons : $(x^2-1)^2 \leqslant 1+x+x^2$, soit encore $x^4 - 3x^2 - x \leqslant 0$, d'où enfin $x^3 \leqslant 3x+1$. Si $x \geqslant 2$, alors $3x+1 < 4x \leqslant x^3$, ce qui est exclu ; donc $x = 1$. La condition s'écrit alors : $(y-1)(z-1) = 3$. La seule solution (y, z) en nombres entiers où $y \leqslant z$ est donc $(y, z) = (2, 4)$. La seule solution pour (x, y, z) est donc le triplet $(1, 2, 4)$, ce qui correspond à l'identité :

$$1 \times 2 \times 4 = 1 + 1 + 2 + 4.$$

Exercice 9 :

Démontrer, pour $n \in \mathbb{N}$, $n \geqslant 2$, que $S_n = \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} \notin \mathbb{N}$; généraliser pour $T_n = \frac{1}{a+b} + \frac{1}{a+2b} + \ldots + \frac{1}{a+nb}$, où a et $b \in \mathbb{N}^*$. ■

Nous ne traiterons pas le cas particulier $b = 1$, car sa résolution n'est pas différente de la résolution du cas général b impair. Nous utiliserons des notions d'arithmétique qui seront vues dans le chapitre IV.

On peut supposer que les entiers a et b sont premiers entre eux. En effet, posons $d = \text{pgcd}(a, b)$, et $a = da'$, $b = db'$. Si T_n est

$T'_n = \dfrac{1}{a'+b'} + \dfrac{1}{a'+2b'} + \ldots + \dfrac{1}{a'+nb'} = dT_n$, est aussi entier, et a' et b' sont premiers entre eux.

On suppose d'abord que b est impair.
Les nombres $a+b, a+2b, \ldots, a+nb$, sont alternativement pairs et impairs ; comme il y en a au moins 2, l'un d'eux est divisible par 2. Soit α le plus grand entier tel que 2^α divise l'un de ces nombres, d'après ce qui précède, $\alpha > 0$. Montrons que 2^α divise un seul de ces nombres. Sinon, si 2^α divise $a+ib$ et $a+jb$, où $1 \leqslant i < j \leqslant n$, alors 2^α divise $(j-i)b$ donc divise $(j-i)$; nous en déduisons : $1 \leqslant i < i+2^\alpha \leqslant j \leqslant n$, mais comme $a+ib$ est de la forme $(2k+1)2^\alpha$, le nombre $a+(i+2^\alpha)b$ est de la forme $(2k+1+b)2^\alpha$, donc divisible par $2^{\alpha+1}$ puisque b est impair, ce qui contredit la définition de α .
Le ppcm des nombres $a+b, a+2b, \ldots, a+nb$ est de la forme $\Pi = 2^\alpha(2h+1)$; quand on réduit les fractions $\dfrac{1}{a+b}, \dfrac{1}{a+2b}, \ldots, \dfrac{1}{a+nb}$ à leur dénominateur commun on trouve des numérateurs tous pairs sauf un. La somme T_n est donc une fraction de la forme : $\dfrac{2p+1}{2^\alpha(2q+1)}$ $(\alpha > 0)$, et ne peut donc être un entier.

Supposons maintenant que b est pair, nous poserons $b = 2b'$. Remarquons que comme a et b sont premiers entre eux, a est impair.
On raisonne ici par l'absurde, en supposant que T_n est un entier, donc $\geqslant 1$.
Etablissons d'abord quelques inégalités.
En majorant toutes les fractions par $1/(a+b)$, ce qui donne une majoration stricte de T_n , on obtient : $n/(a+b) > T_n \geqslant 1$, donc $n > a+b \geqslant 3$, soit $n \geqslant 4$.
D'autre part :

$$T_n = \frac{1}{a+b} + \frac{1}{a+2b} + \ldots + \frac{1}{a+nb} < \frac{1}{b} + \frac{1}{2b} + \ldots + \frac{1}{nb} = \\ = \frac{1}{b}\left(1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}\right).$$

On démontre alors facilement par des méthodes d'analyse que $1 \leqslant T_n < (1/b)(1+\ln n)$, soit $\ln(n) > b-1$.

Soit p le plus grand nombre premier $\leqslant n$, donc $p \geqslant 3$; d'après le théorème de Bertrand, on sait que $n < 2p$. Le lecteur pourra trouver une démonstration de ce théorème dans : HARDY G. H., WRIGHT E. M., *An introduction to the theory of numbers,* Oxford Un. Press, 1959.
Comme $n > a+b$, d'où $n > b$, on voit que $p > b'$, donc p est premier avec b' , et avec b . Parmi les nombres $a+b, a+2b, \ldots, a+nb$, l'un au moins est divisible par p ; en effet l'équation en i entier $a+ib \equiv 0 \ [p]$ a exactement une solution dans chaque intervalle de p entiers successifs p

premier avec p.
Si un seul de ces nombres est divisible par p, en raisonnant comme dans le cas où b est impair, on voit que T_n peut s'exprimer sous la forme $\frac{u}{p^\alpha v}$, où $\alpha \geqslant 1$, u et v entiers premiers avec p ; le nombre T_n ne peut donc être entier, il y a contradiction.
Dans le cas contraire, exactement deux des nombres $a+b, a+2b, \ldots, a+nb$ sont divisibles par p, car $n < 2p$. Ces deux nombres sont $a+ib = kp$ et $a+ib+pb = (k+b)p$ (k est impair puisque comme a est impair, les nombres $a+b, a+2b, \ldots, a+nb$ sont tous impairs). Or :

$$\frac{1}{a+ib} + \frac{1}{a+(i+p)b} = \frac{1}{kp} + \frac{1}{(k+b)p} = \frac{2k+p}{pk(k+b)} .$$

Si p ne divise pas $2k+b$, on peut encore utiliser l'argument du cas précédent, et il y a contradiction.
Si p divise $2k+b = 2(k+b')$, alors p divise $k+b'$, et par conséquent $p \leqslant k+b'$. Mais $a+(i-p)b = (k-b)p < a+b \leqslant a+ib = kp$, donc $k-b < (a+b)/p < 2(a+b)/n < 2$, soit $k < b+2$ ou encore $k \leqslant b+1$. Nous pouvons déduire de ce qui précède : $p \leqslant 3b'+1$ et $n < 2(3b'+1) = 3b+2$, soit enfin $n \leqslant 3b+1$.
Rappelons que $b-1 < \ln(n)$; d'où $\exp(b-1) < 3b+1$ soit :

$$\frac{e^{b-1}-1}{b-1} < \frac{3b}{b-1} = 3 + \frac{3}{b-1} .$$

Si $b \geqslant 4$, c'est impossible car :

$$\frac{e^{b-1}-1}{b-1} \geqslant \frac{e^3-1}{3} > 6.$$

(en utilisant la convexité de la fonction exponentielle), alors que :

$$3 + \frac{3}{b-1} \leqslant 3 + \frac{3}{3} = 4.$$

Il reste à examiner le cas $b = 2$, soit $b' = 1$. Dans ce cas, $p \leqslant 3b'+1 = 4$; comme $p \geqslant 3$ et p premier, nécessairement $p = 3$. Comme $k \leqslant b+1$, $k \leqslant 3$ et k est impair ; il faudrait donc que le nombre premier 3 divise $k+b'$ égal à 2 ou 4, ce qui est impossible.
Le nombre T_n ne peut donc être dans aucun cas entier.

Exercice 13 :

Résoudre dans $\mathbb{N}^2$ l'équation $\frac{x-y}{x^2+xy+y^2} = \frac{2}{67}$, où x et y ne sont pas tous les deux nuls. ■

La condition s'écrit : $67(x-y) = 2(x^2+xy+y^2)$. Nous voyons que néces sairement $x > y$ et que $x-y$ est pair. Posons $x+y = 2u$ et $x-y = 2v$, d'où $u \geqslant v > 0$, $x = u+v$, $y = u-v$. La condition devient :

$$67v = (u+v)^2 + (u+v)(u-v) + (u-v)^2 = 3u^2 + v^2,$$

ce qui s'écrit aussi $(67-v)v = 3u^2$. Nous pouvons remarquer que $(67-v)v = 3u^2 \geqslant 3v^2$, donc $4v \leqslant 67$, soit $v \leqslant 16$. Un peu d'arithmétique permet d'accélérer cette recherche qui donne une seule solution : $u = 8$, $v = 3$ donc $x = 11$, $y = 5$.

Les nombres entiers $(67-v)$ et v sont premiers entre eux, en effet si un nombre premier les divisait tous les deux, il diviserait 67 donc serait 67 ; mais alors 67 diviserait v, donc $v \geqslant 67$, ce qui est exclu. L'un des deux est divisible par 3.
Si v est divisible par 3, en posant $v = 3v'$, la condition s'écrit : $(67-3v')v' = u^2$. Comme $67-3v'$ et v' sont premiers entre eux, chacun d'eux est un carré. L'entier v' est donc un carré plus petit que 16, il ne peut être que 1, 4, 9 ou 16, ce qui donne pour valeurs de $67-3v'$ les nombres 64, 55, 40 et 19. Comme 64 est le seul carré d'entier parmi ces 4 nombres, la seule solution est $v' = 1$, d'où $v = 3$ et $u = 8$.
Si $w = 67-v$ est divisible par 3, posons $w = 3w'$. L'entier w' est un carré majoré par $67/3$ et minoré par $(67-16)/3 = 17$, il est facile de voir qu'il n'y a aucun carré d'entier dans cet intervalle.
La seule solution est donc $(x,y) = (11,5)$.

Exercice 17 :

> *a*) Le seul automorphisme du corps $\mathbb{Q}$ est $\mathrm{Id}_{\mathbb{Q}}$, et c'est le seul isomorphisme de $\mathbb{Q}$ dans $\mathbb{Q}$.
>
> *b*) Montrer que le seul isomorphisme du corps $\mathbb{R}$ dans lui-même est l'automorphisme $\mathrm{Id}_{\mathbb{R}}$. ■

a) Si f est un isomorphisme de $\mathbb{Q}$ dans $\mathbb{Q}$, alors pour tout entier relatif p et tout entier q, $q > 0$:

$$q \cdot f\left(\frac{p}{q}\right) = f\left(q \cdot \frac{p}{q}\right) = f(p) = p \cdot f(1) = p \cdot 1 = p,$$

d'où :

$$f\left(\frac{p}{q}\right) = \frac{p}{q}\,.$$

L'isomorphisme f est donc nécessairement l'identité de $\mathbb{Q}$. L'identité est a fortiori le seul automorphisme du corps $\mathbb{Q}$.

b) Soit σ un isomorphisme du corps $\mathbb{R}$ dans lui-même. Pour tout entier relatif p, tout entier q, $q > 0$, et tout réel x, nous pouvons écrire :

$$q \cdot \sigma\left(\frac{p}{q} \cdot x\right) = \sigma\left(q \cdot \frac{p}{q} \cdot x\right) = \sigma(p \cdot x) = p \cdot \sigma(x),$$

d'où :

$$\sigma\left(\frac{p}{q} \cdot x\right) = \frac{p}{q} \cdot \sigma(x).$$

Nous dirons que l'application σ est $\mathbb{Q}$-linéaire. Nous en déduisons facilement, en prenant $x = 1$, que la restriction de σ à $\mathbb{Q}$ est l'identité.
Si x est un réel > 0, on sait que c'est le carré d'un réel y ; donc $\sigma(x) = \sigma(y^2) = (\sigma(y))^2 > 0$. Si maintenant x et y sont deux réels et $x > y$, alors $\sigma(x) - \sigma(y) = \sigma(x - y) > 0$, donc $\sigma(x) > \sigma(y)$. L'application σ est donc strictement croissante. Supposons que l'application σ ne soit pas l'identité ; il existe alors un réel x tel que $\sigma(x) \neq x$.
Si $\sigma(x) < x$, alors il existe un rationnel r, tel que $\sigma(x) < r < x$ (propriété bien connue des réels) ; comme σ est strictement croissante, on obtient $r = \sigma(r) < \sigma(x)$, ce qui est contradictoire.
Si $\sigma(x) > x$, il existe un rationnel r tel que $\sigma(x) > r > x$, d'où $r = \sigma(r) > \sigma(x)$, ce qui est contradictoire. L'isomorphisme σ est donc nécessairement l'automorphisme $\mathrm{Id}_{\mathbb{R}}$.

Chapitre III

BASES DU CALCUL ALGÉBRIQUE ET COMBINATOIRE

§ III.3 *COMPOSÉ DE FAMILLES A SUPPORT FINI. NUMÉRATION*

Exercice 1 :

(*numération anglaise*) : Soit $(r_k)_{k\geqslant 1}$ une suite d'entiers > 1 ; on considère l'ensemble $\mathscr{A}_r$ des suites *à support fini* $s = (s_i)_{i\in\mathbb{N}}$ d'entiers tels que $s_i < r_{i+1}$ pour tout $i \geqslant 0$. Montrer que l'application :

$$\mathscr{A}_r \to \mathbb{N}, \quad s \mapsto \sum_{i\in\mathbb{N}} s_i \left(\prod_{k=1}^{i} r_k\right) = s_0 + s_1 r_1 + s_2 r_1 r_2 + \dots$$

est bijective. ■

Associons à tout entier n la suite $(n_i)_{i\in\mathbb{N}}$ telle que $n_0 = n$ et telle que pour tout i entier, n_{i+1} soit le quotient dans la division euclidienne de n_i par r_{i+1}.

Montrons que l'application introduite par l'énoncé est injective.
Si $n = s_0 + s_1 r_1 + s_2 r_1 r_2 + \dots$, montrons que pour tout i entier, $n_i = s_i + s_{i+1} r_{i+1} + s_{i+2} r_{i+1} r_{i+2} + \dots$, la suite $(n_i)_{i\in\mathbb{N}}$ étant la suite associée à l'entier n. C'est vrai pour $i = 0$ et si c'est vrai pour i, comme $s_i < r_{i+1}$, s_i est le reste dans la division euclidienne de n_i par r_{i+1} et le quotient est $n_{i+1} = s_{i+1} + s_{i+2} r_{i+2} + s_{i+3} r_{i+2} r_{i+3} + \dots$. Cette égalité est donc vraie pour tout i entier. On voit aussi que pour tout i entier, s_i est nécessairement le reste dans la division euclidienne de n_i par r_{i+1}. Cela démontre l'unicité de la suite $(s_i)_{i\in\mathbb{N}}$, l'entier n étant fixé. L'application introduite par l'énoncé est donc injective.

Montrons qu'elle est surjective.
Il suffit de montrer que la suite $(s_i)_{i\in\mathbb{N}}$ trouvée ci-dessus a bie

l'entier n. Montrons pour cela que pour tout $i > 0$:

(E_i) $\quad n = s_0 + s_1 r_1 + \ldots + s_{i-1} r_1 r_2 \ldots r_{i-1} + n_i r_1 r_2 \ldots r_{i-1} r_i.$

Pour $i = 1$ cette égalité s'écrit $n = s_0 + n_1 r_1$, ce qui est vrai. Si l'égalité est vraie pour i, alors en remplaçant dans (E_i), n_i par $s_i + n_{i+1} r_{i+1}$, on obtient l'égalité (E_{i+1}). L'égalité (E_i) est donc vraie pour tout entier i. Si pour tout j, $n_j > 0$, alors pour tout i, $n_i > n_{i+1}$ (puisque $r_{i+1} > 1$), ce qui est impossible ; il existe donc un entier j tel que $n_j = 0$. On voit facilement que pour tout $i \geqslant j$, $n_i = s_i = 0$. Les suites $(n_i)_{i \in \mathbb{N}}$ et $(s_i)_{i \in \mathbb{N}}$ sont par conséquent à support fini, et comme :

$$n = s_0 + s_1 r_1 + \ldots + s_{j-1} r_1 r_2 \ldots r_{j-1}$$

on voit que :

$$n = \sum_{i \in \mathbb{N}} s_i \left(\prod_{k=1}^{i} r_k \right).$$

Cela démontre que l'application introduite dans l'énoncé est surjective. Elle est donc bijective, ce qu'il fallait démontrer.

§ III.4 *DÉNOMBREMENT*

Exercice 2 :

Pour $n \in \mathbb{N}^*$ montrer que :
$1\,1! + 2\,2! + \ldots + n\,n! = (n+1)! - 1$. ■

On vérifie que pour tout i entier : $i\,i! = ((i+1) - 1)i! = (i+1)! - i!$, donc pour tout $n \in \mathbb{N}^*$:

$$1\,1! + 2\,2! + \ldots + n\,n! = (2! - 1!) + (3! - 2!) + \ldots + ((n+1)! - n!) = (n+1)! - 1,$$

ce qu'il fallait démontrer.

Exercice 4 :

Soit $\alpha \in \mathbb{C}$, n et $r \in \mathbb{N}$. Montrer que :
$$\sum_{i=0}^{n} \binom{\alpha - i}{r} = \binom{\alpha + 1}{r+1} - \binom{\alpha - n}{r+1} \cdot \blacksquare$$

On sait que (voir l'exemple 3 du paragraphe III.4) pour tout $\alpha \in \mathbb{C}$ et $r \in \mathbb{N}$:

$$\binom{\alpha+1}{r+1} = \binom{\alpha}{r+1} + \binom{\alpha}{r} \quad \text{soit} \quad \binom{\alpha+1}{r+1} - \binom{\alpha}{r+1} = \binom{\alpha}{}$$

Nous pouvons donc écrire :

$$\sum_{i=0}^{n}\binom{\alpha-i}{r}=\sum_{i=0}^{n}\binom{\alpha-i+1}{r+1}-\sum_{i=0}^{n}\binom{\alpha-i}{r+1}=$$
$$=\binom{\alpha+1}{r+1}-\binom{\alpha-n}{r+1},$$

ce qu'il fallait démontrer.

Exercice 5 :

Soit p, q, n des entiers tels que $0 \leqslant q < p \leqslant n$. Etablir la relation :

$$\sum_{k=q+1}^{k=n-p+q+1}\binom{n-k}{p-(q+1)}\binom{k-1}{q}=\binom{n}{p}.$$

En déduire : $\displaystyle\sum_{k=0}^{n}2^k\binom{2n-k}{n}=2^{2n}$. ■

Une partie P de $[\![1,n]\!]$, de cardinal p, peut être identifiée à une suite strictement croissante de p entiers $(x_1,x_2,\ldots,x_i,\ldots,x_p)$, à valeurs dans $[\![1,n]\!]$. Nous dirons que l'élément x_i, où $i\in[\![1,n]\!]$, est l'élément de numéro i dans P.
Pour tout $k\in[\![1,n]\!]$, notons A_k l'ensemble des parties de $[\![1,n]\!]$ de cardinal p et dont l'élément de numéro $q+1$ est k. Une partie P est élément de A_k si, et seulement si, elle est constituée d'une partie de $[\![1,k-1]\!]$ qui a q éléments, de l'élément k, et d'une partie de $[\![k+1,n]\!]$ qui a $p-(q+1)$ éléments. L'ensemble A_k est non vide si, et seulement si : $q\leqslant k-1$, soit $k\geqslant q+1$, et $p-(q+1)\leqslant n-k$ soit $k\leqslant n-p+q+1$. D'après ce qui précède, le cardinal de A_k est $\binom{n-k}{p-(q+1)}\binom{k-1}{q}$. Comme la famille $(A_k)_{k\in[\![q+1,n-p+q+1]\!]}$ est un partage de l'ensemble des parties de $[\![1,n]\!]$ de cardinal p, nous en déduisons :

$$\sum_{k=q+1}^{k=n-p+q+1}\binom{n-k}{p-(q+1)}\binom{k-1}{q}=\binom{n}{p}.$$

Comme pour tout i entier $2^i=\displaystyle\sum_{q=0}^{i}\binom{i}{q}$, nous voyons que pour tout m entier :

$$(1)\qquad \sum_{i=0}^{m}2^i\binom{2m-i}{m}=\sum_{i=0}^{m}\sum_{q=0}^{i}\binom{i}{q}\binom{2m-i}{m}.$$

En intervertissant l'ordre des sommations nous obtenons :

$$\sum_{i=0}^{m} 2^i \binom{2m-i}{m} = \sum_{q=0}^{m} \sum_{i=q}^{m} \binom{i}{q} \binom{2m-i}{m} =$$

$$= \sum_{q=0}^{m} \sum_{k=q+1}^{m+1} \binom{2m+1-k}{m} \binom{k-1}{q} .$$

Pour $q \in [\![0, m]\!]$, posons $p = m+q+1$ et $n = 2m+1$, on vérifie que $0 \leqslant q < p \leqslant n$, que $p-(q+1) = m$, que $n-p+q+1 = m+1$, et que pour tout k entier, $n-k = 2m+1-k$. En utilisant la formule (1) démontrée ci-dessus, on obtient :

$$\sum_{k=q+1}^{m+1} \binom{k-1}{q} \binom{2m+1-k}{m} = \binom{2m+1}{m+q+1} .$$

Donc :

$$\sum_{i=0}^{m} 2^i \binom{2m-i}{m} = \sum_{q=0}^{m} \binom{2m+1}{m+q+1} = \sum_{q=0}^{m} \binom{2m+1}{m-q} =$$

$$= \frac{1}{2} \sum_{h=0}^{2m+1} \binom{2m+1}{h} = \frac{1}{2} 2^{2m+1} = 2^{2m} .$$

Exercice 8 :

Démontrer, pour $q \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$:

$$\sum_{k=0}^{n-1} \frac{1}{2^k} \binom{q+k-1}{k} = \frac{1}{2^{n-1}} \sum_{k=0}^{n-1} \binom{q+n-1}{k} .$$

Cas particulier où $q = n$. ■

Posons pour q et n entiers > 0,

$$u_{q,n} = \sum_{k=0}^{n-1} \frac{1}{2^k} \binom{q+k-1}{k} \quad \text{et} \quad v_{q,n} = \frac{1}{2^{n-1}} \sum_{k=0}^{n-1} \binom{q+n-1}{k} .$$

En utilisant la relation de Pascal, nous obtenons, si $n > 1$ et

$$u_{q,n} = 1 + \sum_{k=1}^{n-1} \frac{1}{2^k} \binom{q+k-1}{k} =$$

$$= 1 + \sum_{k=1}^{n-1} \frac{1}{2^k} \binom{q+k-2}{k} + \sum_{k=1}^{n-1} \frac{1}{2^k} \binom{q+k-2}{k-1} =$$

$$= \sum_{k=0}^{n-1} \frac{1}{2^k} \binom{q+k-2}{k} + \frac{1}{2} \sum_{h=0}^{n-2} \frac{1}{2^h} \binom{q+h-1}{h} =$$

$$= u_{q-1,n} + \frac{1}{2} u_{q,n-1} \ .$$

De manière analogue :

$$v_{q,n} = \frac{1}{2^{n-1}} \sum_{k=0}^{n-1} \binom{q+n-1}{k} = \frac{1}{2^{n-1}} + \frac{1}{2^{n-1}} \sum_{k=1}^{n-1} \binom{q+n-1}{k} =$$

$$= \frac{1}{2^{n-1}} + \frac{1}{2^{n-1}} \sum_{k=1}^{n-1} \binom{q+n-2}{k} + \frac{1}{2^{n-1}} \sum_{k=1}^{n-1} \binom{q+n-2}{k-1} =$$

$$= \frac{1}{2^{n-1}} \sum_{k=0}^{n-1} \binom{q+n-2}{k} + \frac{1}{2^{n-1}} \sum_{h=0}^{n-2} \binom{q+n-2}{h} =$$

$$= v_{q-1,n} + \frac{1}{2} v_{q,n-1} \ .$$

D'autre part, pour tout $n \geqslant 1$:

$$u_{1,n} = \sum_{k=0}^{n-1} \frac{1}{2^k} = 2\left(1 - \frac{1}{2^n}\right),$$

et :

$$v_{1,n} = \frac{1}{2^{n-1}} \sum_{k=0}^{n-1} \binom{n}{k} = \frac{1}{2^{n-1}} (2^n - 1) = u_{1,n} \ .$$

On vérifie aussi que pour tout $q \geqslant 1$, $u_{q,1} = 1 = v_{q,1}$.
Montrons maintenant par récurrence sur l'entier $p \geqslant 2$ que pour tous $n \geqslant 1$ et $q \geqslant 1$, tels que $n + q = p$, $u_{q,n} = v_{q,n}$. Cette égalité est vraie pour $p = 2$, car alors $n = 1$ et $q = 1$. Si cette relation est vraie pour $p \geqslant 2$, et que n et q sont des entiers $\geqslant 1$ tels que $n + q = p + 1$, si $n = 1$ ou $q = 1$ alors on a vu que $u_{q,n} = v_{q,n}$, si $q > 1$ et $n > 1$, alors comme $q - 1 + n = p$ et $q + n - 1 = p$, par récurrence :

$$u_{q,n} = u_{q-1,n} + \frac{1}{2} u_{q,n-1} = v_{q-1,n} + \frac{1}{2} v_{q,n-1} = v_{q,n} \ .$$

L'égalité : $u_{q,n} = v_{q,n}$ est donc vraie pour tous entiers $q \geqslant 1$ et $n \geqslant 1$, ce qu'il fallait démontrer.

Exercice 9 :

(*formule du crible*) : Soit $E_1, E_2, \ldots, E_n$ des ensembles finis. Démontrer :

$$\operatorname{card}\left(\bigcup_{i=1}^{n} E_i\right) = \sum_{k=1}^{n} (-1)^{k-1} \sum_{I \in \mathcal{P}_k} \operatorname{card}\left(\bigcap_{i \in I} E_i\right),$$

où $\mathcal{P}_k$ désigne l'ensemble des parties de $[\![1, n]\!]$ de cardinal k . ■

Soit E un ensemble fini qui contient $\bigcup_{i=1}^{n} E_i$. Nous utiliserons les propriétés suivantes de la fonction caractéristique d'une partie de E , considérée comme application de E vers l'anneau $\mathbb{Z}$ (mais à valeurs dans $\{0, 1\}$) :
Pour toute partie A de E :

$$\chi_{E \setminus A} = 1 - \chi_A.$$

Pour toutes parties A et B de E :

$$\chi_{A \cap B} = \chi_A \times \chi_B.$$

Et enfin, pour toute partie A de E :

$$\operatorname{card}(A) = \sum_{x \in E} \chi_A(x).$$

Nous en déduisons que :

$$1 - \chi_{\bigcup_{i=1}^{n} E_i} = \chi_{E \setminus \bigcup_{i=1}^{n} E_i} = \chi_{\bigcap_{i=1}^{n} (E \setminus E_i)} = \prod_{i=1}^{n} \chi_{E \setminus E_i} = \prod_{i=1}^{n} (1 - \chi_{E_i}).$$

Nous avons maintenant à développer le dernier produit ; pour cela démontrons par récurrence sur l'entier n la formule :

$$\prod_{i=1}^{n} (a_i + b_i) = \sum_{P \subset [\![1,n]\!]} \left(\prod_{i \in P} a_i\right) \left(\prod_{i \notin P} b_i\right),$$

où $(a_i)_{i \in [\![1,n]\!]}$ et $(b_i)_{i \in [\![1,n]\!]}$ sont des familles à valeurs dans un anneau commutatif A (le produit d'une famille vide est par convention égal à 1). Cette formule est évidemment vraie pour $n = 1$. Supposons la vraie pour n ; soient $(a_i)_{i \in [\![1,n+1]\!]}$ et $(b_i)_{i \in [\![1,n+1]\!]}$ deux familles à valeurs dans A . Soit :

$$D = \sum_{P \subset [\![1,n+1]\!]} \left(\prod_{i \in P} a_i\right) \left(\prod_{i \in [\![1,n+1]\!] \setminus P} b_i\right).$$

Nous pouvons écrire :

$$D = \sum_{P\subset[\![1,n+1]\!],\ (n+1)\in P} \prod_{i\in P} a_i \prod_{i\in[\![1,n+1]\!]\setminus P} b_i + \sum_{P\subset[\![1,n]\!]} \prod_{i\in P} a_i \prod_{i\in[\![1,n+1]\!]\setminus P} b_i.$$

En posant, dans la première somme $Q = P\setminus\{n+1\}$, partie de $[\![1,n]\!]$, nous obtenons :

$$\begin{aligned} D &= \sum_{Q\subset[\![1,n]\!]} a_{n+1} \prod_{i\in Q} a_i \prod_{i\in[\![1,n]\!]\setminus Q} b_i + \sum_{P\subset[\![1,n]\!]} b_{n+1} \prod_{i\in P} a_i \prod_{i\in[\![1,n]\!]\setminus P} b_i \\ &= (a_{n+1}+b_{n+1}) \sum_{P\subset[\![1,n]\!]} \prod_{i\in P} a_i \prod_{i\in[\![1,n]\!]\setminus P} b_i. \end{aligned}$$

En utilisant l'hypothèse de récurrence nous obtenons :

$$D = (a_{n+1}+b_{n+1}) \prod_{i\in[\![1,n]\!]} (a_i+b_i) = \prod_{i\in[\![1,n+1]\!]} (a_i+b_i).$$

La formule est donc vraie à l'ordre $n+1$.
Cette formule de développement d'un produit est donc vraie pour tout entier n.

En prenant pour anneau A l'anneau des applications de E vers l'anneau $\mathbb{Z}$, nous obtenons :

$$\prod_{i=1}^{n} (1-\chi_{E_i}) = \sum_{P\subset[\![1,n]\!]} \prod_{i\in P} (-\chi_{E_i}),$$

d'où, en notant $\mathcal{P}_k$ l'ensemble des parties de $[\![1,n]\!]$ de cardinal k :

$$\prod_{i=1}^{n} (1-\chi_{E_i}) = 1 + \sum_{k=1}^{n} (-1)^k \sum_{P\in\mathcal{P}_k} \prod_{i\in P} \chi_{E_i}.$$

Soit encore :

$$\chi_{\bigcup_{i=1}^{n} E_i} = 1 - \prod_{i=1}^{n} (1-\chi_{E_i}) = \sum_{k=1}^{n} (-1)^{k-1} \sum_{P\in\mathcal{P}_k} \chi_{\bigcap_{i\in P} E_i}.$$

En faisant la somme des valeurs de ces deux fonctions nous obtenons finalement :

$$\operatorname{card}\left(\bigcup_{i=1}^{n} E_i\right) = \sum_{k=1}^{n} (-1)^{k-1} \sum_{I\in\mathcal{P}_k} \operatorname{card}\left(\bigcap_{i\in I} E_i\right),$$

ce qu'il fallait démontrer.

Exercice 13 *(familles spernéennes)* : :

Soit E un ensemble fini à n éléments et $(A_1, A_2, \ldots, A_h)$ une famille de parties de E. On dit qu'une telle famille possède la propriété S si, pour tout couple (i,j) tels que $i \in [\![1,h]\!]$, $j \in [\![1,h]\!]$ et $i \neq j$, la relation $A_i \subset A_j$ n'est jamais vérifiée.

a) Soit k fixé $\in [\![1,n]\!]$. Montrer que la famille des k-parties de E (prise dans un ordre quelconque) possède la propriété S.

b) On prend $h = 2$. Combien y a-t-il de couples (A_1, A_2) qui possèdent la propriété S ?

c) On appelle chaîne de E une famille $(C_1, C_2, \ldots, C_n)$ de parties de E vérifiant : $(\forall i \in [\![1,n]\!])$ $\operatorname{card}(C_i) = i$ et $C_i \subset C_{i+1}$ pour $i \in [\![1, n-1]\!]$. Combien y a-t-il de chaînes dans E ? Montrer que si une famille $\mathscr{A} = (A_1, A_2, \ldots, A_h)$ de parties de E possède la propriété S, pour toute chaîne $\mathscr{C} = (C_1, C_2, \ldots, C_n)$ on a $\operatorname{card}(\mathscr{A} \cap \mathscr{C}) \leqslant 1$.

d) Soit $\mathscr{A} = (A_1, A_2, \ldots, A_h)$ une famille de parties de E possédant la propriété S. Soit $\Gamma_{\mathscr{A}}$ l'ensemble des chaînes $\mathscr{C}$ de E telles que $\operatorname{card}(\mathscr{A} \cap \mathscr{C}) = 1$. On définit l'application $\varphi : \Gamma_{\mathscr{A}} \to \mathscr{A}$ qui, à toute chaîne $\mathscr{C} \in \Gamma_{\mathscr{A}}$, associe $\varphi(\mathscr{C})$, le seul élément commun à $\mathscr{A}$ et à $\mathscr{C}$. Montrer que φ est surjective et calculer, en fonction de $\operatorname{card}(A)$, le cardinal de $\varphi^{-1}(\{A\})$, c'est-à-dire le nombre de chaînes dont l'image par φ est A.

e) Montrer que :

$$\sum_{i=1}^{h} \frac{1}{\binom{n}{\operatorname{card} A_i}} \leqslant 1 ,$$

et en déduire que $h \leqslant \sup_{p \in [\![0,n]\!]} \binom{n}{p}$, ce dernier nombre étant noté $\omega(n)$. Vérifier que $\omega(2n-1) = \omega(2n)/2$. Existe-t-il une famille $(A_1, A_2, \ldots, A_{\omega(n)})$ de parties de E possédant la propriété S ?

f) On pose $E = [\![1,n]\!]$ et on donne n réels $a_1, a_2, \ldots, a_n$, tous > 0 (non nécessairement distincts). On définit l'application f de $\mathscr{P}(E)$ dans $\mathbb{R}$ par : $f(A) = \sum_{i \in A} a_i$; $f(\emptyset) = 0$. Montrer que, pour tout $t \in \mathbb{R}$, le nombre $g(t)$ de parties A de E telles que $f(A) = t$ est nécessairement $\leqslant \omega(n)$. ■

a) Si A et B sont des parties de E, distinctes, de cardinal k, il est impossible que $A \subset B$ ou $B \subset A$ car alors A et B seraient identiques. Toute famille injective de k-parties de E est donc une famille spernéenne.

b) Soit $\mathscr{C}$ l'ensemble des couples (A, B) de parties de E telles que $A \subset B$. Pour B fixée de cardinal k, le nombre de parties A de E telles que $A \subset B$ est 2^k ; le nombre de parties B de cardinal k étant $\binom{n}{k}$, le cardinal de $\mathscr{C}$ est $\sum_{k=0}^{n} 2^k \binom{n}{k} = 3^n$ (voir le chapitre III.5). De même le cardinal de l'ensemble $\mathscr{F}$ des couples (A, B) de parties de E telles que $B \subset A$ est 3^n ; l'intersection de $\mathscr{C}$ et de $\mathscr{F}$ est l'ensemble des couples (A, A), où A est une partie de E, son cardinal est donc 2^n. Nous pouvons en déduire que le cardinal de l'ensemble des couples (A, B) de parties de E telles que $A \subset B$ ou $B \subset A$ est $3^n + 3^n - 2^n$. Comme le nombre de couples (A, B) de parties de E est $2^n \times 2^n$, on voit que le nombre de couples (A, B) possédant la propriété S est $4^n - 2 \times 3^n + 2^n$.

c) Remarquons que le dernier élément d'une chaîne dans E est nécessairement E lui-même.
Montrons par récurrence sur l'entier $n \geqslant 1$, que le nombre de chaînes dans E de cardinal n est $n!$. C'est évidemment vrai si $n = 1$. Supposons le résultat vrai pour $n \geqslant 1$ et soit E un ensemble de cardinal $n + 1$. Considérons l'application f qui à une chaîne $\mathscr{C} = (C_1, C_2, \ldots, C_n, C_{n+1})$ dans E, fait correspondre le seul élément de E qui ne soit pas dans C_n ; il est clair que l'ensemble des chaînes $\mathscr{C}$ dont l'image est un élément x donné de E est l'ensemble des chaînes $(C_1, C_2, \ldots, C_n, E)$, où $(C_1, C_2, \ldots, C_n)$ est une chaîne dans $E \setminus \{x\}$. Le nombre de chaînes dans E de cardinal $n + 1$ est donc, en utilisant la récurrence, $(n + 1) \cdot n! = (n + 1)!$. L'égalité est donc vraie pour tout ensemble de cardinal $n + 1$. L'égalité est donc, par récurrence, toujours vraie.
Si $\mathscr{C} = (C_1, C_2, \ldots, C_n)$ est une chaîne dans E, et que $1 \leqslant i < j \leqslant n$, alors C_i est strictement inclus dans C_j ; ces deux parties ne peuvent donc pas être éléments d'une même famille spernéenne. Une chaîne et une famille spernéenne ne peuvent donc avoir qu'au plus un élément commun.

d) Reprenons les notations de l'énoncé et posons $k = \operatorname{card}(A)$. Si $\mathscr{C} = (C_1, C_2, \ldots, C_n)$ est une chaîne élément de $\Gamma_{\mathscr{A}}$ dont l'image est A, comme pour tout $i \in [\![1, n]\!]$ $\operatorname{card}(C_i) = i$, nécessairement $A = C_k$. On voit alors facilement que $\mathscr{C} = (C_1, C_2, \ldots, C_n)$ est une chaîne d'image A si, et seulement si, $(C_1, C_2, \ldots, C_k)$ est une chaîne dans A, et $(C_{k+1} \setminus A, C_{k+2} \setminus A, \ldots, C_n \setminus A)$ une chaîne dans $E \setminus A$; le nombre de telles chaînes est donc $k! \times (n - k)!$. Ce nombre n'étant jamais nul, l'application φ ∈

e) En posant $k_i = \text{card}\,(A_i)$, on vérifie que :

$$\sum_{i=1}^{h} \frac{1}{\binom{n}{k_i}} = \sum_{i=1}^{h} \frac{k_i\,!\,(n-k_i)\,!}{n\,!} =$$

$$= \frac{1}{n\,!} \sum_{i=1}^{h} \text{card}\,(\varphi^{-1}(\{A_i\})) = \frac{1}{n\,!}\text{card}\,(\Gamma_{\mathcal{A}})\,.$$

Comme le nombre de chaînes dans E est $n\,!$, ce quotient est $\leqslant 1$, ce qu'il fallait démontrer.

Pour tout $i \in [\![1, n]\!]$, $\binom{n}{k_i} \leqslant \omega(n)$, donc :

$$1 \geqslant \sum_{i=1}^{h} \frac{1}{\binom{n}{k_i}} \geqslant \frac{h}{\omega(n)},$$

d'où $h \leqslant \omega(n)$.

On sait que pour tout n entier > 0 et pour tout $h \in [\![0, n-1]\!]$:

$$\binom{n}{h+1} = \frac{n-h}{h+1}\binom{n}{h}.$$

On peut en déduire que dans le cas où n est pair, $n = 2p$, la fonction $k \mapsto \binom{2p}{k}$ est strictement croissante sur $[\![0, p]\!]$ et strictement décroissante sur $[\![p, 2p]\!]$, d'où $\omega(2p) = \binom{2p}{p}$. On voit de même que dans le cas où n est impair, $n = 2p+1$, la fonction $k \mapsto \binom{2p+1}{k}$ est strictement croissante sur $[\![0, p]\!]$ et strictement décroissante sur $[\![p+1, 2p]\!]$, d'où $\omega(2p+1) = \binom{2p+1}{p} = \binom{2p+1}{p+1}$. Nous voyons alors que pour tout n entier > 0,

$$2\,\omega(2n-1) = 2\binom{2n-1}{n} = 2\,\frac{(2n-1)\,!}{(n-1)\,!\,n\,!} =$$

$$= \frac{2n\,(2n-1)\,!}{n\,(n-1)\,!\,n\,!} = \frac{(2n)\,!}{n\,!\,n\,!} = \binom{2n}{n} = \omega(2n).$$

Soit k tel que $\binom{n}{k} = \omega(n)$, le nombre de parties de E de cardinal k est $\omega(n)$; une famille injective dont les éléments sont les k-parties de E est une famille spernéenne de cardinal $\omega(n)$ (voir *a*)).

f) Comme les nombres a_i sont tous strictement positifs, l'application f est strictement croissante, l'ensemble des parties de E étant muni de l'ordre de l'inclusion. Nous pouvons en déduire que si A et B sont des parties de E distinctes et telles que $f(A) = f(B) = t$, il est impossible que $A \subset B$ ou que $B \subset A$. Toute famille injective composée de parties A de E telles que $f(A) = t$ est donc spernéenne ; d'après le *e*) le cardinal de cet ensemble de parties est $\leqslant \omega(n)$, ce qui signifie ici que : $g(t) \leqslant \omega(n)$.

§ III.5 *FORMULE DU BINÔME*

Exercice 6 :

Démontrer par récurrence, en utilisant la formule du binôme, que :

$$\binom{n}{1}\frac{1}{1} - \binom{n}{2}\frac{1}{2} + \ldots + (-1)^{n-1}\binom{n}{n}\frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}.$$

Essayer de trouver une solution plus élégante à partir de $\sum_{k=0}^{n-1}(1-t)^k$. ■

Posons pour n entier $\geqslant 1$:

$$u_n = \sum_{i=1}^{n}(-1)^{i-1}\binom{n}{i}\frac{1}{i}.$$

Nous obtenons pour tout $n > 0$:

$$u_{n+1} = \sum_{i=1}^{n+1}(-1)^{i-1}\binom{n+1}{i}\frac{1}{i} =$$
$$= \sum_{i=1}^{n}(-1)^{i-1}\binom{n+1}{i}\frac{1}{i} + (-1)^n\binom{n+1}{n+1}\frac{1}{n+1}.$$

D'où en utilisant la relation de Pascal :

$$u_{n+1} = \sum_{i=1}^{n}(-1)^{i-1}\binom{n}{i}\frac{1}{i} + \sum_{i=1}^{n}(-1)^{i-1}\binom{n}{i-1}\frac{1}{i} + (-1)^n\binom{n}{n}\frac{1}{n+1} =$$
$$= u_n + \sum_{j=0}^{n}(-1)^j\binom{n}{j}\frac{1}{j+1}.$$

On sait que pour tout $j \in [\![0, n]\!]$:

$$\frac{1}{j+1}\binom{n}{j} = \frac{1}{n+1}\binom{n+1}{j+1} .$$

Nous pouvons en déduire :

$$u_{n+1} = u_n + \frac{1}{n+1}\sum_{j=0}^{n}(-1)^j\binom{n+1}{j+1} =$$

$$= u_n + \frac{1}{n+1}\left(1 - \sum_{k=0}^{n+1}(-1)^k\binom{n+1}{k}\right).$$

Soit :

$$u_{n+1} = u_n + \frac{1}{n+1}(1-(1-1)^{n+1}) = u_n + \frac{1}{n+1} .$$

Comme $u_1 = 1$, il est clair que pour tout n entier > 0 , on a bien l'égalité :

$$u_n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} .$$

Autre méthode. Pour tout t réel $\neq 0$ on a l'égalité :

$$\sum_{k=0}^{n-1}(1-t)^k = \frac{1-(1-t)^n}{1-(1-t)} =$$

$$= \frac{1}{t}\left(1 - \sum_{k=0}^{n}(-1)^k\binom{n}{k}t^k\right) = \sum_{k=1}^{n}(-1)^{k-1}\binom{n}{k}t^{k-1} .$$

En intégrant sur l'intervalle $]0, 1]$, nous obtenons l'égalité de l'énoncé :

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} = \binom{n}{1}\frac{1}{1} - \binom{n}{2}\frac{1}{2} + \ldots (-1)^{n-1}\binom{n}{n}\frac{1}{n} .$$

Exercice 7 :

Vérifier, pour $a \in \mathbb{Q}^*$, la formule de Reyley (1825) :

$$a = \left[\frac{a^6 + 45a^4 - 81a^2 + 27}{6a(a^2+3)^2}\right]^3 + \left[\frac{-a^4 + 30a^2 - 9}{6a(a^2+3)}\right]^3 + \left[\frac{-6a^3 + 18a}{(a^2+3)^2}\right]^3$$

(*N.B. :* Cette formule montre que tout nombre rationnel peut s'écrire comme la somme de trois cubes de nombres rationnels.)

On constate l'égalité :

$$\begin{aligned}(a^4-30a^2+9)(a^2+3) &= \\ &= a^6-30a^4+9a^2+3a^4-90a^2+27 = a^6-27a^4-81a^2+27 \\ &= a^6+9a^4-81a^2+27-36a^4 = (a^2+3)^3-108a^2-36a^4.\end{aligned}$$

Et :

$$a^6+45a^4-81a^2+27 = a^6+9a^4-81a^2+27+36a^4 = (a^2+3)^3-108a^2+36a^4.$$

Le membre de droite de l'égalité de l'énoncé est donc la fraction F égale à :

$$\frac{\left[(a^2+3)^3-108a^2+36a^4\right]^3-\left[(a^2+3)^3-108a^2-36a^4\right]^3}{6^3a^3(a^2+3)^6}-\frac{6^3a^3(a^2-3)^3}{(a^2+3)^6}\,.$$

Comme pour tous rationnels A et B :

$$(A+B)^3-(A-B)^3 = 6A^2B+2B^3 = 2B(3A^2+B^2),$$

on voit que :

$$\begin{aligned}\left[(a^2+3)^3-108a^2+36a^4\right]^3-\left[(a^2+3)^3-108a^2-36a^4\right]^3 &= \\ &= 2\cdot 6^2a^4\left[3((a^2+3)^3-3\cdot 6^2a^2)^2+6^4a^8\right] \\ &= 6^3a^4\left[((a^2+3)^3-3\cdot 6^2a^2)^2+2^4\cdot 3^3a^8\right].\end{aligned}$$

On trouve après simplification :

$$F = a\frac{\left((a^2+3)^3-3\cdot 6^2a^2\right)^2+2^43^3a^8-6^3a^2(a^2-3)^3}{(a^2+3)^6}\,.$$

Le numérateur N de la fraction est :

$$\begin{aligned}N &= (a^2+3)^6-6^3a^2(a^2+3)^3+3^26^4a^4+2^43^3a^8-6^3a^2(a^2-3)^3 = \\ &= (a^2+3)^6+6^3a^2\left[6\cdot 3^2a^2+2a^6-(a^2+3)^3-(a^2-3)^3\right].\end{aligned}$$

Pour terminer on voit que :

$$(a^2+3)^3+(a^2-3)^3 = 2a^6+2\cdot 27a^2 = 6\cdot 3^2a^2+2a^6,$$

et donc que $N=(a^2+3)^6$, d'où $F=a$, ce qu'il fallait démontrer.

Exercice 10 :

‖ Dans un anneau commutatif, prouver l'identité :

$$2\sum_{k=1}^{n} a_k(a_1 + a_2 + \ldots + a_k) = \left(\sum_{k=1}^{n} a_k\right)^2 + \sum_{k=1}^{n} a_k^2 \,. \quad \blacksquare$$

On vérifie que :

$$S = 2\sum_{k=1}^{n} a_k(a_1 + a_2 + \ldots + a_k) = 2\sum_{k=1}^{n}\left(a_k \sum_{h=1}^{k} a_h\right) =$$

$$= 2\sum_{1\leqslant h\leqslant k\leqslant n} a_k a_h = 2\sum_{1\leqslant h<k\leqslant n} a_k a_h + 2\sum_{k=1}^{n} a_k^2 \,.$$

Comme :

$$\sum_{1\leqslant h<k\leqslant n} a_k a_h = \sum_{1\leqslant k<h\leqslant n} a_k a_h \,,$$

nous voyons que :

$$S = \sum_{h\neq k} a_h a_k + 2\sum_{k=1}^{n} a_k^2 = \sum_{(h,k)\in[\![1,n]\!]^2} a_h a_k + \sum_{k=1}^{n} a_k^2 \,.$$

Soit enfin :

$$S = \left(\sum_{k=1}^{n} a_k\right)\left(\sum_{h=1}^{n} a_h\right) + \sum_{k=1}^{n} a_k^2 = \left(\sum_{k=1}^{n} a_k\right)^2 + \sum_{k=1}^{n} a_k^2 \,,$$

ce qu'il fallait démontrer.

§ III.7 *NOTION D'IDÉAL D'UN ANNEAU COMMUTATIF*

Exercice 1 :

Soit A un anneau commutatif non nul. On appelle **nilradical** de A l'ensemble des éléments *nilpotents* de A, c'est-à-dire l'ensemble $\mathcal{R}(A)$ formé des $x \in A$ tels que $x^n = 0$ pour au moins un $n \in \mathbb{N}^*$. Montrer que $\mathcal{R}(A)$ est un idéal de A. ■

Il est clair que $\mathcal{R}(A)$ n'est pas vide car il contient 0. Soit $x \in \mathcal{R}(A)$, et $a \in A$; il existe un entier $n > 0$ tel que $x^n = 0$, donc $(ax)^n = a^n x^n = 0$; l'élément ax est donc aussi nilpotent. En particulier, si x est nilpotent, $-x$ est nilpotent. Soient x et y deux éléments nilpotents, et

$n > 0$ et $m > 0$ tels que $x^n = y^m = 0$. En utilisant la formule du binôme on obtient :

$$(x+y)^{n+m-1} = \sum_{i=0}^{n+m-1} \binom{n+m-1}{i} x^i y^{n+m-1-i} .$$

Mais si $i \in [\![0, n-1]\!]$, alors $n+m-1-i \geqslant m$, donc $y^{n+m-1-i} = 0$; de même, si $i \in [\![n, n+m-1]\!]$, alors $x^i = 0$; tous les termes dans le développement de $(x+y)^{n+m-1}$ sont donc nuls et $(x+y)^{n+m-1} = 0$. L'élément $(x+y)$ de A est donc nilpotent. L'ensemble $\mathcal{R}(A)$ des éléments nilpotents de A est donc un idéal de l'anneau A.

Exercice 2 :

Soit $\mathfrak{a}$ un idéal d'un anneau commutatif A. On appelle **racine** de $\mathfrak{a}$ (que l'on peut noter $\sqrt{\mathfrak{a}}$) l'ensemble des $x \in A$ tels que $x^n \in \mathfrak{a}$ pour au moins un $n \in \mathbb{N}^*$. Montrer que $\sqrt{\mathfrak{a}}$ est un idéal de A. Que se passe-t-il si $\mathfrak{a} = \{0_A\}$? Montrer que : $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$ et que, si $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux de A, on a :

$$\sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}} \; ; \; \sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}} \subset \sqrt{\mathfrak{a} + \mathfrak{b}} \; ;$$

et $$\sqrt{\mathfrak{a} + \mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}} \; . \blacksquare$$

Il est clair que $\sqrt{\mathfrak{a}}$ n'est pas vide car il contient 0. Soit $x \in \sqrt{\mathfrak{a}}$, et $a \in A$; il existe un entier $n > 0$ tel que $x^n \in \mathfrak{a}$, donc $(ax)^n = a^n x^n \in \mathfrak{a}$; donc $ax \in \sqrt{\mathfrak{a}}$. En particulier, si $x \in \sqrt{\mathfrak{a}}$ alors $-x \in \sqrt{\mathfrak{a}}$. Soient x et y deux éléments de $\sqrt{\mathfrak{a}}$, et deux entiers $n > 0$ et $m > 0$ tels que $x^n \in \mathfrak{a}$ et $y^m \in \mathfrak{a}$. En utilisant la formule du binôme on obtient :

$$(x+y)^{n+m-1} = \sum_{i=0}^{n+m-1} \binom{n+m-1}{i} x^i y^{n+m-1-i} .$$

Mais si $i \in [\![0, n-1]\!]$, alors $n+m-1-i \geqslant m$, donc $y^{n+m-1-i} \in \mathfrak{a}$; de même, si $i \in [\![n, n+m-1]\!]$, alors $x^i \in \mathfrak{a}$; tous les termes dans le développement de $(x+y)^{n+m-1}$ sont donc dans $\mathfrak{a}$ et $(x+y)^{n+m-1} \in \mathfrak{a}$. L'élément $(x+y)$ de A est donc dans $\sqrt{\mathfrak{a}}$. L'ensemble $\sqrt{\mathfrak{a}}$ est donc un idéal de l'anneau A. Dans le cas où $\mathfrak{a} = \{0_A\}$, il est clair que $\sqrt{\mathfrak{a}} = \mathcal{R}(A)$. On remarque que l'application $\mathfrak{a} \mapsto \sqrt{\mathfrak{a}}$ est croissante pour l'ordre de l'inclusion et que pour tout idéal $\mathfrak{a}$ de A, $\mathfrak{a} \subset \sqrt{\mathfrak{a}}$.

Montrons que si $\mathfrak{a}$ est un idéal de A, $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$. Comme $\sqrt{\mathfrak{a}} \subset \sqrt{\sqrt{\mathfrak{a}}}$, il suffit de montrer l'inclusion opposée. Soit $x \in \sqrt{\sqrt{\mathfrak{a}}}$, il existe un entier $n > 0$ tel que $x^n \in \sqrt{\mathfrak{a}}$, et un entier $m > 0$ tel que $(x^n)^m$

$x^{nm} \in \mathfrak{a}$; nous en déduisons que $x \in \sqrt{\mathfrak{a}}$. Cela prouve que $\sqrt{\sqrt{\mathfrak{a}}} \subset \sqrt{\mathfrak{a}}$, et donc finalement que $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$.

Montrons que si $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux de A, $\sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}}$.
Il est clair que $\sqrt{\mathfrak{a} \cap \mathfrak{b}} \subset \sqrt{\mathfrak{a}}$ et $\sqrt{\mathfrak{a} \cap \mathfrak{b}} \subset \sqrt{\mathfrak{b}}$, par conséquent $\sqrt{\mathfrak{a} \cap \mathfrak{b}} \subset \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$. Montrons l'inclusion opposée. Si $x \in \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$, il existe un entier $n > 0$ et un entier $m > 0$ tels que $x^n \in \mathfrak{a}$ et $x^m \in \mathfrak{b}$, alors $x^{nm} = (x^n)^m \in \mathfrak{a}$ et $x^{nm} = (x^m)^n \in \mathfrak{b}$, donc $x \in \sqrt{\mathfrak{a} \cap \mathfrak{b}}$. Nous en déduisons que $\sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}} \subset \sqrt{\mathfrak{a} \cap \mathfrak{b}}$, et finalement $\sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}}$.

Si $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux de A, $\sqrt{\mathfrak{a}} \subset \sqrt{\mathfrak{a}+\mathfrak{b}}$ et $\sqrt{\mathfrak{b}} \subset \sqrt{\mathfrak{a}+\mathfrak{b}}$, donc $\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}} \subset \sqrt{\mathfrak{a}+\mathfrak{b}}$, et par conséquent $\sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}} \subset \sqrt{\sqrt{\mathfrak{a}+\mathfrak{b}}} = \sqrt{\mathfrak{a}+\mathfrak{b}}$. Comme $\mathfrak{a} \subset \sqrt{\mathfrak{a}}$ et $\mathfrak{b} \subset \sqrt{\mathfrak{b}}$, on voit que $\mathfrak{a}+\mathfrak{b} \subset \sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}$, donc $\sqrt{\mathfrak{a}+\mathfrak{b}} \subset \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}$. Finalement, par double inclusion, nous obtenons l'égalité :

$$\sqrt{\mathfrak{a}+\mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}.$$

Exercice 3 :

> Dans un anneau commutatif non nul A, un idéal $\mathfrak{a}$ est dit **maximal** ssi : $\mathfrak{a} \neq A$, et les seuls idéaux de A contenant $\mathfrak{a}$ sont $\mathfrak{a}$ et A. On donne un ensemble *fini* non vide E, un corps commutatif K et on considère l'anneau K^E.
> *a*) Pour chaque $a \in E$, l'ensemble $\mathfrak{M}_a = \{f \in K^E \mid f(a) = 0\}$ est un idéal maximal de K^E.
> *b*) Montrer que $a \mapsto \mathfrak{M}_a$ est une bijection de E sur l'ensemble des idéaux maximaux de K^E.
> *c*) Montrer que cette propriété tombe en défaut si E n'est plus supposé fini. ■

a) Un élément a de E étant fixé, l'application $f \mapsto f(a)$ de K^E vers K est un homomorphisme d'anneaux (Définition II.5.3 exemple 5). Le noyau de cet homomorphisme d'anneaux, $\mathfrak{M}_a$, est donc un idéal (Proposition III.7.1). Soit $\mathfrak{I}$ un idéal de K^E qui contient $\mathfrak{M}_a$. Si $\mathfrak{I} \neq \mathfrak{M}_a$, il existe une application f, élément de $\mathfrak{I}$, telle que $f(a) \neq 0$; soit g une application de K vers E, l'application $h = g - (g(a)/f(a)) \cdot f$ prend la valeur 0 en a et est donc un élément de $\mathfrak{M}_a$, donc de $\mathfrak{I}$; nous pouvons en déduire que g est élément de $\mathfrak{I}$. Comme ceci est vrai pour toute application $g : K \to E$, nous voyons que $\mathfrak{I} = A$. L'idéal $\mathfrak{M}_a$ est donc maximal.

b) Montrons d'abord que l'application $a \mapsto \mathfrak{M}_a$ est injective. Soit pour $x \in E$ l'application $\delta_x : E \to K$ définie par : $\delta_x(y) = 0$ si $x \neq y$ et $\delta_x(y) = 1$ si $x = y$. Si a et b sont des éléments de E distincts, on voit que $\delta_a \in \mathfrak{M}_b \setminus \mathfrak{M}_a$ et $\delta_b \in \mathfrak{M}_a \setminus \mathfrak{M}_b$; les idéaux $\mathfrak{M}_a$ et $\mathfrak{M}_b$ sont donc distincts si a et b le sont.
Montrons maintenant que l'application $a \mapsto \mathfrak{M}_a$ est surjective. Soit $\mathfrak{I}$ un idéal de l'anneau K^E qui n'est inclus dans aucun des idéaux $\mathfrak{M}_a$. Pour tout élément a de E, l'inclusion $\mathfrak{M}_a \subset \mathfrak{M}_a + \mathfrak{I}$ est donc stricte, donc $\mathfrak{M}_a + \mathfrak{I} = K^E$. Il existe donc, pour tout $a \in E$, une application ψ_a élément de $\mathfrak{M}_a$ et une application φ_a élément de $\mathfrak{I}$ telles que $\psi_a + \varphi_a = 1$ (1 désigne ici l'application constante égale à 1). Nous pouvons alors écrire :

$$\prod_{a \in E} (\psi_a + \varphi_a) = 1.$$

En développant ce produit, on trouve des termes qui sont tous dans l'idéal $\mathfrak{I}$, puisque $(\forall a \in E)\ \varphi_a \in \mathfrak{I}$, sauf peut-être le terme $\prod_{a \in E} \psi_a$, mais ce terme est l'application nulle puisque $(\forall a \in E)\ \psi_a(a) = 0$. Nous pouvons déduire de ce qui précède que $1 \in \mathfrak{I}$ et donc que $\mathfrak{I} = A$. Si $\mathfrak{M}$ est un idéal maximal de l'anneau K^E, il est nécessairement inclus dans l'un des idéaux maximaux $\mathfrak{M}_a$, donc égal à l'un d'entre eux, ce qu'il fallait démontrer.

c) On suppose ici que E est un ensemble infini. Si f est un élément de K^E, notons $\text{support}(f) = \{x \in E \mid f(x) \neq 0\}$. On voit facilement que le support de l'application nulle est $\emptyset$ et que si f et g sont deux éléments quelconques de K^E, $\text{support}(f \times g) = \text{support}(f) \cap \text{support}(g)$, et $\text{support}(f + g) \subset \text{support}(f) \cup \text{support}(g)$. L'ensemble des applications de support fini est donc un idéal $\mathfrak{I}$ de K^E. Cet idéal $\mathfrak{I}$ n'est inclus dans aucun des idéaux $\mathfrak{M}_a$ puisque pour tout $a \in E$, $\delta_a \in \mathfrak{I} \setminus \mathfrak{M}_a$. L'idéal $\mathfrak{I}$ n'est sans doute pas maximal, mais s'il est inclus dans un idéal maximal $\mathfrak{M}$, cet idéal maximal ne sera inclus dans aucun des $\mathfrak{M}_a$, donc ne sera égal à aucun de ces idéaux. Il reste à démontrer la proposition suivante :

Proposition :

> Dans un anneau commutatif tout idéal strict est inclus dans un idéal maximal. ■

Le lecteur pourra d'abord se reporter à l'exercice 9 du chapitre I.6.
Considérons l'ensemble E des idéaux stricts de l'anneau A, ordonné par l'inclusion. Les idéaux maximaux de A sont les éléments maximaux de cet ensemble ordonné. Soit $\mathscr{C}$ une chaîne dans E, c'est-à-dire un ensemble non vide d'idéaux stricts de A, totalement ordonné par l'inclusion.
Montrons que : $J = \bigcup_{I \in \mathscr{C}} I$ est un idéal de A. Cet ensemble n'est évidemment pas vide. Si $x \in J$ et $a \in A$, alors il existe $I \in \mathscr{C}$ tel que

$ax \in I$, donc $ax \in J$. Si $x \in J$ et $x' \in J$, il existe deux idéaux $I \in \mathscr{C}$ et $I' \in \mathscr{C}$ tels que $x \in I$ et $x' \in I'$; comme $\mathscr{C}$ est totalement ordonné par l'inclusion, $I \subset I'$ ou $I' \subset I$; supposons par exemple $I \subset I'$, alors x et x' sont tous les deux éléments de l'idéal I' donc $x+y$ aussi, donc $x+y \in J$. L'ensemble J est donc bien un idéal de l'anneau A.
Cet idéal J est strict, sinon $1 \in J$, donc 1 serait élément de l'un des idéaux stricts I où $I \in \mathscr{C}$, ce qui est impossible. Cet idéal est donc la borne supérieure de $\mathscr{C}$, puisque c'est un majorant de $\mathscr{C}$ et que c'est le plus petit possible (pour l'inclusion).
Toute chaîne dans l'ensemble E a une borne supérieure : l'ensemble E est par définition inductif. Le théorème de Zorn nous permet alors d'affirmer que cet ensemble ordonné possède au moins un élément maximal, ce qu'il fallait démontrer.
Fin de la démonstration de la proposition.

Reprenons les notations de l'exercice. Si E est infini, l'idéal de l'anneau K^E dont les éléments sont les applications de support fini, qui est évidemment un idéal strict, est inclus dans un idéal maximal qui n'est aucun des idéaux $\mathfrak{M}_a$ où $a \in E$. L'application $a \mapsto \mathfrak{M}_a$ de E vers l'ensemble des idéaux maximaux de l'anneau K^E n'est donc pas surjective.

Exercice 7 :

> Pour qu'un sous-anneau A de $\mathbb{Q}$ soit *partout dense* (cf. exercice 6), il faut et il suffit que $A \cap]0,1[\neq \emptyset$. ■

Nous utiliserons les résultats de l'exercice 6. Si A est un sous-anneau de $\mathbb{Q}$ qui n'est pas partout dense, comme c'est un sous-groupe additif de $\mathbb{Q}$, il existe $a \in \mathbb{Q}_+$ tel que $A = a\mathbb{Z}$. Comme A est un sous-anneau, $1 \in A$ donc $a \neq 0$, d'où $a > 0$; de plus $a^2 \in A$, il existe donc un entier $n > 0$ tel que $a^2 = n \cdot a$, d'où $a = n$ et $A = n\mathbb{Z}$. Comme $1 \in A$, nécessairement $n = 1$, donc $A = \mathbb{Z}$. Le seul sous-anneau de $\mathbb{Q}$ qui ne soit pas partout dense est donc $\mathbb{Z}$. Tout sous-anneau de $\mathbb{Q}$ qui coupe l'intervalle $]0,1[$ n'est pas $\mathbb{Z}$ et est donc partout dense. Inversement un sous-anneau de $\mathbb{Q}$ qui est dense coupe l'intervalle $]0,1[$. L'équivalence est donc démontrée.

Exercice 9 :

> On dit qu'un idéal $\mathfrak{I}$ d'un anneau commutatif est **primaire** ssi,
> $$(\forall (x,y) \in A^2) \quad (xy \in \mathfrak{I} \text{ et } x \notin \mathfrak{I}) \Rightarrow (\exists n \in \mathbb{N}^* \mid y^n \in \mathfrak{I}).$$
> Montrer que la racine (cf. exercice 2) d'un idéal primaire est un idéal premier. Si $\mathfrak{M}$ est un idéal maximal de A, montrer que les puissances $\mathfrak{M}^p$ ($p \in \mathbb{N}^*$) de $\mathfrak{M}$ sont des idéaux primaires ayant $\mathfrak{M}$ pour racine (voir l'exercice 4 pour la définitio

‖ d'idéaux). ■

Soit $\mathfrak{I}$ un idéal primaire. Supposons que x et y soient des éléments de A tels que $xy \in \sqrt{\mathfrak{I}}$. Il existe un entier $m > 0$ tel que $x^m y^m = (xy)^m \in \mathfrak{I}$. Si $x \notin \sqrt{\mathfrak{I}}$, nécessairement $x^m \notin \mathfrak{I}$. Puisque l'idéal $\mathfrak{I}$ est primaire, par définition il existe $n > 0$ tel que $(y^m)^n = y^{mn} \in \mathfrak{I}$, donc $y \in \sqrt{\mathfrak{I}}$. L'idéal $\sqrt{\mathfrak{I}}$ est donc premier.

Montrons d'abord qu'un idéal maximal est premier. Si $\mathfrak{M}$ est un idéal maximal de l'anneau A, et x et y deux éléments de A tels que $xy \in \mathfrak{M}$ et $x \notin \mathfrak{M}$, l'idéal $\mathfrak{M} + xA$ contient strictement $\mathfrak{M}$ donc est égal à A. Il existe donc un élément $a \in A$ et un élément $m \in \mathfrak{M}$ tels que $ax + m = 1$. Nous en déduisons que $y = axy + my$ est élément de l'idéal $\mathfrak{M}$. L'idéal $\mathfrak{M}$ est donc premier.
Montrons ensuite que si $\mathfrak{I}$ est un idéal premier, $\sqrt{\mathfrak{I}} = \mathfrak{I}$. En effet si $x \in A$ est tel que $\exists n \in \mathbb{N}^*$, $x^n \in \mathfrak{I}$, alors $x \cdot x \cdot \ldots \cdot x \in \mathfrak{I}$. Par conséquent $\sqrt{\mathfrak{I}} \subset \mathfrak{I}$ et finalement $\sqrt{\mathfrak{I}} = \mathfrak{I}$. Cette propriété est vraie aussi pour tout idéal maximal.
Soit maintenant $\mathfrak{M}$ un idéal maximal et p un entier > 0. Comme $\mathfrak{M}^p \subset \mathfrak{M}$, on voit que $\sqrt{\mathfrak{M}^p} \subset \sqrt{\mathfrak{M}} = \mathfrak{M}$. Démontrons l'inclusion opposée. Soit $x \in \mathfrak{M}$, $x^p \in \mathfrak{M}^p$, donc $x \in \sqrt{\mathfrak{M}^p}$. Nous en déduisons $\mathfrak{M} \subset \sqrt{\mathfrak{M}^p}$ et finalement $\mathfrak{M} = \sqrt{\mathfrak{M}^p}$.
Montrons que les idéaux $\mathfrak{M}^p$ sont primaires. Soient x et y des éléments de A tels que $xy \in \mathfrak{M}^p$ et $y \notin \mathfrak{M}$; alors l'idéal $\mathfrak{M} + yA$ contient strictement $\mathfrak{M}$ et est par conséquent égal à A ; il existe donc un élément $a \in A$ et un élément $m \in \mathfrak{M}$ tels que $ay + m = 1$; nous pouvons alors écrire $x = axy + mx$, ce qui prouve que $x \in \mathfrak{M}$; mais puisque $x \in \mathfrak{M}$, alors $x \in \mathfrak{M}^2$ etc. ; on peut poursuivre ce raisonnement pour montrer que $x \in \mathfrak{M}^{p-1}$, puis, comme $xy \in \mathfrak{M}^p$ et $m \in \mathfrak{M}$, en déduire finalement $x \in \mathfrak{M}^p$. Par conséquent si $xy \in \mathfrak{M}^p$ et $x \notin \mathfrak{M}^p$, alors $y \in \mathfrak{M}$ et $y^p \in \mathfrak{M}^p$. L'idéal $\mathfrak{M}^p$ est donc primaire.

Chapitre IV

NOTIONS D'ARITHMÉTIQUE

§ IV.1 *CONGRUENCES DANS $\mathbb{Z}$, ANNEAUX $\mathbb{Z}/n\mathbb{Z}$*

Exercice 2 :

Calculer le reste $\mod(31)$ de $(1\,986)^{10\,000}$, le reste $\mod(41)$ de l'entier $(51\,200)^{2^{100}}$ et le reste $\mod(17)$ de $(1\,035\,125)^{5\,642}$. ■

On vérifie par division euclidienne que $1\,986 \equiv 2 \ [31]$ donc $(1\,986)^{10\,000} \equiv 2^{10\,000} \ [31]$. Or $2^5 \equiv 1 \ [31]$, donc $2^{10\,000} \equiv (2^5)^{2\,000} \equiv 1^{2\,000} \equiv 1 \ [31]$. Nous avons démontré la relation $(1\,986)^{10\,000} \equiv 1 \ [31]$.

On vérifie par division euclidienne que $51\,200 \equiv 32 \equiv -9 \ [41]$ et que $(-9)^2 \equiv 81 \equiv -1 \ [41]$, donc $51\,200^4 \equiv 1 \ [41]$. Comme 4 divise 2^{100}, on voit comme ci-dessus que $(51\,200)^{2^{100}} \equiv 1 \ [41]$.

On vérifie par division euclidienne que $1\,035\,125 \equiv 12 \equiv -5 \ [17]$, puis que $(-5)^2 \equiv 25 \equiv 8 \ [17]$, $(-5)^4 \equiv 64 \equiv -4 \ [17]$, $(-5)^8 \equiv 16 \equiv -1 \ [17]$, et enfin $(-5)^{16} \equiv 1 \ [17]$ (le petit théorème de Fermat donne ce résultat sans calcul). On obtient facilement l'égalité $5642 = 16 \times 352 + 8 + 2$, donc $(1\,035\,125)^{5\,642} \equiv (-5)^{5\,642} \equiv (-5)^8 \times (-5)^2 \equiv (-1) \times 8 \equiv -8 \equiv 9 \ [17]$.

Exercice 3 :

Vérifier que $10^6 \equiv 1 \mod(7)$ et en déduire :

$$\sum_{k=1}^{10} 10^{10^k} \equiv 5 \mod(7) .$$ ■

On vérifie que $1001 = 7 \times 143$, donc $10^3 \equiv -1 \ [7]$ et $10^6 \equiv 1 \ [7]$. La classe de 10^n modulo 7 ne dépend donc que de la classe de n modulo 6. Or $10^1 \equiv 4 \ [6]$, $10^2 \equiv 16 \equiv 4 \ [6]$ et on voit facilement que pour tout k entier > 0, $10^k \equiv 4 \ [6]$. Tous les termes de la somme $S = \sum_{k=1}^{10} 10^{10^k}$ sont donc congrus à 10^4 modulo 7, donc la somme est congrue à $10^5 = 10^2 \times 10^3$ modulo 7. Donc $S \equiv 2 \times (-1) \equiv 5 \ [7]$.

Exercice 9 :

Démontrer $(\forall n \in \mathbb{N}^*)$:

a) $10^{6n} + 10^{3n} - 2 \equiv 0 \mod(111)$,

b) $7^{2n+1} - 48n - 7 \equiv 0 \mod(288)$. ■

a) On voit que $10^3 = 9 \times 111 + 1$, donc $10^3 \equiv 1$ [111]. Par conséquent pour tout $n \in \mathbb{N}$, $10^{6n} + 10^{3n} - 2 \equiv 1^{2n} + 1^n - 2 \equiv 0$ [111].

b) On vérifie que pour tout $n \in \mathbb{N}^*$:

$$7^{2n+1} - 48n - 7 = 7(49^n - 1) - 48n = \\ = 48 \times \left(7(49^{n-1} + \ldots + 49 + 1) - n\right).$$

Comme $288 = 6 \times 48$, l'égalité de l'énoncé sera vraie si, et seulement si, 6 divise le nombre $7(49^{n-1} + \ldots + 49 + 1) - n$, soit encore si, et seulement si, $7(49^{n-1} + \ldots + 49 + 1) \equiv n$ [6]. Comme $7 \equiv 1$ [6], cette relation est vraie.

Exercice 11 :

Démontrer : $(\forall n \in \mathbb{N})$

a) $4^{2^n} + 2^{2^n} + 1 \equiv 0 \mod(7)$ (Stifel)

b) $2^{2n} + 15n - 1 \equiv 0 \mod(9)$. ■

a) Posons pour n entier $x_n = 2^{2^n}$. On vérifie facilement que $x_0 = 2$ et que pour tout n entier, $x_{n+1} = x_n^2$; d'où $x_1 = 4$, $x_2 \equiv 16 \equiv 2$ [7], $x_3 \equiv 4$ [7] etc. Les classes modulo 7 des entiers x_n sont donc alternativement 2 (si n est pair), et 4 (si n est impair) ; la classe modulo 7 de $4^{2^n} + 2^{2^n} = x_{n+1} + x_n$ est donc toujours celle de $2 + 4 \equiv -1$ [7]. Donc pour tout $n \in \mathbb{N}$, $4^{2^n} + 2^{2^n} + 1 \equiv 0$ [7].

b) L'égalité est vraie pour $n = 0$. Pour tout $n > 0$, on voit que : $2^{2n} + 15n - 1 \equiv 2^{2n} - 1 - 3n$ [9], et que $2^{2n} - 1 - 3n = 4^n - 1 - 3n = 3\left[(4^{n-1} + \ldots + 4 + 1) - n\right]$. Par conséquent l'entier $2^{2n} + 15n - 1$ sera divisible par 9 si, et seulement si $4^{n-1} + \ldots + 4 + 1 \equiv n$ [3] ; ce qui est évidemment vrai puisque $4 \equiv 1$ [3].

Exercice 14 :

Si 9 divise $a^3 + b^3 + c^3$, alors 3 divise a ou b o

Ecrivons les entiers a, b et c sous la forme: $a = 3q_a + r_a$, $b = 3q_b + r_b$, $c = 3q_c + r_c$, où r_a, r_b, r_c sont 0, 1 ou -1. On voit que:

$$a^3 = (3q_a + r_a)^3 = 27q_a^3 + 27q_a^2 r_a + 9q_a r_a^2 + r_a^3 ,$$

donc:

$$a^3 \equiv r_a^3 \equiv r_a \ [9].$$

Il en est de même pour b et pour c, donc:

$$a^3 + b^3 + c^3 \equiv r_a + r_b + r_c \ [9].$$

Comme $r_a + r_b + r_c$ est compris entre -3 et 3, l'entier $a^3 + b^3 + c^3$ est divisible par 9 si, et seulement si, $r_a + r_b + r_c = 0$. On voit que cela n'est possible que si $\{r_a, r_b, r_c\} = \{-1, 0, 1\}$. En particulier l'un des nombres est divisible par 3.

Exercice 20 :

Pour $n \in \mathbb{N}$, le nombre $\sum_{k=0}^{n} 2^{3k} \binom{2n+1}{2k+1}$ n'est jamais divisible par 5. ■

Soit dans l'anneau $A = \mathfrak{M}_2(\mathbb{Z}/5\mathbb{Z})$, la matrice $x = \begin{pmatrix} 0 & 3 \\ 1 & 0 \end{pmatrix}$. On vérifie facilement que $x^2 = 3 \cdot 1_A$. Le sous-espace vectoriel (sur le corps $\mathbb{Z}/5\mathbb{Z}$) engendré par les matrices 1_A et x est donc un sous-anneau commutatif B de l'anneau A. On vérifie que 3 n'est pas un carré modulo 5, ce qui implique que l'anneau B est un corps. En effet, pour tous éléments a et b non tous les deux nuls de $\mathbb{Z}/5\mathbb{Z}$ on voit que $(a1_A + bx)(a1_A - bx) = (a^2 - 3b^2)1_A$; comme 3 n'est pas un carré, l'élément $a^2 - 3b^2$ ne peut être nul et est donc inversible dans le corps $\mathbb{Z}/5\mathbb{Z}$; par conséquent la matrice $a1_A + bx$ est inversible dans l'anneau B, d'inverse $(a^2 - 3b^2)^{-1}(a1_A - bx)$. Dans la suite de l'exercice nous utiliserons seulement l'existence d'un corps B contenant $\mathbb{Z}/5\mathbb{Z}$, donc de caractéristique 5, et d'un élément x de B tel que $x^2 = 3 = 8 = 2^3$.

En utilisant la formule du binôme nous obtenons pour tout n entier:

$$(1 + x)^{2n+1} = \sum_{h=0}^{n} \binom{2n+1}{2h} x^{2h} + \sum_{h=0}^{n} \binom{2n+1}{2h+1} x^{2h+1} ,$$

et de manière analogue:

$$(1 - x)^{2n+1} = \sum_{h=0}^{n} \binom{2n+1}{2h} x^{2h} - \sum_{h=0}^{n} \binom{2n+1}{2h+1} x^{2h+1}$$

Nous en déduisons :

$$(1+x)^{2n+1} - (1-x)^{2n+1} = 2\sum_{h=0}^{n} \binom{2n+1}{2h+1} x^{2h+1} .$$

Comme pour tout h entier $x^{2h+1} = x\,x^{2h} = x\,8^h = x\,2^{3h}$, nous voyons que pour tout n entier :

$$(1+x)^{2n+1} - (1-x)^{2n+1} = 2x\sum_{h=0}^{n} \binom{2n+1}{2h+1} 2^{3h} ,$$

d'où, en notant u_n la classe modulo 5 de l'entier $\displaystyle\sum_{k=0}^{n} 2^{3k}\binom{2n+1}{2k+1}$:

$$u_n = \frac{1}{2x}\left[(1+x)^{2n+1} - (1-x)^{2n+1}\right].$$

Posons pour n entier $a_n = (1+x)^{2n}$ et $b_n = (1-x)^{2n}$. Comme x est racine d'une équation du second degré, on devine que ces suites vérifient des relations de récurrence simples. En effet :

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

et :

$$(1+x)^3 = 2(2+x)(1+x) = 2(2+3x+3) = 6x = x,$$

donc $(1+x)^6 = x^2 = 3$. On voit alors que pour tout n entier :

$$a_{n+3} = (1+x)^{2n+6} = 3a_n.$$

Un calcul analogue, en remplaçant x par $-x$, montre que la suite (b_n) vérifie la même relation de récurrence, et il en est donc de même pour la suite (u_n). Donc si $n = 3q + r$, où $r \in [\![0, 2]\!]$, alors $u_n = u_{3q+r} = 3^q u_r$. Bien que ce ne soit pas indispensable ici, on peut remarquer aussi que :

$$(1+x)^4 = x(1+x) = 3 + x = 6(2+x) + 1 = 3(1+x)^2 + 1,$$

et que par conséquent, pour tout n entier :

$$a_{n+2} = 3a_{n+1} + a_n.$$

La suite (b_n) vérifie aussi cette relation et il en est de même pour la suite (u_n).

On voit que $u_0 = 1$, $u_1 = 1$, et $u_2 = 3 + 1 = 4$. Il est alors clair que u_n n'est jamais nul, et donc que pour tout $n \in \mathbb{N}$ l'entier $\displaystyle\sum_{k=0}^{n} 2^{3k}\binom{2n+1}{2k+1}$ n'est pas divisible par 5.

Exercice 21 :

Soit A la somme des chiffres de $4\,444^{4\,444}$ et B la somme des chiffres de A. Trouver la somme des chiffres de B ; la numération est la numération décimale. (*Olympiades, 1975.*) ■

Notons $S(n)$ la somme des chiffres de l'entier n dans son écriture décimale. On sait que $S(n) \equiv n$ [9] (cf. preuve par 9) ; par conséquent $4\,444 \equiv 16 \equiv 7$ [9] et $4\,444^{4\,444} \equiv 7^{4\,444}$ [9]. D'autre part $7^2 \equiv 49 \equiv 4$ [9] et $7^3 \equiv 28 \equiv 1$ [9]. Comme $4\,444 \equiv 7$ [9], on voit que $4\,444 \equiv 7 \equiv 1$ [3]. Finalement nous en déduisons $4\,444^{4\,444} \equiv 7^1 \equiv 7$ [9].

On vérifie d'autre part que $X = 4\,444^{4\,444} < 10\,000^{4\,444} = 10^{4\times 4\,444}$. Nous pouvons en déduire que le nombre entier X s'écrit en notation décimale avec un nombre de chiffres $\leqslant 4 \times 4\,444$ et que par conséquent $S(X) \leqslant 9 \times 4 \times 4\,444 < 10^6$. Le nombre A s'écrit donc en numération décimale avec un nombre de chiffres $\leqslant 6$ et $B = S(A) \leqslant 9 \times 6 = 54$. On voit facilement que la somme des chiffres des nombres entiers $\leqslant 54$ est majorée par $4 + 9 = 13$. La somme C des chiffres de B est donc $\leqslant 13$ et comme $C = S(B) = S(S(A)) = S(S(S(X)))$, elle est congrue à 7 modulo 9 ; elle ne peut donc être qu'égale à 7.

§ IV.2 *ARITHMÉTIQUE DANS* $\mathbb{Z}$ *ET* $\mathbb{N}$

Exercice 2 :

Soit $a > 1$, b, c dans $\mathbb{N}^*$ avec b et c premiers entre eux.
Démontrer : $(a^b - 1)(a^c - 1)$ divise $(a - 1)(a^{bc} - 1)$. ■

Montrons par récurrence sur l'entier $n \geqslant 0$, que si b et c sont des entiers $\geqslant 0$ et $b \leqslant n$, alors :

$$\text{pgcd}\left((a^b - 1), (a^c - 1)\right) = a^{\text{pgcd}(b,c)} - 1 .$$

C'est vrai si $n = 0$ car alors, $b = 0$, $a^b - 1 = 0$, et $\text{pgcd}(b, c) = c$. Supposons que ce soit vrai pour n ; soient b et c des entiers $\geqslant 0$ et $b \leqslant n + 1$. Posons $c = db + r$, où $d \in \mathbb{N}$ et $0 \leqslant r < b$, donc $r \leqslant n$. On vérifie que :

$$a^c - 1 = a^{db+r} - 1 = a^r(a^{db} - 1) + a^r - 1,$$

Comme $a^{db} - 1 = (a^b - 1)(a^{b(d-1)} + \ldots + a^b + 1)$ si $d \geqslant 1$, et $a^{db} - 1 = 0$ si $d = 0$, on voit que $a^b - 1$ divise l'entier $a^r(a^{db} - 1)$. Nous pouvons en déduire l'égalité :

$$\text{pgcd}\left((a^b - 1), (a^c - 1)\right) = \text{pgcd}\left((a^r - 1), (a^b - 1)\right)$$

L'hypothèse de récurrence nous permet d'affirmer que :

$$\text{pgcd}\left((a^r-1),(a^b-1)\right) = a^{\text{pgcd}(r,b)} - 1.$$

On remarque que les couples (b,c) et (r,b) ont même ensemble de diviseurs communs, donc même pgcd, d'où :

$$\text{pgcd}\left((a^b-1),(a^c-1)\right) = a^{\text{pgcd}(b,c)} - 1.$$

La propriété est donc vraie pour $n+1$. Nous avons donc démontré par récurrence la propriété annoncée.
En particulier si b et c sont des entiers premiers entre eux, alors :

$$\text{pgcd}\left(a^b-1, a^c-1\right) = a-1\ .$$

Soient $a>1$, $b>0$, $c>0$ trois entiers, b et c premiers entre eux. Posons $a^b-1=(a-1)B$ et $a^c-1=(a-1)C$. D'après ce qui précède, les entiers A et B sont premiers entre eux. Posons aussi $a^{bc}-1=(a-1)D$. Comme a^b-1 divise $a^{bc}-1$, c'est-à-dire $(a-1)B$ divise $(a-1)D$, nous voyons que B divise D ; de même C divise D et puisque B et C sont premiers entre eux, BC divise D. Finalement $(a^b-1)(a^c-1)=(a-1)^2BC$ divise $(a-1)^2D=(a-1)(a^{bc}-1)$, ce qu'il fallait démontrer.

Exercice 5 :

‖ Trouver l'ensemble $\left\{(m,n)\in\mathbb{N}^2 \mid 2^m-3^n=1\right\}$. ■

Cherchons d'abord l'ensemble des solutions pour lesquelles $n=0$; il est clair que la seule solution est le couple $(1,0)$. On voit de même que la seule solution pour laquelle $n=1$ est le couple $(2,1)$. Montrons qu'il n'y a pas d'autres solutions. En effet si $m\geqslant 0$ et $n\geqslant 2$ sont deux entiers tels que $2^m-1=3^n$, alors $2^m\equiv 1\ [9]$. Or les classes des puissances $0,1,2,3,4,5,6$ de 2 modulo 9 sont $1,2,4,8,7,5,1$. Par conséquent, comme $2^m\equiv 1\ [9]$, 6 divise m ; posons $m=6m'$. Alors $2^m-1=(2^6)^{m'}-1^{m'}$ est divisible par $2^6-1=63=9\times 7$, et ne peut donc pas être une puissance de 3, ce qui est contradictoire.
Les seules solutions sont donc les couples $(1,0)$ et $(2,1)$.

Exercice 6 :

‖ Prouver que pour tout $n\in\mathbb{Z}$, la fraction $\dfrac{15\,n^2+8\,n+6}{30\,n^2+21\,n+13}$ est irréductible. ■

Nous avons à démontrer que $a=15n^2+8n+6$ est premier avec $b=30n^2+21n+13$. On vérifie d'abord que $b-2a=5n+1$, puis $a=(3n+1$

Si l'entier d divise a et b, alors d divise a et $5n+1$, donc $5n+1$ et 5, donc finalement d divise 1. Les entiers a et b sont donc bien premiers entre eux. Le lecteur remarquera que la méthode utilisée ici est une adaptation assez libre de l'algorithme d'Euclide.

Exercice 11 :

Soit $P \in \mathbb{N}^*$ multiple commun à $a_1, a_2, \ldots, a_n$ ($a_i \in \mathbb{N}^*$, $n \geqslant 2$). On pose $P_i = \dfrac{P}{a_i}$ et $D = \text{pgcd}\,(P_1, P_2, \ldots, P_n)$. Montrer : $\text{ppcm}\,(a_1, a_2, \ldots, a_n) = \dfrac{P}{D}$. ■

Pour tout $i \in [\![1, n]\!]$, $D|P_i|P$, donc $D|P$; posons $q = P/D$, q est entier. Montrons que q est un multiple commun des a_i. Posons pour $i \in [\![1, n]\!]$, $P_i = DQ_i$; alors $a_i DQ_i = a_i P_i = P$, donc $a_i Q_i = q$.

Si M est un multiple commun des a_i, posons pour $i \in [\![1, n]\!]$, $M = R_i a_i$; alors $MP_i = R_i a_i P_i = R_i P$, donc P divise $MP_1, MP_2, \ldots, MP_n$; donc :

$$P \mid \text{pgcd}\,(MP_1, MP_2, \ldots, MP_n) = M\ \text{pgcd}\,(P_1, P_2, \ldots, P_n) = MD\ ;$$

finalement $q = P/D$ divise M.
Nous avons donc démontré : $\text{ppcm}\,(a_1, a_2, \ldots, a_n) = q = P/D$.

Exercice 12 :

Soit $a_1, a_2, \ldots, a_n \in \mathbb{N}^*$, $(n \geqslant 2)$; $M = a_1 a_2 \ldots a_n$;
$\mu = \text{ppcm}\,(a_1, a_2, \ldots, a_n)$; $M_i = \dfrac{M}{a_i}$ $(1 \leqslant i \leqslant n)$;
$\Delta = \text{pgcd}\,(M_1, M_2, \ldots, M_n)$.
a) Prouver : $M = \mu\Delta$.
b) Soient :
$R = \text{ppcm}\,(M_1, M_2, \ldots, M_n)$ et $D = \text{pgcd}\,(a_1, a_2, \ldots, a_n)$.
Prouver : $M = RD$. ■

a) On peut appliquer le résultat de l'exercice précédent, puisque M est un multiple commun de $a_1, a_2, \ldots, a_n$; il suffit de remplacer P par M, P_i par M_i, D par Δ ; nous obtenons : $M = \Delta\ \text{ppcm}\,(a_1, a_2, \ldots, a_n)$, c'est-à-dire $M = \mu\Delta$.

b) Posons pour $i \in [\![1, n]\!]$, $a_i = Da'_i$; alors pour tout $i \in [\![1, n]\!]$, $M = M_i D a'_i$; donc D divise M et le quotient q est un multiple com

Si Q est un multiple commun des M_i, posons pour $i \in [\![1,n]\!]$, $Q = M_i u_i$; donc pour tout $i \in [\![1,n]\!]$, $Qa_i = M_i a_i u_i = M u_i$, et $M \mid Qa_i$; par conséquent $M \mid \operatorname{pgcd}(Qa_1, Qa_2, \ldots, Qa_n) = Q \operatorname{pgcd}(a_1, a_2, \ldots, a_n) = Q\,D$. Nous en déduisons que Q est un multiple de $q = M/D$.
Ce qui précède montre que q est le plus petit commun multiple des M_i, c'est-à-dire $M/D = R$, soit encore $M = R\,D$.

Exercice 18 :

> Soit a et b deux entiers premiers entre eux $\geqslant 1$. On pose $S = \{ax + by \mid (x,y) \in \mathbb{N}^2\}$. Montrer qu'il existe un entier m_0, le plus petit possible, tel que $(\forall m \in \mathbb{N})\ (m \geqslant m_0) \Rightarrow (m \in S)$. Quelle est la valeur de m_0 ? ■

Les entiers a et b sont premiers entre eux, il existe donc deux entiers relatifs u et v tels que $u\,a + v\,b = 1$, et on peut supposer $u \geqslant 0$ et $v \geqslant 0$ car pour tout $\lambda \in \mathbb{N}$, $(u + \lambda\,b)a - (v + \lambda\,a)b = 1$.
Soit m entier cherchons d'abord l'ensemble des couples $(x,y) \in \mathbb{Z}^2$ tels que $ax + by = m$, soit $ax + by = aum - bvm$ ou encore $b(y + vm) = a(um - x)$.
Comme a et b sont premiers entre eux, le théorème de Gauss nous permet d'affirmer que cette égalité est équivalente à la proposition :

$$(\exists k \in \mathbb{Z})\ \ x = um - kb \text{ et } y = ka - vm\ .$$

L'entier m est donc dans l'ensemble S si, et seulement si, il existe un entier relatif k tel que $um \geqslant kb$ et $ka \geqslant vm$, ce qui s'écrit :

$$\frac{vm}{a} \leqslant k \leqslant \frac{um}{b}\ .$$

Finalement on voit que $m \in S$ si, et seulement si, il existe un entier dans l'intervalle $[(vm)/a, (um)/b]$, ce qui est certainement vrai si $m \geqslant ab$, car alors :

$$\frac{um}{b} - \frac{vm}{a} = \frac{au - bv}{ab} m = \frac{m}{ab} \geqslant 1.$$

Cela répond à la première partie de la question. Déterminons maintenant le plus grand nombre entier n_0 qui n'est pas dans S.

Si $m \notin S$, il n'y a pas d'entier dans l'intervalle $[(vm)/a, (um)/b]$, donc $\lfloor (vm)/a \rfloor = \lfloor (um)/b \rfloor$ (parties entières) et (vm/a) et $(um)/b$ ne sont pas entiers. Soit $q = [(vm)/a] = [(um)/b]$, on peut donc poser $vm = qa + r$ où $0 < r < a$, et $um = qb + s$ où $0 < s < b$. On constate alors que $m = (au - bv)m = a(qb + s) - b(qa + r) = as - br \leqslant a(b-1) - b = ab - a - b$.
Vérifions que ce nombre $n_0 = ab - a - b$ n'est pas dans S ; il sera alors le plus grand entier qui n'est pas dans S. On constate que :

$$\frac{v(ab - a - b)}{a} = v(b-1) - \frac{bv}{a} = v(b-1) - \frac{ua - 1}{a} = vb - v \qquad 1$$

et :

$$\frac{u(ab-a-b)}{b} = u(a-1) - \frac{vb+1}{b} = ua - u - v - \frac{1}{b} = vb - u - v + 1 - \frac{1}{b} .$$

En posant $p = vb - u - v$ (entier), nous obtenons :

$$p < \frac{vn_0}{a} = p + \frac{1}{a} \leqslant p + 1 - \frac{1}{b} = \frac{un_0}{b} < p + 1.$$

L'entier n_0 n'est donc pas dans S, c'est le plus grand entier qui n'est pas dans S. L'entier m_0 est donc $m_0 = n_0 + 1 = ab - a - b + 1 = (a-1)(b-1)$.

Exercice 19 :

> On définit les entiers a_n et b_n par $(1+\sqrt{2})^n = a_n + b_n\sqrt{2}$ $(n \in \mathbb{Z})$. Montrer que a_n et b_n sont premiers entre eux. ■

Notons $x = \sqrt{2}$. Pour tout entier relatif n, on peut écrire :

$$(1+x)^{n+1} = (a_n + b_n x)(1+x) = a_n + 2b_n + x(a_n + b_n) = a_{n+1} + xb_{n+1} .$$

Comme x est irrationnel, nous en déduisons que pour tout $n \in \mathbb{Z}$, $a_{n+1} = a_n + 2b_n$ et $b_{n+1} = a_n + b_n$. On voit facilement que tout diviseur commun de a_n et de b_n est aussi diviseur commun de a_{n+1} et de b_{n+1}. Mais on constate aussi que pour tout $n \in \mathbb{Z}$, $b_n = a_{n+1} - b_{n+1}$ et $a_n = b_{n+1} - b_n = 2b_{n+1} - a_{n+1}$; par conséquent tout diviseur commun de a_{n+1} et de b_{n+1} est aussi diviseur commun de a_n et de b_n. Nous pouvons en déduire que pour tout $n \in \mathbb{Z}$, $\operatorname{pgcd}(a_n, b_n) = \operatorname{pgcd}(a_{n+1}, b_{n+1})$. On voit donc que l'application $n \mapsto \operatorname{pgcd}(a_n, b_n)$ est constante sur $\mathbb{Z}$, sa valeur étant $\operatorname{pgcd}(a_0, b_0) = \operatorname{pgcd}(1, 0) = 1$. Les nombres a_n et b_n sont donc toujours premiers entre eux.

Autre solution :
On vérifie facilement que l'application $\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$, $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ est un automorphisme du corps $\mathbb{Q}(\sqrt{2})$ (cf. § IX.7). Par conséquent, pour tout $n \in \mathbb{Z}$, on a les égalités :

$$a_n - b_n\sqrt{2} = \varphi\big(a_n + b_n\sqrt{2}\big) = \varphi\big((1+\sqrt{2})^n\big) = \big(\varphi(1+\sqrt{2})\big)^n = (1-\sqrt{2})^n .$$

Nous en déduisons :

$$(1)\quad a_n^2 - 2\,b_n^2 = (a_n - b_n\sqrt{2})(a_n + b_n\sqrt{2}) = (1-\sqrt{2})^n(1+\sqrt{2})^n = (-1)^n .$$

L'égalité (1) est une relation de Bézout entre les entiers a_n et b_n ; ces entiers sont donc premiers entre eux.

Exercice 24 :

Démontrer que tout sous-anneau du corps $\mathbb{Q}$ est un anneau principal. ■

Soit A un sous-anneau de $\mathbb{Q}$, et I un idéal de A. On sait que $\mathbb{Z} \subset A$, et on vérifie facilement que $I \cap \mathbb{Z}$ est un idéal de l'anneau $\mathbb{Z}$, donc de la forme $d\mathbb{Z}$, où $d \in \mathbb{N}$. Montrons que $I = dA$.
Comme $d \in I$, $dA \subset I$; il nous faut montrer l'inclusion opposée. Supposons $r = n/m \in I$, $n \in \mathbb{Z}$ et $m \in \mathbb{N}^*$ entiers premiers entre eux. Alors $m \cdot (n/m) = n \in I \cap \mathbb{Z} = d\mathbb{Z}$; on peut donc poser $n = dn'$ ($n' \in \mathbb{Z}$), d'où $r = d(n'/m)$. Or les entiers n et m sont premiers entre eux, et il existe donc deux entiers u et v tels que $un + vm = 1$; donc $(1/m) = u(n/m) + v \in A$ (puisque $\mathbb{Z} \subset A$) ; nous en déduisons que $(n'/m) \in A$ et que $r = d(n'/m) \in dA$. Donc $I \subset dA$.

Nous avons bien démontré que $I = dA$, si $I \cap \mathbb{Z} = d\mathbb{Z}$. Tout sous-anneau du corps $\mathbb{Q}$ est un anneau intègre, dans lequel tout idéal est principal ; c' est donc un anneau principal.

§ IV.3 *ÉLÉMENTS INVERSIBLES DES ANNEAUX* $\mathbb{Z}/_{n\mathbb{Z}}$

Exercice 7 :

Montrer $\varphi(n) = \sum_{k=1}^{n-1} \left[\frac{1}{n \vee k}\right]$, où φ est *l'indicateur d'Euler*, et où $[x]$ est la *partie entière* du réel x. ■

Il est clair que $\left[\frac{1}{n \vee k}\right] = 0$ si $n \vee k > 1$, et $= 1$ si n et k sont premiers entre eux. La somme $\sum_{k=1}^{n-1} \left[\frac{1}{n \vee k}\right]$ est donc le nombre d'entiers dans l'intervalle $[\![1, n-1]\!]$ qui sont premiers avec n ; ce nombre est $\varphi(n)$ d'après le théorème IV.3.2.

Exercice 8 :

Soit $(a_i)_{i \in \mathbb{N}}$ une suite d'entiers en progression arithmétique. Montrer qu'on peut extraire de cette suite une sous-suite de termes en progression géométrique. Généraliser si $a_i \in \mathbb{Q}$ pour tout i. ■

Puisque la suite $(a_i)_{i\in\mathbb{N}}$ est en progression arithmétique, il existe deux entiers a et b tels que pour tout $i \in \mathbb{N}$, $a_i = a + ib$. Si $b = 0$ la proposition est évidemment vraie. Nous supposerons désormais $b \neq 0$. Nous pouvons supposer $b > 0$, puisque si on peut extraire une suite en progression géométrique de la suite $(-a_i)_{i\in\mathbb{N}}$, alors on peut extraire une suite en progression géométrique de la suite $(a_i)_{i\in\mathbb{N}}$. Nous pouvons aussi supposer $a > 0$, car puisque $b > 0$, pour i assez grand $a_i > 0$.

Nous devons trouver deux entiers μ et k tels que pour tout $j \in \mathbb{N}$, μk^j soit un terme de la suite $(a + ib)_{i\in\mathbb{N}}$; les entiers μ et k doivent nécessairement vérifier la condition $\forall j \in \mathbb{N}\ \mu k^j \equiv a\ [b]$. Prenons $\mu = a$ et choisissons un entier $k > 1$ tel que $k \equiv 1\ [b]$ (par exemple $b + 1$) ; alors pour tout j entier $a k^j \equiv a\ [b]$, donc il existe un entier p_j tel que $a k^j = a + p_j b$; la suite $(p_j)_{j\in\mathbb{N}}$ est strictement croissante puisque la suite $(a k^j)_{j\in\mathbb{N}}$ l'est, et comme $p_0 = 0$, c'est une suite strictement croissante d'entiers naturels. La suite $(a k^j)_{j\in\mathbb{N}}$ est donc bien extraite de la suite $(a_i)_{i\in\mathbb{N}}$.

Si $(a_i)_{i\in\mathbb{N}}$ est une suite de rationnels en progression arithmétique, il existe deux rationnels r et s tels que pour tout $i \in \mathbb{N}$, $a_i = r + s\,i$. En réduisant les fractions r et s à leur dénominateur commun, on peut écrire $r = a/d$ et $s = b/d$ où $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $d \in \mathbb{N}^*$. D'après ce qui précède on peut extraire de la suite d'entiers $(da_i)_{i\in\mathbb{N}}$, une suite d'entiers en progression géométrique. On peut donc extraire de la suite $(a_i)_{i\in\mathbb{N}}$ une suite de rationnels en progression géométrique.

§ IV.4 *NOMBRES PREMIERS*

Exercice 2 :

‖ Montrer : $(\forall n \in \mathbb{N})\quad n^7 - n \equiv 0 \mod (42)$. ■

Comme $42 = 2\times3\times7$ et que 2, 3 et 7 sont premiers entre eux deux à deux, la proposition de l'énoncé est vraie si, et seulement si : $(\forall n \in \mathbb{N})\quad n^7 \equiv n$ modulo 2, 3 et 7. Comme 7 est premier, la congruence est vraie modulo 7 (théorème de Fermat). En considérant que les classes modulo 3 sont celles de -1, 0 et 1, on voit facilement que pour tout n entier, $n^7 \equiv n\ [3]$. La relation est évidemment vraie modulo 2 puisque les classes modulo 2 sont celles de 0 et de 1.

Exercice 4 :

‖ Trouver $a \in \mathbb{N}^*$ pour que $1 + a + a^2 + a^3 + a^4$ soit un carré *parfait*. (Réponse $a = 3$.) ■

Si ce nombre est un carré parfait, il s'écrit n^2 où n est un entier $> a^2$. Posons $n = a^2 + b$, où $b \in \mathbb{N}^*$. Le nombre b doit vérifier l'égalité : $2ba^2 + b^2 = 1 + a + a^2 + a^3$, soit encore $a^2(a - 2b) = b^2 - (1 + a + a^2)$. Si $a \geqslant 2b$, alors $b^2 \geqslant 1 + a + a^2 \geqslant 1 + 2b + 4b^2$, d'où $1 + 2b + 3b^2 \leqslant 0$ ce qui est impossible, donc $a < 2b$, soit $a \leqslant 2b - 1$. La condition sur b s'écrit alors $a^2(a - 2b + 1) = b^2 - (1 + a)$, d'où $b^2 \leqslant 1 + a \leqslant 2b$ et $b \leqslant 2$. Il est impossible que b soit égal à 1 car il faudrait $a^2(a - 1) = -a$, soit $1 = a(1 - a)$. La seule possibilité est donc $b = 2$. La condition sur a s'écrit alors $a^2(a - 3) = 3 - a$, soit $(a^2 + 1)(a - 3) = 0$. La seule solution est donc bien $a = 3$, et $1 + a + a^2 + a^3 + a^4 = (2 + a^2)^2 = 121$.

Exercice 8 :

> Soit a et n deux entiers, $a \geqslant 1$, $n \geqslant 2$. On suppose $a \vee n = 1$, et que *la période de* $a \bmod(n)$ est $n - 1$. Montrer que n est premier. ■

Soit x la classe de a modulo n. La classe x est inversible, puisque a et n sont premiers entre eux. Comme la période de x est $n - 1$ les classes $1, x, x^2, \ldots, x^{n-2}$ sont deux à deux distinctes, et inversibles. Il y a donc au moins $n - 1$ éléments inversibles dans l'anneau $\mathbb{Z}/_{n\mathbb{Z}}$, qui a n éléments. Tous les éléments non nuls de cet anneau sont donc inversibles, et cet anneau est donc un corps. Nous pouvons en déduire que n est premier (Théorème IV.4.4).

Exercice 11 :

> Pour $m \neq n$ entiers naturels, montrer que $2^{2^m} + 1$ et $2^{2^n} + 1$ sont premiers entre eux. En déduire que l'ensemble des nombres premiers est infini. ■

On peut supposer $m > n$ et poser $m = n + p$, où $p \in \mathbb{N}^*$. Nous pouvons alors écrire :

$$b = 2^{2^m} + 1 = 2^{2^{n+p}} + 1 = 2^{2^n \times 2^p} + 1 = \left(2^{2^n}\right)^{2^p} + 1 .$$

Posons $a = 2^{2^n} + 1$. On voit que $b = (a - 1)^{2^p} + 1$, et par conséquent $b \equiv 2 \bmod(a)$ (puisque $p > 0$). Soit k entier tel que $b = 2 + ka$; si d entier divise a et b, il divise 2, mais comme a et b sont impairs, d ne peut être que 1. Les entiers a et b sont donc premiers entre eux, ce qu'il fallait démontrer.

Soit pour tout n entier p_n le plus petit nombre premier qui divise $2^{2^n} + 1$, d'après ce qui précède la suite $(p_n)_{n\in\mathbb{N}}$ est injective. L'ensemble des nombres premiers est donc infini.

Exercice 12 :

Soit p_n le n-ième nombre premier. Montrer que si $n \geqslant 3$
$$p_1 p_2 \dots p_n \geqslant p_{n+1} + p_{n+2} \,.\, \blacksquare$$

Puisque $n \geqslant 3$, $p_2 \dots p_n - 2 \geqslant 3 \times 5 - 2 = 13 > 1$; ce nombre n'est pas divisible par $p_1 = 2$ car il est impair, et il n'est pas divisible par les nombres premiers $p_2, p_3, \dots, p_n$; son plus petit diviseur premier est donc $\geqslant p_{n+1}$; nous pouvons en déduire $p_2 \dots p_n - 2 \geqslant p_{n+1}$. On voit qu'a fortiori $p_1 p_2 \dots p_n - p_{n+1} \geqslant 2 > 1$; cet entier n'est divisible par aucun des nombres premiers $p_1, p_2, \dots, p_n$ et p_{n+1}, son plus petit diviseur premier est donc $\geqslant p_{n+2}$. Donc $p_1 p_2 \dots p_n - p_{n+1} \geqslant p_{n+2}$, soit $p_1 p_2 \dots p_n \geqslant p_{n+1} + p_{n+2}$, ce qu'il fallait démontrer.

On remarquera que $2 \times 3 \times 5 \geqslant 7 + 11$, mais que $2 \times 3 < 5 + 7$.

§ IV.5 *DÉCOMPOSITION EN FACTEURS PREMIERS*

Exercice 1 :

Montrer que $p = 1093$ est un nombre premier et prouver que :
$$2^{1\,092} - 1 \equiv 0 \bmod (p^2) \,.\, \blacksquare$$

Si $p = 1093$ n'était pas premier, son plus petit diviseur > 1 serait un nombre premier q tel que $q^2 \leqslant p$, donc $q \leqslant 34$ puisque $34^2 = 1156$. Pour montrer que le nombre entier impair 1093 est premier, il suffit donc de vérifier qu'il n'est divisible par aucun des nombres premiers impairs $\leqslant 34$, c'est-à-dire $3, 5, 7, 11, 13, 17, 19, 23, 29, 31$; cette vérification ne pose pas de problèmes.

Comme $182 = 2 \cdot 13 \cdot 7$, on peut écrire $2^{182} = \left((2^{13})^2\right)^7$. On vérifie facilement que :
$$2^{13} = 8\,192 = 7 \times p + 541 \ ;$$
en élevant au carré on obtient :
$$2^{26} \equiv 1082 \times 7 \times p + (541)^2 \quad [p^2] \,.$$
Or :
$$1082 \times 7 \times p + (541)^2 = 7(p - 11)p + 267\,p + 850 = 7\,p^2 + 190\,p + 850$$
$$= 7\,p^2 + 191\,p - 243 = 7\,p^2 + 191\,p - 3^5 \ ,$$
d'où :
$$2^{26} \equiv 191\,p - 3^5 \quad [p^2] \,.$$

Elevons cette congruence à la puissance 7 en utilisant la formule du binôme ; dans une congruence modulo p^2 nous pouvons ne garder que deux termes ; nous obtenons par conséquent :

$$(2^{26})^7 \equiv 7 \times 191 \times p \times 3^{30} - 3^{35} \quad [p^2] \ .$$

Nous pouvons ne calculer le coefficient de p que modulo p. On constate d'autre part que $3^7 = 2187 = 1 + 2p$. Après un calcul facile, nous voyons que :

$$7 \times 191 \times 3^{30} \equiv 7 \times 191 \times 3^2 \equiv 10 \quad [p] \ .$$

En utilisant comme précédemment la formule du binôme, nous obtenons finalement :

$$2^{182} \equiv 10p - (1 + 2p)^5 \equiv 10p - (1 + 10p) \equiv -1 \quad [p^2] \ .$$

Par conséquent :

$$2^{1092} = 2^{6 \times 182} \equiv (-1)^6 \equiv 1 \ [p^2] \ .$$

On peut évidemment trouver de nombreuses autres méthodes, plus ou moins rapides, pour vérifier que $2^{1092} \equiv 1 \ [p^2]$. On peut aussi appliquer un algorithme (rapide) de calcul de puissance (modulo p^2).

Exercice 2 :

Soit p un nombre premier > 17.
Alors $p^{16} - 1 \equiv 0 \mod (16\,320)$. ■

On vérifie que $16\,320 = 64 \times 3 \times 5 \times 17$. Comme les nombres 64, 3, 5, et 17 sont premiers entre eux deux à deux, le nombre p^{16} est congru à 1 modulo $64 \times 3 \times 5 \times 17$, si, et seulement si, cette relation est vraie modulo 64, 3, 5, et 17. Les nombres 3, 5 et 17 étant premiers, en utilisant le théorème de Fermat on voit que : $p^2 \equiv 1 \mod (3)$, donc $p^{16} \equiv 1 \mod (3)$; $p^4 \equiv 1 \mod (5)$, donc $p^{16} \equiv 1 \mod (5)$; et $p^{16} \equiv 1 \mod (17)$. Il reste donc à prouver $p^{16} \equiv 1 \mod (64)$. Puisque p est impair, nous pouvons poser $p = 2k + 1$, où k est entier ; on obtient alors : $p^2 = 1 + 4k + 4k^2 = 1 + 4k(k+1)$, et comme $k(k+1)$ est pair, nous pouvons écrire $p^2 = 1 + 8h$, où h est entier ; en utilisant la formule du binôme de Newton pour développer $p^{16} = (1 + 8h)^8$, on voit facilement que $p^{16} \equiv 1 + 8 \times 8h \equiv 1 \mod (64)$, ce qui restait à démontrer.

Exercice 4 :

Trouver tous les nombres premiers de la forme $n^n + 1$ qui ont moins de 300 000 chiffres (Sierpinski). ■

Montrons que si a et h sont entiers, $a > 1$ et $h \geqslant 1$, le nombre $a^{2h+1} + 1$ n'est pas premier. En effet $a^{2h+1} + 1 = (a+1)q$, où :

$$q = a^{2h} - a^{2h-1} + a^{2h-2} - \ldots + a^2 - a + 1 = (a-1)(a^{2h-1} + \ldots + 1) + 1.$$

Comme $h \geqslant 1$, $q \geqslant (a-1)(a+1) + 1 = a^2 > 1$; le nombre $a^{2h+1} + 1$ est donc composé.

Nous pouvons déduire de ce qui précède que si $a > 1$ et que le nombre $a^m + 1$ est premier, alors m est une puissance de 2 (éventuellement $m = 1$). En effet si $m > 1$ et m a un facteur premier impair $k > 1$, posons $m = kq$; comme $a^m + 1 = (a^q)^k + 1$, ce nombre n'est pas premier.

Supposons que le nombre $n^n + 1$ soit premier, alors n est une puissance de 2 (ou $n = 1$) ; posons $n = 2^k$, $k \in \mathbb{N}$. Comme $n^n + 1 = (2^k)^{2^k} + 1 = 2^{k2^k} + 1$ est premier, d'après ce qui précède, $k2^k$, donc k, est une puissance de 2. Posons $k = 2^h$, $h \in \mathbb{N}$, on voit que $k2^k = 2^{h+k}$ et donc que $n^n + 1 = 2^{2^{h+k}} + 1 = F_{h+k} = F_{h+2^h}$ (voir l'exercice précédent).

Calculons quelques valeurs :

h	=	0	1	2	3	4
2^h	=	1	2	4	8	16
$h + 2^h$	=	1	3	6	11	20

On voit donc que si $h \geqslant 4$, alors $h + 2^h \geqslant 20$, et donc $F_{h+2^h} \geqslant 2^{2^{20}}$. On vérifie que $2^{10} = 1\,024 > 10^3$, donc $2^{20} > 10^6$, d'où $2^{2^{20}} > 2^{10^6} = 2^{10 \times 10^5} > 10^{3 \times 10^5} = 10^{300\,000}$. Les nombres F_{h+2^h}, où $h \geqslant 4$ ont donc strictement plus de 300 000 chiffres. On vérifie que $F_1 = 2^{2^1} + 1 = 5$, et $F_3 = 2^{2^3} + 1 = 257$ sont premiers. Comme F_6 et F_{11} sont composés, 5 et 257 sont les seuls nombres premiers de la forme $n^n + 1$ qui ont moins de 300 000 chiffres.

Exercice 8 :

a) Soit a un entier impair premier avec 3 et 5. Prouver que :
$(a^2 - 1)(a^4 - 16)[a^2 - (2n+1)^2]^2 \equiv 0 \bmod (23\,040)$.

b) Si a est impair et premier avec 5,
$(a^2 - 1)(a^2 - 9)(a^2 - 49) \equiv 0 \bmod (23\,040)$. ■

a) Posons $q = (a^2-1)(a^4-16)[a^2-(2n+1)^2]^2$. Comme $23\,040 = 2^9 \times 3^2 \times 5$, q est divisible par 23 040 si, et seulement si, il est divisible par 2^9, 9 et 5. Comme a est premier avec 5, et que 5 est premier, on sait que $a^4 \equiv 1 \bmod (5)$, par conséquent 5 divise $a^4 - 16$ et donc divise q. (

premier avec 3, sa classe modulo 9 est celle de 1, 2, 4, ou l'une des classes opposées, son carré est donc congru à 1, 4 ou 7 modulo 9 ; la classe de $(a^2-1)(a^4-16) = (a^2-1)(a^2-4)(a^2+4)$ est bien nulle dans les deux premiers cas, et si $a^2 \equiv 7 \bmod (9)$, alors $(a^2-1)(a^4-16) \equiv 6\times 33 \equiv 0 \bmod (9)$, donc q est bien dans tous les cas divisible par 9. Comme a est impair, $a = 2k+1$ où $k \in \mathbb{N}$, donc $a^2 = 1 + 4k + 4k^2 = 1 + 4k(k+1)$ et $a^2 \equiv 1 \bmod (8)$ puisque $k(k+1)$ est pair ; de même $a^2 - (2n+1)^2$ est divisible par 8, donc $(a^2-1)[a^2-(2n+1)^2]^2$ est divisible par $8^3 = 2^9$. Nous en déduisons que q est divisible par 2^9, 9 et 5 donc divisible par leur produit 23 040.

b) Posons $q = (a^2-1)(a^2-9)(a^2-49)$.
Nous pouvons écrire $q \equiv (a^2-1)(a^2+1)(a^2+1) \equiv (a^4-1)(a^2+1) \bmod (5)$; comme a est premier avec 5, et que 5 est premier, $a^4 \equiv 1 \bmod (5)$, donc 5 divise q.
On voit que $q \equiv (a^2-1)a^2(a^2-4) \bmod (9)$; les classes modulo 9 sont celles de 0, 1, 2, 3, 4 et les classes opposées, les classes des carrés sont donc celles de 0, 1, 4 et 7 ; si a^2 est congru à 0,1 ou 4 modulo 9, alors $q \equiv 0 \bmod (9)$, et si a^2 est congru à 7 modulo 9, alors $q \equiv 6 \times 7 \times 3 \equiv 0 \bmod (9)$.
Puisque a est impair, nous pouvons poser $a = 2k+1$, où $k \in \mathbb{N}$; alors $a^2 - 1 = 4k(k+1) = 8h$, où $h \in \mathbb{N}$; avec ces notations $q = 8h(8h-8)(8h-48) = 8^3 h(h-1)(h-6)$; on voit donc que q est divisible par $8^3 = 2^9$, et même par 2^{10} puisque $h(h-1)$ est pair.

Nous pouvons déduire de ce qui précède que $q = (a^2-1)(a^2-9)(a^2-49)$ est divisible par $23\,040 = 2^9 \times 3^2 \times 5$ (et même par 46080).

Exercice 11 :

Soit m, n, k entiers > 1 tels que $m = nk$
a) prouver : $(n!)^k$ et $(k!)^n$ divisent $m!$;
b) prouver que ppcm $\left((n!)^k, (k!)^n\right)$ divise $m!$. ■

a) Montrons par récurrence sur l'entier $k \geqslant 1$ que $(n!)^k$ divise $(nk)!$. C'est vrai pour $k = 1$. Si c'est vrai pour $k \geqslant 1$, alors comme :

$$(n(k+1))! = n!(nk)!\binom{n(k+1)}{n},$$

il est clair que $(n!)^{k+1}$ divise $(n(k+1))!$. La propriété est donc vraie pour tout k entier. Par symétrie il est évident que $(k!)^n$ divise $(nk)!$.

b) Nous pouvons déduire de ce qui précède que $(nk)!$ est un multiple commun de $(n!)^k$ et de $(k!)^n$, donc un multiple du ppcm de ces deux entiers.

Exercice 14 (*nombres parfaits*) :

$n \in \mathbb{N}^*$ s'appelle nombre *parfait* ssi la somme $D(n)$ de ses diviseurs est égale à $2n$.

a) Montrer que si p est un nombre premier tel que $2^p - 1$ soit premier, alors $E_p = 2^{p-1}(2^p - 1)$ est un nombre parfait (E_p est le p-ième *nombre d'Euclide*). Calculer E_2, E_3, E_5, E_7.

b) Réciproquement soit n un nombre parfait *pair*. Mettre n sous la forme $2^a \times b$, où $a \geqslant 1$ et où b est impair. En déduire que $D(n) = D(b) \times (2^{a+1} - 1) = 2n = 2^{a+1} \times b$, d'où $b = (2^{a+1} - 1)c$ et $D(b) = 2^{a+1}c$. Prouver que $c = 1$ et que $2^{a+1} - 1$ est premier. Conclure que les seuls nombres parfaits pairs sont les nombres d'Euclide E_p.

N.B. : Peut-être un jour trouvera-t-on un nombre parfait impair, mais il devra être très grand, à moins que l'on puisse prouver qu'il n'en existe pas ! ■

Vérifions d'abord que si $2^p - 1$ est premier, alors p est premier. En effet si a et b sont des entiers > 1, comme $2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + \ldots + 2^a + 1)$, ce nombre est composé. Si $2^p - 1$ est premier, alors p n'est pas composé et n'est évidemment pas 1, donc il est premier.

a) Puisque $2^p - 1$ est premier, les diviseurs de $E_p = 2^{p-1}(2^p - 1)$ sont les nombres 2^k et les nombres $2^k(2^p - 1)$ où $k \in [\![0, p-1]\!]$. Leur somme est donc $D(E_p) = 2^p - 1 + (2^p - 1)(2^p - 1) = 2^p(2^p - 1) = 2E_p$. Les nombres E_p, si $2^p - 1$ est premier, sont donc parfaits. On trouve facilement $E_2 = 6$, $E_3 = 28$, $E_5 = 496$.

b) Les diviseurs du nombre $n = 2^a \times b$ sont les nombres de la forme $2^{a'} \times b'$, où $a' \in [\![0, a]\!]$ et b' est un diviseur de b. Donc :

$$D(n) = \sum_{0 \leqslant a' \leqslant a,\ b' | b} 2^{a'} b' = \left(\sum_{0 \leqslant a' \leqslant a} 2^{a'} \right) D(b) = (2^{a+1} - 1) D(b).$$

Puisque n est parfait, $2n = 2^{a+1}b = (2^{a+1} - 1)D(b)$. Nous déduisons de cela que l'entier $2^{a+1} - 1$, qui est premier avec 2^{a+1}, divise b. Soit c entier > 0 tel que $b = (2^{a+1} - 1)c$, par division $D(b) = 2^{a+1}c$. On vérifie que $2^{a+1} - 1 > 1$ car $a \geqslant 1$ (c'est ici qu'intervient le fait que n est pair), donc si $c > 1$ alors l'entier b a au moins 3 diviseurs $(2^{a+1} - 1)c$, c, et 1, distincts, dont la somme est $2^{a+1}c + 1 > D(b) = 2^{a+1}c$, ce qui est contradictoire ; donc $c = 1$. Le nombre $b = 2^{a+1} - 1$ a au moins pour diviseurs 2^{a+1} -

la somme est 2^{a+1}, mais comme on a $D(b) = 2^{a+1}$, cela signifie que b n'a pas d'autres diviseurs, c'est-à-dire qu'il est premier. Posons enfin $p = a+1$, comme $2^p - 1$ est premier, le nombre p est nécessairement premier. Le nombre parfait n est donc un nombre d'Euclide.

Exercice 20 :

Montrer que $(\forall m \in \mathbb{N})\ (\forall n \in \mathbb{N})$, le nombre $\dfrac{(2m)!\,(2n)!}{m!\,n!\,(m+n)!}$ est entier. ■

Nous utiliserons la propriété démontrée dans l'exercice 10b), c'est-à-dire pour tout n entier $\geqslant 2$ et p premier,

$$v_p(n!) = \sum_{k \geqslant 1} \left[\frac{n}{p^k}\right].$$

La somme ci-dessus a un sens car elle ne comporte qu'un nombre fini de termes non nuls.

Soit p un nombre premier, on constate l'égalité :

$$v_p((2m)!\,(2n)!) - v_p(m!\,n!\,(m+n)!) = \\ = \sum_{k \geqslant 1} \left(\left[\frac{2m}{p^k}\right] + \left[\frac{2n}{p^k}\right] - \left[\frac{m}{p^k}\right] - \left[\frac{n}{p^k}\right] - \left[\frac{m+n}{p^k}\right] \right).$$

Pour $k \geqslant 1$ donné, posons $\dfrac{m}{p^k} = a + x$, $\dfrac{n}{p^k} = b + y$, où a et b sont entiers et x et y rationnels dans l'intervalle $[0, 1[$. On voit que :

$$\left[\frac{2m}{p^k}\right] + \left[\frac{2n}{p^k}\right] - \left[\frac{m}{p^k}\right] - \left[\frac{n}{p^k}\right] - \left[\frac{m+n}{p^k}\right] = \\ = 2a + [2x] + 2b + [2y] - a - b - (a+b) - [x+y] = [2x] + [2y] - [x+y].$$

Ce nombre est toujours $\geqslant 0$, car si par exemple $x \geqslant y$, alors $[2x] \geqslant [x+y]$. Nous en déduisons que pour tout p premier,

$$v_p((2m)!\,(2n)!) \geqslant v_p(m!\,n!\,(m+n)!).$$

Par conséquent $m!\,n!\,(m+n)!$ divise $(2m)!\,(2n)!$, ce qu'il fallait démontrer.

Exercice 21 :

Soit $a_1, a_2, \ldots, a_n \in \mathbb{N}^*$. Soit P_k le produit des pgcd de ces nombres pris k à k $(1 \leqslant k \leqslant n\ ;\ P_1 = a_1 a_2 \ldots a_n)$

Démontrer : $\operatorname{ppcm}(a_1, a_2, \ldots, a_n) = \dfrac{P_1 \cdot P_3 \cdot P_5 \ldots}{P_2 \cdot P_4 \cdot P_6 \ldots}$. ■

Nous utiliserons ici la formule du crible, démontrée dans l'exercice 9 du chapitre III.4.

Soit p un nombre premier, posons $E_i = \{k \in \mathbb{N}^*,\ p^k | a_i\}$ pour $i \in [\![1, n]\!]$; il est clair que $v_p(a_i) = \operatorname{card}(E_i)$. On observe que :

$$\bigcup_{i=1}^{n} E_i = \{k \in \mathbb{N}^*,\ (\exists i \in [\![1, n]\!])\quad p^k |\ a_i\} =$$

$$= \{k \in \mathbb{N}^*,\quad p^k |\ \operatorname{ppcm}(a_1, a_2, \ldots, a_n)\}\ ,$$

d'où :

$$\operatorname{card}\left(\bigcup_{i=1}^{n} E_i\right) = v_p(\operatorname{ppcm}(a_1, a_2, \ldots, a_n)).$$

Si P est une partie de $[\![1, n]\!]$, on voit aussi que :

$$\bigcap_{i \in P} E_i = \{k \in \mathbb{N}^*,\ (\forall i \in P)\quad p^k |\ a_i\} =$$

$$= \left\{k \in \mathbb{N}^*,\quad p^k |\ \operatorname*{pgcd}_{i \in P}(a_i)\right\}\ ,$$

d'où :

$$\operatorname{card}\left(\bigcap_{i \in P} E_i\right) = v_p\left(\operatorname*{pgcd}_{i \in P}(a_i)\right).$$

Par définition, pour tout k entier, en notant $\mathcal{P}_k$ l'ensemble des parties de $[\![1, n]\!]$ de cardinal k (on peut supposer $k \leqslant n$), on a :

$$P_k = \prod_{P \in \mathcal{P}_k} \operatorname*{pgcd}_{i \in P}(a_i)\quad ,$$

donc :

$$v_p(P_k) = \sum_{P \in \mathcal{P}_k} \operatorname{card}\left(\bigcap_{i \in P} E_i\right)\ .$$

La formule du crible nous permet d'affirmer que :

$$\operatorname{card}\left(\bigcup_{i=1}^{n} E_i\right) = \sum_{k=1}^{n} (-1)^{k-1} \sum_{P \in \mathcal{P}_k} \operatorname{card}\left(\bigcap_{i \in P} E_i\right)\ ,$$

soit ici :

$$v_p(\operatorname{ppcm}(a_1, a_2, \ldots, a_n)) = \sum_{k=1}^{n} (-1)^{k-1} v_p(P_k)\ .$$

En reprenant les notations de l'énoncé nous obtenons pour tout p premier l'égalité :

$$v_p(\text{ppcm}\,(a_1, a_2, \ldots, a_n)) = v_p(P_1 \cdot P_3 \cdot P_5 \ldots) - v_p(P_2 \cdot P_4 \cdot P_6 \ldots) \,.$$

Cela prouve que :

$$\text{ppcm}\,(a_1, a_2, \ldots, a_n) = \frac{P_1 \cdot P_3 \cdot P_5 \ldots}{P_2 \cdot P_4 \cdot P_6 \ldots} \,.$$

NUMÉRATION

Exercice 2 :

Le carré de $111\,111\,111$ est $N = 12\,345\,678\,987\,654\,321$. Montrer sans calculer N^2 que son chiffre du milieu est un 2. ■

On vérifie facilement que $111\,111\,111 = \sum_{i=0}^{8} 10^i$. On voit que :

$$N = \left(\sum_{i=0}^{8} 10^i\right) \times \left(\sum_{j=0}^{8} 10^j\right) = \sum_{k=0}^{16} \sum_{(i,j)\in\mathscr{C}_k} 10^{i+j} = \sum_{k=0}^{16} \text{card}\,(\mathscr{C}_k)\, 10^k \,,$$

où $\mathscr{C}_k = \left\{(i,j) \in [\![0,8]\!]^2 \;\middle|\; i+j=k\right\}$. Les éléments de $\mathscr{C}_k$ sont les couples $(i, k-i)$ où $0 \leqslant i \leqslant 8$ et $k-8 \leqslant i \leqslant k$; si $0 \leqslant k \leqslant 8$, alors $\text{card}\,(\mathscr{C}_k) = k+1 \leqslant 9$, et si $16 \geqslant k \geqslant 9$, alors $\text{card}\,(\mathscr{C}_k) = 8-(k-8)+1 = 17-k \leqslant 8$. Les cardinaux des ensembles $\mathscr{C}_k$ sont donc les chiffres du nombre N ; d'où $N = 12\,345\,678\,987\,654\,321$.

De manière analogue, nous pouvons écrire :

$$N^2 = \sum_{(a,b,c,d)\in[\![0,8]\!]^4} 10^{a+b+c+d} = \sum_{k=0}^{32} \sum_{(a,b,c,d)\in\mathscr{F}_k} 10^k \,,$$

où $\mathscr{F}_k = \left\{(a,b,c,d) \in [\![0,8]\!]^4, \quad a+b+c+d=k\right\}$. Pour tout $k \in [\![0,32]\!]$, posons $c_k = \text{card}\,(\mathscr{F}_k)$; on obtient :

$$N^2 = \sum_{k=0}^{32} c_k\, 10^k \,.$$

Cette formule ne donne pas directement l'écriture décimale de N^2 car les nombres c_k ne sont en général pas < 10. On remarque que, le r

k étant fixé dans l'intervalle $[\![0,32]\!]$, si $(a,b,c,d) \in [\![0,8]\!]^4$ et $a+b+c+d = k$, alors la valeur de d est déterminée par la valeur du triplet (a,b,c) ; le cardinal c_k de $\mathcal{F}_k$ est donc majoré par $9^3 = 729$. Déterminons ces nombres (qui ont tous au plus 3 chiffres).
Soit $k \in [\![0,8]\!]$. Si $(a,b,c,d) \in \mathbb{N}^4$ et que $a+b+c+d = k$ alors $(a,b,c,d) \in [\![0,8]\!]^4$. L'entier c_k est donc le nombre de solutions en entiers $\geqslant 0$ de l'équation $a+b+c+d = k$. On sait que ce nombre est $\binom{k+3}{3}$.
Soit $k \in [\![9,17]\!]$. Si $(a,b,c,d) \in \mathbb{N}^4$, et que $a+b+c+d = k$, il est possible que l'un de ces nombres soit $\geqslant 9$, mais s'il y en a un, il y en a un seul. Le nombre de quadruplets d'entiers (a,b,c,d) tels que $a+b+c+d = k$ et $a \geqslant 9$ est le nombre de solutions en entiers $\geqslant 0$ de l'équation $a'+b+c+d = k-9$, soit $\binom{k-6}{3}$. Le nombre de quadruplets d'entiers (a,b,c,d) tels que $a+b+c+d = k$ et dont l'une des composantes est $\geqslant 9$ est donc $4\binom{k-6}{3}$. Le cardinal de $\mathcal{F}_k$ est donc $\binom{k+3}{3} - 4\binom{k-6}{3}$.
Pour les autres valeurs de k nous pouvons utiliser l'égalité $c_k = c_{32-k}$; en effet, si $(a,b,c,d) \in [\![0,8]\!]^4$ et $a+b+c+d = k$, alors $(8-a,8-b,8-c,8-d) \in [\![0,8]\!]^4$ et la somme de ce quadruplet est $32-k$.

Les premières valeurs de ces coefficients sont $1, 4, 10, 20, 35, 56, \ldots$. Pour calculer N^2, on peut "poser l'opération" :

$$\begin{array}{r}
\cdots 971041 \\
\hline
\cdots \\
056 \\
035 \\
020 \\
010 \\
004 \\
001
\end{array}$$

Dans l'écriture décimale de N^2, on peut déterminer le chiffre a_k (coefficient de 10^k) si on connait le nombre c_k, les deux nombres (éventuellement) précédents : c_{k-1} et c_{k-2}, et la retenue r_k qui provient de le somme de la colonne précédente. La retenue est initialement 0, et elle reste $\leqslant 2$, car si la retenue sur une colonne est $\leqslant 2$, la somme des chiffres de cette colonne, compte tenu de la retenue, est au plus $2+9+9+9 = 29$. Les retenues sont donc toujours $0, 1$ ou 2. On pourra déterminer la retenue r_k en utilisant aussi la valeur de c_{k-3} et, si besoin est, les valeurs des nombres précédents. Vérifions par exemple que le premier chiffre de l'écriture décimale de N^2 est $a_{32} = 1$ ($10^{16} \leqslant N \leqslant 1,3\,10^{16}$, donc $10^{32} \leqslant N^2 \leqslant 1,69\,10^{32}$). L'opération à poser est :

$$\begin{array}{r} \cdots \\ 0\,2\,0 \\ 0\,1\,0 \\ 0\,0\,4 \\ 0\,0\,1 \\ \hline 0\,0\,1\,x\,\cdots \end{array}$$

La valeur du chiffre x est $5, 6$ ou 7, et il n'y pas de retenue à reporter sur la colonne suivante. Le premier chiffre non nul de l'écriture décimale de N^2 est donc $a_{32} = 1$.

Le chiffre médian est donc a_{16}. Il nous faut au moins déterminer les valeurs de c_{16}, c_{15}, et c_{14} ; nous aurons besoin aussi des valeurs de c_{13} et c_{12}. A l'aide des formules précédemment démontrées, on trouve facilement que les valeurs de ces nombres sont $489, 480, 456, 420$ et 375. L'opération à effectuer est :

$$\begin{array}{r} \cdots \\ 3\,7\,5 \\ 4\,2\,0 \\ 4\,5\,6 \\ 4\,8\,0 \\ 4\,8\,9 \\ \cdots \\ \hline \cdots a\,b\,c\,\cdots \end{array}$$

La somme à effectuer dans la colonne 14 au dessus de c est $r_{14}+3+2+6$; comme r_{14} est 0, 1 ou 2, on trouve que c est 1, 2 ou 3 et que $r_{15} = 1$; on trouve ensuite que $b = 0$ et que $r_{16} = 1$. La somme à effectuer dans la colonne 16 est donc 1+4+8+9= 22. Nous pouvons en déduire que $a = a_{16} = 2$ (et que $r_{17} = 2$), ce qu'il fallait démontrer. On remarquera qu'il aurait été impossible de déterminer a sans utiliser la valeur de $c_{12} = 375$.

Exercice 5 :

> Trouver les six derniers chiffres d'un nombre sachant que son cube se termine par $777\,777$. ■

Il s'agit de résoudre l'équation (1) $x^3 = \pi(777\,777)$ dans l'anneau $A = \mathbb{Z}/_{10^6\,\mathbb{Z}}$ (π désigne la projection canonique sur le quotient). Montrons que cette équation admet une solution et une seule.
Comme l'entier $777\,777$ est premier avec 10, il est premier avec 10^6 et sa classe modulo 10^6, $\pi(777\,777)$, est inversible dans l'anneau A ; nous en déduisons que toute solution de l'équation (1) est inversible. Le nombre des éléments inversibles dans l'anneau A est $\varphi(10^6) = 10^5\,(2-1)(5-1) = 400\,000$; comme ce nombre est premier avec 3, il existe un entier u tel que $3u \equiv 1 \bmod (400\,000)$; on voit alors que pour tout x in

l'anneau A, $x^{3u} = x$. Les endomorphismes $x \mapsto x^3$ et $y \mapsto y^u$, du groupe multiplicatif des éléments inversibles de l'anneau A, sont visiblement bijectifs réciproques l'un de l'autre. L'équation (1) a donc une solution et une seule : $\pi(777\,777)^u$. Déterminons une valeur pour u ; on voit que $400\,000 \equiv 1 \bmod (3)$ (somme des chiffres) : $400\,000 = 1 + 399\,999 = 1 + 3 \times 133\,333$; on peut donc choisir $u = -133\,333$, ou $u = 400\,000 - 133\,333 = 266\,667$. Les 6 chiffres cherchés sont donc les 6 derniers chiffres du nombre $777\,777^{266\,667}$.

Comme il n'est pas immédiat de trouver ainsi ces chiffres (bien que ce soit possible en utilisant un algorithme rapide de calcul de puissance), nous utiliserons une autre méthode. Dans ce qui suit n désignera un entier tel que $n^3 \equiv 777\,777 \bmod (10^6)$.

Soit a_0 le dernier chiffre de n. On voit que $a_0^3 \equiv n^3 \equiv 7 \bmod (10)$. Une solution évidente est $a_0 = 3$ et il n'y en a pas d'autre, car si x est une classe modulo 10 telle que $x^3 = 7$, alors x est inversible, et comme $\varphi(10) = 4$, $x^4 = 1$, donc $x^4 = 7x = 1$, d'où $21x = x = 3$.
Le chiffre a_1 de l'entier n, est tel que $(10\,a_1 + a_0)^3 \equiv n^3 \equiv 77 \bmod (100)$. En utilisant la formule du binôme nous obtenons : $3 \cdot 10\,a_1 a_0^2 + a_0^3 \equiv 77 \bmod (100)$, soit $3 \cdot 10\,a_1 a_0^2 \equiv 77 - 27 \equiv 50 \bmod (100)$. On peut diviser cette congruence par 10, pour obtenir : $3 a_1 a_0^2 \equiv 5 \bmod (10)$, soit en multipliant par $a_0 = 3$ des deux cotés, $3 \cdot a_0^3 \cdot a_1 \equiv 3 \cdot 7 \cdot a_1 \equiv a_1 \equiv 3 \cdot 5 \equiv 5 \bmod (10)$. On peut vérifier qu'en posant $n_2 = 53$ alors $n_2^3 = 148877$; mais nous pouvons ne retenir pour la suite que $n_2^3 \equiv 877 \bmod (10^3)$.
Les autres chiffres s'obtiennent de manière analogue. Notons $a_0, a_2, \ldots, a_5$, les 6 derniers chiffres de n. Posons pour $k \in [\![1, 6]\!]$, $n_k = \overline{a_{k-1} a_{k-2} \cdots a_0}$ et notons r_k le reste dans la division euclidienne de n_k^3 par 10^{k+1}. Supposons $k < 6$, on voit que $(10^k a_k + n_k)^3 \equiv n^3 \equiv 777\,777 \bmod (10^{k+1})$. En développant le cube, on obtient : $3 \cdot 10^k a_k n_k^2 + n_k^3 \equiv 777\,777 \bmod (10^{k+1})$, soit encore (1) $3 \cdot 10^k a_k n_k^2 \equiv 777\,777 - r_k \bmod (10^{k+1})$. Or $777\,777 - r_k$ est divisible par 10^k ; posons $m_k = (777\,777 - r_k)/10^k$, et notons c_k le reste dans la division euclidienne de m_k par 10. En divisant la congruence (1) par 10^k, nous obtenons : $3 a_k n_k^2 \equiv c_k \bmod (10)$, soit encore $3 a_k n_k^3 \equiv n_k c_k \bmod (10)$. Comme $n_k \equiv a_0 \equiv 3 \bmod (10)$ et que $n_k^3 \equiv 7 \bmod (10)$, nous obtenons finalement $3 \cdot 7\,a_k \equiv a_k \equiv 3 c_k \bmod (10)$. Cela permet de calculer a_k connaissant n_k pour tout $k \in [\![1, 5]\!]$, et donc de déterminer $a_1, \ldots, a_5$, sachant que $a_0 = n_1 = 3$.

Le tableau ci-dessous résume les calculs à effectuer :

k :	1	2	3	4	5	6
n_k :	3	53	753	0 753	60 753	660 753
r_k :	27	877	7 777	57 777	577 777	
c_k :	5	9	0	2	2	
$3c_k$:	15	27	0	6	6	
a_k :	5	7	0	6	6	

Les nombres entiers n tels que les six derniers chiffres de n^3 soient 777 777 sont donc les entiers dont l'écriture décimale se termine par 660 753 .

Exercice 7 :

> Quelle que soit la base du système de numération, montrer qu'aucun des nombres 10 101 , 101 010 101 , 1 010 101 010 101 etc., n'est premier (Catalan). ■

Ces nombres s'écrivent $u_n = 1 + a^2 + a^4 + \ldots + a^{4n-2} + a^{4n}$, où a est la base du système de numération, et n est un entier > 0 . On vérifie alors facilement que si on pose $b = a^2$:

$$\begin{aligned} u_n &= 1 + b + b^2 + \ldots + b^{2n} = \\ &= \frac{b^{2n+1} - 1}{b - 1} = \frac{a^{4n+2} - 1}{a^2 - 1} = \frac{a^{2n+1} - 1}{a - 1} \times \frac{a^{2n+1} + 1}{a + 1} \\ &= (a^{2n} + a^{2n-1} + \ldots + a^2 + a + 1) \times (a^{2n} - a^{2n-1} + \ldots + a^2 - a + 1). \end{aligned}$$

On voit que $(a^{2n} - a^{2n-1}) + \ldots + (a^2 - a) + 1 > 1$ pour tous n et a entiers, $n > 0$, $a > 1$. Le nombre u_n n'est donc jamais premier.

Chapitre V

GROUPES

§ V.1 *GÉNÉRATION DE GROUPES*

Exercice 1 :

> Vérifier que le groupe additif $\mathbb{Q}$ n'est pas de type fini. Quels sont ses sous-groupes de type fini ? (*Réponse* : ce sont les sous-groupes monogènes). Ce résultat subsiste-t-il avec les sous-groupes de $\mathbb{R}$? ■

Soit G un sous-groupe de type fini du groupe additif $\mathbb{Q}$, et $r_1, r_2, \ldots, r_k$ une famille génératrice finie de G. Si l'entier q, $q > 0$, est un dénominateur commun des fractions $r_1, r_2, \ldots, r_k$, on voit que $qG \subset \mathbb{Z}$. L'ensemble qG étant un sous-groupe additif de $\mathbb{Q}$ inclus dans $\mathbb{Z}$, c'est un sous-groupe additif de $\mathbb{Z}$. Il est donc de la forme $d\mathbb{Z}$, où $d \in \mathbb{N}$ et par conséquent $G = (d/q)\,\mathbb{Z}$. Le sous-groupe G est donc le sous-groupe monogène engendré dans $\mathbb{Q}$ par la fraction (d/q).

Si le groupe additif $\mathbb{Q}$ était de type fini, il serait monogène, de la forme $r\mathbb{Z}$ où $r \in \mathbb{Q}_+^*$; c'est impossible car $r/2$ n'est pas dans le sous-groupe $r\mathbb{Z}$.

Il en est autrement dans le groupe additif $\mathbb{R}$. Par exemple le sous-groupe engendré dans $\mathbb{R}$ par 1 et $\sqrt{2}$, c'est-à-dire $\mathbb{Z} + \sqrt{2}\,\mathbb{Z}$, n'est pas monogène : sinon, il existerait un réel $x > 0$ et deux entiers relatifs n et m tels que $1 = n \cdot x$ et $\sqrt{2} = m \cdot x$, ce qui impliquerait $\sqrt{2} \in \mathbb{Q}$.

Exercice 3 :

> Soit G un groupe ; un élément μ de G est dit *mou* ssi il possède la propriété suivante : pour toute partie génératrice E de G, la partie $E \setminus \{\mu\}$ est encore génératrice. Montrer que l'ensemble $\mathcal{M}$ des éléments mous de G, augmenté de e_G, est un sous-groupe de G, et vérifier que $s(\mathcal{M}) = \mathcal{M}$ pour tout automorphisme s du groupe G. Calculer $\mathcal{M}$ dans les cas suivants :
> *a*) $G = (\mathbb{Q}, +)$.

b) $G = \mathbb{Z}^{(\mathbb{N})}$.
c) $G = \mathbb{Z}$.
d) $G = \mathbb{Z}/_{n\mathbb{Z}}$. ■

Soit E une partie génératrice du groupe G ; le sous-groupe engendré par la partie $E \setminus \{e_G\}$ contient $E \setminus \{e_G\}$ et évidemment $\{e_G\}$, donc E ; ce sous-groupe est donc G ; la partie $E \setminus \{e_G\}$ est donc aussi génératrice. L'élément e_G est par conséquent mou.

Démontrons maintenant que l'élément μ de G est mou si, et seulement si, pour toute partie génératrice E du groupe G, les parties μE et $\mu^{-1} E$ sont génératrices (propriété que nous noterons T).
Si μ est mou, et E génératrice, il est clair que la partie $\{\mu\} \cup \mu E$ est génératrice, donc μE l'est ; on montre de même que $\mu^{-1} E$ est génératrice.
Si μ possède la propriété T, et que E est une partie génératrice, alors $\mu^{-1} E$ est génératrice, donc $(\mu^{-1} E) \setminus \{e_G\} = \mu^{-1}(E \setminus \{\mu\})$ l'est. Nous pouvons encore en déduire que $E \setminus \{\mu\} = \mu\mu^{-1}(E \setminus \{\mu\})$ est génératrice. L'élément μ est donc mou.

Montrons maintenant que $\mathcal{M}$ est un sous-groupe. Nous avons vérifié $e_G \in \mathcal{M}$. Si λ et μ sont mous, et E génératrice, alors $\mu^{-1} E$ est génératrice, donc $\lambda\mu^{-1} E$ est génératrice ; de même nous pouvons démontrer que $\mu\lambda^{-1} E$ est génératrice. L'élément $\lambda\mu^{-1}$ possède donc la propriété T et est donc mou. La partie $\mathcal{M}$ est donc un sous-groupe de G.

Soit s un automorphisme du groupe G. Si μ est mou, et que E est génératrice, on voit que $E \setminus \{s(\mu)\} = s\left(s^{-1}(E) \setminus \{\mu\}\right)$ est l'image par l'automorphisme s d'une partie génératrice, donc est génératrice. L'élément $s(\mu)$ est donc mou. Cela implique $s(\mathcal{M}) \subset \mathcal{M}$. En appliquant le résultat précédent avec s^{-1}, on voit que $s^{-1}(\mathcal{M}) \subset \mathcal{M}$ et donc finalement que $s(\mathcal{M}) = \mathcal{M}$.

a) $G = (\mathbb{Q}, +)$.
Montrons que tout rationnel n/m, où $n \in \mathbb{Z}$ et $m \in \mathbb{N}^*$ est mou. Soit E une partie génératrice de G. La partie $E \setminus \{n/m\}$ engendre un sous-groupe H de $\mathbb{Q}$. Ce sous-groupe n'est pas nul, sinon $E \setminus \{n/m\}$ ne contiendrait aucun élément non nul, le groupe $(\mathbb{Q}, +)$ serait monogène engendré par la fraction (n/m), cela est impossible (voir exercice 1). Le groupe mH n'est donc pas nul et contient par conséquent des entiers non nuls. Le sous-groupe $mH \cap \mathbb{Z}$ est donc de la forme $d\mathbb{Z}$, où d est entier > 0. Nous pouvons écrire :

$$\frac{1}{md} = u\frac{n}{m} + n_1 r_1 + n_2 r_2 + \ldots + n_k r_k \ ,$$

où u, $n_1, n_2, \ldots, n_k$ sont des entiers relatifs, et $r_1, r_2, \ldots, r_k$ des éléments de E différents de (n/m) (E est génératrice). On obtient l'égalité :

$$1 - und = md(n_1 r_1 + \ldots + n_k r_k) \in mH \cap \mathbb{Z} = d\mathbb{Z}$$

Nous en déduisons que d divise 1 et donc que $d = 1$. Par conséquent, $1 \in mH$, soit $(1/m) \in H$ et $(n/m) \in H$. Cela implique $E \subset H$ et finalement $H = \mathbb{Q}$. La partie $E \setminus \{(n/m)\}$ est donc génératrice.

Ce qui précède montre que tout rationnel (n/m) est mou. Dans ce cas $\mathcal{M} = \mathbb{Q}$.

b) Montrons que dans ce cas $\mathcal{M} = \{0\}$. Nous utiliserons dans ce qui suit le fait que l'image d'une partie génératrice par un homomorphisme surjectif est une partie génératrice.
Soit $\mu = (\mu_n)_{n\in\mathbb{N}}$ un élément mou du groupe $G = \mathbb{Z}^{(\mathbb{N})}$. Pour tout i entier, notons δ_i la suite telle que $\forall j \in \mathbb{N}$, $j \neq i$, $\delta_i(j) = 0$ et $\delta_i(i) = 1$. La famille $(\delta_i)_{i\in\mathbb{N}}$ est une famille génératrice du groupe G. Pour $k > 0$ entier fixé soit a la famille telle que $a_i = \delta_k + \delta_i$ si $i \neq k$ et $a_k = \delta_k$. On voit que la famille a est génératrice. La famille $(\mu + a_i)_{i\in\mathbb{N}}$ est donc génératrice. L'image de cette famille par l'homomorphisme de groupe qui à une suite s, élément de G, fait correspondre $s(k)$, est donc une famille génératrice de $\mathbb{Z}$. Or pour tout i entier, $(\mu + a_i)(k) = \mu_k + 1$, par conséquent, l'élément $\mu_k + 1$ est un générateur de $\mathbb{Z}$; il en est de même pour $1 - \mu_k$. Comme les générateurs du groupe $\mathbb{Z}$ sont 1 et -1, il est clair que $\mu_k = 0$. Ceci étant vrai pour tout entier k, la suite μ est nulle. Le groupe $\mathcal{M}$ est donc réduit à l'élément neutre.

c) $G = \mathbb{Z}$. Si μ est un élément mou du groupe additif $\mathbb{Z}$, $\mu + 1$, ainsi que $1 - \mu$, est un générateur du groupe $\mathbb{Z}$. Il est alors clair que $\mu = 0$. Le groupe $\mathcal{M}$ est donc réduit à $\{0\}$.

d) $G = \mathbb{Z}/_{n\mathbb{Z}}$. Nous noterons π_n l'homomorphisme canonique, de $\mathbb{Z}$ vers $\mathbb{Z}/_{n\mathbb{Z}}$. Soit d un entier dont la classe modulo n est un élément mou du groupe G. Montrons que tout diviseur premier de n divise d.
Supposons qu'il existe un nombre premier p tel que p divise n et tel que p ne divise pas d ; p est alors premier avec d. Il existe donc deux entiers relatifs u et v tels que $up + vd = 1$; en écrivant cette égalité modulo n, on voit que $\{\pi_n(p), \pi_n(d)\}$ est une partie génératrice du groupe G. Puisque $\pi_n(d)$ est mou, nous en déduisons que $\pi_n(p)$ est un générateur du groupe G, ce qui est faux puisque p n'est pas premier avec n. On voit donc que tout diviseur premier de n divise aussi d.

Inversement, montrons que si d est divisible par tous les nombres premiers qui divisent n (donc par leur produit), alors $\pi_n(d)$ est un élément mou du groupe G. Soit d un tel nombre et $E = \{\pi_n(n_1), \pi_n(n_2), \ldots, \pi_n(n_k)\}$ une partie génératrice du groupe G. Il existe des entiers $u_1, u_2, \ldots, u_k$ tels que $1 = u_1\pi_n(n_1) + u_2\pi_n(n_2) + \ldots + u_k\pi_n(n_k)$ et donc aussi un ent

$1 = vn + u_1n_1 + u_2n_2 + \ldots + u_kn_k$. Les nombres n, et $n_1, n_2, \ldots, n_k$ sont donc premiers entre eux dans leur ensemble. Les nombres n, $n_1 + d, n_2 + d, \ldots, n_k + d$ sont aussi premiers entre eux dans leur ensemble, car s'il existait un nombre premier p qui les divisait tous, il diviserait n, donc d, et par conséquent aussi tous les nombres $n_1, n_2, \ldots, n_k$. Le sous groupe engendré par $\pi_n(n_1) + \pi_n(d), \ldots, \pi_n(n_k) + \pi_n(d)$ contient donc $\pi_n(1)$. Nous pouvons en déduire que la famille $\pi_n(n_1) + \pi_n(d), \ldots, \pi_n(n_k) + \pi_n(d)$ est génératrice. Le raisonnement est identique avec $-d$. Nous voyons donc, d'après le lemme préliminaire, que $\pi_n(d)$ est mou.

Les entiers dont la classe est dans $\mathcal{M}$ sont donc les éléments de l'idéal $\sqrt{n\mathbb{Z}}$ (voir §III.7 exercice 2 pour la définition de la racine d'un idéal).

Exercice 5 :

> Montrer que $(\mathbb{Q}, +)$ n'est pas isomorphe à un produit $G_1 \times G_2 \times \ldots \times G_n$, où chaque G_i serait un sous-groupe de $\mathbb{Q}$ non réduit à $\{0\}$. ■

Supposons que $\varphi : \mathbb{Q} \to G_1 \times G_2 \times \ldots \times G_n$ soit un tel isomorphisme. Posons pour $i \in [\![1, n]\!]$, $H_i = \varphi^{-1}(\{0\} \times \ldots \times G_i \times \ldots \times \{0\})$. Les parties H_i, où $i \in [\![1, n]\!]$ sont des sous-groupes du groupe additif $\mathbb{Q}$. Soient i et j distincts dans $[\![1, n]\!]$, on voit que $H_i \cap H_j = \{0\}$; si H_i et H_j étaient tous les deux non nuls, ils contiendraient tous les deux des entiers non nuls, donc auraient des éléments non nuls communs. Nous pouvons en déduire qu'un seul des groupes H_i n'est pas nul, tous les autres étant nuls. Il en est de même pour les sous-groupes G_i de $\mathbb{Q}$, mais comme on les suppose tous non nuls, c'est qu'il n'y en a qu'un seul, c'est-à-dire $n = 1$. Pour résumer, la propriété utilisée ici est que deux sous-groupes non nuls du groupe additif $\mathbb{Q}$ ont toujours une intersection non nulle.

Exercice 7 :

> Soit G le sous-groupe du groupe $\mathrm{GL}(2, \mathbb{R})$ (des matrices carrées réelles inversibles d'ordre 2) engendré par les matrices $A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Soit H le sous-ensemble de G formé des matrices $M = \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \in G$ telles que $a = b = 1$.
>
> Montrer que H est un sous-groupe de G, et que le groupe H n'est pas de type fini. (*N.B.* Cela prouve qu'il existe des groupes de type fini admettant des sous-groupes qui ne le sont pas.) ■

Soit K l'ensemble des matrices $\begin{pmatrix} a & c \\ 0 & 1 \end{pmatrix}$ où $a \neq 0$; c'est un

puisqu'il contient la matrice unité, et que pour tous réels a et a' non nuls, et c et c' réels quelconques, on a les égalités matricielles :

$$\begin{pmatrix} a & c \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} a' & c' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} aa' & ac'+c \\ 0 & 1 \end{pmatrix},$$

et :

$$\begin{pmatrix} a & c \\ 0 & 1 \end{pmatrix}^{-1} = \frac{1}{a}\begin{pmatrix} 1 & -c \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1/a & -c/a \\ 0 & 1 \end{pmatrix}.$$

Comme $A \in K$ et $B \in K$, nous en déduisons $G \subset K$. On remarque aussi que l'application $\varphi : \begin{pmatrix} a & c \\ 0 & 1 \end{pmatrix} \mapsto a$, de K vers le groupe multiplicatif $(\mathbb{R}^*, \times)$, est un homomorphisme de groupes. On voit alors que H est un sous-groupe puisque $H = G \cap \mathrm{Ker}\,(\varphi)$.

Soit $\mathcal{B}$ l'ensemble des réels binaires, c'est-à-dire les réels dont l'écriture à base 2 est finie (ou encore $x \in \mathcal{B}$ si, et seulement si, $\exists h \in \mathbb{N}\ \ 2^h x \in \mathbb{Z}$). On sait que $\mathcal{B}$ est un sous-anneau de l'anneau $\mathbb{Q}$. Montrons que les éléments de G sont les matrices de la forme $\begin{pmatrix} 2^k & b \\ 0 & 1 \end{pmatrix}$, où $k \in \mathbb{Z}$, et $b \in \mathcal{B}$.
L'ensemble G' de ces matrices est un sous-groupe, car il contient la matrice unité, et que pour tous entiers relatifs k et k', et tous nombres binaires b et b', on a les égalités :

$$\begin{pmatrix} 2^k & b \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 2^{k'} & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2^{k+k'} & 2^k b'+b \\ 0 & 1 \end{pmatrix},$$

et :

$$\begin{pmatrix} 2^k & b \\ 0 & 1 \end{pmatrix}^{-1} = 2^{-k}\begin{pmatrix} 1 & -b \\ 0 & 2^k \end{pmatrix} = \begin{pmatrix} 2^{-k} & -2^{-k}b \\ 0 & 1 \end{pmatrix}.$$

Comme G' contient les matrices A et B, nous en déduisons $G \subset G'$.
Inversement si h, k et n sont des entiers relatifs, on vérifie facilement que :

$$A^{-h}B^nA^h = \begin{pmatrix} 2^{-h} & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2^h & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n2^{-h} \\ 0 & 1 \end{pmatrix},$$

et :

$$A^{-h}B^nA^hA^k = \begin{pmatrix} 1 & n2^{-h} \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2^k & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2^k & n2^{-h} \\ 0 & 1 \end{pmatrix}.$$

Nous en déduisons $G' \subset G$ et finalement $G' = G$.

Le sous-groupe H est donc l'ensemble des matrices de la forme $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ où $b \in \mathcal{B}$. On voit que le groupe H est isomorphe au groupe additif $\mathcal{B}$. Il nous suffit alors de montrer que le groupe additif $\mathcal{B}$ n'est pas

Si E est une partie finie de $\mathcal{B}$, il existe un entier m tel que $2^m E \subset \mathbb{Z}$. Soit Γ le sous-groupe engendré par E, on a $2^m \Gamma \subset \mathbb{Z}$. Le sous groupe Γ ne peut donc être $\mathcal{B}$, il ne peut par exemple pas contenir le nombre binaire $2^{-(m+1)}$. Le groupe $\mathcal{B}$, et le groupe H, ne sont donc pas de type fini, alors que H est un sous-groupe d'un groupe de type fini, G, engendré par les matrices A et B.

Exercice 8 :

Soit $\mathrm{SL}(2,\mathbb{Z})$ le sous-groupe du groupe $\mathrm{GL}(2,\mathbb{R})$ formé des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telles que $(a,b,c,d) \in \mathbb{Z}^4$ et $ad - bc = 1$.
On considère les deux matrices suivantes dans $\mathrm{SL}(2,\mathbb{Z})$: $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. On note I_2 la matrice $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et on considère le sous-groupe G engendré par $\{S,T\}$ dans $\mathrm{SL}(2,\mathbb{Z})$.

a) Vérifier que $-I_2 \in G$, et que $U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in G$. Calculer T^n et U^n, pour $n \in \mathbb{Z}$.

b) Montrer que $G = \mathrm{SL}(2,\mathbb{Z})$, autrement dit que le groupe $\mathrm{SL}(2,\mathbb{Z})$ est engendré par $\{S,T\}$. ■

a) En effectuant le calcul directement, ou en utilisant le théorème de Cayley pour les matrices carrées de taille 2, on obtient :

$$S^2 = (\mathrm{Tr}S)\,S - (\det S)\,I_2 = -I_2 \ \in G.$$

On vérifie d'autre part que si $n \in \mathbb{Z}$, l'égalité $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ est vraie si, et seulement si l'égalité :

$$T^n T = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{soit} \quad T^{n+1} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix},$$

est vraie. La valeur logique de l'égalité $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, est donc constante sur $\mathbb{Z}$, avec pour valeur "vrai" puisque l'égalité est vraie pour $n = 1$.
Un calcul facile permet de vérifier aussi que pour tout $n \in \mathbb{Z}$:

$$S\,T^n\,S^{-1} = -S\,T^n\,S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \cdot & \end{pmatrix}$$

En particulier :

$$U = ST^{-1}S^{-1} \quad \text{et} \quad U^n = ST^{-n}S^{-1} = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} .$$

b) Montrons par récurrence sur l'entier naturel n, la propriété : tout élément $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\mathrm{SL}(2,\mathbb{Z})$ tel que $|c| \leqslant n$ est dans le sous-groupe G engendré par $\{S,T\}$.
Si $n = 0$: comme a et d sont des entiers relatifs tels que $ad = 1$, il suffit de démontrer que pour tout $b \in \mathbb{Z}$, les matrices $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix}$ sont dans G. C'est évident puisque $T^b \in G$ et $-T^{-b} = S^2T^{-b} \in G$.
Supposons la propriété vraie pour $n \geqslant 0$ et soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ un élément de $\mathrm{SL}(2,\mathbb{Z})$ tel que $|c| \leqslant n+1$. Si $c = 0$ alors $M \in G$, sinon soit k un entier relatif tel que $|a/c - k| \leqslant 1/2$ (entier le plus proche de a/c). On observe que :

$$ST^{-k}M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a-kc & b-kd \end{pmatrix} = M' .$$

Comme $|a/c - k| \leqslant 1/2$, on voit que $|a - kc| \leqslant |c|/2 < |c| \leqslant n+1$. La matrice M' est donc, par récurrence, dans le sous-groupe G. La matrice M est donc aussi dans le sous-groupe G.
La propriété est donc vraie pour tout n ; c'est-à-dire $\mathrm{SL}(2,\mathbb{Z}) \subset G$. Comme les matrices S et T sont éléments de $\mathrm{SL}(2,\mathbb{Z})$, on a aussi $G \subset \mathrm{SL}(2,\mathbb{Z})$, et finalement $G = \mathrm{SL}(2,\mathbb{Z})$. On voit clairement que l'algorithme est rapide, puisqu'à chaque étape du calcul, on divise au moins par 2 la valeur du coefficient c.

§ V.2 *ORDRE D'UN ÉLÉMENT*

Exercice 1 :

> Soit G un groupe cyclique de cardinal n, engendré par g. On donne $r \in \mathbb{Z}^*$ et on pose $\delta = r \vee n$. Montrer que l'homomorphisme de groupes $f_r : G \to G$, $x \mapsto x^r$ admet pour image $\mathrm{Gr}(g^\delta)$ et pour noyau $\mathrm{Gr}(g^{n/\delta})$. Calculer $\mathrm{card}(f_r^{-1}(y))$ pour $y \in G$. ■

Notons I_r l'image de l'homomorphisme f_r et K_r son noyau. Puisque g est générateur, pour tout $m \in \mathbb{Z}$, $g^m \in I_r$ si, et seulement si, $\exists k$

$g^{kr} = g^m$, donc $g^m \in I_r$ si, et seulement si $\exists k \in \mathbb{Z},\ kr \equiv m\ [n]$, soit encore $m \in r\mathbb{Z} + n\mathbb{Z} = \delta\mathbb{Z}$. L'image de f_r est donc l'ensemble des puissances de g^δ, c'est-à-dire $\mathrm{Gr}\left(g^\delta\right)$.

Pour tout $m \in \mathbb{Z}$, $g^m \in K_r$ si, et seulement si, $g^{mr} = e_G$, donc si, et seulement si $n \mid mr$, soit encore $(n/\delta) \mid m(r/\delta)$; comme (n/δ) et (r/δ) sont premiers entre eux, $g^m \in K_r$ si, et seulement si, $(n/\delta) \mid m$. Le noyau de f_r est donc l'ensemble des puissances de $g^{n/\delta}$, c'est-à-dire $\mathrm{Gr}\left(g^{n/\delta}\right)$.

Supposons $y \in I_r$ (sinon $f_r^{-1}(y) = \emptyset$). Il existe alors un élément $x_0 \in G$ tel que $x_0^r = y$. Donc pour tout $x \in G$, $x^r = y$ si, et seulement si $x^r = x_0^r$, soit $x_0^{-1}x \in K_r$, (puisque G est abélien) ou encore $x \in x_0 K_r$. On voit donc que $f_r^{-1}(y)$ a pour cardinal le cardinal de K_r, donc l'ordre de $g^{n/\delta}$. On voit facilement que cet ordre est δ. Nous avons donc démontré que pour tout élément $y \in I_r$, $\mathrm{card}\left(f_r^{-1}(y)\right) = \delta$.

Exercice 3 :

> Soit G un groupe cyclique de cardinal n, engendré par g. A chaque r on associe l'endomorphisme f_r de G tel que $f_r(x) = x^r$ pour tout x de G. Montrer que $r \mapsto f_r$ définit une bijection de $[\![0, n-1]\!]$ sur l'ensemble $\mathrm{Hom}(G,G)$. Soit $Y_n : \mathbb{Z} \to \mathbb{Z}/_{n\mathbb{Z}}$ l'application canonique. On munit $\mathrm{Hom}(G,G)$ de sa structure naturelle de groupe. Montrer que $s \mapsto f_{\widehat{Y}_n^{-1}(s)}$ est un *isomorphisme* de $(\mathbb{Z}/_{n\mathbb{Z}}, +)$ sur $\mathrm{Hom}(G,G)$. (On note $\widehat{Y}_n$ la restriction de Y_n à $[\![0, n-1]\!]$.) ■

Soient r et r' des entiers relatifs quelconques, les homomorphismes f_r et $f_{r'}$ sont égaux si, et seulement si, il coïncident en g, générateur, donc si, et seulement si, $g^r = g^{r'}$. Comme g est d'ordre n, $f_r = f_{r'}$ si, et seulement si, $r \equiv r'\ [n]$. L'application $r \mapsto f_r$, $[\![0, n-1]\!] \to \mathrm{Hom}(G,G)$ est donc injective.
Soit φ un homomorphisme $G \to G$. Il existe un entier $r \in [\![0, n-1]\!]$ (unique) tel que $\varphi(g) = g^r$. Les deux homomorphismes φ et f_r coïncident en g, donc sont égaux. L'application $r \mapsto f_r$, $[\![0, n-1]\!] \to \mathrm{Hom}(G,G)$ est donc surjective, et par conséquent bijective.

Notons $\Phi : \mathbb{Z} \to \mathrm{Hom}(G,G)$, $r \mapsto f_r$. C'est un homomorphisme de groupes puisque si r et s sont des entiers relatifs, pour tout $x \in G$, $f_r(x) \star f_s(x) = x^r \star x^s = x^{r+s} = f_{r+s}(x)$. Il est évidemment surjectif, et son noyau est, d'après ce qui précède, le sous-groupe $n\mathbb{Z}$. Notons F l'application $s \mapsto f_{\widehat{Y}_n^{-1}(s)}$ introduite par l'énoncé. Par définition, pour tout $r \in [\![0, n-1]\!]$, $F(Y_n(r)) = f_r = \Phi(r)$; mais comme f_r

dépendent que de la classe de r modulo n, cette égalité est vraie pour tout $r \in \mathbb{Z}$. L'application F apparaît donc comme la factorisée de l'application Φ, par la relation d'équivalence qui définit l'ensemble quotient $\mathbb{Z}/_{n\mathbb{Z}}$. Le théorème de factorisation ensembliste permet d'affirmer que F est une application surjective (factorisée d'une application surjective) et injective (la relation d'équivalence utilisée est équivalente à la relation $\Phi(r) = \Phi(r')$). Le théorème de factorisation de la théorie des groupes (Théorème V.7.3) permet d'affirmer que *de plus* F est un homomorphisme de groupes. Montrons ce dernier résultat dans ce cas particulier. Si h et k sont des entiers relatifs quelconques :

$$F(Y_n(h) + Y_n(k)) = F(Y_n(h+k)) =$$
$$= \Phi(h+k) = \Phi(h) \star \Phi(k) = F(Y_n(h)) \star F(Y_n(k)) \ .$$

Donc pour toutes classes s et t, $F(s+t) = F(s) \star F(t)$. En conclusion, nous avons donc bien démontré que F était un isomorphisme de groupes.

Exercice 4 :

> Soient $G_1, G_2, \ldots, G_n$ des groupes en nombre fini, $g_i \in G_i$ ($1 \leqslant i \leqslant n$) et g l'élément $(g_1, g_2, \ldots, g_n)$ dans le groupe produit $G_1 \times G_2 \times \ldots \times G_n$.
> *a*) Si chaque g_i est de torsion dans G_i, d'ordre ω_i, montrer que g est de torsion dans G, d'ordre $\text{ppcm}\,(\omega_1, \omega_2, \ldots, \omega_n)$.
> *b*) On suppose chaque groupe G_i cyclique. Montrer que G est cyclique si, et seulement si, les entiers $\text{card}\,(G_i)$ sont *deux à deux* premiers entre eux. ■

a) Cherchons l'ensemble des périodes de l'élément g pour trouver la plus petite strictement positive. Pour tout $k \in \mathbb{Z}$, $g^k = (g_1^k, g_2^k, \ldots, g_n^k)$ est par définition neutre si, et seulement si, $\forall i \in [\![1, n]\!] \quad g_i^k = e_{G_i}$, c'est-à-dire si, et seulement si, $\forall i \in [\![1, n]\!] \quad \omega_i \,|\, k$. L'élément g est donc de torsion et l'ensemble de ses périodes est l'ensemble des multiples communs des ω_i ($i \in [\![1, n]\!]$). Nous en déduisons que l'ordre de g est $\text{ppcm}\,(\omega_1, \omega_2, \ldots, \omega_n)$.

b) Supposons que les G_i soient cycliques et que pour tout $i \in [\![1, n]\!]$, g_i soit un générateur du groupe G_i. Pour tout $i \in [\![1, n]\!]$, l'ordre ω_i de g_i est égal au cardinal de l'ensemble G_i.
Si ces ordres sont premiers entre eux deux à deux, alors $\omega_1 \cdot \omega_2 \cdot \ldots \cdot \omega_n = \text{card}\,(G) = \text{ppcm}\,(\omega_1, \omega_2, \ldots, \omega_n)$. D'après le *a*), nous pouvons en déduire que l'élément $g = (g_1, g_2, \ldots, g_n)$ est un générateur du groupe G. Ce groupe est par conséquent cyclique.

Supposons inversement que les cardinaux ω_i des groupes G_i ne soient pas premiers entre eux deux à deux. Il existe deux entiers h et k dans $[\![1,n]\!]$ et un entier $q > 1$ tels que $q \,|\, \omega_h$ et $q \,|\, \omega_k$; on voit alors que l'entier $p = (\omega_1 \cdot \omega_2 \cdot \ldots \cdot \omega_n)/q$ est un multiple commun des ω_i. Comme pour tout $i \in [\![1,n]\!]$, ω_i est une période de tout élément de groupe G_i, l'entier p est une période de tout élément du groupe G. Il n'y donc dans G aucun élément dont la période soit $\omega_1 \cdot \omega_2 \cdot \ldots \cdot \omega_n = \mathrm{card}\,(G)$. Le groupe G n'est donc pas cyclique.

Exercice 5 :

> *a*) Soit p un nombre premier et $\alpha \in \mathbb{N}^*$. Pour $k \in \mathbb{N}^*$ calculer le nombre d'éléments d'ordre p^α dans le groupe $\left(\mathbb{Z}/_{p^\alpha\,\mathbb{Z}}\right)^k$.
>
> *b*) Soit $n \in \mathbb{N}$, $n \geqslant 2$. On décompose n en facteurs premiers : $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ (avec les p_i premiers et distincts, les $\alpha_i \geqslant 1$). Pour $k \in \mathbb{N}^*$, montrer que les groupes additifs $\left(\mathbb{Z}/_{n\,\mathbb{Z}}\right)^k$ et $\left(\mathbb{Z}/_{p_1^{\alpha_1}\,\mathbb{Z}}\right)^k \times \ldots \times \left(\mathbb{Z}/_{p_r^{\alpha_r}\,\mathbb{Z}}\right)^k$ sont isomorphes. En déduire le nombre d'éléments d'ordre n dans $\left(\mathbb{Z}/_{n\,\mathbb{Z}}\right)^k$. ■

a) On sait que le nombre de générateurs du groupe $\mathbb{Z}/_{p^\alpha\,\mathbb{Z}}$ est $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Le nombre d'éléments dans ce groupe dont la période divise strictement p^α est donc $p^{\alpha-1}$. En utilisant l'exercice précédent, on voit que l'ordre d'un élément du groupe $\left(\mathbb{Z}/_{p^\alpha\,\mathbb{Z}}\right)^k$ divise strictement p^α si, et seulement si, chacune de ses composantes dans $\mathbb{Z}/_{p^\alpha\,\mathbb{Z}}$ a un ordre qui divise strictement p^α. Le nombre de ces éléments est donc $(p^{\alpha-1})^k = p^{(\alpha-1)k}$. Le nombre des éléments dont l'ordre est exactement p^α est donc $p^{\alpha k} - p^{(\alpha-1)k}$.

b) Montrons que les groupes $\mathbb{Z}/_{n\,\mathbb{Z}}$ et $\mathbb{Z}/_{p_1^{\alpha_1}\,\mathbb{Z}} \times \ldots \times \mathbb{Z}/_{p_r^{\alpha_r}\,\mathbb{Z}}$ sont isomorphes ; nous pourrons en déduire que les puissances k-ièmes (au sens du produit cartésien des groupes) sont isomorphes.
Pour tout $i \in [\![1,r]\!]$ notons $\pi_i : \mathbb{Z} \to \mathbb{Z}/_{p_i^{\alpha_i}\,\mathbb{Z}}$, l'homomorphisme canonique. Le noyau de cet homomorphisme est par définition le groupe $p_i^{\alpha_i}\,\mathbb{Z}$. Considérons l'application $\varphi : \mathbb{Z} \to \mathbb{Z}/_{p_1^{\alpha_1}\,\mathbb{Z}} \times \ldots \times \mathbb{Z}/_{p_r^{\alpha_r}\,\mathbb{Z}}$, telle que pour tout n entier, $\varphi(n) = (\pi_1(n), \ldots, \pi_r(n))$; c'est un homomorphisme de groupes, dont le noyau est $\bigcap_{i=1}^{r} p_i^{\alpha_i}\,\mathbb{Z} = n\,\mathbb{Z}$. On peut donc définir un homomorphisme factorisé injectif $\overline{\varphi} : \mathbb{Z}/_{n\,\mathbb{Z}} \to \mathbb{Z}/_{p_1^{\alpha_1}\,\mathbb{Z}} \times \ldots \times \mathbb{Z}/_{p_r^{\alpha_r}\,\mathbb{Z}}$. Cet homomorphisme est bijectif car l'ensemble de départ et l'ensemble d'arrivée ont

nal : n ; c'est donc un isomorphisme de groupes. Les groupes $\left(\mathbb{Z}/_{n\mathbb{Z}}\right)^k$ et $\left(\mathbb{Z}/_{p_1^{\alpha_1}\mathbb{Z}}\right)^k \times \ldots \times \left(\mathbb{Z}/_{p_r^{\alpha_r}\mathbb{Z}}\right)^k$ sont donc isomorphes.
Ces deux groupes ont donc même nombre d'éléments d'ordre n. En utilisant les résultats de l'exercice précédent, on voit qu'un r-uplet $g = (g_1, g_2, \ldots, g_r)$ élément du groupe $\left(\mathbb{Z}/_{p_1^{\alpha_1}\mathbb{Z}}\right)^k \times \ldots \times \left(\mathbb{Z}/_{p_r^{\alpha_r}\mathbb{Z}}\right)^k$ est d'ordre n si, et seulement si, pour tout $i \in [\![1, r]\!]$, g_i est d'ordre $p_i^{\alpha_i}$. Le nombre de ces éléments est donc d'après le a) :

$$\prod_{i=1}^{r}\left(p_i^{k\,\alpha_i} - p_i^{k\,(\alpha_i-1)}\right) = n^k \prod_{i=1}^{r}\left(1 - \frac{1}{p_i^k}\right) .$$

Exercice 6 :

Soit G un groupe abélien fini de cardinal $n \in \mathbb{N}^*$, on considère sur l'ensemble $D = G \times \mathbb{Z}/_{2\mathbb{Z}}$, la loi de composition suivante :

$$(a, b) * (a', b') = (a + (-1)^b a', b + b') .$$

a) Vérifier que $(D, *)$ est un groupe. On notera $D(G)$ ce groupe. Déterminer le nombre d'éléments d'ordre 2 dans le groupe $D(G)$ en fonction de n et du nombre d'éléments d'ordre 2 dans le groupe G.

b) Soit Γ un groupe de cardinal $2n$ possédant *exactement* n éléments d'ordre 2. Démontrer que n est *impair* et que Γ est isomorphe à un groupe $D(G)$, où G est un groupe abélien de cardinal n.

c) Pour $n \in \mathbb{N}^*$, $n \geqslant 2$, donner un modèle géométrique simple du groupe $D_n = D\left(\mathbb{Z}/_{n\mathbb{Z}}\right)$, à l'aide d'un polygone régulier à n côtés. ■

a) Le symbole $(-1)^b$, où $b \in \mathbb{Z}/_{2\mathbb{Z}}$ a bien un sens puisque $(-1)^2 = 1$. Il faut comprendre que $(-1)^b$ est un entier qui est $+1$ ou -1. On vérifie aussi facilement que pour tous b et b' éléments de $\mathbb{Z}/_{2\mathbb{Z}}$, $(-1)^b (-1)^{b'} = (-1)^{b+b'}$. Montrons que $D(G)$ est un groupe.

Associativité : $\forall (a, a', a'') \in G^3 \quad \forall (b, b', b'') \in \left(\mathbb{Z}/_{2\mathbb{Z}}\right)^3$

$$\begin{aligned}\big((a, b) * (a', b')\big) * (a'', b'') &= (a + (-1)^b a', b + b') * (a'', b'') = \\ &= \Big(a + (-1)^b a' + (-1)^{b+b'} a'', b +\end{aligned}$$

$$(a,b) * \big((a',b') * (a'',b'')\big) = (a,b) * \big(a' + (-1)^{b'} a'', b' + b''\big) =$$
$$= \Big(a + (-1)^b (a' + (-1)^{b'} a''), b + b' + b''\Big) .$$

On voit donc que $\big((a,b) * (a',b')\big) * (a'',b'') = (a,b) * \big((a',b') * (a'',b'')\big)$.

Neutre : $\forall (a,b) \in G \times \mathbb{Z}/_{2\mathbb{Z}}$

$$(a,b) * (0_G, 0) = \big(a + (-1)^b 0_G, b + 0\big) = (a,b)$$
$$(0_G, 0) * (a,b) = \big(0_G + (-1)^0 a, 0 + b\big) = (a,b) .$$

Inverse : $\forall (a,b) \in G \times \mathbb{Z}/_{2\mathbb{Z}}$

$$(a,b) * \big((-1)^{b+1} a, b\big) = \big(a + (-1)^b (-1)^{b+1} a, b + b\big) = (0_G, 0)$$
$$\big((-1)^{b+1} a, b\big) * (a,b) = \big((-1)^{b+1} a + (-1)^b a, b + b\big) = (0_G, 0) .$$

Donc $D(G) = (G \times \mathbb{Z}/_{2\mathbb{Z}}, *)$ est un groupe.

Un élément (a,b) du groupe $D(G)$ est d'ordre 2 si, et seulement si, il n'est pas neutre et :

$$(a,b) * (a,b) = \big(a + (-1)^b a, b + b\big) = (0_G, 0) ,$$

soit si, et seulement si, $(1 + (-1)^b)\, a = 0_G$. Les éléments d'ordre 2 du groupe $D(G)$ sont donc tous les éléments de la forme $(a,1)$, où $a \in G$, et les éléments $(a,0)$ où a est un élément d'ordre 2 dans le groupe G . Si n est impair, G n'a aucun élément d'ordre 2 (car l'ordre d'un élément divise le cardinal du groupe) ; dans ce cas le nombre d'éléments d'ordre 2 dans $D(G)$ est $n = \text{card}\,(G)$. Si n est pair, et que q est le nombre des éléments d'ordre 2 dans G , le nombre d'éléments d'ordre 2 du groupe $D(G)$ est $n + q$. Par exemple, si $G = \mathbb{Z}/_{2m\mathbb{Z}}$, le nombre d'éléments d'ordre 2 du groupe $D(G)$ est $2m + 1$, puisque le seul élément d'ordre 2 dans $\mathbb{Z}/_{2m\mathbb{Z}}$ est la classe de m .

b) Montrons d'abord que n est impair. Considérons la relation $\mathcal{R}$ sur Γ définie par $x \mathcal{R} y$ si, et seulement si, $x = y$ ou $x = y^{-1}$, ce que nous pouvons écrire $x = y^{\varepsilon}$, où $\varepsilon \in \{1, -1\}$. On voit facilement qu'il s'agit d'une relation d'équivalence dont les classes ont 1 ou 2 éléments. Précisément, la classe de x a un seul élément si, et seulement si, x est d'ordre 2 ou est neutre ; le nombre de ces classes est donc par hypothèse $n + 1$. Si q est le nombre de classes de cardinal 2, on voit que $2n = 2q + n + 1$, soit $n = 2q + 1$. Le cardinal de Γ est donc $2n$, où n est impair.
Soit E l'ensemble des éléments x tels que $x^2 = e$, et E^* l'ensemble des éléments d'ordre 2, de telle sorte que $E = E^* \cup \{e\}$. Soient x et

distincts. Si $(xy)^2 = e$, alors $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$. Les éléments x et y engendreraient un sous-groupe $\{e, x, y, xy\}$, abélien de cardinal 4, donc 4 diviserait $2n$, ce qui est en contradiction avec le fait que n est impair. Donc $xy \notin E$. Nous pouvons facilement en déduire que si x et y sont des éléments d'ordre 2, éventuellement confondus, alors $xy \notin E^*$.
Si $x \in E^*$, alors la partie E^*x a pour cardinal n et est disjointe de E^*. Le groupe Γ étant de cardinal $2n$, nous en déduisons que $E^*x = \Gamma \setminus E^*$. Montrons que $G = \Gamma \setminus E^*$ est un sous-groupe de Γ. Il contient bien l'élément neutre e et si a et b sont des éléments de G, on peut écrire $a = yx$ et $b = zx$, où y et z sont dans E^* ; alors $ab^{-1} = yxx^{-1}z^{-1} = yz \notin E^*$, donc $ab^{-1} \in G$.
Soit $x \in E^*$, et $b \in G$; écrivons $b = yx$, où $y \in E^*$; on a $xbx^{-1} = xyxx^{-1} = x^{-1}y^{-1} = (yx)^{-1} = b^{-1}$. Nous pouvons en déduire que G est abélien, en effet, si a et b sont éléments de G, écrivons $a = xy$, où x et y sont dans E^* (i.e. d'ordre 2) ; on a $aba^{-1} = xybyx^{-1} = xb^{-1}x^{-1} = \left(b^{-1}\right)^{-1} = b$, d'où $ab = ba$.

Soit x un élément d'ordre 2 donné. Tout élément y de Γ est soit dans $G = E^*x$, soit dans $Gx = E^*xx = E^*$; tout élément de G s'écrit donc sous la forme gx^b, où $b \in \{0,1\}$, ou plutôt $b \in \mathbb{Z}/_{2\mathbb{Z}}$, et $g \in G$. On vérifie aussi que pour tous g et g' dans G et b et b' dans $\mathbb{Z}/_{2\mathbb{Z}}$: $gx^b \star g'x^{b'} = gg'x^{b+b'}$ si $b = 0$, et $gx^b \star g'x^{b'} = gg'^{-1}x^{b+b'}$ si $b = 1$ (car $xg'x^{-1} = g'^{-1}$) ; dans les deux cas, on voit que $gx^b \star g'x^{b'} = gg'^{(-1)^b}x^{b+b'}$. L'application $(g,b) \mapsto gx^b$ est donc un homomorphisme surjectif de groupes, de l'ensemble $G \times \mathbb{Z}/_{2\mathbb{Z}}$ muni de la loi définie dans le a), dans le groupe Γ. Il est injectif, car si $gx^b = e$, où $g \in G$ et $b \in \mathbb{Z}/_{2\mathbb{Z}}$, alors $x^{-b} = g$, donc $b = 0$ (sinon x ne serait pas d'ordre 2) et $g = e$. Il s'agit donc d'un isomorphisme de groupes.

c) Pour n entier > 0, notons μ_n le groupe multiplicatif des racines n-ièmes de 1 dans $\mathbb{C}$, et $\mathbb{U}$ le groupe des complexes de module 1. On sait que l'application $f \mapsto f(1)$ est un isomorphisme de groupes, entre le groupe $\mathrm{SO}(\mathbb{C})$ des isométries directes du $\mathbb{R}$-espace vectoriel euclidien $\mathbb{C}$, et le groupe $\mathbb{U}$; l'isomorphisme réciproque étant l'application qui à $u \in \mathbb{U}$ fait correspondre la multiplication par u dans le corps $\mathbb{C}$. Soit S l'ensemble des éléments de $\mathrm{SO}(\mathbb{C})$ qui laissent l'ensemble μ_n globalement invariant. Il est clair qu'il s'agit d'un groupe. On voit aussi facilement qu'une isométrie directe f est dans S si, et seulement si, $f(1) \in \mu_n$. Notons S_+ le sous-groupe des isométries directes dans S, d'après ce qui précède, ce groupe a n éléments et est isomorphe à μ_n, donc à $\mathbb{Z}/_{n\mathbb{Z}}$. Nous connaissons une isométrie indirecte élément de S, c'est la conjugaison $c : z \mapsto \overline{z}$; une isométrie indirecte s est élément S si et seulement si $s \circ c \in S_+$, soit $s \in S_+ c$. Il y a donc exactement n isométries indirectes éléments de S, qui sont toutes d'ordre 2 (car involutives). Soit γ un générateur du groupe S_+ ; il existe un

$\varphi : D_n \to S$, telle que pour tout k entier et tout élément $b \in \mathbb{Z}/2\mathbb{Z}$ ($\pi_n(k)$ désignant la classe de k modulo n) $\varphi(\pi_n(k), b) = \gamma^k \circ c^b$, car γ est d'ordre n et c d'ordre 2 ; d'après ce qui précède, cette application est surjective. Les deux ensembles ayant $2n$ éléments, c'est une bijection. Montrons qu'il s'agit d'un homomorphisme de groupes. Pour tous entiers k et k' et tous éléments b et b' de $\mathbb{Z}/2\mathbb{Z}$, si $b = 0$ alors $\gamma^k \circ c^b \circ \gamma^{k'} \circ c^{b'} = \gamma^{k+k'} \circ c^{b+b'}$, et si $b = 1$, $\gamma^k \circ c^b \circ \gamma^{k'} \circ c^{b'} = \gamma^{k-k'} \circ c^{b+b'}$, car $c \circ \gamma^{k'} = \gamma^{-k'} \circ c$; dans tous les cas, $\gamma^k \circ c^b \circ \gamma^{k'} \circ c^{b'} = \gamma^{k+(-1)^b k'} \circ c^{b+b'}$. Il est donc clair que φ est un homomorphisme de groupes. Le groupe géométrique S est donc isomorphe au groupe D_n.

§ V.3 *CLASSES SUIVANT UN SOUS-GROUPE. INDICE*

Exercice 3 :

Soit G un groupe abélien fini de cardinal $N = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ (les p_i premiers et distincts, les $\alpha_i \geqslant 1$, et $r \geqslant 1$). Pour tout diviseur d de N, on note S_d l'ensemble des $x \in G$ tels que $x^d = e_G$. On fait l'hypothèse :

($\mathcal{H}$) pour tout diviseur d de N, on a $\operatorname{card}(S_d) \leqslant d$.

a) Soit d un diviseur de N. Déterminer le noyau et l'image de l'homomorphisme $G \to G$, $x \mapsto x^d$. En déduire $\operatorname{card}(S_d)$.

b) Pour toute partie I de $[\![1, r]\!]$, on note $R_I = \prod_{i \in I} p_i$, avec la convention $R_\emptyset = 1$. Montrer, si $I \subset [\![1, r]\!]$, que :

$$S_{N/R_I} = \bigcap_{i \in I} S_{N/p_i} .$$

c) En appliquant la formule du crible (cf. §III.4, exercice 9), en déduire :

$$\operatorname{card}\left(\bigcup_{i=1}^{r} S_{N/p_i}\right) = \sum_{k=1}^{r} (-1)^{k-1} \sum_{\substack{I \subset [\![1,r]\!] \\ \operatorname{card}(I)=k}} N/R_I .$$

En déduire que le nombre d'éléments d'ordre N dans G est $N\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right)$ et que G est cyclique.

N.B. Cet exercice n'utilise pas le résultat de l'exercice 7 du §V.2, ni la proposition V.3.3. ■

Soit δ entier tel que $d\delta = N$. Pour tout k entier, notons f_k l'h

me $x \mapsto x^k$. Pour tout $x \in G$, $x^{d\delta} = x^N = e_G$, donc $\mathrm{Im}(f_\delta) \subset \mathrm{Ker}(f_d)$. En utilisant le corollaire 3 du théorème V.3.1., on obtient $\mathrm{card}(\mathrm{Im}(f_\delta)) = N/\mathrm{card}(\mathrm{Ker}(f_\delta)) \geqslant N/\delta = d$. Donc $d \leqslant \mathrm{card}(\mathrm{Im}(f_\delta)) \leqslant \mathrm{card}(\mathrm{Ker}(f_d)) \leqslant d$. Par conséquent $d = \mathrm{card}(\mathrm{Ker}(f_d))$, et $\mathrm{Ker}(f_d) = \mathrm{Im}(f_\delta)$.

a) Pour tout $i \in I$, N/p_i est un multiple de N/R_I, donc :

$$S_{N/R_I} \subset \bigcap_{i \in I} S_{N/p_i} .$$

Inversement, si $x \in \bigcap_{i \in I} S_{N/p_i}$, soit d l'ordre de x ; c'est un diviseur de N et on peut donc trouver des entiers $\geqslant 0$, $\alpha'_1, \alpha'_2, \ldots, \alpha'_r$, tels que pour tout $i \in [\![1, r]\!]$, $0 \leqslant \alpha'_i \leqslant \alpha_i$, et $d = \prod_{i=1}^{r} p_i^{\alpha'_i}$; comme pour tout $i \in I$, $d \mid (N/p_i)$, $\alpha'_i \leqslant \alpha_i - 1$, donc d divise N/R_I, et $x \in S_{N/R_I}$. Nous avons donc démontré l'égalité :

$$S_{N/R_I} \subset \bigcap_{i \in I} S_{N/p_i} .$$

b) Pour k entier, nous noterons $\mathcal{P}_k$ l'ensemble des parties de $[\![1, r]\!]$ de cardinal k. Appliquons la formule du crible à la famille $(S_{N/p_i})_{i \in [\![1,r]\!]}$; nous obtenons :

$$\begin{aligned} \mathrm{card}\left(\bigcup_{i=1}^{r} S_{N/p_i}\right) &= \sum_{k=1}^{r} (-1)^{k-1} \sum_{I \in \mathcal{P}_k} \mathrm{card}\left(\bigcap_{i \in I} S_{N/p_i}\right) = \\ &= \sum_{k=1}^{r} (-1)^{k-1} \sum_{I \in \mathcal{P}_k} \mathrm{card}\left(S_{N/R_I}\right) = \\ &= \sum_{k=1}^{r} (-1)^{k-1} \sum_{I \in \mathcal{P}_k} N/R_I , \end{aligned}$$

ce qu'il fallait démontrer. En remplaçant R_I par sa valeur, on obtient encore :

$$\begin{aligned} \mathrm{card}\left(\bigcup_{i=1}^{r} S_{N/p_i}\right) &= = N \sum_{k=1}^{r} (-1)^{k-1} \sum_{I \in \mathcal{P}_k} \prod_{i \in I} \frac{1}{p_i} = \\ &= N \left(1 - \sum_{k=0}^{r} (-1)^k \sum_{I \in \mathcal{P}_k} \prod_{i \in I} \frac{1}{p_i}\right) . \end{aligned}$$

On reconnaît ci-dessus le développement de l'expression :

$$N\left(1-\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)\right) .$$

Finalement nous obtenons :

$$N-\operatorname{card}\left(\bigcup_{i=1}^{r} S_{N/p_i}\right)=N\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)=\varphi(N) .$$

Les éléments du complémentaire de $\bigcup_{i=1}^{r} S_{N/p_i}$ sont les éléments dont l'ordre ne divise aucun des nombres $q_i = N/p_i$; ce sont les éléments d'ordre N. D'après ce qui précède, il y en a (leur nombre est $\varphi(N)$, où $N \geqslant 2$) et par conséquent G est cyclique.

Exercice 5 :

Soient H et K deux sous-groupes d'un groupe G.

a) Montrer que la relation binaire $\mathcal{R}$ définie sur G par :

$$x \mathcal{R} y \quad \text{ssi} \quad \exists (h,k) \in H \times K \mid y = hxk$$

est d'équivalence et que, si H et K sont finis, chaque classe mod $(\mathcal{R})$ est finie, de cardinal diviseur de $\operatorname{card}(H)\operatorname{card}(K)$ (cf. exercice 4 ci-dessus).

b) Si G est fini, en déduire une expression de $\operatorname{card}(G)$ sous la forme :

$$\operatorname{card}(G)=\operatorname{card}(H)\operatorname{card}(K)\sum\frac{1}{d_i}$$

où les d_i sont des entiers à préciser. ■

a) La relation $\mathcal{R}$ s'écrit aussi $\exists (h,k) \in H \times K \mid y = hxk^{-1}$. Pour tout couple $(h,k) \in H \times K$ soit $\varphi_{h,k} : G \to G$, $x \mapsto hxk^{-1}$. On voit que pour tout $(h,k) \in H \times K$, $\varphi_{h,k}$ est bijective de réciproque $\varphi_{h^{-1},k^{-1}}$. D'autre part, pour tous (h,k) et (h',k') dans $H \times K$, et pour tout élément $x \in G$, $\varphi_{h,k}(\varphi_{h',k'}(x)) = \varphi_{hh',kk'}(x)$, donc $(h,k) \mapsto \varphi_{h,k}$ est un homomorphisme de groupes, du groupe $H \times K$ vers le groupe des permutations de l'ensemble G. Nous avons donc ici une opération à gauche du groupe $H \times K$ sur l'ensemble G (voir §V.6). La relation $\mathcal{R}$ est la relation d'équivalence associée à cette opération, dont les classes sont les orbites de G sous l'action du groupe $H \times K$. Les orbites sont finies, et le cardinal de l'orbite de l'élément x est $(\operatorname{card}(H \times K)/\operatorname{card}(S_x)) = [H \times K : S_x]$, où S_x est le stabilisateur de x ; c'est donc un diviseur de $\operatorname{card}(H)\operatorname{card}(K)$.

b) La formule de l'énoncé est la formule des classes :

$$\operatorname{card}(G) = \sum_{x \in S} \frac{\operatorname{card}(H \times K)}{\operatorname{card}(S_x)}$$

où S est un système de représentants pour la relation d'équivalence $\mathcal{R}$.

Exercice 6 :

Soit p un nombre premier et m, n deux entiers $\geqslant 1$. On considère le groupe $G = \left(\mathbb{Z}/_{p^2\mathbb{Z}}\right)^m \times \left(\mathbb{Z}/_{p\mathbb{Z}}\right)^n$. Démontrer :

a) le nombre des sous-groupes cycliques de G de cardinal p^2 est :

$$p^{m+n-1}\frac{p^m - 1}{p - 1} \; ;$$

b) le nombre des sous-groupes non cycliques de G de cardinal p^2 est :

$$\frac{(p^{m+n} - 1)(p^{m+n-1} - 1)}{(p^2 - 1)(p - 1)} \; . \blacksquare$$

a) Cherchons le nombre d'éléments d'ordre p^2, nous en déduirons ensuite le nombre de sous-groupes cycliques d'ordre p^2.
Soit $(x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_n)$ un élément du groupe G ; l'ordre de ce $(n+m)$-uplet est le ppcm des ordres de ses composantes ; comme les ordres des x_i, pour $i \in [\![1, m]\!]$, sont 1, p, ou p^2, et que les ordres des y_j, où $j \in [\![1, n]\!]$, sont 1 ou p, l'ordre de cet élément n'est pas p^2 si, et seulement si tous les x_i, où $i \in [\![1, m]\!]$, sont d'ordre 1 ou p, ou encore ne sont pas des générateurs du groupe $\mathbb{Z}/_{p^2\mathbb{Z}}$. Le nombre d'éléments non générateurs du groupe $\mathbb{Z}/_{p^2\mathbb{Z}}$ étant p, nous en déduisons que le nombre d'éléments de G qui ne sont pas d'ordre p^2 est $p^m p^n$. Le nombre d'éléments d'ordre p^2 est donc $p^{2m}p^n - p^{m+n} = p^{m+n}(p^m - 1)$.
Considérons l'application Φ qui à un élément c de G d'ordre p^2 fait correspondre le sous-groupe engendré par c. Cette application est une surjection de l'ensemble des éléments de G d'ordre p^2 sur l'ensemble des sous-groupes cycliques d'ordre p^2. Un sous-groupe H d'ordre p^2 étant donné, les éléments c de G tels que $\Phi(c) = H$ sont les générateurs de ce sous-groupe H ; il y en a $p^2 - p = \varphi(p)$. Le théorème du Berger nous permet d'affirmer que le nombre de sous-groupes cycliques d'ordre p^2 est :

$$p^{m+n-1}\frac{p^m - 1}{p - 1} \; .$$

b) Considérons l'ensemble E des couples (x,y) d'éléments d'ordre p de G tels que y n'est pas dans le sous-groupe engendré par x. Le nombre d'éléments de G dont l'ordre divise p est p^{m+n}, donc le nombre d'éléments d'ordre exactement p est $p^{m+n}-1$; si x est un élément d'ordre p donné, le nombre d'éléments d'ordre p qui ne sont pas dans le sous-groupe engendré par x est $p^{m+n}-p$. Le cardinal de E est donc $(p^{m+n}-1)(p^{n+m}-p)$.

Soit $(x,y) \in E$. Le sous-groupe engendré par $\{x,y\}$ est l'ensemble des $ix+jy$ où $(i,j) \in \mathbb{Z}^2$. L'application $(i,j) \mapsto ix+jy$, $\mathbb{Z}^2 \to G$ est un homomorphisme de groupes dont l'image est le sous-groupe engendré par $\{x,y\}$. Le noyau de cet homomorphisme est $\{(i,j) \mid ix=-jy\}$. Notons H le sous-groupe engendré par x et K le sous-groupe engendré par y ; ces deux sous-groupes ont p éléments, p premier ; leur intersection a donc soit 1 élément, et $H \cap K = \{0_G\}$, soit p éléments et $H \cap K = H$; la deuxième éventualité est exclue car $y \notin H$. Nous pouvons déduire de ce qui précède que pour tous i et j entiers, $ix=-jy$ si, et seulement si, $ix=0_G$ et $jy=0_G$. Le noyau de l'homomorphisme $(i,j) \mapsto ix+jy$ est donc l'ensemble des couples (i,j) d'entiers tous les deux divisibles par p. Le groupe engendré par (x,y) est donc isomorphe au groupe $(\mathbb{Z}\times\mathbb{Z})/(p\mathbb{Z}\times p\mathbb{Z})$ lui-même isomorphe au groupe $\left(\mathbb{Z}/p\mathbb{Z}\right)^2$; c'est un groupe non cyclique de cardinal p^2.

Soit U un sous-groupe non cyclique de cardinal p^2 dans G. Tout élément non neutre dans U est d'ordre p ; soit x un tel élément, et y un élément de U qui n'est pas dans le sous-groupe H engendré par x. On voit que $(x,y) \in E$ et que le sous-groupe engendré par (x,y), qui a p^2 éléments d'après ce qui précède, est U. Le sous-groupe U est donc dans l'image de l'application Ψ qui à $(x,y) \in E$ fait correspondre le sous-groupe non cyclique d'ordre p^2 engendré par $\{x,y\}$. L'ensemble des couples $(x,y) \in E$ tel que $\Psi(x,y)=U$, est l'ensemble des couples (x,y) tels que x est un élément d'ordre p de U, et y un élément d'ordre p de U qui n'est pas dans le sous-groupe engendré par x. Le groupe U étant isomorphe au groupe $\left(\mathbb{Z}/p\mathbb{Z}\right)^2$, le nombre de ces couples est $(p^2-1)(p^2-p)$. En utilisant le théorème du Berger, nous trouvons que le nombre des sous-groupes non cycliques de cardinal p^2 est :

$$\frac{(p^{m+n}-1)(p^{m+n}-p)}{(p^2-1)(p^2-p)} = \frac{(p^{m+n}-1)(p^{m+n-1}-1)}{(p^2-1)(p-1)} .$$

Exercice 8 :

Montrer que le sous-groupe $\mathbb{Z}^{(\mathbb{N})}$ de $\mathbb{Z}^{\mathbb{N}}$ n'est pas d'indice fini dans $\mathbb{Z}^{\mathbb{N}}$. ■

Le groupe $\mathbb{Z}^{\mathbb{N}}$ étant abélien, il s'agit de démontrer que le groupe quotient $\mathbb{Z}^{\mathbb{N}}/_{\mathbb{Z}^{(\mathbb{N})}}$ n'est pas fini. Soient des suites $s_1, s_2, \ldots, s_k$, éléments de $\mathbb{Z}^{\mathbb{N}}$. Il existe une suite u, élément de $\mathbb{Z}^{\mathbb{N}}$, telle que $\forall j \in \mathbb{N} \quad \forall i \in [\![1,k]\!] \quad u(j) \neq s_i(j)$; on peut par exemple choisir de poser :

$$\forall j \in \mathbb{N} \quad u(j) = 1 + \sup_{i \in [\![1,k]\!]} (s_i(j)) \ .$$

La suite u n'est dans aucun des ensembles $s_i + \mathbb{Z}^{(\mathbb{N})}$, où $i \in [\![1,k]\!]$, car si c'était le cas, la suite u coïnciderait avec la suite s_i à partir d'un certain rang, ce qui est impossible par construction. La classe modulo le sous-groupe $\mathbb{Z}^{(\mathbb{N})}$ de la suite u est donc distincte des classes des suites $s_1, s_2, \ldots, s_k$. Ceci étant vrai quelles que soient les suites $s_1, s_2, \ldots, s_k$, le groupe quotient est infini.

On peut remarquer que le sous-groupe $\mathbb{Z}^{(\mathbb{N})}$ est dénombrable, et donc que toute union finie (ou dénombrable) de classes à gauche modulo ce sous-groupe est dénombrable. Or l'ensemble $\mathbb{Z}^{\mathbb{N}}$ n'est pas dénombrable ; on peut en déduire que l'ensemble des classes à gauche de $\mathbb{Z}^{\mathbb{N}}$ modulo le sous-groupe $\mathbb{Z}^{(\mathbb{N})}$, n'est pas dénombrable.

Exercice 9 :

> Soient H et K deux sous-groupes d'indice fini d'un groupe G. On suppose $[G : H]$ et $[G : K]$ premiers entre eux. Montrer que $G = H\,K$. ■

Soit $\mathcal{P}$ l'ensemble des parties de la forme $xH \cap yK$, où x et y sont des éléments de G. L'ensemble $\mathcal{P}$ est l'ensemble des parties de G de la forme $X \cap Y$, où X est une classe à gauche modulo H, et Y une classe à gauche modulo K ; on voit donc que $\mathcal{P}$ est fini et que $\text{card}\,(\mathcal{P}) \leqslant [G : H] \times [G : K]$. De plus pour tout $z \in G$, $z(H \cap K) = (zH) \cap (zK) \in \mathcal{P}$; le nombre de classes à gauche modulo $H \cap K$ est donc fini et $[G : H \cap K] \leqslant \text{card}\,(\mathcal{P}) \leqslant [G : H] \times [G : K]$. Le théorème V.3.1. nous permet d'affirmer que $[G : H \cap K] = [G : H] \times [H : H \cap K]$, donc $[G : H]$ divise $[G : H \cap K]$; de manière analogue $[G : K]$ divise $[G : H \cap K]$. Comme ces entiers sont par hypothèse premiers entre eux, nous pouvons en déduire que $[G : H] \times [G : K]$ divise $[G : H \cap K]$. Bien sûr cela n'est possible que si $[G : H] \times [G : K] = [G : H \cap K] = \text{card}\,(\mathcal{P})$. Cela implique que pour tous x et y éléments de G, il existe un élément z de G tel que $xH \cap yK = z(H \cap K)$. En particulier, aucun des éléments de $\mathcal{P}$ n'est vide. Pour tout élément $y \in G$, $H \cap yK \neq \emptyset$, donc il existe $h \in H$ et $k \in K$ tels que $h = y\,k$, soit $y = h\,k^{-1}$, d'où enfin $y \in H\,K$. Nous avons bien démontré $G = H\,K$.

§ V.4 *GROUPES DE PERMUTATIONS*

Exercice 2 :

Trouver le **centre** de $\mathfrak{S}_n$, c'est-à-dire le sous-groupe formé dans $\mathfrak{S}_n$ par les éléments permutables avec tous les autres. Trouver le centre de $\mathfrak{A}_n$. ■

Si σ est une permutation d'un ensemble E, appelons support de la permutation σ l'ensemble des éléments de E non invariants par σ ; nous utiliserons la notation : $\text{supp}(\sigma) = \{x \in E,\ \sigma(x) \neq x\}$. Le complémentaire du support de la permutation σ est l'ensemble des éléments invariants par σ, et c'est donc une partie globalement invariante par σ ; le support de σ est donc aussi une partie globalement invariante par σ.
Montrons que si deux permutations de E commutent, alors le support de l'une est stable par l'autre. Si s et σ sont des permutations de E qui commutent, et que $\sigma(x) \neq x$, alors $\sigma(s(x)) = s(\sigma(x)) \neq s(x)$, donc $s(x)$ n'est pas invariant par σ.
Si σ est une permutation de E qui commute avec toute permutation, elle commute en particulier avec toute transposition, donc, d'après ce qui précède, toute paire est stable par σ. Supposons que E ait au moins trois éléments distincts ; si x est un élément quelconque de E, on peut trouver deux autres éléments y et z de E ; les paires $\{x, y\}$ et $\{x, z\}$ étant stables par σ, leur intersection x est stable par σ, d'où $\sigma(x) = x$.
Nous pouvons déduire de ce qui précède que si E a au moins 3 éléments distincts, le centre du groupe $\mathfrak{S}_E$ est $\{\text{Id}_E\}$. Si E a 0, 1, ou 2 éléments, le groupe $\mathfrak{S}_E$ est abélien, égal à son centre.

Supposons maintenant que la permutation σ commute avec toutes les permutations paires. Elle commute en particulier avec tous les cycles d'ordre 3, donc toutes les parties de cardinal 3 sont stables par σ. Supposons que E ait au moins 4 éléments distincts. Si x est un élément quelconque de E, on peut trouver 3 autres éléments de E, u, v et w. Les parties $\{x, u, v\}$, $\{x, v, w\}$ et $\{x, u, w\}$ étant stables par σ, leur intersection $\{x\}$ aussi, d'où $\sigma(x) = x$.
Nous pouvons en déduire que si E a au moins 4 éléments, une permutation qui commute avec toute permutation paire est Id_E ; en particulier le centre du groupe $\mathfrak{A}_E$ est $\{\text{Id}_E\}$. Si E a 0,1, 2 ou 3 éléments, on sait que le groupe $\mathfrak{A}_E$ est abélien, donc confondu avec son centre.

Exercice 3 :

Montrer que, si $n \geqslant 2$, le groupe $\mathfrak{S}_n$ est engendré par les transpositions $\tau_{1,i}$, $2 \leqslant i \leqslant n$; ($\tau_{1,i}(1) = i, \tau_{1,i}(i) = 1, \tau_{1,i}(k) = k$ pour $k \neq 1, k \neq i$). Montrer aussi que $\mathfrak{S}_n$ est engendré par les transpositions $\tau_{i,i+1}, 1 \leqslant i \leqslant n-1$. Existe-t-il des parties strictes de ces ensembles qui engendrent encore $\mathfrak{S}_n$

On vérifie facilement que si i et j sont distincts dans $[\![2,n]\!]$, alors $\tau_{i,j} = \tau_{1,i}\circ\tau_{1,j}\circ\tau_{1,i}$; les transpositions $\tau_{1,j}$ et $\tau_{i,j}$ sont conjuguées. Le sous-groupe engendré par les transpositions $\tau_{1,i}$ où $2 \leqslant i \leqslant n$ contient donc toutes les transpositions ; c'est donc le groupe $\mathfrak{S}_n$.
Soit $i_0 \in [\![2,n]\!]$, l'élément i_0 de $[\![1,n]\!]$ est invariant par toutes les transpositions $\tau_{1,i}$, $2 \leqslant i \leqslant n$ et $i \neq i_0$; le sous-groupe des permutations de $[\![1,n]\!]$ qui laissent l'élément i_0 invariant contient donc le sous-groupe engendré par ces permutations ; ce sous-groupe engendré n'est donc pas $\mathfrak{S}_n$.
On voit donc qu'aucun sous-ensemble strict de l'ensemble des transpositions $\tau_{1,i}$, $2 \leqslant i \leqslant n$, n'est générateur.

Soient i et j entiers tels que $1 \leqslant i < j-1 \leqslant n-1$; on vérifie facilement que $\tau_{i,j} = \tau_{j-1,j} \circ \tau_{i,j-1} \circ \tau_{j-1,j}$ (nous utilisons ici encore la formule générale $\tau_{\sigma(x),\sigma(y)} = \sigma \circ \tau_{x,y} \circ \sigma^{-1}$). Il est donc clair qu'on peut démontrer par récurrence que toute transposition est dans le groupe engendré par les transpositions entre éléments consécutifs. L'ensemble des transpositions entre éléments consécutifs est donc générateur.
Soit $i_0 \in [\![1,n-1]\!]$. On voit que l'intervalle $[\![1,i_0]\!]$ est stable par toutes les transpositions $\tau_{i,i+1}$, si $1 \leqslant i < i_0$, et aussi si $i_0 < i \leqslant n-1$; le sous-groupe engendré par les transpositions $\tau_{i,i+1}$, où $i \in [\![0,n-1]\!] \setminus \{i_0\}$, est donc inclus dans le sous-groupe des permutations de $[\![1,n]\!]$ qui laissent la partie $[\![1,i_0]\!]$ stable. Le sous-groupe engendré par ces transpositions n'est donc pas $\mathfrak{S}_n$: il ne contient pas la transposition τ_{i_0,i_0+1}. On voit donc qu'aucun sous-ensemble strict de l'ensemble des transpositions $\tau_{i,i+1}$, où $i \in [\![0,n-1]\!]$, n'est générateur.

Exercice 4 :

Soit $n \geqslant 2$. Montrer que $\mathfrak{S}_n$ est engendré par les deux éléments suivants :
$\tau_{1,2}$ (voir exercice 3), et $c_n = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix}$. ■

Pour tout $i \in [\![1,n-1]\!]$, on voit que $c_n^{i-1}(1) = i$ et $c_n^{i-1}(2) = i+1$, donc $\tau_{i,i+1} = c_n^{i-1} \circ \tau_{1,2} \circ c_n^{-(i-1)}$. Le sous-groupe engendré par la transposition $\tau_{1,2}$ et le cycle c_n contient donc toutes les transpositions entre éléments consécutifs ; c'est donc, d'après l'exercice 3, le groupe $\mathfrak{S}_n$. L'ensemble $\{\tau_{1,2}, c_n\}$ est donc générateur dans le groupe $\mathfrak{S}_n$.

Exercice 5 :

Dans le groupe G, on appelle **groupe des commutateurs de** G le sous-groupe de G engendré par les éléments $xyx^{-1}y^{-1}$, où (x,y) parcourt $G \times G$. Ce sous-groupe se note $[G,G]$; si $x,y \in G$, l'élément $xyx^{-1}y^{-1}$ s'appelle *commuta*

y et se note $[x, y]$. Si $n \geqslant 3$, déterminer les groupes $[\mathfrak{S}_n, \mathfrak{S}_n]$ et $[\mathfrak{A}_n, \mathfrak{A}_n]$. Pour $n = 4$ on pourra se reporter au §V.7. ■

Il est clair que les commutateurs sont des permutations paires et que par conséquent le sous-groupe $[\mathfrak{S}_n, \mathfrak{S}_n]$, engendré par les commutateurs, est inclus dans le sous-groupe des permutations paires : $\mathfrak{A}_n$.
Soient (x, y) et (z, t) deux couples d'éléments distincts dans $[\![1, n]\!]$. Il existe une permutation σ de $[\![1, n]\!]$ telle que $\sigma(x) = z$ et $\sigma(y) = t$; on voit alors que $\tau_{z,t} = \sigma \circ \tau_{x,y} \circ \sigma^{-1}$. Nous en déduisons l'égalité :

$$\tau_{x,y} \circ \tau_{z,t} = \tau_{x,y} \circ \sigma \circ \tau_{x,y} \circ \sigma^{-1} = [\tau_{x,y}, \sigma] .$$

Le composé de deux transpositions est donc un commutateur, et est a fortiori dans le groupe $[\mathfrak{S}_n, \mathfrak{S}_n]$. Toute permutation paire, qui peut s'écrire comme composée d'un nombre pair de transpositions, est donc dans le groupe $[\mathfrak{S}_n, \mathfrak{S}_n]$. Le groupe $[\mathfrak{S}_n, \mathfrak{S}_n]$ est donc le groupe des permutations paires : $\mathfrak{A}_n$.

Soient maintenant x, y, z, t quatre éléments distincts dans $[\![1, n]\!]$. Considérons les permutations paires $s = \tau_{z,t} \circ \tau_{y,z}$ et $\sigma = \tau_{x,t} \circ \tau_{y,z}$. On vérifie que :

$$\begin{aligned} \sigma \circ s \circ \sigma^{-1} &= \sigma \circ \tau_{z,t} \circ \sigma^{-1} \circ \sigma \circ \tau_{y,z} \circ \sigma^{-1} \\ &= \tau_{\sigma(z),\sigma(t)} \circ \tau_{\sigma(y),\sigma(z)} = \tau_{y,x} \circ \tau_{z,y} . \end{aligned}$$

Nous en déduisons que :

$$\tau_{x,y} \circ \tau_{z,t} = (\tau_{x,y} \circ \tau_{y,z}) \circ (\tau_{y,z} \circ \tau_{z,t}) = \sigma \circ s \circ \sigma^{-1} \circ s^{-1} .$$

Ce qui précède montre que la composée de deux transpositions de supports disjoints est un commutateur.

Pour $n = 1$, 2 ou 3, le groupe $\mathfrak{A}_n$ est commutatif donc $[\mathfrak{A}_n, \mathfrak{A}_n] = \{\mathrm{Id}\}$.
Supposons $n \geqslant 5$. Si x, y et z sont trois éléments distincts dans $[\![1, n]\!]$, alors on peut trouver deux éléments u et v de $[\![1, n]\!]$ tels que x, y, z, u, v soient distincts. On peut alors écrire :

$$\tau_{x,y} \circ \tau_{y,z} = (\tau_{x,y} \circ \tau_{u,v}) \circ (\tau_{u,v} \circ \tau_{y,z}) .$$

La composée de deux transpositions distinctes est donc un commutateur si les supports des transpositions sont disjoints, ou bien le composé de deux commutateurs si les supports des transpositions ont un élément commun. Toute permutation paire, qui peut s'écrire comme composée d'un nombre pair de transpositions, peut aussi s'écrire comme composée de commutateurs. Nous en déduisons que si $n \geqslant 5$, alors $[\mathfrak{A}_n, \mathfrak{A}_n] = \mathfrak{A}_n$.

Il reste à déterminer le groupe $[\mathfrak{A}_4, \mathfrak{A}_4]$. On sait que c'est un sous-groupe de $\mathfrak{A}_4$ qui contient les composés de deux transpositions de suppc

Montrons que cet ensemble de permutations, auquel on adjoint Id, est un sous-groupe (distingué). Notons H cet ensemble de permutations ; Il est clair qu'il a 4 éléments. L'ensemble H est évidemment stable par l'inverse (d'ailleurs tout élément de H est son propre inverse, car deux transpositions de supports disjoints commutent et sont involutives). Soit $\tau_{x,y} \circ \tau_{z,t}$ un élément de H (différent de Id), où $\{x,y,z,t\} = [\![1,4]\!]$. Les deux autres éléments non neutres de H sont $\tau_{x,z} \circ \tau_{y,t}$ et $\tau_{x,t} \circ \tau_{y,z}$. On vérifie que :

$$(\tau_{x,y} \circ \tau_{z,t}) \circ (\tau_{x,z} \circ \tau_{y,t}) = \tau_{x,t} \circ \tau_{y,z} \ ,$$

et que (en échangeant z et t) :

$$(\tau_{x,y} \circ \tau_{z,t}) \circ (\tau_{x,t} \circ \tau_{y,z}) = \tau_{x,z} \circ \tau_{y,t} \ .$$

L'ensemble H est donc stable par la composition, et est par conséquent un sous-groupe. On voit facilement qu'il s'agit d'un sous-groupe distingué, car une permutation conjuguée de la composée de deux transpositions de supports disjoints, est la composée de deux transpositions de supports disjoints.

Montrons maintenant $[\mathfrak{A}_4, \mathfrak{A}_4] = H$. On a vu que :

$$\mathfrak{A}_4 \supset [\mathfrak{A}_4, \mathfrak{A}_4] \supset H \ .$$

Le cardinal du groupe $[\mathfrak{A}_4, \mathfrak{A}_4]$ est donc un multiple de 4 qui divise 12, c'est donc 4 ou 12. Nous en déduisons que soit $\mathfrak{A}_4 = [\mathfrak{A}_4, \mathfrak{A}_4]$, soit $[\mathfrak{A}_4, \mathfrak{A}_4] = H$. Remarquons que le groupe quotient $\mathfrak{A}_4/_H$ est de cardinal 3, donc abélien. Notons $\pi : \mathfrak{A}_4 \to \mathfrak{A}_4/_H$ l'homomorphisme canonique, et e l'élément neutre du groupe quotient. Si on avait l'égalité $\mathfrak{A}_4 = [\mathfrak{A}_4, \mathfrak{A}_4]$, pour tout $\sigma \in \mathfrak{A}_4$, il existerait $(s, s') \in \mathfrak{A}_4^2$ tel que $\sigma = [s, s']$, d'où

$$\pi(\sigma) = \pi(s \circ s' \circ s^{-1} \circ s'^{-1}) = \pi(s)\,\pi(s')\,\pi(s)^{-1}\,\pi(s')^{-1} = e \ ;$$

on en déduirait que pour tout $\sigma \in \mathfrak{A}_4$, $\sigma \in H$, ce qui est évidemment faux. On voit donc que $[\mathfrak{A}_4, \mathfrak{A}_4] = H$, ce qu'il fallait démontrer.

Exercice 6 :

> A isomorphisme près, montrer qu'il n'y a que deux groupes de cardinal 6, à savoir $(\mathbb{Z}/_{6\mathbb{Z}}, +)$ et $\mathfrak{S}_3$. ■

Soit G un groupe de cardinal 6, les périodes des éléments de G sont des diviseurs de 6 ; elles peuvent donc être 1 (période du neutre e), 2, 3 ou 6. S'il y a dans G un élément de période 6, alors G est cyclique, isomorphe au groupe $(\mathbb{Z}/_{6\mathbb{Z}}, +)$; nous supposerons dans la suite que ce n'est pas le cas. L'objectif poursuivi est de démontrer que G est alors isomorphe au groupe $\mathfrak{S}_3$. Nous noterons $\star$ la loi du groupe.

Supposons que x et y soient des éléments de G de période 2. Si l'élément $x \star y$ est d'ordre 2, alors $x \star y = (x \star y)^{-1} = y^{-1} \star x^{-1} = y \star x$; les éléments x et y commutent et engendrent donc un sous-groupe $\{e, x, y, x \star y\}$ de cardinal 4 ; cela est impossible car 4 ne divise pas 6. Le composé de deux éléments d'ordre 2, distincts, est donc d'ordre 3.

Il y a donc nécessairement dans G des éléments d'ordre 3. Soit x l'un d'eux, il engendre un sous-groupe H de cardinal 3. Si $y \notin H$, yH est une partie disjointe de H et elle a 3 éléments, c'est donc $\complement H$; de même $Hy = \complement H$, d'où $Hy = yH$, soit encore $H = yHy^{-1}$. Cette égalité étant bien entendu vraie pour tout élément y de H, on voit que le sous-groupe H est distingué. Le groupe quotient, $G/_H$, a deux éléments.

Soit comme ci-dessus x un élément d'ordre 3, H le sous-groupe qu'il engendre et $y \notin H$. La classe de y^2 dans le groupe quotient $G/_H$, de cardinal 2, est neutre ; cela signifie $y^2 \in H$. Supposons $y^2 = x$, ou $y^2 = x^{-1}$, on voit facilement que y serait d'ordre 6, ce que nous avons exclu. Donc tout élément $y \notin H$ est tel que $y^2 = e$, et est par conséquent d'ordre 2 (ce n'est pas e). Il y a donc dans G trois éléments d'ordre 2, deux éléments d'ordre 3 inverses l'un de l'autre, et l'élément neutre.

Si x est d'ordre 3 et y d'ordre 2, puisque le sous-groupe H engendré par x est distingué, $y \star x \star y^{-1} \in H$; donc $y \star x \star y^{-1} = e$ ou x ou x^{-1}. La première éventualité est évidemment exclue ; si $y \star x \star y^{-1} = x$, c'est-à-dire si x et y commutent, on voit facilement que l'élément $x \star y$ est d'ordre 6, ce qui a été exclu par hypothèse ; nous en déduisons que nécessairement : $y \star x \star y^{-1} = x^{-1}$.

La propriétés démontrées ci-dessus sont suffisantes pour établir que G est isomorphe au groupe $\mathfrak{S}_3$. Nous pouvons rendre concret cet isomorphisme de la manière suivante. Si $y \in G$ nous noterons σ_y l'automorphisme intérieur de G, $z \mapsto y \star z \star y^{-1}$. Soit H le sous-groupe engendré par un élément de période 3, et H' son complémentaire dans G, c'est-à-dire l'ensemble des éléments de période 2. La partie H étant globalement invariante par σ_y, pour tout $y \in G$, la partie H' l'est aussi. On peut donc considérer l'application $\Phi : y \mapsto \sigma'_y$, $G \to \mathfrak{S}_{H'}$, où σ'_y est la permutation induite par σ_y sur H'. Cette application est évidemment un homomorphisme de groupes ; comme les deux groupes ont même cardinal, il suffit de démontrer qu'il est injectif pour pouvoir affirmer que c'est un isomorphisme. Les éléments de $\mathrm{Ker}\,(\Phi)$ sont les éléments de G qui commutent avec tous les éléments de H'. Or deux éléments d'ordre 2 différents y et y' ne commutent pas entre eux ($y \star y'$ n'est pas d'ordre 2), et un élément d'ordre 3, x, et un élément d'ordre 2, y, ne commutent pas ($y \star x \star y^{-1} = x^{-1}$). Le noyau de Φ est donc réduit à $\{e_G\}$. Cet homomorphisme de groupes est donc injectif, et par conséquent bijectif.

Un groupe G de cardinal 6 qui n'a aucun élément de période 6 est donc nécessairement isomorphe au groupe $\mathfrak{S}_3$.

Exercice 9 :

Soit $n \geqslant 2$ et c_n la permutation $\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix}$.

Montrer que si c_n est produit de k transpositions, on a $k \geqslant n-1$. ■

Soit E un ensemble fini et $\sigma \in \mathfrak{S}_E$. Notons $n(\sigma)$ le nombre de classes d'équivalence pour la relation $\mathcal{R}_\sigma$ définie par :

$$\forall (x,y) \in E \times E \quad (x \mathcal{R}_\sigma y \iff (\exists n \in \mathbb{Z} \quad y = \sigma^n(x))) .$$

Montrons que si τ est une transposition, $n(\sigma \circ \tau) \geqslant n(\sigma) - 1$.
Supposons que τ soit la transposition entre deux éléments d'une même classe $\mathcal{O}$ pour la relation $\mathcal{R}_\sigma$. Les classes pour $\mathcal{R}_\sigma$ différentes de $\mathcal{O}$ sont aussi des classes pour $\mathcal{R}_{(\sigma \circ \tau)}$, et $\mathcal{O}$, qui est stable par $\sigma \circ \tau$, est réunion de classes pour $\sigma \circ \tau$; dans ce cas on voit que $n(\sigma \circ \tau) \geqslant n(\sigma)$.
Supposons que τ soit la transposition entre deux éléments x et y qui ne sont pas dans la même classe pour $\mathcal{R}_\sigma$; notons $\mathcal{O}_x$ et $\mathcal{O}_y$ ces classes. Les autres classes pour $\mathcal{R}_\sigma$ sont aussi des classes pour $\mathcal{R}_{(\sigma \circ \tau)}$, et la partie $\mathcal{O}_x \cup \mathcal{O}_y$, qui est stable par $\sigma \circ \tau$, est réunion de classes pour $\sigma \circ \tau$, et elle contient donc au moins une classe. Dans ce cas on voit que $n(\sigma \circ \tau) \geqslant n(\sigma) - 1$.
Une étude moins rapide du problème permet de montrer que si τ est une transposition entre éléments d'une même classe, alors $n(\sigma \circ \tau) = n(\sigma) + 1$, et si τ est une transposition entre éléments de classes différentes, alors $n(\sigma \circ \tau) = n(\sigma) - 1$.

Supposons que $\tau_1, \tau_2, \dots, \tau_k$ soient des transpositions. Comme $n(\mathrm{Id}) = n$, on voit que $n(\tau_1) \geqslant n-1$, $n(\tau_1 \circ \tau_2) \geqslant n-2$, etc., $n(\tau_1 \circ \tau_2 \circ \dots \circ \tau_k) \geqslant n-k$.
Si $c_n = \tau_1 \circ \tau_2 \circ \dots \circ \tau_k$, alors $n(c_n) = 1 \geqslant n - k$; d'où $k \geqslant n-1$.

Exercice 12 :

Si $n \geqslant 2$, trouver les permutations permutables avec

$$c_n = \langle 1, 2, \dots, n \rangle \qquad (c_n \in \mathfrak{S}_n) . \blacksquare$$

Les puissances du cycle c_n commutent avec le cycle c_n ; montrons que ce sont les seules (il y en a donc n). Soit $\sigma \in \mathfrak{S}_n$ qui commute avec c_n ; il existe $i \in [\![1, n]\!]$ tel que $\sigma(1) = i = c_n^{i-1}(1)$. Pour tout $j \in \mathbb{Z}$, $\sigma(c_n(j)) = \sigma(c_n^{j-1}(1)) = (\sigma \circ c_n^{j-1})(1) = (c_n^{j-1} \circ \sigma)(1) = c_n^{j-1}(\sigma(1)) = c_n^{j-1}(c_n^{i-1}(1)) = c_n^{i+j-2}(1) = c_n^{i-1}(c_n^{j-1}(1)) = c_n^{i-1}(c_n(j))$. Donc pour tout élément $k \in [\![1, n]\!]$, $\sigma(k) = c_n^{i-1}(k)$, soit $\sigma = c_n^{i-1}$, ce qu'il fallait démontre

Exercice 13 :

Soit $s \in \mathfrak{S}_{10}$ la permutation $u \circ v$, où
$$u = \langle 1,2,3,4,5\rangle\,, \qquad v = \langle 6,7,8,9,10\rangle\,.$$
Trouver les permutations $\sigma \in \mathfrak{S}_{10}$ telles que $\sigma \circ s = s \circ \sigma$. Montrer qu'il y en a 50 et qu'elles forment un sous-groupe de $\mathfrak{S}_{10}$. ■

Montrons que si s est une permutation donnée de l'ensemble fini E, l'ensemble $\mathscr{C}_s$ des permutations $\sigma \in \mathfrak{S}_E$ telles que $s\circ\sigma = \sigma\circ s$ est un sous-groupe du groupe $\mathfrak{S}_E$. On voit que $\mathrm{Id} \in \mathscr{C}_s$; si $s\circ\sigma = \sigma\circ s$, alors $\sigma^{-1}\circ s = s\circ\sigma^{-1}$; si σ et σ' commutent avec s, alors $s\circ\sigma\circ\sigma' = \sigma\circ s\circ\sigma' = \sigma\circ\sigma'\circ s$. La partie $\mathscr{C}_s$ est donc un sous-groupe de $\mathfrak{S}_E$.

On peut remarquer que les permutations u et v commutent. Nous poserons $A = \{1,2,3,4,5\}$ et $B = \{6,7,8,9,10\}$. Ces deux ensembles sont stables par u, v et s ; le support de u est A, le support de v est B. On voit facilement que $A = \{s^i(1),\ i \in \mathbb{Z}\}$ et que $B = \{s^i(6),\ i \in \mathbb{Z}\}$.
Cherchons d'abord l'ensemble $\mathscr{C}'_s$ des permutations σ qui commutent avec s et telles que $\sigma(1) \in A$. Si σ commute avec s et que $\sigma(1) \in A$, alors il existe un entier $i \in [\![0,4]\!]$ tel que $\sigma(1) = s^i(1)$; pour tout entier relatif j, on a alors $\sigma(s^j(1)) = s^j(\sigma(1)) = s^j(s^i(1)) = s^{i+j}(1)$. L'ensemble A est donc stable par σ ; il en est de même pour son complémentaire B. Si $x \in A$, alors $v(x) = x$, donc $\sigma(u(x)) = \sigma(u(v(x))) = \sigma((u\circ v)(x)) = (u\circ v)(\sigma(x))$; comme $\sigma(x)$ est dans A, il est invariant par v donc $\sigma(u(x)) = u(v(\sigma(x))) = u(\sigma(x))$. Nous en déduisons que la permutation σ commute avec u, et aussi avec v, puisque $v = u\circ s^{-1}$. La permutation induite par σ sur A commute avec le cycle induit par u sur A ; en utilisant le résultat de l'exercice précédent, nous pouvons en déduire que σ coïncide sur A avec une puissance de u ; de même, σ coïncide sur B avec une puissance de v. On voit alors facilement qu'il existe deux entiers i et j (qu'on peut supposer dans $[\![0,4]\!]$) tels que $\sigma = u^i \circ v^j$. Inversement toutes les permutations qui s'écrivent ainsi commutent avec s et laissent les parties A et B stables. En conclusion : $\mathscr{C}'_s = \left\{u^i \circ v^j,\ (i,j) \in [\![0,4]\!]^2\right\}$; on trouve ainsi 25 permutations.

Soit maintenant la permutation :
$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 7 & 8 & 9 & 10 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

On vérifie facilement que $\sigma_0\circ u\circ\sigma_0^{-1} = v$ et $\sigma_0\circ v\circ\sigma_0^{-1} = u$; par conséquent $\sigma_0\circ u\circ v\circ\sigma_0^{-1} = v\circ u = u\circ v$, d'où $\sigma_0\circ s = s\circ\sigma_0$. Une permutation σ commute avec s si, et seulement si, $\sigma_0^{-1}\circ\sigma$ commute avec s ($\mathscr{C}_s$ est un sous-groupe), et $\sigma(1) \in B$ si, et seulement si, $\sigma_0^{-1}\circ\sigma(1) \in A$.

de $\mathscr{C}_s$ qui ne sont pas dans $\mathscr{C}'_s$ sont donc les permutations σ telles que $\sigma_0^{-1} \circ \sigma \in \mathscr{C}'_s$; leur nombre est 25.

En résumé : $\mathscr{C}_s = \mathscr{C}'_s \cup \sigma_0\mathscr{C}'_s$, où $\mathscr{C}'_s = \left\{u^i \circ v^j,\ (i,j) \in [\![0,4]\!]^2\right\}$, et $\text{card}\,(\mathscr{C}_s) = 50$.

Exercice 16 :

Soit $N = pq + 1$ avec $p \geqslant 2$, $p \in \mathbb{N}^*$, $q \in \mathbb{N}^*$. On considère les permutations

$s_1 = \langle 1, 2, \ldots, q+1\rangle$, $\quad s_2 = \langle 1, q+2, \ldots, 2q+1\rangle, \ldots,$

$s_p = \langle 1, (p-1)q+2, \ldots, pq+1\rangle$.

Démontrer :

a) Si q est impair, $\{s_1, s_2, \ldots, s_p\}$ engendre le groupe $\mathfrak{S}_N$.

b) Si q est pair, $\{s_1, s_2, \ldots, s_p\}$ engendre le groupe $\mathfrak{A}_N$. ■

Pour la suite nous considérerons connu le résultat suivant. Soit E un ensemble fini, σ une permutation de E et un cycle $\langle x_1, x_2, \ldots, x_p\rangle$ de support inclus dans E, alors :

$$\sigma \circ \langle x_1, x_2, \ldots, x_p\rangle \circ \sigma^{-1} = \langle \sigma(x_1), \sigma(x_2), \ldots, \sigma(x_p)\rangle\ .$$

Pour tout entier $n \in [\![1,p]\!]$, notons $E_n = \{(n-1)q+2, \ldots, nq+1\}$, de telle sorte que le support du cycle s_n est $\{1\} \cup E_n$. Les ensembles E_n sont disjoints et ont tous q éléments, et les cycles s_n sont d'ordre $q+1$. Nous appellerons H le sous-groupe engendré par les cycles s_n, où $n \in [\![1,p]\!]$, et nous noterons E l'ensemble $[\![1, pq+1]\!]$.

Soient n et m deux entiers distincts dans $[\![1,p]\!]$, et $(i,j) \in [\![1,q]\!]^2$. Calculons le commutateur $\sigma = s_n^j \circ s_m^i \circ s_n^{-j} \circ s_m^{-i}$.
Si $x \neq 1$, élément de E, n'est ni dans E_n, ni dans E_m, il est invariant par les cycles s_n et s_m donc $\sigma(x) = x$.
Si $x \in E_m$, mais $x \neq s_m^i(1)$, alors $s_m^{-i}(x)$ est différent de 1, donc est dans E_m et est invariant par s_n ; dans ce cas :

$$\sigma(x) = s_n^j \circ s_m^i \circ s_n^{-j} \circ s_m^{-i}(x) = s_n^j \circ s_m^i \circ s_m^{-i}(x) = s_n^j(x) = x\ ;$$

si $x \in E_n$ et $x \neq s_n^j(1)$, x est invariant par s_m ; de plus $s_n^{-j}(x)$ est différent de 1, donc est dans E_n et est invariant par s_m ; d'où :

$$\sigma(x) = s_n^j \circ s_m^i \circ s_n^{-j} \circ s_m^{-i}(x) = s_n^j \circ s_m^i \circ s_n^{-j}(x) = s_n^j \circ s_n^{-j}(x) = x\ .$$

En utilisant le fait que $s_m^{-i}(1)$ et $s_m^i(1)$ sont dans E_m, donc sont invariants par s_n, et que de même $s_n^{-j}(1)$ et $s_n^j(1)$ sont dans E_n, donc s

par s_m, on voit que :

$$\begin{aligned}
\sigma(1) &= s_n^j \circ s_m^i \circ s_n^{-j} \circ s_m^{-i}(1) = s_n^j \circ s_m^i \circ s_m^{-i}(1) = s_n^j(1) \ ; \\
\sigma(s_n^j(1)) &= s_n^j \circ s_m^i \circ s_n^{-j} \circ s_m^{-i}(s_n^j(1)) = s_n^j \circ s_m^i \circ s_n^{-j}(s_n^j(1)) = \\
&= s_n^j \circ s_m^i(1) = s_m^i(1) \ ; \\
\sigma(s_m^i(1)) &= s_n^j \circ s_m^i \circ s_n^{-j} \circ s_m^{-i}(s_m^i(1)) = s_n^j \circ s_m^i \circ s_n^{-j}(1) = \\
&= s_n^j \circ s_n^{-j}(1) = 1 \ .
\end{aligned}$$

Nous voyons donc que $\sigma = [s_n^j, s_m^i] = \langle 1, s_n^j(1), s_m^i(1) \rangle$.
Nous pouvons déduire de ce qui précède que tout cycle d'ordre 3 de la forme $\langle 1, a, b \rangle$, où a et b sont des éléments de E, différents de 1, et qui ne sont pas dans le même ensemble E_n, est dans le sous-groupe engendré H.

Supposons maintenant que a et b soient des éléments de E différents de 1 mais dans le même ensemble E_n, où $n \in [\![1, p]\!]$. Il existe des entiers i et j (on peut supposer $i < j$) dans $[\![1, q]\!]$ tels que $a = s_n^i(1)$ et $b = s_n^j(1)$; puisque $p \geqslant 2$, on peut aussi trouver un entier $m \in [\![1, p]\!]$, $m \neq n$. En utilisant ce qui précède, on voit que $\sigma = \langle 1, s_m^{-1}(1), s_n^{j-i}(1) \rangle \in H$, donc :

$$s_m \circ \sigma \circ s_m^{-1} = \langle s_m(1), 1, s_m(s_n^{j-i}(1)) \rangle = \langle s_m(1), 1, s_n^{j-i}(1) \rangle \in H \ ;$$

nous en déduisons encore :

$$s_n^i \circ s_m \circ \sigma \circ s_m^{-1} \circ s_n^{-i} = \langle s_m(1), s_n^i(1), s_n^j(1) \rangle \in H \ ;$$

et pour finir :

$$s_m^{-1} \circ \langle s_m(1), s_n^i(1), s_n^j(1) \rangle \circ s_m = \langle 1, s_n^i(1), s_n^j(1) \rangle \in H \ .$$

Le cycle $\langle 1, a, b \rangle$ et le cycle inverse $\langle 1, b, a \rangle$ sont donc dans H.
De ce qui précède nous pouvons déduire que tout cycle d'ordre 3 de la forme $\langle 1, a, b \rangle$, où a et b sont des éléments de E différents de 1, est dans H.

Montrons que tous les cycles d'ordre 3, de la forme $\langle a, b, c \rangle$ (a, b, c distincts dans E) sont dans H. D'après ce qui précède, c'est vrai si $a = 1$. Si $a \neq 1$, soit $n \in [\![1, p]\!]$ tel que $a \in E_n$, et $i \in [\![1, q]\!]$ tel que $a = c_n^i(1)$. Comme $\sigma = \langle 1, c_n^{-i}(b), c_n^{-i}(c) \rangle \in H$, on voit que :

$$c_n^i \circ \sigma \circ c_n^{-i} = \langle c_n^i(1), b, c \rangle = \langle a, b, c \rangle \in H \ .$$

Le groupe H contient toutes les permutations qui s'écrivent comme composées de deux transpositions. En effet pour tous éléments a, b, c distincts dans E, $\tau_{a,b} \circ \tau_{b,c} = \langle a, b, c \rangle$, et pour tous éléments a, b, c, d c

E, $\tau_{a,b} \circ \tau_{c,d} = \tau_{a,b} \circ \tau_{b,c} \circ \tau_{b,c} \circ \tau_{c,d} = \langle a,b,c\rangle \circ \langle b,c,d\rangle$. Le groupe H contient donc toutes les permutations paires, soit $\mathfrak{A}_N \subset H$.

Si q est pair, les cycles $s_1, s_2, \ldots, s_p$, qui sont d'ordre $q+1$, sont pairs et le groupe engendré H est par conséquent inclus dans $\mathfrak{A}_N$. Dans ce cas, $H = \mathfrak{A}_N$.
Si q est impair, les cycles $s_1, s_2, \ldots, s_p$ sont impairs ; le groupe H contient toutes les permutations paires et des permutations impaires ; par conséquent, dans ce cas $H = \mathfrak{S}_N$.

§ V.5 *CYCLES DANS LES GROUPES $\mathfrak{S}_E$ (E fini)*

Exercice 1 :

> Montrer que pour tout $N \geqslant 3$, $\mathfrak{A}_N$ est engendré par les cycles de longueur 3. Montrer même que chacun des ensembles suivants suffit à engendrer $\mathfrak{A}_N$:
> *a)* $\{\langle 1,2,3\rangle, \langle 1,4,5\rangle, \ldots, \langle 1,2n,2n+1\rangle\}$
> si $N = 2n+1$.
> *b)* $\{\langle 1,2,3\rangle, \ldots, \langle 1,2n-2,2n-1\rangle, \langle 1,2,2n\rangle\}$
> si $N = 2n$.
> Peut-on diminuer ces ensembles générateurs ?
> Montrer aussi que les cycles $\langle 1,2,3\rangle, \langle 1,2,4\rangle, \ldots, \langle 1,2,N\rangle$ engendrent $\mathfrak{A}_N$. ■

a) Si $n = 1$ alors $N = 3$, le groupe $\mathfrak{A}_3$ est bien engendré par le cycle $\langle 1,2,3\rangle$. Si $n \geqslant 2$, nous pouvons appliquer les résultats de l'exercice 16 du chapitre précédent, avec $p = n$ et $q = 2$. L'ensemble de ces cycles d'ordre 3 est donc un système générateur de $\mathfrak{A}_N$.

Soit $i_0 \in [\![1,n]\!]$, $2i_0$ et $2i_0+1$ sont invariants par les cycles $\langle 1, 2i, 2i+1\rangle$, où $i \in [\![1,n]\!] \setminus \{i_0\}$; cet ensemble decycles engendre donc un sous-groupe inclus dans l'ensemble des permutations de $[\![1,N]\!]$ qui laissent les éléments $2i_0$ et $2i_0+1$ invariants, et n'est donc pas un système générateur. On ne peut donc pas diminuer le système générateur de $\mathfrak{A}_N$ constitué par les cycles $\langle 1, 2i, 2i+1\rangle$, où $i \in [\![1,n]\!]$.

b) Comme $N \geqslant 4$, $n \geqslant 2$ et $2n-1 \geqslant 3$. Nous noterons H le sous-groupe engendré par cet ensemble de cycles d'ordre 3 ; c'est a priori un sous-groupe du groupe $\mathfrak{A}_N$.

Si $\sigma \in \mathfrak{A}_N$ et que $\sigma(2n) = 2n$, alors σ induit sur $[\![1, 2n-1]\!]$ une permutation paire qui est, d'après *a*), dans le sous-groupe engendré par les cycles $\langle 1, 2i, 2i+1\rangle$, où $i \in [\![1, n-1]\!]$; il est alors clair que $\sigma \in H$.
Si $\sigma(2n) = 1$, on voit que $\langle 1, 2, 2n\rangle^{-1} \circ \sigma(2n) = 2n$. Comme $\langle 1, 2, 2n\rangle$ et $\langle 1, 2, 2n\rangle^{-1} \circ \sigma$ sont dans H, σ est dans H.
Si $\sigma(2n) = 2$, on voit que $\langle 1, 2, 2n\rangle \circ \sigma(2n) = 2n$. Comme $\langle 1, 2, 2n\rangle$ et $\langle 1, 2, 2n\rangle \circ \sigma$ sont dans H, σ est dans H.
Sinon posons $\sigma(2n) = i$, où $i \in [\![3, 2n-1]\!]$. On vérifie que $\langle 1, 2, 2n\rangle^{-1} \circ$, $\langle 1, 2, i\rangle \circ \sigma(2n) = 2n$. Comme $\langle 1, 2, i\rangle \in H$, puisque c'est une permutation paire qui laisse $2n$ invariant, on voit que $\sigma \in H$.
Toutes les permutations paires sont donc dans H, donc $H = \mathfrak{A}_N$.

Aucun sous-système n'est générateur ; en effet si $i_0 \in [\![1, n-1]\!]$, l'élément $2i_0+1$ est invariant par tous les cycles $\langle 1, 2i, 2i+1\rangle$, où $i \in [\![1, n-1]\!] \setminus \{i_0\}$, et par le cycle $\langle 1, 2, 2n\rangle$; et d'autre part l'élément $2n$ est invariant par tous les cycles d'ordre 3 de la forme $\langle 1, 2i, 2i+1\rangle$, où $i \in [\![1, n-1]\!]$. On peut donc conclure comme dans le *a*) qu'on ne peut pas diminuer le système générateur de l'énoncé.
Montrons par récurrence sur $N \geqslant 3$, que si H_N est le sous-groupe engendré par les 3-cycles de la forme $\langle 1, 2, i\rangle$, où $i \in [\![3, N]\!]$, alors $H_N = \mathfrak{A}_N$. Il est clair que pour tout $N \geqslant 3$, $H_N \subset \mathfrak{A}_N$; il suffit donc de démontrer l'inclusion opposée. Elle est vraie pour $N = 3$. Supposons la vraie pour N et montrons qu'elle est vraie pour $N+1$. Soit $\sigma \in \mathfrak{A}_{N+1}$.
Si $\sigma(N+1) = N+1$, la permutation induite par σ sur $[\![1, N]\!]$ est une permutation paire de $[\![1, N]\!]$ qui est dans le sous-groupe H_N (hypothèse de récurrence) ; donc $\sigma \in H_{N+1}$.
Si $\sigma(N+1) = i$, où $i \in [\![1, N]\!]$, on vérifie que :

$$\langle 1, 2, N+1\rangle^{-1} \circ \langle 1, 2, i\rangle \circ \sigma(N+1) = N+1 \ ;$$

comme la permutation paire $s = \langle 1, 2, N+1\rangle^{-1} \circ \langle 1, 2, i\rangle \circ \sigma$ laisse $N+1$ invariant, elle est dans le sous-groupe H_{N+1} ; on peut alors écrire :

$$\sigma = \langle 1, 2, i\rangle^{-1} \circ \langle 1, 2, N+1\rangle \circ s \in H_{N+1} \ .$$

On voit donc que dans tous les cas $\sigma \in H_{N+1}$. Nous en déduisons que $H_{N+1} = \mathfrak{A}_{N+1}$.
La propriété est donc démontrée par récurrence.

Exercice 2 :

Montrer que pour $n \geqslant 2$, $\mathfrak{A}_{2n}$ est engendré par s et t :
$s = \langle 1, 2, 3\rangle$ et $t = \langle 2, 3, \ldots, 2n\rangle$. ■

On voit que $t \circ s \circ t^{-1} = \langle 1, 3, 4\rangle$, que $t^2 \circ s \circ t^{-2} = \langle 1, 4, 5\rangle$, ..., $t^{2n-3} \circ s \circ t^{-2n+3} = \langle 1, 2n-1, 2n\rangle$ et que $t^{2n-2} \circ s \circ t^{-2n+2} = \langle 1,$

permutations sont dans le sous-groupe engendré par s et t, et d'après les résultats de l'exercice 1 b), elles engendrent le sous-groupe $\mathfrak{A}_{2n}$. Le sous-groupe engendré par s et t contient donc le sous-groupe $\mathfrak{A}_{2n}$. Comme les permutations s et t sont paires, le sous-groupe engendré est $\mathfrak{A}_{2n}$.

Exercice 3 :

Soit $p \in [\![2, n]\!]$, $(n \geqslant 2)$. Combien y a-t-il de cycles de longueur p dans $\mathfrak{S}_n$? ■

Soit P une partie de $[\![1, n]\!]$ de cardinal p, déterminons le nombre de cycles d'ordre p dont le support est P. Nous considérerons ces cycles comme des permutations de l'ensemble P.

Soit c_0 un cycle de support P, une permutation c est un cycle de support P si, et seulement si, il existe une bijection $\varphi : P \to P$ telle que $c = \varphi \circ c_0 \circ \varphi^{-1}$. L'ensemble des cycles de support P est donc l'orbite de l'un d'entre eux, c_0, sous l'action de $\mathfrak{S}_P$ sur lui-même par automorphismes intérieurs (voir §V.6 exemple 3). Le stabilisateur de c_0 est $\{\varphi \in \mathfrak{S}_P, \quad \varphi \circ c_0 \circ \varphi^{-1} = c_0\}$, c'est-à-dire l'ensemble des permutations φ de P qui commutent avec c_0. D'après l'exercice 12 du §V.4, ces permutations sont les puissances du cycle c_0, leur nombre est p. Le cardinal de l'orbite de c_0 est donc $p!/p = (p-1)!$ (voir théorème V.6.2 corollaire 1). Le nombre de cycles de support P est donc $(p-1)!$.

Le nombre de cycles d'ordre p dans le groupe $\mathfrak{S}_n$ est $\binom{n}{p}(p-1)!$, puisqu'il y a dans $[\![1, n]\!]$, $\binom{n}{p}$ parties de cardinal p.

Exercice 7 :

Soit $n \in \mathbb{N}$, $n \geqslant 2$ et E un ensemble fini de cardinal n. On note $\nu_k(\sigma)$ le nombre de cycles de longueur k de $\sigma \in \mathfrak{S}_E$ et par $\mathcal{P}_n$ l'ensemble des $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{N}^n$ tels que

$$\alpha_1 + 2\alpha_2 + \ldots + n\alpha_n = n,$$

de sorte que $(\nu_1(\sigma), \nu_2(\sigma), \ldots, \nu_n(\sigma)) \in \mathcal{P}_n$.

Soit $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathcal{P}_n$.

Montrer que le nombre d'éléments de $\mathfrak{S}_n$ tels que $(\nu_1(\sigma), \ldots, \nu_n(\sigma)) = \alpha$ est $\dfrac{n!}{\alpha_1! \ldots \alpha_n! 1^{\alpha_1} 2^{\alpha_2} \ldots n^{\alpha_n}}$

(commencer par compter les cycles de support don

Soit Σ l'ensemble des permutations σ vérifiant les conditions de l'énoncé, et Π l'ensemble des partitions de $[\![1,n]\!]$ qui comprennent α_1 singletons, α_2 paires, etc., α_n parties de cardinal n. Soit $\varphi : \Sigma \to \Pi$ qui à une permutation $\sigma \in \Sigma$ fait correspondre la partition de $[\![1,n]\!]$ par les orbites de σ.
Un élément $\mathcal{P}$ de Π étant donné, déterminons le nombre de permutations σ telles que $\varphi(\sigma) = \mathcal{P}$. Soient $O_1, O_2, \ldots, O_p$ les éléments de $\mathcal{P}$ qui ne sont pas des singletons. Pour que ces parties de $[\![1,n]\!]$ soient les orbites de la permutation σ, il faut et il suffit que ces parties soient stables par σ, que la permutation induite par σ sur chacune de ces parties soit un cycle, et que tous les autres éléments soient invariants par σ. L'application $\sigma \mapsto (\sigma_{|O_1}, \ldots, \sigma_{|O_p})$ est donc une bijection de l'image réciproque de $\mathcal{P}$ par φ, vers l'ensemble $\mathcal{C}(O_1) \times \ldots \times \mathcal{C}(O_p)$, où $\mathcal{C}(O_i)$ désigne l'ensemble des cycles sur O_i ($i \in [\![1,p]\!]$) ; le cardinal de cet ensemble est donc, d'après l'exercice 3, $\prod_{i=1}^{p} (\mathrm{card}\,(O_i) - 1)\,!$. Comme la partition $\mathcal{P}$ compte α_2 paires, α_3 parties de cardinal 3, etc., α_n parties de cardinal n (certains de ces nombres peuvent être nuls), le nombre des permutations σ dont l'image par φ est $\mathcal{P}$, est $(1\,!)^{\alpha_2} \ldots ((n-1)\,!)^{\alpha_n}$. Nous en déduisons, d'après le théorème du Berger, que :

$$\mathrm{card}\,(\Sigma) = \mathrm{card}\,(\Pi) \times (1\,!)^{\alpha_2} \ldots ((n-1)\,!)^{\alpha_n}\ .$$

Il reste maintenant à déterminer le nombre de partitions de $[\![1,n]\!]$ en α_1 singletons, α_2 paires, etc., α_n parties de cardinal n. D'après le lemme 1 du théorème III.5.1, nous savons que le nombre de partages de $[\![1,n]\!]$ en α_1 singletons puis α_2 paires, etc., puis α_n parties de cardinal n est :

$$\frac{n\,!}{(1\,!)^{\alpha_1}(2\,!)^{\alpha_2} \ldots (n\,!)^{\alpha_n}}\ .$$

On voit que pour obtenir le nombre de partitions vérifiant les conditions exprimées ci-dessus, il faut diviser ce nombre par $\alpha_1\,! \ldots \alpha_n\,!$. Nous obtenons finalement :

$$\mathrm{card}\,(\Pi) = \frac{n\,!}{(2\,!)^{\alpha_2} \ldots (n\,!)^{\alpha_n}} \frac{1}{\alpha_1\,! \ldots \alpha_n\,!}\ ,$$

d'où :

$$\begin{aligned} \mathrm{card}\,(\Sigma) &= \frac{n\,!\ (1\,!)^{\alpha_2} \ldots ((n-1)\,!)^{\alpha_n}}{(2\,!)^{\alpha_2} \ldots (n\,!)^{\alpha_n}\ \alpha_1\,! \ldots \alpha_n\,!} \\ &= \frac{n\,!}{2^{\alpha_2} \ldots n^{\alpha_n}\ \alpha_1\,! \ldots \alpha_n\,!}\ . \end{aligned}$$

Exercice 10 :

‖ (Cauchy). Soit $n \in \mathbb{N}$, $n \geqslant 5$; on note p le plus g

premier $\leqslant n$, et l'on suppose $p \geqslant 5$. Soit enfin $e \in [\![3, p-1]\!]$. Montrer que $\mathfrak{S}_n$ n'a aucun sous-groupe d'indice e. ■

Nous utiliserons dans la résolution de cet exercice la notion d'opération d'un groupe sur un ensemble (§V.6). Nous allons montrer que si H est un sous-groupe de $\mathfrak{S}_n$ d'indice e, et que $e < p$, alors $H = \mathfrak{S}_n$, ou $H = \mathfrak{A}_n$.

a) Soit H_p le sous-groupe de $\mathfrak{S}_n$ engendré par les cycles d'ordre p. Montrons que $H_p = \mathfrak{A}_n$. Comme p est impair ($p \geqslant 3$), il est clair que $H_p \subset \mathfrak{A}_n$. Montrons l'inclusion opposée.
Soit σ un cycle d'ordre p, et x dans le support de σ. Notons τ la transposition entre x et $\sigma(x)$; on vérifie que la permutation $s = [\tau, \sigma] = \tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1} = (\tau \circ \sigma \circ \tau^{-1}) \circ \sigma^{-1}$ est dans H_p, comme composé de deux cycles d'ordre p : σ^{-1}, et le cycle $\tau \circ \sigma \circ \tau^{-1}$ conjugué de σ. On voit aussi que : $s = \tau \circ (\sigma \circ \tau^{-1} \circ \sigma^{-1}) = \tau_{x,\sigma(x)} \circ \tau_{\sigma(x),\sigma^2(x)} =< x, \sigma(x), \sigma^2(x) > \in H_p$.
Si i, j, k sont trois éléments de $[\![1, n]\!]$, il est clair qu'il existe un cycle σ d'ordre p tel que $\sigma(i) = j$ et $\sigma(j) = k$, et donc que $< i, j, k > \in H_p$. Comme le groupe $\mathfrak{A}_n$ est engendré par les cycles d'ordre 3, nous en déduisons que $H_p = \mathfrak{A}_n$.

b) Soit s une permutation d'ordre p et L le sous-groupe engendré par s dans $\mathfrak{S}_n$. Nous noterons ici $G = \mathfrak{S}_n$. Faisons agir le groupe L sur l'ensemble G/H des classes à gauche modulo le sous-groupe H : si C est une classe à gauche modulo H et $y \in L$, on fait correspondre au couple (y, C) l'ensemble yC ; c'est bien une classe à gauche modulo H car si $C = xH$, où $x \in G$, alors $yC = (yx)H$; on vérifie facilement qu'on définit ainsi une opération à gauche du groupe L sur l'ensemble G/H. Soit φ l'homomorphisme de groupes $L \to \mathfrak{S}_{G/H}$ associé à cette opération à gauche. Comme $\operatorname{card}(G/H) = e$, et que $\operatorname{Im}(\varphi)$ est un sous-groupe de $\mathfrak{S}_{G/H}$, le cardinal de ce groupe divise $e!$; mais il divise aussi le cardinal du groupe de départ, soit p ; comme p est premier et que $e < p$, on voit que $e!$ et p sont premiers entre eux, et donc que $\operatorname{Im}(\varphi)$ n'a un seul élément. Cela signifie que pour tout $y \in L$, $\varphi(y) = \mathrm{Id}_{G/H}$, donc en particulier $sH = H$, soit $s \in H$. Nous avons donc démontré que le sous-groupe H contient tous les éléments d'ordre p.

c) D'après le *b*), le sous-groupe H contient le sous-groupe engendré par les cycles d'ordre p, qui est $\mathfrak{A}_n$ d'après le *a*). Nous pouvons en déduire que $H = \mathfrak{A}_n$ ou que $H = \mathfrak{S}_n$, ce qui termine la démonstration.

Exercice 12 :

a) Soit c un cycle de longueur n dans $\mathfrak{S}_n$ ($n \geqslant 2$

quelle est la décomposition en cycles de c^k ?

b) Réciproquement, soit $\sigma \in \mathfrak{S}_n$ dont la décomposition en cycles disjoints ne contient que des cycles de même longueur l (une telle permutation est dite alors *régulière*) ($l \geqslant 2$), d'où l divise n. Existe-t-il des cycles c de longueur n tels que $c^{n/l} = \sigma$? Combien y en a-t-il ? ■

a) Posons $E = [\![1, n]\!]$. Soit $x \in E$, cherchons le cardinal de l'orbite par c^k de x. Comme c est un cycle d'ordre n, on vérifie que si $i \in \mathbb{Z}$, $(c^k)^i(x) = x$ si, et seulement si $n \mid ki$, soit si, et seulement si, $n/\text{pgcd}(n,k)$ divise i. L'orbite de x par c^k est donc toujours de longueur $n/\text{pgcd}(n,k)$. La décomposition en cycles de supports disjoints de la permutation c^k est donc constituée de $\text{pgcd}(n,k)$ cycles de longueur $n/\text{pgcd}(n,k)$.

b) Posons $k = n/l$, et notons $O_1, O_2, \ldots, O_k$ les orbites de la permutation σ (toutes de cardinal l). Choisissons pour tout $i \in [\![1,k]\!]$ un élément a_i dans l'orbite O_i. Définissons la permutation c de la manière suivante : si $x \in E$, alors il existe un unique $i \in [\![1,k]\!]$ tel que $x \in O_i$, et il existe un unique entier $j \in [\![0, l-1]\!]$ tel que $x = \sigma^j(a_i)$; nous poserons alors $c(x) = \sigma^j(a_{i+1})$ si $i < k$ et $c(x) = \sigma^{j+1}(a_1)$ si $i = k$. Remarquons que comme $\sigma^l = \text{Id}$, les égalités : $c(\sigma^j(a_i)) = \sigma^j(a_{i+1})$ si $i < k$, et $c(\sigma^j(a_k)) = \sigma^{j+1}(a_1)$, vraies par définition si $j \in [\![0, l-1]\!]$, sont aussi vraies pour tout $j \in \mathbb{Z}$. Montrons que $c^k = \sigma$, ce qui justifiera aussi que c est une permutation.
On voit en effet que si $j \in [\![0, l-1]\!]$ et $i \in [\![1,k]\!]$, $c^{k-i}(\sigma^j(a_i)) = \sigma^j(a_k)$, puis que $c^k(\sigma^j(a_i)) = c^i(c^{k-i}(\sigma^j(a_i))) = c^i(\sigma^j(a_k)) = c^{i-1}(\sigma^{j+1}(a_1)) = \sigma^{j+1}(a_i) = \sigma(\sigma^j(a_i))$.
La permutation c est bien un cycle sur E, car pour tout $i \in [\![1,k]\!]$, $a_i = c^{i-1}(a_1)$, donc pour tout $i \in [\![1,k]\!]$ et tout $j \in [\![0, l-1]\!]$, $\sigma^j(a_i) = c^{kj+i-1}(a_1)$; l'orbite pour c de l'élément a_1 est donc E.

Dénombrement des solutions.

Soit a un élément fixe de E et c un cycle sur E tel que $c^k = \sigma$. Montrons que les orbites pour σ des éléments $a, c(a), \ldots, c^{k-1}(a)$ sont distinctes, donc sont les k orbites de σ. Soient i_1 et i_2 dans l'intervalle $[\![0, k-1]\!]$ tels que $c^{i_1}(a)$ et $c^{i_2}(a)$ soient dans la même orbite pour σ ; il existe $j \in [\![0, l-1]\!]$ tel que $\sigma^j(c^{i_1}(a)) = c^{i_2}(a)$, donc $c^{kj+i_1}(a) = c^{i_2}(a)$, d'où $c^{kj+i_1-i_2}(a) = a$; comme c est un cycle de longueur $n = kl$, cela implique $kl \mid kj + i_1 - i_2$, d'où $k \mid i_1 - i_2$; comme i_1 et i_2 sont dans l'intervalle $[\![0, k-1]\!]$. nous en déduisons $i_1 = i_2$, ce qu'il fallait démontrer.

Considérons comme ci-dessus un élément a fixe dans E, et l'application qui à c cycle tel que $c^k = \sigma$ fait correspondre $(c(a), c^2(a), \ldots, c^{k-1}(a))$, $(k-1)$-uplet d'éléments de E dont les orbites par σ sont distinctes et distinctes de celle de a. Nous pouvons déduire du début de cette question *b*) que cette application est surjective (existence de solutions). Montrons qu'elle est injective. Soit $a_2, \ldots, a_k$ un $(k-1)$-uplet vérifiant ces conditions ; notons aussi $a = a_1$. Si c est un cycle tel que $c^k = \sigma$, et tel que pour tout $i \in [\![1, k]\!]$, $a_i = c^{i-1}(a_1)$, alors pour tout $j \in [\![0, l-1]\!]$, $c(\sigma^j(a_i)) = c^{kj+i}(a_1)$, donc $c(\sigma^j(a_i)) = \sigma^j(c(a_i)) = \sigma^j(a_{i+1})$ si $i < k$ et $c(\sigma^j(a_k)) = \sigma^{j+1}(a_1)$. Le cycle c est donc déterminé par les valeurs $c(a), \ldots, c^{k-1}(a)$.

Un élément a de E étant fixé, le nombre de suites $O_2, \ldots, O_k$ d'orbites pour σ, distinctes, et distinctes de l'orbite O_1 de a, est évidemment $(k-1)!$. Une telle suite étant fixée, le nombre de $(k-1)$-uplets $a_2, \ldots, a_k$, tels que $\forall i \in [\![2, k]\!]$ $a_i \in O_i$, est l^{k-1}. Le nombre de cycles c tel que $c^k = \sigma$ est donc $(k-1)!\, l^{k-1}$ $(n = k\,l)$.

§ V.6 *OPÉRATION D'UN GROUPE SUR UN ENSEMBLE*

Exercice 5 :

> Soit n entier $\geqslant 2$; un sous-groupe G de $\mathfrak{S}_n$ est dit **régulier** ssi 1°) $\mathrm{card}\,(G) = n$ et 2°) G opère *transitivement* sur $[\![1, n]\!]$ par l'opération naturelle. Montrer que tout $\sigma \in G$, $\sigma \neq \mathrm{Id}$ est un *dérangement*, c'est-à-dire vérifie $\sigma(x) \neq x$ pour tout $x \in [\![1, n]\!]$. ■

Soit $x \in [\![1, n]\!]$ fixé. Comme G opère transitivement sur $[\![1, n]\!]$, l'application $\sigma \mapsto \sigma(x)$, de G dans $[\![1, n]\!]$, est surjective ; mais puisque G est de cardinal n, elle est aussi injective. Il existe donc un seul élément σ de G tel que $\sigma(x) = x$, c'est l'identité. Tout élément de G différent de l'identité est donc un dérangement.

Exercice 6 :

> Soit p un nombre premier $\geqslant 3$ et G un groupe de cardinal $p+1$. On suppose trouvé un automorphisme α de G d'ordre p. Démontrer que G est abélien. ■

Notons e l'élément neutre du groupe G.
Soit $x \in G$, l'ensemble $\{i \in \mathbb{Z},\ \alpha^i(x) = x\}$ est un sous-groupe de $\mathbb{Z}$ qui contient $p\mathbb{Z}$ puisque α est d'ordre p ; comme p est un non

ce sous-groupe est $p\mathbb{Z}$ ou $\mathbb{Z}$. L'orbite pour α d'un élément x de G est donc soit un singleton, soit une partie de cardinal p. Si aucune des orbites des éléments de G n'était de cardinal p, α serait l'identité de G, donc ne serait pas d'ordre p. Il existe donc un élément x de G, nécessairement distinct de e, dont l'orbite par α a p éléments ; comme $\text{card}(G) = p+1$, on voit que α est un cycle sur cette orbite (et il laisse e invariant).

Si x et y sont des éléments de G, différents de e, il existe un entier i tel que $\alpha^i(x) = y$ (puissance au sens de la composition des automorphismes), donc y est l'image de x par un automorphisme du groupe. Deux éléments de $G\setminus\{e\}$ ont donc toujours même période k. Le nombre k est nécessairement premier, car si $k = a \times b$, et que x est de période k, alors x^a est de période b, donc $b = 1$ ou $b = k$. Les classes dans $G \setminus \{e\}$ pour la relation d'équivalence "x et y engendrent le même sous-groupe" ont donc toutes $k-1$ éléments ; si ce nombre était pair, $p = \text{card}(G \setminus \{e\})$ serait pair, ce qui est faux ($p \geqslant 3$), donc $k-1$ est impair, et k est pair, donc $k = 2$ (k est premier). Nous pouvons en déduire que G est abélien : pour tout x dans G, $x^{-1} = x$, donc pour tous x et y dans G, $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.

N.B. : Nous aurions pu utiliser l'exercice 7 (théorème de Cauchy), pour démontrer que G a au moins un élément de période 2 ($p+1$ est pair). Nous voyons aussi que $p+1$ ne peut avoir que 2 comme diviseur premier ; le nombre premier p est donc nécessairement de la forme $2^k - 1$ où $k \in \mathbb{N}$, $k \geqslant 2$. On sait que k est nécessairement premier ; le nombre premier p est un nombre de Mersenne (voir exercices 13 et 14 du IV.5).

Exercice 11 :

> Soit n un entier $\geqslant 3$ tel que $n \vee \varphi(n) = 1$, où φ est l'indicateur d'Euler. Montrer que tout groupe de cardinal un tel n est abélien, donc cyclique, compte tenu de l'exercice 2 du §V.3. ■

Nous utiliserons dans la résolution de cet exercice la notion de sous-groupe distingué et le résultat suivant, dû à Burnside :

Lemme :

> Soit G un groupe fini non abélien dont tous les sous-groupes stricts sont abéliens, alors G n'est pas simple. ■

Notons N le cardinal de G ; il est clair que $N \geqslant 6$. L'élément neutre du groupe G sera noté e. Supposons que G soit simple.

1) Soit K un sous-groupe strict maximal (pour l'inclusion). Il en existe car un sous-groupe strict de cardinal maximum est maximal pour l'inclusion. On voit d'autre part que $K \neq \{e\}$: puisque G n'est pas abélien, le

engendré par un élément $\neq e$ est strict, donc $\{e\}$ n'est pas un sous-groupe strict maximal.
On sait que $K \subset \mathcal{N}_K$ ($\mathcal{N}_K$ désignant le normalisateur de K dans G) ; comme K n'est pas distingué (G est simple, K est strict et $\neq \{e\}$), $\mathcal{N}_K \neq G$, et comme K est strict maximal, $K = \mathcal{N}_K$. Le nombre de conjugués du sous-groupe K est $[G : \mathcal{N}_K] = [G : K] = N/\mathrm{card}\,(K)$.

2) Soit K un sous-groupe strict maximal pour l'inclusion et H un sous-groupe strict qui n'est pas inclus dans K. Montrons que $K \cap H = \{e\}$.
Puisque tous les sous-groupes stricts de G sont abéliens, les sous-groupes H et K le sont. Le sous-groupe $H \cap K$ est donc invariant par les automorphismes intérieurs σ_x, où $x \in H$, et $x \in K$. Donc $\mathcal{N}_{H\cap K} \supset H \cup K$. Comme K est un sous-groupe strict maximal et que H n'est pas inclus dans K, cela implique $\mathcal{N}_{H\cap K} = G$. Le sous-groupe $H \cap K$ est donc distingué, et comme c'est un sous-groupe strict, $H \cap K = \{e\}$.

3) Soit K un sous-groupe strict maximal. Notons k son cardinal. Il est clair que ses conjugués sont aussi maximaux (pour l'inclusion dans l'ensemble des sous-groupes stricts), donc d'après le point 2), l'intersection de deux conjugués de K distincts, est $\{e\}$. Le nombre de conjugués de K étant N/k (point 1), le cardinal de l'union U des conjugués de K est $(k-1)N/k + 1 = N + 1 - N/k < N$ car $k < N$.

4) Soit K un sous-groupe strict maximal. D'après le point 3, il existe un élément a de G, qui n'est pas dans U, union des conjugués de K (donc $a \neq e$). Soit H un sous-groupe strict maximal qui contienne a ; un tel sous groupe existe ; il existe en effet des sous-groupes stricts contenant a, par exemple le sous-groupe engendré par a (G n'est pas abélien) donc des sous-groupes stricts contenant a et de cardinal maximum. Notons h son cardinal. En appliquant le point 3 à H, on voit que l'intersection de deux conjugués de H distincts, est $\{e\}$. De plus un conjugué quelconque $y\,H\,y^{-1}$ de H n'est pas inclus dans un conjugué quelconque $x\,K\,x^{-1}$ de K, sinon $a \in H \subset y^{-1}x\,K\,x^{-1}y$. D'après le point 2, cela prouve que les N/h conjugués de H et les N/k conjugués de K se coupent deux à deux suivant $\{e\}$. D'où : $(h-1)N/h + (k-1)N/k \leqslant N-1$; cela s'écrit encore : $N - N/h + N - N/k \leqslant N - 1$, d'où $1/h + 1/k > 1$. Cela est contradictoire car $k \geqslant 2$ et $h \geqslant 2$.

Il est donc contradictoire de supposer G simple. Le groupe G possède par conséquent des sous-groupes distingués non triviaux.

Fin de la démonstration du lemme.

Soit n un entier > 1 tel que n et $\varphi(n)$ sont premiers entre eux. On sait que si la décomposition en facteurs premier de n est $n = \prod_{i=1}^{k} p_i^{n_i}$, où $p_1, \ldots, p_k$ sont les facteurs premiers de n et $n_1, \ldots, n_k$ des entiers > 0,

$\prod_{i=1}^{k} p_i^{n_i-1}(p_i-1)$. Nous en déduisons que n et $\varphi(n)$ sont premiers entre eux si, et seulement si, $\forall i \in [\![1,k]\!]$, $n_i = 1$ et $\forall (i,j) \in [\![1,k]\!]^2$, $p_i \vee (p_j - 1) = 1$. Nous en déduisons en particulier que $n = p_1 \times \ldots \times p_k$, et que tout diviseur m de n possède la même propriété, c'est-à-dire $m \vee \varphi(m) = 1$.

Montrons par récurrence sur N que tout groupe de cardinal $n \leqslant N$ tel que $n \vee \varphi(n) = 1$ est abélien (donc cyclique). C'est évidemment vrai si $N = 1$. Supposons que ce soit vrai pour N. Soit G un groupe de cardinal $n \leqslant N+1$ tel que $n \vee \varphi(n) = 1$. On a vu que pour tout diviseur m de n, $m \vee \varphi(m) = 1$; en utilisant l'hypothèse de récurrence, nous voyons que tout sous-groupe strict de G, de cardinal m diviseur strict de n, est abélien. D'après le lemme de Burnside, nous savons qu'alors soit G est abélien, soit G n'est pas abélien et que dans ce cas il a un sous-groupe distingué non trivial H. Montrons que cette éventualité est à exclure, ce qui terminera la démonstration par récurrence.

D'après l'hypothèse de récurrence, le sous-groupe H est cyclique ; soit h son cardinal. Comme H est distingué, il est stable par les automorphismes intérieurs σ_x, où $x \in G$; l'application $\Phi : x \mapsto \sigma_x\|_H$, est un homomorphisme de groupes, du groupe G vers le groupe des automorphismes du groupe cyclique H. On sait que le nombre des automorphismes d'un groupe cyclique est le nombre de ses générateurs, soit ici $\varphi(h)$. Le cardinal de l'image de l'homomorphisme Φ est un diviseur de n et un diviseur de $\varphi(h)$, lui-même diviseur de $\varphi(n)$; comme $n \vee \varphi(n) = 1$, ce cardinal est 1, c'est-à-dire $\forall x \in G$, $\sigma_x\|_H = \mathrm{Id}_H$. Cela signifie que $\forall x \in G$, $\forall y \in H$, $xyx^{-1} = y$, ou encore que H est inclus dans le centre de G. Mais le groupe quotient $G/_H$ a aussi un cardinal m qui est un diviseur strict de n ; en utilisant encore une fois l'hypothèse de récurrence nous voyons qu'il s'agit d'un groupe cyclique. Si x est un générateur du groupe cyclique H et y élément de G dont la classe modulo H est un générateur du groupe $G/_H$, on voit que pour tout élément z de G, il existe $i \in \mathbb{Z}$ tel que $\pi_H(z) = \pi_H(y^i)$, soit $zy^{-i} \in H$, puis qu'il existe $j \in \mathbb{Z}$ tel que $zy^{-i} = x^j$, soit finalement $z = x^j y^i$. Comme les éléments x et y commutent entre eux, le groupe G devrait être commutatif, ce qui est contradictoire.

Cela termine comme annoncé la démonstration par récurrence, et achève la résolution de cet exercice.

Exercice 12 :

> Soit n et d deux entiers, $n \geqslant 2$, $d \geqslant 1$. On note $S_{n,d}$ l'ensemble $\{(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{N}^n \mid \alpha_1 + \alpha_2 + \ldots + \alpha_n = d\}$.
> On fait opérer $\mathfrak{S}_n$ sur $S_{n,d}$ à gauche ainsi : si $\sigma \in \mathfrak{S}_n$ et $\alpha = (\alpha_q) \in S_{n,d}$, $\sigma \cdot \alpha = (\alpha_{\sigma^{-1}(1)}, \ldots, \alpha_{\sigma^{-1}(n)})$.

a) Soit $\mathcal{T}_{n,d}$ l'ensemble des suites $(k_0, k_1, \ldots, k_d) \in \mathbb{N}^{d+1}$ telles que $k_0 + k_1 + \ldots + k_d = n$ et $k_1 + 2k_2 + \ldots + dk_d = d$.
Si $\alpha = (\alpha_q) \in S_{n,d}$, on définit $\varphi(\alpha) = (k_0, k_1, \ldots, k_d) \in \mathcal{T}_{n,d}$ de la manière suivante :

$$k_i = \text{card}\,(\{q \in [\![1,n]\!] \mid \alpha_q = i\}) \text{ pour } 0 \leqslant i \leqslant d.$$

Montrer : $\varphi(\alpha) = \varphi(\beta) \Leftrightarrow \alpha$ et β sont dans la même $\mathfrak{S}_n$-orbite de $S_{n,d}$. Si Ω est l'ensemble de ces orbites, en déduire une bijection naturelle $\Phi : \Omega \to \mathcal{T}_{n,d}$.

b) Soit $k = (k_0, \ldots, k_d) \in \mathcal{T}_{n,d}$ et $\omega = \Phi^{-1}(k)$. Montrer :

$$\text{card}\,(\omega) = \frac{n!}{k_0!\, k_1! \ldots k_d!} .$$

En déduire $$\sum_{k \in \mathcal{T}_{n,d}} \frac{n!}{k_0!\, k_1! \ldots k_d!} = \binom{n+d-1}{n-1} .$$

c) On développe le multinôme $(x_1 + x_2 + \ldots + x_n)^d$ où les x_i sont éléments d'un anneau commutatif A. Montrer :

$$(x_1 + x_2 + \ldots + x_n)^d = \sum_{\omega \in \Omega} \frac{d!}{(1!)^{k_1(\omega)} (2!)^{k_2(\omega)} \ldots (d!)^{k_d(\omega)}} F_\omega ,$$

où $\quad (k_0(\omega), k_1(\omega), \ldots, k_d(\omega)) = \Phi(\omega)$ pour $\omega \in \Omega$

et où $\quad F_\omega = \sum_{(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \omega} x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ pour $\omega \in \Omega$.

d) Application numérique à $d = 7$. ■

a) Supposons que α et β, éléments de $S_{n,d}$, soient dans la même $\mathfrak{S}_n$-orbite ; il existe une permutation σ telle que $\forall q \in [\![1,n]\!] \quad \beta_{\sigma^{-1}(q)} = \alpha_q$. Notons pour tout $i \in [\![0,d]\!]$ et tout $\gamma \in S_{n,d}$, $E_{\gamma,i} = \{q \in [\![1,n]\!] \mid \gamma_q = i\}$. On voit que pour tout $i \in [\![0,d]\!]$, $q \in E_{\alpha,i}$ si, et seulement si, $\sigma^{-1}(q) \in E_{\beta,i}$, d'où $E_{\alpha,i} = \sigma(E_{\beta,i})$. Nous en déduisons que pour tout $i \in [\![0,d]\!]$, $\varphi(\alpha)_i = \text{card}\,(E_{\alpha,i}) = \text{card}\,(E_{\beta,i}) = \varphi(\beta)_i$, c'est-à-dire $\varphi(\alpha) = \varphi(\beta)$.

Supposons maintenant $\varphi(\alpha) = \varphi(\beta)$, où α et β sont des éléments de $S_{n,d}$. Pour tout $i \in [\![0,d]\!]$ les ensembles $E_{\alpha,i}$ et $E_{\beta,i}$ sont finis de même cardinal donc en bijection ; comme les familles $(E_{\alpha,i})_{i \in [\![0,d]\!]}$ et $(E_{\beta,i})_{i \in [\![0,d]\!]}$ sont des partages de l'ensemble $[\![1,n]\!]$, on voit qu'il existe une bijection $\sigma \in \mathfrak{S}_n$, telle que $\forall i \in [\![0,d]\!]$, $\sigma(E_{\alpha,i}) = E_{\beta,i}$. Montrons que pour tout entier q dans $[\![1,n]\!]$, $\beta_q = \alpha_{\sigma(q)}$; soit $i = \beta_q$, alors $q \in E_{\beta,i}$, donc $\sigma^{-1}(q) \in E_{\alpha,i}$, soit $\alpha_{\sigma^{-1}(q)} = i = \beta_q$. Nous voyons donc que $\beta = \sigma \cdot \alpha$.

D'après ce qui précède, nous pouvons factoriser l'application φ par la relation d'équivalence dont les classes sont les $\mathfrak{S}_n$-orbites ; l'application factorisée obtenue, Φ, est injective. Il reste à démontrer qu'elle est surj

est vrai si, et seulement si, φ l'est. Soit $(k_0, k_1, \ldots, k_d)$ un élément de $\mathcal{T}_{n,d}$; considérons la famille $(\alpha_q)_{q \in [\![1,n]\!]}$, dont les k_0 premiers termes (si $k_0 > 0$) sont 0, dont les k_1 termes suivants (si $k_1 > 0$) sont 1, etc., dont les k_d derniers termes (si $k_d > 0$) sont d ; cela est possible car $k_0 + k_1 + \ldots + k_d = n$; la famille α est bien dans $S_{n,d}$, car $\alpha_1 + \alpha_2 + \ldots + \alpha_n = 1\,k_1 + 2\,k_2 + \ldots + d\,k_d = d$; on voit que la famille α prend exactement k_0 fois la valeur 0, k_1 fois la valeur 1, etc., k_d fois la valeur d, c'est-à-dire $\varphi(\alpha) = (k_0, k_1, \ldots, k_d)$. L'application φ est donc bien surjective ; sa factorisée $\Phi : \Omega \to \mathcal{T}_{n,d}$ est donc une bijection.

b) L'orbite $\Phi^{-1}(k)$ est l'ensemble des $\alpha \in S_{n,d}$ telles que $\varphi(\alpha) = k$, c'est-à-dire l'ensemble des applications $[\![1, n]\!] \to [\![0, d]\!]$ qui prennent k_0 fois la valeur 0, k_1 fois la valeur 1, etc., k_d fois la valeur d. D'après le lemme 1 du théorème III.5.2. (formule du multinôme), le nombre de ces applications est $\dfrac{n!}{k_0!\,k_1!\,\ldots\,k_d!}$, ce qu'il fallait démontrer.

Le théorème III.4.5. nous donne le cardinal de l'ensemble $S_{n,d}$ qui est $\binom{n+d-1}{n-1}$. Comme l'ensemble des $\mathfrak{S}_n$-orbites dans $S_{n,d}$ est une partition de cet ensemble, nous en déduisons :

$$\binom{n+d-1}{n-1} = \sum_{\omega \in \Omega} \operatorname{card}(\omega) = \sum_{k \in \mathcal{T}_{n,d}} \operatorname{card}\left(\Phi^{-1}(k)\right) = \sum_{k \in \mathcal{T}_{n,d}} \frac{n!}{k_0!\,k_1!\,\ldots\,k_d!}\,.$$

c) La formule du multinôme s'écrit :

$$(x_1 + x_2 + \ldots + x_n)^d = \sum_{\alpha \in S_{n,d}} \frac{d!}{\alpha_1!\,\alpha_2!\,\ldots\,\alpha_n!}\, x_1^{\alpha_1}\, x_2^{\alpha_2} \ldots x_n^{\alpha_n}\,.$$

En partageant cette somme suivant les $\mathfrak{S}_n$-orbites dans $S_{n,d}$ nous obtenons :

$$\begin{aligned}(x_1 + x_2 + \ldots + x_n)^d &= \sum_{\omega \in \Omega} \sum_{\alpha \in \omega} \frac{d!}{\alpha_1!\,\alpha_2!\,\ldots\,\alpha_n!}\, x_1^{\alpha_1}\, x_2^{\alpha_2} \ldots x_n^{\alpha_n} \\ &= \sum_{k \in \mathcal{T}_{n,d}} \sum_{\varphi(\alpha) = k} \frac{d!}{\alpha_1!\,\alpha_2!\,\ldots\,\alpha_n!}\, x_1^{\alpha_1}\, x_2^{\alpha_2} \ldots x_n^{\alpha_n}\,.\end{aligned}$$

Or si $\varphi(\alpha) = k$, alors :

$$\alpha_1!\,\alpha_2!\,\ldots\,\alpha_n! = (0!)^{k_0}(1!)^{k_1}(2!)^{k_2}\ldots(d!)^{k_d} = (2!)^{k_2}\ldots(d!)^{k_d}\,,$$

puisque la suite α prend k_0 fois la valeur 0, k_1 fois la valeur 1, etc., k_d fois la valeur d (certains des nombres $k_0, k_1, \ldots, k_d$, peuve

Cette valeur ne dépend plus de α mais uniquement de k. Nous voyons donc que :

$$(x_1 + x_2 + \ldots + x_n)^d = \sum_{k \in \mathcal{T}_{n,d}} \frac{d!}{(2!)^{k_2} \ldots (d!)^{k_d}} \sum_{\varphi(\alpha)=k} x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n} .$$

Nous obtenons la formule de l'énoncé en posant $k = \Phi(\omega)$.

On voit facilement que $F_{\Phi^{-1}(k)}$ est le symétrisé sans répétitions du monôme $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$, où la famille α est la famille dont les k_d premiers termes ont pour valeur d, les k_{d-1} suivants pour valeur $d-1$, etc., les k_0 derniers pour valeur 0.

d) Nous supposerons ici que $n \geqslant 7$, ce qui simplifie l'étude de l'ensemble $\mathcal{T}_{n,7}$. On établit assez facilement, en respectant un ordre lexicographique, la liste des solutions en entiers de l'équation (1) : $k_1 + 2k_2 + \ldots + 7k_7 = 7$; si $(k_1, k_2, \ldots, k_7)$ est une solution, alors $k_1 + k_2 + \ldots + k_7 \leqslant 7 \leqslant n$, donc $(n - (k_1 + \ldots + k_7), k_1, k_2, \ldots, k_7)$ est un élément de $\mathcal{T}_{n,7}$. Il est clair qu'on obtient ainsi tous les éléments de $\mathcal{T}_{n,7}$. On trouvera dans le tableau ci-dessous la liste des solutions de l'équation (1), une expression symbolique du symétrisé correspondant, et le coefficient de ce symétrisé dans le développement de $(x_1 + x_2 + \ldots + x_n)^7$.

$(k_1, k_2, k_3, k_4, k_5, k_6, k_7)$		
$(7, 0, 0, 0, 0, 0, 0)$	$\sum x_1 x_2 x_3 x_4 x_5 x_6 x_7$	$7! = 5040$
$(5, 1, 0, 0, 0, 0, 0)$	$\sum x_1^2 x_2 x_3 x_4 x_5 x_6$	$\frac{7!}{2!} = 2520$
$(3, 2, 0, 0, 0, 0, 0)$	$\sum x_1^2 x_2^2 x_3 x_4 x_5$	$\frac{7!}{(2!)^2} = 1260$
$(1, 3, 0, 0, 0, 0, 0)$	$\sum x_1^2 x_2^2 x_3^2 x_4$	$\frac{7!}{(2!)^3} = 630$
$(4, 0, 1, 0, 0, 0, 0)$	$\sum x_1^3 x_2 x_3 x_4 x_5$	$\frac{7!}{3!} = 840$
$(2, 1, 1, 0, 0, 0, 0)$	$\sum x_1^3 x_2^2 x_3 x_4$	$\frac{7!}{3!2!} = 420$
$(0, 2, 1, 0, 0, 0, 0)$	$\sum x_1^3 x_2^2 x_3^2$	$\frac{7!}{3!(2!)^2} = 210$
$(1, 0, 2, 0, 0, 0, 0)$	$\sum x_1^3 x_2^3 x_3$	$\frac{7!}{(3!)^2} = 140$
$(3, 0, 0, 1, 0, 0, 0)$	$\sum x_1^4 x_2 x_3 x_4$	$\frac{7!}{4!} = 210$
$(1, 1, 0, 1, 0, 0, 0)$	$\sum x_1^4 x_2^2 x_3$	$\frac{7!}{4!2!} = 105$
$(0, 0, 1, 1, 0, 0, 0)$	$\sum x_1^4 x_2^3$	$\frac{7!}{4!3!}$

$(2,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0)$	$\sum x_1^5 x_2 x_3$	$\frac{7!}{5!}$	$=$	42
$(0,\ 1,\ 0,\ 0,\ 1,\ 0,\ 0)$	$\sum x_1^5 x_2^2$	$\frac{7!}{5!\,2!}$	$=$	21
$(1,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0)$	$\sum x_1^6 x_2$	$\frac{7!}{6!}$	$=$	7
$(0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1)$	$\sum x_1^7$	$\frac{7!}{7!}$	$=$	1

§ V.7 *SOUS-GROUPES DISTINGUÉS. GROUPE QUOTIENT*

Exercice 1 :

Soit p un nombre premier. Montrer que tous les groupes de cardinal p sont isomorphes à $(\mathbb{Z}/_{p\mathbb{Z}}, +)$. ■

Soit G un groupe de cardinal p premier ; l'élément neutre du groupe G sera noté e, et la loi du groupe sera notée multiplicativement.
Soit $x \in G \setminus \{e\}$; l'ordre de x divise p mais n'est pas 1, c'est donc p. Tout élément non neutre dans G est donc générateur. Le groupe G est donc cyclique de cardinal p. Si x est un générateur de G, l'homomorphisme de groupes $\mathbb{Z} \to G$, $n \mapsto x^n$, est surjectif et a pour noyau le sous-groupe $p\mathbb{Z}$ du groupe $\mathbb{Z}$; on obtient donc par factorisation un homomorphisme de groupes bijectif, du groupe additif $\mathbb{Z}/_{p\mathbb{Z}}$ vers le groupe G, donc un isomorphisme de groupes, ce qu'il fallait démontrer.

Exercice 2 :

Soit $\mathfrak{Z}(G)$ le centre d'un groupe G. Montrer que si $G/_{\mathfrak{Z}(G)}$ est un groupe cyclique, alors G est abélien. En déduire que si G est fini de cardinal p^2, et p premier, alors G est abélien. ■

Le sous-groupe $\mathfrak{Z}(G)$ est distingué, et nous noterons $\pi_{\mathfrak{Z}(G)}$ l'homomorphisme canonique $G \to G/_{\mathfrak{Z}(G)}$.
Soit x dans G tel que $\pi_{\mathfrak{Z}(G)}(x)$ soit un générateur du groupe quotient $G/_{\mathfrak{Z}(G)}$. Pour tout y dans G il existe un entier i tel que $\pi_{\mathfrak{Z}(G)}(y) = \pi_{\mathfrak{Z}(G)}(x)^i = \pi_{\mathfrak{Z}(G)}(x^i)$, ce qui s'écrit aussi $y\,x^{-i} \in \mathfrak{Z}(G)$. Pour tout $y \in G$ il existe donc un entier i et un élément c du centre de G tels que $y = c\,x^i$. Il est alors clair que deux éléments du groupe G commutent entre eux, et par conséquent que le groupe G est abélien (et $\mathfrak{Z}(G) = G$!).

Si G est un groupe fini de cardinal p^2, où p est premier, alors son centre n'est pas réduit à $\{e\}$ (voir Exemple 8 du §V.6). Le groupe $\mathfrak{Z}(G)$ a donc p ou p^2 éléments ; le groupe quotient $G/\mathfrak{Z}(G)$ a 1 ou p éléments, et est donc cyclique (c.f. exercice 1). D'après ce qui précède, le groupe G est abélien.

Exercice 9 :

> Montrer que tout sous-groupe *fini* du groupe quotient $G = \mathbb{Q}/\mathbb{Z}$ est cyclique, et que $\mathbb{Q}/\mathbb{Z}$ est union de ses sous-groupes finis, mais n'est pas de type fini. Pour tout sous-groupe fini H de G, montrer que $G/H \cong G$. ■

Notons π l'homomorphisme canonique de groupes $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$. Nous utiliserons le fait que les sous-groupes de type fini du groupe additif $\mathbb{Q}$ sont monogènes (cf. exercice 1 du §V.1).

Soit H un sous-groupe fini du groupe $\mathbb{Q}/\mathbb{Z}$, et $r_1, r_2, \ldots, r_k$ des rationnels dont les classes modulo $\mathbb{Z}$ sont les éléments de H. Il est clair que le sous-groupe $\pi^{-1}(H)$ est engendré dans $\mathbb{Q}$ par $1, r_1, r_2, \ldots, r_k$. Il est donc de type fini, donc monogène, de la forme $r\mathbb{Z}$ où $r \in \mathbb{Q}$. Comme $1 \in \pi^{-1}(H)$, il existe un entier n tel que $n \cdot r = 1$; on peut supposer $n > 0$ et $\pi^{-1}(H) = (1/n)\mathbb{Z}$. Le sous-groupe H est donc le sous-groupe engendré par $\pi(1/n)$. Il est clair que $\pi(1/n)$ a pour période n, le cardinal de H est donc n. Nous pouvons déduire de cela que tous les sous-groupes finis de $\mathbb{Q}/\mathbb{Z}$ sont cycliques, et que pour tout entier $n > 0$ il existe un et un seul sous-groupe fini de cardinal n, le sous-groupe engendré par $\pi(1/n)$.

Soit $r = p/q$, où $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$, un rationnel ; on voit que $\pi(r)$ est dans le sous-groupe cyclique engendré par $\pi(1/q)$. Tout élément du groupe quotient $\mathbb{Q}/\mathbb{Z}$ est donc dans un sous-groupe fini. Supposons que le groupe $\mathbb{Q}/\mathbb{Z}$ soit de type fini, et soient $r_1, r_2, \ldots, r_k$ des rationnels dont les classes modulo $\mathbb{Z}$ forment un système générateur fini de $\mathbb{Q}/\mathbb{Z}$; il est clair que $1, r_1, r_2, \ldots, r_k$ serait alors un système générateur de $\mathbb{Q}$, ce qui est impossible ($\mathbb{Q}$ n'est pas de type fini). Le groupe $\mathbb{Q}/\mathbb{Z}$ n'est donc pas de type fini.

Soit H un sous-groupe fini de $\mathbb{Q}/\mathbb{Z}$ de cardinal n ; H est donc le sous-groupe engendré par $\pi(1/n)$. Considérons l'homomorphisme de groupes $G \to G$, $c \mapsto n \cdot c$. Il est surjectif, car si $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$, $\pi(p/q) = n \cdot \pi(p/nq)$. Son noyau est l'ensemble des classes des rationnels p/q, $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tels que $n \cdot p/q \in \mathbb{Z}$; c'est donc l'ensemble des classes des rationnels de la forme k/n, où $k \in \mathbb{Z}$, c'est-à-dire le sous-groupe H engendré par $\pi(1/n)$. En factorisant cet homomorphisme surjectif par son noyau, nous obtenons un isomorphisme de groupes, du groupe G/H vers le groupe G. Ces deux groupes sont donc isomorphes.

Exercice 11 :

> Soit p un nombre premier. Dans le groupe quotient $\mathbb{Q}/\mathbb{Z}$, on considère le sous-groupe G formé des éléments dont l'ordre est une puissance de p (on vérifiera que G est bien un sous-groupe). Montrer que G n'est pas de type fini et que tout sous-groupe strict H de G est fini et vérifie : G/H est isomorphe à G. ■

Nous noterons π l'homomorphisme canonique de groupes $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$.

L'ordre de l'élément neutre est $1 = p^0$. Si u et v sont des éléments de $\mathbb{Q}/\mathbb{Z}$ d'ordres respectifs p^i et p^j, où i et j sont des entiers, alors $p^{\sup(i,j)} \cdot (u - v) = 0$. L'ordre de $u - v$ divise donc $p^{\sup(i,j)}$, et est par conséquent une puissance de p. L'ensemble des éléments de $\mathbb{Q}/\mathbb{Z}$ dont l'ordre est une puissance de p est donc un sous-groupe de $\mathbb{Q}/\mathbb{Z}$. Nous obtiendrions un résultat analogue dans tout groupe abélien.
Il est clair que l'ordre de $\pi(n/m)$, où $(n, m) \in \mathbb{Z} \times \mathbb{N}^*$ et $n \vee m = 1$, est m. On voit donc que G est l'ensemble des éléments de $\mathbb{Q}/\mathbb{Z}$ de la forme $\pi(n/p^i)$, où $n \in \mathbb{Z}$ et $i \in \mathbb{N}$; si $n \vee p = 1$, ce qu'on peut toujours supposer, l'ordre d'un tel élément est p^i.

Soient $r_1, r_2, \ldots, r_k$ des éléments de G, et p^h le plus grand des ordres de ces éléments. Le sous-groupe engendré par ces éléments est inclus dans le sous-groupe $\{x \in G,\ p^h \cdot x = 0\}$ des éléments dont l'ordre divise p^h. Ce sous-groupe n'est pas G : la classe modulo $\mathbb{Z}$ du rationnel $1/p^{h+1}$ n'y est pas. Comme aucune partie finie de G n'est génératrice, le groupe G n'est pas de type fini.

Soit H un sous-groupe strict de G et $r \in H$ d'ordre p^k où $k \in \mathbb{N}$, donc $r = \pi(n/p^k)$, $n \vee p = 1$. Comme p^k et n sont premiers entre eux, il existe deux entiers u et v tels que $un + vp^k = 1$, d'où :

$$u\frac{n}{p^k} + v = \frac{1}{p^k}\ .$$

Nous en déduisons que $\pi(1/p^k) \in H$, et donc que tout élément d'ordre $\leqslant p^k$ est dans H. L'ensemble des ordres des éléments de H est donc majoré, sinon H contiendrait tous les éléments de G. Soit p^h l'ordre maximum d'un élément de H ; d'après ce qui précède, $\pi(1/p^h) \in H$. Nous voyons alors que $H \supset \{\pi(n/p^h),\ n \in \mathbb{Z}\}$; comme les ordres des éléments de H sont $\leqslant p^h$, l'inclusion opposée est évidente. Le groupe H est donc le sous-groupe de G engendré par $\pi(1/p^h)$, sous-groupe de cardinal p^h.

Soit H un sous-groupe strict de G, de cardinal p^k où $k \in \mathbb{N}$, donc engendré par $\pi(1/p^k)$. Considérons l'homomorphisme de groupes φ : C

$p^k \cdot x$. Cet homomorphisme est surjectif, car pour tout $n \in \mathbb{Z}$ et pour tout $i \in \mathbb{N}$, $\pi(n/p^i) = p^k \cdot \pi(n/p^{i+k})$. Un élément $\pi(n/p^i)$ de G est dans le noyau de cet homomorphisme si, et seulement si, $p^k \cdot n/p^i \in \mathbb{Z}$, donc si, et seulement si, $\pi(n/p^i)$ est dans le sous-groupe engendré par $\pi(1/p^k)$; ce sous-groupe est H. En factorisant l'homomorphisme φ par son noyau H, on obtient un isomorphisme de groupes, $G/_H \to G$. Ces deux groupes sont donc isomorphes.

Exercice 12 :

Soit G le groupe engendré dans $\mathrm{GL}(2,\mathbb{C})$ par les matrices :

$$A = \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} .$$

Montrer que G est de cardinal 8, non abélien, que tous ses sous-groupes sont distingués et que G contient, outre e_G, un élément d'ordre 2 et 6 éléments d'ordre 4 (G s'appelle le **groupe quaternionique**). Quel est le centre de G ? le groupe quotient $G/_{\mathcal{Z}(G)}$? ■

Les matrices A et B sont des matrices carrées, 2 lignes 2 colonnes, de trace nulle et de déterminant 1 ; nous pouvons en déduire (théorème d'Hamilton-Cayley) que $A^2 = B^2 = -\mathrm{I}_2$, où I_2 désigne la matrice unité dans $\mathrm{GL}(2,\mathbb{C})$, donc $A^{-1} = -A$ et $B^{-1} = -B$. Par le calcul on obtient :

$$AB = \begin{pmatrix} -\mathrm{i} & 0 \\ 0 & \mathrm{i} \end{pmatrix} = -BA = BA^{-1} = B^{-1}A ,$$

et par conséquent $(AB)^2 = ABAB = ABB^{-1}A = -\mathrm{I}_2$. Nous en déduisons aussi que $\sigma_A(B) = ABA^{-1} = A^2B = -B = B^{-1}$, et donc que pour tout entier $p \in \mathbb{Z}$, $AB^pA^{-1} = B^{-p}$, soit encore $AB^p = B^{-p}A$. Le groupe G engendré par A et B n'est pas abélien, puisque $AB \neq BA$

On voit que B est d'ordre 4 ; les matrices $\mathrm{I}_2, B, B^2, B^3$ sont donc distinctes ; il en est de même pour les matrices A, AB, AB^2, AB^3, et comme A n'est pas dans le sous-groupe engendré par B, on obtient ainsi un ensemble H de 8 matrices. Montrons que H est le sous-groupe engendré par A et B ; il suffit bien sûr de montrer que H est un sous-groupe. Remarquons d'abord que $H = \{B^p \mid p \in \mathbb{Z}\} \cup \{AB^q \mid q \in \mathbb{Z}\}$. Soient x et y deux éléments de H, montrons que $xy^{-1} \in H$, en distinguant 4 cas (dans ce qui suit p et q désignent des entiers relatifs).

1) $x = B^p$ et $y = B^q$, alors $xy^{-1} = B^{p-q} \in H$;
2) $x = B^p$ et $y = AB^q$, alors $xy^{-1} = B^{p-q}A^{-1} = -B^{p-q}A = AB^{q-p+2}$.
3) $x = AB^q$ et $y = B^p$, alors $xy^{-1} = AB^{q-p}$;
4) $x = AB^p$ et $y = AB^q$, alors $xy^{-1} = AB^{p-q}A^{-1} = B^{q-p}$

Comme H n'est pas vide, c'est un sous-groupe, donc le sous-groupe engendré par A et B ; il a 8 éléments. On constate que I_2 est d'ordre 1, que $B^2 = -I_2$, et que les autres éléments sont de carré $-I_2$, donc d'ordre 4. Le groupe H comporte donc un élément d'ordre 1 : I_2, un élément d'ordre 2 : $-I_2$ et 6 éléments d'ordre 4.

Soit K un sous-groupe de G qui contient un élément autre que I_2 ou $-I_2$, cet élément est d'ordre 4, et par conséquent le groupe K a pour cardinal 4 ou 8. Les sous-groupes de G sont donc $\{I_2\}$, $\{I_2, -I_2\}$, ou l'un des sous-groupes cycliques d'ordre 4 engendrés par l'un des 6 éléments d'ordre 4, et G. Les sous-groupes d'ordre 4 sont, le sous-groupe engendré par A (ou A^{-1}), le sous-groupe engendré par B (ou B^{-1}) et le sous-groupe engendré par AB (ou $(AB)^{-1} = B^{-1}A^{-1} = BA$) ; on voit facilement que ces 3 sous-groupes sont différents. Le groupe G comporte donc en tout 6 sous-groupes. Le sous-groupe $\{I_2, -I_2\}$ est distingué car il est inclus dans le centre de G ; les sous-groupes d'ordre 4 sont d'indice 2, donc nécessairement distingués. Tous les sous-groupes de G sont donc distingués.

Le centre de G contient le sous-groupe $\{I_2, -I_2\}$; son cardinal est donc 2 ou 4 (G n'est pas abélien) ; ce n'est pas 4, car dans ce cas le groupe quotient $G/\mathcal{Z}(G)$ serait de cardinal de 2, donc cyclique, et G serait abélien (exercice 2). Le centre du groupe G est donc le sous-groupe $\{I_2, -I_2\}$.

Nous avons vu que le carré de tout élément de G est I_2 ou $-I_2$, éléments du centre ; nous pouvons en déduire que pour tout $x \in G/\mathcal{Z}(G)$, $x^2 = e$, où e désigne l'élément neutre du groupe quotient. Un tel groupe de cardinal 4 est abélien, et isomorphe au groupe $\left(\mathbb{Z}/2\mathbb{Z}\right)^2$ (dit groupe de Klein).

Exercice 13 :

> Faire le recensement de tous les groupes de cardinal 8. On montrera que tout groupe non abélien de cardinal 8 est isomorphe soit au groupe du carré, soit au groupe quaternionique. Quant aux groupes abéliens on en trouvera trois différents isomorphes à $\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ additifs. ■

Les périodes des éléments d'un groupe G de cardinal 8 peuvent être 1,2,4 ou 8. La discussion principale porte sur l'existence dans G d'au moins un élément de période 8, ou 4 ; la discussion secondaire porte sur les différentes relations algébriques possibles que vérifient deux éléments qui engendrent le groupe.

I) On suppose qu'il y a dans G un élément de période 8. Le groupe G est alors nécessairement isomorphe à $\mathbb{Z}/8\mathbb{Z}$, donc abélien. Le groupe $\mathbb{Z}/8\mathbb{Z}$ est un exemple de tel groupe.

II) On suppose qu'il n'y a pas dans G d'élément de période 8, mais au moins un élément de période 4 : a. Les groupes G vérifiant ces conditions sont nécessairement non isomorphes aux groupes rencontrés dans la partie I). Notons H le sous-groupe engendré par a ; il est distingué car d'indice 2. Soit b un élément de G qui n'est pas dans H ; il est clair que $G = H \cup bH = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$. On remarque que $bab^{-1} \in H$, puisque H est distingué, et est comme a un élément de période 4 ; nous pouvons en déduire que $bab^{-1} = a$ ou $bab^{-1} = a^{-1}$. D'autre part b^2 est nécessairement dans H car il n'est pas dans Hb, et il n'est pas d'ordre 4, sinon b serait d'ordre 8 ; on voit donc que $b^2 = e$ ou $b^2 = a^2$.

1) Supposons que $bab^{-1} = a$ soit $ba = ab$. Le groupe G est alors abélien. Soit $b^2 = e$, soit $b^2 = a^2$, mais dans le deuxième cas on vérifie que $(ab)^2 = a^2b^2 = a^4 = e$, et que $ab \notin H$; on peut donc remplacer b par ab. Il existe donc dans G un élément c d'ordre 2 qui n'est pas dans H. Soit $\varphi : \mathbb{Z}^2 \to G$, $(p, q) \mapsto a^p c^q$; c'est un homomorphisme surjectif de groupes. Déterminons son noyau. Si $a^p c^q = e$, alors $a^p = c^{-q}$, q est nécessairement pair car $c \notin H$, et p est multiple de 4 ; ces conditions sont suffisantes. Le noyau de l'homomorphisme φ est donc le sous-groupe $4\mathbb{Z} \times 2\mathbb{Z}$; le groupe G est donc nécessairement isomorphe au groupe quotient $(\mathbb{Z} \times \mathbb{Z})/(4\mathbb{Z} \times 2\mathbb{Z})$. Il y a donc dans ce cas une seule structure de groupe possible. Comme le groupe $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ vérifie ces conditions, il y en a une et une seule.

2) Supposons $bab^{-1} = a^{-1}$, soit $ba = a^{-1}b$. Les groupes vérifiant ces conditions sont non abéliens et par conséquent non isomorphes aux groupes précédemment trouvés. Nous étudierons de manière générale les groupes engendrés par deux éléments a et b vérifiant les relations ci-dessus, sans supposer a priori qu'il sont de cardinal 8 ; ceci afin de pouvoir prouver ici explicitement l'existence de tels groupes.

a) On suppose $b^2 = e$.
Soit (G, a, b) le triplet d'un groupe G engendré par $\{a, b\}$, où a est d'ordre 4 (on notera H le sous-groupe engendré par a), b d'ordre 2, et $bab^{-1} = a^{-1}$ (donc $b \notin H$) ; posons $K = H \cup Hb$ et montrons $K = G$, ce qui prouvera que G a exactement 8 éléments.
Il est clair que $K = \{a^p b^q \ (p, q) \in \mathbb{Z}^2\}$ car a est d'ordre 4 et b d'ordre 2. Nous avons supposé que $\sigma_b(a) = bab^{-1} = a^{-1}$, donc pour tout $p \in \mathbb{Z}$ $\sigma_b(a^p) = a^{-p}$, soit $ba^p = a^{-p}b$. Comme b est d'ordre 2, on voit que pour tout couple $(p, q) \in \mathbb{Z}^2$, $b^q a^p = a^{(-1)^q p} b^q$. Nous pouvons en déduire que pour tous entiers p, q, m, n :

$$(1) \qquad a^p b^q a^m b^n = a^p a^{(-1)^q m} b^{q+n} = a^{p+(-1)^q m} b^{q+n} ,$$

et :

$$(a^p b^q)^{-1} = b^{-q} a^{-p} = a^{-(-1)^q p} b^{-q} .$$

L'ensemble K (non vide) est donc bien un sous-groupe, donc le sous-groupe engendré par $\{a, b\}$, c'est-à-dire G.
Il existe des groupes vérifiant ces conditions, par exemple le groupe du carré (voir étude du groupe $\mathfrak{S}_4$ dans le §V.7), c'est-à-dire le groupe engendré dans $\mathfrak{S}_4$ par le cycle $a = \langle 1, 2, 3, 4\rangle$, et la transposition $b = \tau_{1,3}$; on vérifie que a est d'ordre 4, b est d'ordre 2 et que :

$$b\,a\,b^{-1} = \langle 3, 2, 1, 4\rangle = \langle 1, 2, 3, 4\rangle^{-1} = a^{-1} .$$

Il est clair géométriquement, et on peut le vérifier facilement par le calcul, que le groupe de carré contient 1 élément d'ordre 1, 2 éléments d'ordre 4, et 5 éléments d'ordre 2 (5 symétries).

Montrons que tous les groupes vérifiant ces conditions sont nécessairement isomorphes entre eux ; cela démontrera qu'il y a, à isomorphisme près, une et une seule structure de groupe vérifiant ces conditions : la structure du groupe du carré. Soient (G, a, b) et (G', a', b') deux triplets vérifiant ces conditions. On peut établir une bijection (pour l'instant uniquement ensembliste) $\varphi : G \to G'$, en posant $\varphi(a^i\,b^j) = a'^i\,b'^j$ pour tout couple $(i, j) \in [\![0, 3]\!] \times [\![0, 1]\!]$. Comme a et a' sont d'ordre 4, b et b' d'ordre 2, on voit que pour tout $(p, q) \in \mathbb{Z}^2$, $\varphi(a^p\,b^q) = a'^p\,b'^q$. L'égalité (1) étant vraie aussi pour a' et b', on voit que pour tous entiers p, q, n, m :

$$\varphi(a^p\,b^q\,a^m\,b^n) = \varphi(a^{p+(-1)^q m}\,b^{q+n}) =$$
$$= a'^{\,p+(-1)^q m}\,b'^{\,q+n} = a'^p\,b'^q\,a'^m\,b'^n = \varphi(a^p\,b^q)\,\varphi(a^m\,b^n) .$$

L'application bijective φ est donc un isomorphisme de groupes.

Il existe donc un et un seul groupe vérifiant ces conditions, le groupe du carré.

b) On suppose $b^2 = a^2$; b est donc d'ordre 4. La méthode employée est similaire.
Soit (G, a, b) le triplet d'un groupe G engendré par $\{a, b\}$, où a est d'ordre 4 (on notera H le sous-groupe engendré par a), $b\,a\,b^{-1} = a^{-1}$ (donc $b \notin H$) et $b^2 = a^2$; posons $K = H \cup H\,b$ et montrons $K = G$, ce qui prouvera que G a exactement 8 éléments.
On voit que $K = \{a^p\,b^q \ (p, q) \in \mathbb{Z}^2\}$, puisque a commute avec toute puissance paire de b. Nous avons supposé que $\sigma_b(a) = b\,a\,b^{-1} = a^{-1}$, donc pour tout $p \in \mathbb{Z}$ $\sigma_b(a^p) = a^{-p}$, soit $b\,a^p = a^{-p}\,b$. Comme toute puissance paire de b commute avec a, on voit que pour tout couple $(p, q) \in \mathbb{Z}^2$, $b^q\,a^p = a^{(-1)^q p}\,b^q$. Nous pouvons en déduire que pour tous entiers p, q, m, n :

$$(2) \qquad a^p\,b^q\,a^m\,b^n = a^p\,a^{(-1)^q m}\,b^{q+n} = a^{p+(-1)^q m}\,b^{q+n} ,$$

et :

$$(a^p\,b^q)^{-1} = b^{-q}\,a^{-p} = a^{-(-1)^q p}\,b^{-q} .$$

L'ensemble K (non vide) est donc bien un sous-groupe, donc le sous-groupe engendré par $\{a,b\}$, c'est-à-dire G.
Il existe des groupes vérifiant ces conditions, par exemple le groupe quaternionique étudié dans l'exercice précédent. Montrons que tous les groupes vérifiant ces conditions sont nécessairement isomorphes entre eux ; cela démontrera qu'il y a, à isomorphisme près, une et une seule structure de groupe vérifiant ces conditions : la structure du groupe quaternionique. Soient (G,a,b) et (G',a',b') deux triplets vérifiant ces conditions. On peut établir une bijection (pour l'instant uniquement ensembliste) $\varphi : G \to G'$, en posant $\varphi(a^i\,b^j) = a'^i\,b'^j$ pour tout couple $(i,j) \in [\![0,3]\!] \times [\![0,1]\!]$. Comme a et a' sont d'ordre 4, on voit que pour tout $p \in \mathbb{Z}$ et tout $j \in [\![0,1]\!]$, $\varphi(a^p\,b^j) = a'^p\,b'^j$; pour tout $p \in \mathbb{Z}$ et tout $q \in \mathbb{Z}$, $\varphi(a^p\,b^{2q}) = \varphi(a^{p+2q}) = a'^{p+2q} = a'^p\,b'^{2q}$, et $\varphi(a^p\,b^{2q+1}) = \varphi(a^{p+2q}\,b) = a'^{p+2q}\,b' = a'^p\,b'^{2q+1}$; finalement nous voyons que pour tout $(p,q) \in \mathbb{Z}^2$, $\varphi(a^p\,b^q) = a'^p\,b'^q$. L'égalité (2) étant vraie aussi pour a' et b', on voit que pour tous entiers p,q,n,m :

$$\varphi(a^p\,b^q\,a^m\,b^n) = \varphi(a^{p+(-1)^q m}\,b^{q+n}) =$$
$$= a'^{p+(-1)^q m}\,b'^{q+n} = a'^p\,b'^q\,a'^m\,b'^n = \varphi(a^p\,b^q)\,\varphi(a^m\,b^n)\ .$$

L'application bijective φ est donc un isomorphisme de groupes.

Il existe donc un et un seul groupe vérifiant ces conditions, le groupe quaternionique. Le groupe quaternionique et le groupe du carré ne sont pas isomorphes car il y a un seul élément d'ordre 2 dans le groupe quaternionique, alors qu'il y en a 5 dans le groupe du carré.

III) Supposons que G n'ait aucun élément de période 8 ou 4 ; tous les éléments ont donc pour périodes 1 ou 2. Les groupes vérifiant ces conditions ne seront pas isomorphes aux groupes précédemment décrits. Pour tout $x \in G$ on a $x^2 = e$; le groupe G est par conséquent abélien : pour tout $x \in G$, $x = x^{-1}$, donc pour tout $(x,y) \in G^2$, $x\,y = (x\,y)^{-1} = y^{-1}\,x^{-1} = y\,x$. Montrons que G est alors nécessairement isomorphe au groupe $(\mathbb{Z}/2\,\mathbb{Z})^3$. Cela démontrera qu'il existe une, et une seule, structure de groupe vérifiant ces conditions.

Soit G un tel groupe, $x \in G\setminus\{e\}$ et $y \in G\setminus\{e,x\}$. On voit que l'ensemble $H = \{x^p\,y^q \mid (p,q) \in \mathbb{Z}^2\} = \{e,x,y,x\,y\}$ est un sous-groupe de cardinal 4 dans G. Soit $z \in G \setminus H$, l'ensemble $H \cup H\,z$ est de cardinal 8, donc $G = H \cup H\,z$, soit encore : $G = \{x^p\,y^q\,z^r \mid (p,q,r) \in \mathbb{Z}^3\}$. L'application $\varphi : \mathbb{Z}^3 \to G$, $(p,q,r) \mapsto x^p\,y^q\,z^r$ est un homomorphisme de groupes (puisque G est abélien) surjectif. Montrons que son noyau est $(2\,\mathbb{Z})^3$. Si $x^p\,y^q\,z^r = e$, alors $z^{-r} \in H$, donc $z^r = e$ et r est pair ($z \notin H$) ; nous en déduisons alors que $x^p\,y^q = e$, et par conséquent que p et q sont tous les deux pairs ; comme $\mathrm{Ker}\,(\varphi) \supset (2\,\mathbb{Z})^3$ est évident, en déduisons $\mathrm{Ker}\,(\varphi) = (2\,\mathbb{Z})^3$. Le groupe G est donc nécessairement isomorphe au groupe $\mathbb{Z}^3/(2$

groupes vérifiant ces conditions sont donc isomorphes entre eux, donc à l'un d'entre eux, le groupe $(\mathbb{Z}/_{2\mathbb{Z}})^3$.

IV) Conclusion.
Nous avons trouvé 5 structures de groupes de cardinal 8 non isomorphes entre elles : trois structures abéliennes, $\mathbb{Z}/_{8\mathbb{Z}}, \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}, (\mathbb{Z}/_{2\mathbb{Z}})^3$, et deux structures non abéliennes, celle du groupe de carré, et celle du groupe quaternionique.

Exercice 14 :

> Soit G un groupe tel que le groupe quotient $G/_{\mathfrak{Z}(G)}$ soit *fini* ($\mathfrak{Z}(G)$ désigne le centre de G). Démontrer que le groupe des commutateurs $[G,G]$ est fini (cf. définition du §V.4, exercice 5).
> ■

a) Soit $n = [G : \mathfrak{Z}(G)]$, et $x_1, x_2, \ldots, x_n$ un système de représentants des classes modulo le sous-groupe (distingué) $\mathfrak{Z}(G)$. Pour tout couple $(x,y) \in G^2$, il existe des entiers i et j dans $[\![1,n]\!]$ et des éléments α et β de $\mathfrak{Z}(G)$ tels que $x = x_i\,\alpha$ et $y = x_j\,\beta$; on observe que :

$$[x,y] = x_i\,\alpha\,x_j\,\beta(x_i\,\alpha)^{-1}\,(x_j\,\beta)^{-1} = \alpha\,\alpha^{-1}\,\beta\,\beta^{-1}x_i\,x_j\,x_i^{-1}\,x_j^{-1} = [x_i,x_j]\ ,$$

puisque α et β commutent avec tout élément du groupe G. Le nombre de commutateurs est donc $\leqslant n^2$; notons Γ l'ensemble de ces commutateurs et k leur nombre.

Pour $x \in G$, nous noterons σ_x l'automorphisme intérieur du groupe G, $y \mapsto x\,y\,x^{-1}$. On remarque que pour tout $(x,y,z) \in G^3$:

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

Pour tout $(x,y) \in G^2$:

$$\begin{aligned}[x,y^2]\,[y\,x\,y^{-1},y]^{n-1} &= [x,y^2]\,[\sigma_y(x),\sigma_y(y)]^{n-1} = [x,y^2]\,\sigma_y([x,y]^{n-1}) = \\ &= x\,y^2\,x^{-1}\,y^{-2}\,y\,[x,y]^{n-1}\,y^{-1} = x\,y\,(x^{-1}\,x)\,y\,x^{-1}y^{-1}[x,y]^{n-1}\,y^{-1} = \ . \\ &= x\,y\,x^{-1}[x,y]^n\,y^{-1}\end{aligned}$$

Comme $[x,y]^n \in \mathfrak{Z}(G)$, nous voyons que :

$$(1) \qquad [x,y^2]\,[y\,x\,y^{-1},y]^{n-1} = x\,y\,x^{-1}\,y^{-1}\,[x,y]^n = [x,y]^{n+1}\ .$$

Comme nous le verrons dans ce qui suit, cette égalité nous permettra de remplacer un produit de $n+1$ commutateurs par un produit de n commutateurs.

Soit γ un commutateur particulier. Notons, pour $(p,q) \in \mathbb{N}^2$, H_q l'ensemble des éléments de G qui peuvent s'écrire comme composés de q commutateurs différents de γ ($H_0 = \{e\}$), et $K_{p,q}$ l'ensemble des éléments de G qui peuvent s'écrire comme composés de $p+q$ commutateurs dont p égaux à γ et q différents de γ. Comme $\{\gamma\}$ est invariant par l'automorphisme intérieur σ_γ, l'ensemble des commutateurs différents de γ est aussi stable par σ_γ ; on voit alors facilement que pour tout $(p,q) \in \mathbb{N}^2$ les ensembles H_p et $K_{p,q}$ sont stables par σ_γ. Montrons par récurrence sur p que pour tout $q \in \mathbb{N}$, $K_{p,q} = \gamma^p H_q$. Comme l'inclusion $\gamma^p H_q \subset K_{p,q}$ est évidente, il suffit de démontrer l'inclusion opposée. Elle est vraie pour $p = 0$. Supposons cette inclusion vraie pour $p-1$, où $p \in \mathbb{N}^*$; soit $q \in \mathbb{N}$, et $x \in K_{p,q}$; x peut s'écrire comme un composé de $p+q$ commutateurs, dont exactement p (> 0) sont γ ; soit $i \in [\![1, p+q]\!]$ le rang du premier terme dans le produit qui soit γ, on voit que $x \in H_{i-1}\,\gamma\,K_{p-1,q-i+1}$, et que :

$$H_{i-1}\,\gamma\,K_{p-1,q-i+1} = \gamma\,(\gamma^{-1}\,H_{i-1}\gamma)\,K_{p-1,q-i+1} = \\ = \gamma\,H_{i-1}K_{p-1,q-i+1} \subset \gamma\,K_{p-1,q}\ ;$$

en utilisant l'hypothèse de récurrence, nous obtenons :

$$x \in \gamma\,K_{p-1,q} = \gamma\,\gamma^{p-1}\,H_q = \gamma^p\,H_q\ .$$

L'égalité $K_{p,q} = \gamma^p H_q$ est donc vraie pour tout couple $(p,q) \in \mathbb{N}^2$.

Pour tout entier m, notons E_m l'ensemble des éléments de G qui peuvent s'écrire comme composés de m commutateurs. Montrons que si $m > n\,k$ (k est le nombre de commutateurs), alors $E_m \subset E_{m-1}$. Si $x \in G$ peut s'écrire comme composé de m commutateurs, $m > n\,k$, comme il n'y a que k commutateurs, au moins l'un d'eux, que nous noterons γ, est répété dans le produit un nombre p de fois, $p > n$; en reprenant les notations précédentes $x \in K_{p,m-p}$, donc $x \in \gamma^p H_{m-p}$, et puisque $p > n$, $x \in \gamma^{n+1} E_{m-n-1}$. La formule (1) démontrée ci-dessus nous permet d'affirmer $\gamma^{n+1} \in E_n$, et par conséquent $x \in E_n\,E_{m-n-1} \subset E_{m-1}$. Nous en déduisons que pour tout $m \geqslant n\,k$, $E_m \subset E_{nk}$. Il est alors clair que l'ensemble E_{nk} est stable par le produit ; il est aussi stable par l'inverse, car pour tout $(x,y) \in G^2$, $[x,y]^{-1} = (x\,y\,x^{-1}\,y^{-1})^{-1} = y\,x\,y^{-1}\,x^{-1} = [y,x]$ (l'inverse d'un commutateur est un commutateur). Tout commutateur est dans E_{nk} car si γ est un commutateur, on peut trouver un entier p tel que $2p+1 \geqslant nk$, d'où $\gamma = \gamma^{p+1}\,\gamma^{-p} \in E_{2p+1} \subset E_{nk}$. L'ensemble E_{nk} est donc le sous-groupe engendré par l'ensemble des commutateurs, soit $[G,G]$. Comme il y k commutateurs possibles, le nombre de produits de nk commutateurs est majoré par le nombre d'applications de $[\![1, nk]\!]$ dans $[\![1, k]\!]$, donc par k^{nk}. Le groupe $[G : G]$ est donc fini, de cardinal majoré par $k^{nk} \leqslant (n^2)^{n\,n^2} = n^{2n^3}$.

Chapitre VI

STRUCTURE D'ESPACE VECTORIEL ET D'ALGÈBRE ; NOMBRES COMPLEXES

§ VI.1 *STRUCTURE D'ESPACE VECTORIEL*

Exercice 1 :

Soit $(F_i)_{i\in I}$ une famille non vide de sous-K-ev d'un K-ev E pour laquelle $(\forall i \in I)(\forall j \in I)\ \exists k \in I \mid F_i \cup F_j \subset F_k$. Démontrer qu'alors $\bigcup_{i\in I} F_i$ est un sous-K-ev de E. ■

Appliquons à l'ensemble $F = \bigcup_{i\in I} F_i$ le critère de sous-K-ev. Comme 0_E est dans chaque sous-espace F_i, F contient évidemment cet élément. Soient x et y dans F, il existe des éléments $i \in I$ et $j \in I$ tels que $x \in F_i$ et $y \in F_j$; d'après l'hypothèse, il existe $k \in I$ tel que $F_i \subset F_k$ et $F_j \subset F_k$, d'où $x \in F_k$ et $y \in F_k$; comme F_k est un sous-K-ev de E, pour tout scalaire $\lambda \in K$, $x + \lambda \cdot y \in F_k$, donc $x + \lambda \cdot y \in F$. L'ensemble F est donc bien un sous-K-ev de E.

Exercice 7 :

Soit G un groupe abélien, noté additivement.

a) Montrer que G peut être muni d'*au plus une* structure de $\mathbb{Q}$-ev.

b) Montrer que, pour que G puisse être muni d'une structure de $\mathbb{Q}$-ev, il faut et il suffit qu'il vérifie les conditions :

1° G est *sans torsion* (i.e. G n'a pas d'élément de torsion) et

2° G est *divisible* (i.e. $\forall x \in G\ \forall n \in \mathbb{N}^*,\ \exists y \in G \mid n\,y = x$). ■

a) Supposons que le groupe abélien G puisse être muni d'une loi externe $\varphi : \mathbb{Q} \times G \to G$, telle que (G, φ) soit un $\mathbb{Q}$-ev. Si $n \in \mathbb{Z}$ et $x \in G$, "n fois x" sera noté $n \cdot x$.
Montrons que G est nécessairement divisible et sans torsion.

$x \in G$ sont tels que $n \cdot x = 0_G$, alors $0_G = n \cdot \varphi(1,x) = \varphi(n \cdot 1, x)$; comme (G,φ) est un $\mathbb{Q}$-ev, $x = 0$ ou $n \cdot 1 = n = 0$; G est donc sans torsion. Pour tout $n \in \mathbb{N}^*$ et $x \in G$, $n \cdot \varphi(1/n, x) = \varphi(n \cdot 1/n, x) = \varphi(1,x) = x$; le groupe G est donc divisible. Nous pouvons remarquer que pour tout $x \in G$ et tout $n \in \mathbb{N}^*$, il existe un *unique* $y \in G$ tel que $n \cdot y = x$. Pour tout $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$, et $x \in G$, $q \cdot \varphi(p/q, x) = \varphi(q \cdot p/q, x) = \varphi(p \cdot 1, x) = p \cdot \varphi(1,x) = p \cdot x$; nous en déduisons que $\varphi(p/q, x)$ est nécessairement le seul $y \in G$ tel que $q \cdot y = p \cdot x$. Cela démontre l'unicité de l'application φ (s'il en existe) telle que (G,φ) soit un $\mathbb{Q}$-ev.

b) Montrons maintenant que si le groupe abélien G est sans torsion et divisible, alors il peut être muni d'une structure de $\mathbb{Q}$-ev.
Soit $\mathcal{R}$ la relation entre les ensembles $\mathbb{Q} \times G$ et G définie par :

$$(\forall (r,x) \in \mathbb{Q} \times G)\ (\forall y \in G)$$
$$((r,x)\,\mathcal{R}\,y) \Leftrightarrow (\ \exists (p,q) \in \mathbb{Z} \times \mathbb{N}^* |\ (q \cdot y = p \cdot x) \text{ et } (r = p/q)\ )\ .$$

Comme G est divisible, et que tout rationnel s'écrit comme quotient de deux entiers, le domaine de cette relation est $\mathbb{Q} \times G$, ce qui signifie :

$$\forall (r,x) \in \mathbb{Q} \times G,\ \exists y \in G, \quad (r,x)\,\mathcal{R}\,y\ .$$

Soit $(r,x) \in \mathbb{Q} \times G$, supposons que $(r,x)\,\mathcal{R}\,y_1$ et $(r,x)\,\mathcal{R}\,y_2$, où $y_1 \in G$, et $y_2 \in G$; il existe deux couples (p_1,q_1) et (p_2,q_2) dans $\mathbb{Z} \times \mathbb{Q}$ tels que :

$$r = \frac{p_1}{q_1} = \frac{p_2}{q_2} \quad \text{et} \quad (q_1 \cdot y_1 = p_1 \cdot x \text{ et } q_2 \cdot y_2 = p_2 \cdot x)\ ;$$

nous voyons que :

$$p_1\,q_2 = p_2\,q_1 \quad \text{et} \quad (q_1\,q_2 \cdot y_1 = p_1\,q_2 \cdot x = p_2\,q_1 \cdot x = q_1\,q_2 \cdot y_2)\ ;$$

comme G est divisible, et que $q_1\,q_2 > 0$, nous en déduisons $y_1 = y_2$. La relation $\mathcal{R}$ est donc une application $(\mathbb{Q} \times G) \to G$. Nous noterons maintenant cette application φ en utilisant la notation fonctionnelle. Nous retenons la propriété :

$$\forall (p,q) \in \mathbb{Z} \times \mathbb{N}^*, \quad q \cdot \varphi(p/q, x) = p \cdot x\ .$$

Vérifions les axiomes de $\mathbb{Q}$-ev. Soient (a,b) et (u,v) dans $(\mathbb{Z} \times \mathbb{N}^*)$, x et y dans G ;

premier axiome :

$$b\,v \cdot \varphi\left(\frac{a}{b} + \frac{u}{v}\ , x\right) = b\,v \cdot \varphi\left(\frac{a\,v + u\,b}{b\,v}, x\right) = (a\,v + u\,b) \cdot x =$$
$$= v \cdot (a \cdot x) + b \cdot (u \cdot x) = v \cdot \left(b \cdot \varphi\left(\frac{a}{b}, x\right)\right) + b \cdot \left(v \cdot \varphi\left(\frac{u}{v}, x\right)\right) =$$
$$= b\,v \cdot \left(\varphi\left(\frac{a}{b}, x\right) + \varphi\left(\frac{u}{v}, x\right)\right)\ ,$$

d'où, puisque G est sans torsion :

$$\varphi\left(\frac{a}{b}+\frac{u}{v}\,,x\right)=\varphi\left(\frac{a}{b},x\right)+\varphi\left(\frac{u}{v},x\right)\ ;$$

deuxième axiome :

$$b\cdot\varphi\left(\frac{a}{b}\,,x+y\right)=a\cdot(x+y)=a\cdot x+a\cdot y=b\cdot\varphi\left(\frac{a}{b}\,,x\right)+b\cdot\varphi\left(\frac{a}{b}\,,y\right)=$$
$$=b\cdot\left(\varphi\left(\frac{a}{b}\,,x\right)+\varphi\left(\frac{a}{b}\,,y\right)\right)\ ,$$

d'où, comme G est sans torsion :

$$\varphi\left(\frac{a}{b}\,,x+y\right)=\varphi\left(\frac{a}{b}\,,x\right)+\varphi\left(\frac{a}{b}\,,y\right)\ ;$$

troisième axiome :

$$\varphi\left(\frac{1}{1},x\right)=1\cdot\varphi\left(\frac{1}{1},x\right)=1\cdot x=x\ ;$$

quatrième axiome :

$$bv\cdot\varphi\left(\frac{a}{b},\varphi\left(\frac{u}{v},x\right)\right)=v\cdot\left(a\cdot\varphi\left(\frac{u}{v},x\right)\right)=a\cdot\left(v\cdot\varphi\left(\frac{u}{v},x\right)\right)=$$
$$=a\cdot(u\cdot x)=au\cdot x\ ,$$

d'où :

$$\varphi\left(\frac{a}{b},\varphi\left(\frac{u}{v},x\right)\right)=\varphi\left(\frac{au}{bv},x\right)=\varphi\left(\frac{a}{b}\,\frac{u}{v}\,,x\right)\ .$$

Nous avons bien montré que (G,φ) est un $\mathbb{Q}$-espace vectoriel.

§ VI.2 *APPLICATIONS LINÉAIRES*

Exercice 1 :

Soit E un K-ev et $f\in \mathrm{Hom}_K(E)$. On pose $f\circ f=f^2$.
Montrer que :

$\mathrm{Ker}\,(f)=\mathrm{Ker}\,(f^2)$ ssi $\mathrm{Im}\,(f)\cap\mathrm{Ker}\,(f)=$

Comme pour tout endomorphisme $f \in \mathrm{Hom}_K(E)$, $\mathrm{Ker}\,(f) \subset \mathrm{Ker}\,(f^2)$, la première égalité est équivalente à la proposition :

$$\forall x \in E,\ f(f(x)) = 0_E \Rightarrow f(x) = 0_E\ ,$$

qui est équivalente à :

$$\forall y \in f(E),\ f(y) = 0_E \Rightarrow y = 0_E\ ,$$

autrement dit : $\mathrm{Im}\,(f) \cap \mathrm{Ker}\,(f) \subset \{0_E\}$; ce qu'il fallait démontrer.

Exercice 2 :

> Soient f et g deux endomorphismes de l'espace vectoriel E. Montrer que
>
> $$f[\mathrm{Ker}\,(g \circ f)] = \mathrm{Ker}\,(g) \cap \mathrm{Im}\,(f)\ .\ \blacksquare$$

On vérifie que :

$$f[\mathrm{Ker}\,(g \circ f)] = \{y \in E \mid (\exists x \in E) \quad g(f(x)) = 0_E \text{ et } y = f(x)\}\ .$$

Nous en déduisons que :

$$f[\mathrm{Ker}\,(g \circ f)] = \{y \in f(E) \mid g(y) = 0_E\} = f(E) \cap \mathrm{Ker}\,(g)\ ,$$

ce qu'il fallait démontrer.

Exercice 7 :

> Soit K un corps commutatif de cardinal $\geqslant 4$, E un K-ev et F un sous-K-ev de E distinct de E. On considère une application $f \in \mathrm{Hom}_K(E)$ telle que
>
> $$(\forall x \in E \setminus F) \quad \exists \lambda \in K \mid f(x) = \lambda \cdot x\ .$$
>
> Prouver que f est une homothétie. $\blacksquare$

Si $x \in E \setminus F$, alors $x \neq 0_E$; il existe donc un unique scalaire $\lambda \in K$ tel que $f(x) = \lambda \cdot x$; nous noterons λ_x ce scalaire. Montrons que l'application $x \mapsto \lambda_x$, $E \setminus F \to K$, est constante.
Si x et y, éléments de $E \setminus F$ sont linéairement dépendants, il existe $\alpha \in K$ tel que $y = \alpha \cdot x$; alors $f(y) = f(\alpha \cdot x) = \alpha \cdot f(x) = \alpha\,\lambda_x \cdot x = \lambda_x \cdot y$; nous en déduisons $\lambda_y = \lambda_x$.
Soient x et y des éléments de $E \setminus F$ qui sont linéairement indépendants ; il existe au plus un scalaire α tel que $x + \alpha \cdot y \in F$ (sinon $y \in F$) ; comme le corps K a au moins 3 éléments, on peut trouver un scalaire $\beta \neq 0$ tel que $x + \beta \cdot y \notin F$; il existe donc un scalaire μ tel que :

$$f(x + \beta \cdot y) = \mu \cdot (x + \beta \cdot y) = f(x) + \beta \cdot f(y) = \lambda_x \cdot x + \beta$$

comme (x, y) est libre, nous en déduisons :

$$\mu = \lambda_x \quad \text{et} \quad \mu\beta = \beta\lambda_y \ ;$$

d'où $\lambda_x = \mu = \lambda_y$, puisque $\beta \neq 0$.
L'application $x \mapsto \lambda_x$ est donc constante sur $E \setminus F$; nous noterons λ sa valeur.

Montrons que pour tout $x \in E$, $f(x) = \lambda \cdot x$, ce qui est vrai si $x \notin F$. Si $x \in F$, soit $y \notin F$ (F est un sous-espace strict de E) ; on voit que $x + y \notin F$, donc $f(x) = f(x + y) - f(y) = \lambda \cdot (x + y) - \lambda \cdot y = \lambda \cdot x$. L'application f est donc bien l'homothétie de rapport λ.

§ VI.3 *COMBINAISONS LINÉAIRES ; INDÉPENDANCE LINÉAIRE ; BASES*

Exercice 2 :

> *a*) Pour $\alpha \in \mathbb{R}_+^*$, soit $f_\alpha : \mathbb{R} \to \mathbb{R}$, $x \mapsto |x|^\alpha$. Démontrer que la famille de fonctions $(f_\alpha)_{\alpha \in \mathbb{R}_+^*}$ est $\mathbb{R}$-libre dans le $\mathbb{R}$-ev $\mathcal{F}(\mathbb{R}, \mathbb{R})$.
>
> *b*) Soit $I = \mathbb{R}_+^* \setminus \mathbb{N}$. Démontrer que la famille de fonctions $(g_{a,\alpha})_{(a,\alpha) \in \mathbb{R} \times I}$, où $g_{a,\alpha}(x) = f_\alpha(x - a)$ pour $x \in \mathbb{R}$, est $\mathbb{R}$-libre dans le $\mathbb{R}$-ev $\mathcal{F}(\mathbb{R}, \mathbb{R})$. ■

a) Montrons par récurrence sur $n = \text{card}(A)$, que toute sous-famille finie $(f_\alpha)_{\alpha \in A}$, où A est une partie finie de $\mathbb{R}_+^*$, est libre. C'est vrai si $n = 1$ (et si $n = 0$). Supposons que ce soit vrai pour n.
Soit A une partie finie de $\mathbb{R}_+^*$ de cardinal $n + 1$ et $(\lambda_\alpha)_{\alpha \in A}$ une famille de scalaires telle que $\sum_{\alpha \in A} \lambda_\alpha \cdot f_\alpha = 0$, c'est-à-dire $\forall x \in \mathbb{R}$, $\sum_{\alpha \in A} \lambda_\alpha |x|^\alpha = 0$.
Posons $a = \text{Max}(A)$, on peut écrire :

$$\forall x \in \mathbb{R}, \quad \lambda_a |x|^a = - \sum_{\alpha \in A \setminus \{a\}} \lambda_\alpha |x|^\alpha \ ,$$

d'où :

$$\forall x \in \mathbb{R}, \quad \lambda_a = - \sum_{\alpha \in A \setminus \{a\}} \lambda_\alpha |x|^{\alpha - a} \ .$$

Comme pour tout $\alpha \in A \setminus \{a\}$, $|x|^{\alpha - a} \underset{x \to +\infty}{\longrightarrow} 0$, nous en déduisons $\lambda_a = 0$. La famille $(f_\alpha)_{\alpha \in A \setminus \{a\}}$ est, par l'hypothèse de récurrer

$\sum_{\alpha\in A\setminus\{a\}} \lambda_\alpha \cdot f_\alpha = 0$; nous en déduisons $\forall\alpha \in A\setminus\{a\}$, $\lambda_\alpha = 0$, d'où finalement $\forall\alpha \in A$, $\lambda_\alpha = 0$. La famille $(f_\alpha)_{\alpha\in A}$ est donc libre. Cela termine la démonstration par récurrence.

Toute sous-famille finie de la famille $(f_\alpha)_{\alpha\in\mathbb{R}_+^*}$ est libre. Cette famille est donc libre.

On pourrait aussi remarquer que $\forall x > 0$, $x f'_\alpha(x) = \alpha f_\alpha(x)$. La restriction à $\mathbb{R}_+^*$ de la fonction f_α, est donc un vecteur propre relatif à la valeur propre α, de l'endomorphisme linéaire φ du $\mathbb{R}$-ev $\mathscr{C}^\infty(\mathbb{R}_+^*,\mathbb{R})$, qui à $f \in \mathscr{C}^\infty(\mathbb{R}_+^*,\mathbb{R})$ fait correspondre l'application $x \mapsto x f'(x)$. La famille $(f_\alpha)_{\alpha\in\mathbb{R}_+^*}$ est donc libre (théorème XV.3.1).

b) Soit E une partie finie de $\mathbb{R}\times I$, montrons que la famille $(f_{a,\alpha})_{(a,\alpha)\in E}$ est libre. Supposons qu'il existe une famille non nulle $(\lambda_{a,\alpha})_{(a,\alpha)\in E}$ de scalaires telle que :

$$\sum_{(a,\alpha)\in E} \lambda_{a,\alpha} f_{a,\alpha} = 0 .$$

Soit $E' = \{(a,\alpha) \in E \mid \lambda_{a,\alpha} \neq 0\}$, par hypothèse cet ensemble est fini et non vide ; il est clair que :

$$\sum_{(a,\alpha)\in E'} \lambda_{a,\alpha} f_{a,\alpha} = 0 .$$

Soit :

$$a_0 = \mathrm{Max}\,(\{a \in \mathbb{R} \mid \exists\alpha \in I,\ (a,\alpha) \in E'\})$$

et $A_0 = \{\alpha \in I \mid (a_0,\alpha) \in E'\}$, (ensemble fini non vide). Posons :

$$f = \sum_{\alpha\in A_0} \lambda_{a_0,\alpha} f_{a_0,\alpha} = -\sum_{(a,\alpha)\in E',\ a<a_0} \lambda_{a,\alpha} f_{a,\alpha} = g .$$

On voit que g, donc f, est de classe $\mathscr{C}^\infty$ sur un intervalle ouvert V, voisinage de a_0. Soit p un entier qui majore strictement A_0, en dérivant p fois l'application f, nous obtenons pour tout $x \in V \cap]a_0,+\infty[$:

$$f^{(p)}(x) = \sum_{\alpha\in A_0} \alpha(\alpha-1)\ldots(\alpha-p+1)\lambda_{a_0,\alpha}(x-a_0)^{\alpha-p} .$$

Comme $A_0 \cap \mathbb{N} = \emptyset$, les coefficients $\alpha(\alpha-1)\ldots(\alpha-p+1)\lambda_{a_0,\alpha}$ sont tous non nuls. Soit $\alpha_0 = \mathrm{Min}\,(A_0)$, on voit que :

$$f^{(p)}(x) \sim \alpha_0(\alpha_0-1)\ldots(\alpha_0-p+1)\lambda_{a_0,\alpha_0}(x-a_0)^{\alpha_0-p} ,$$

au voisinage à droite de a_0. Si p est choisi tel que $\alpha_0 - p < 0$, $f^{(p)}$ n'est pas bornée au voisinage à droite de a_0, ce qui est contradictoi

La famille finie $(f_{a,\alpha})_{(a,\alpha)\in E}$ est donc libre. Ceci étant vrai pour toute partie finie E de $\mathbb{R}\times I$, la famille $(f_{a,\alpha})_{(a,\alpha)\in\mathbb{R}\times I}$ est libre.

Exercice 5 :

Soit E le $\mathbb{R}$-ev $\mathscr{F}(\mathbb{R}_+,\mathbb{R})$. Si $\alpha\in\mathbb{R}$, soit f_α la fonction $\mathbb{R}_+\to\mathbb{R}$, $t\mapsto\exp(\alpha t)$. Prouver que la famille $(f_\alpha)_{\alpha\in\mathbb{R}}$ est $\mathbb{R}$-libre dans E. ■

Soit F le sous-$\mathbb{R}$-espace de E dont les éléments sont les applications de classe $\mathscr{C}^\infty$ sur $\mathbb{R}_+$. Considérons l'application $D : F\to F$, $f\mapsto f'$, qui à une application fait correspondre sa dérivée. On voit que pour tout $\alpha\in\mathbb{R}$, f_α est élément de F et est un vecteur propre pour la valeur propre α de l'endomorphisme D du $\mathbb{R}$-espace vectoriel F. La famille $(f_\alpha)_{\alpha\in\mathbb{R}}$ est donc libre d'après le théorème XV.3.1. Les démonstrations élémentaires de ce résultat reprennent souvent la méthode utilisée pour la démonstration de ce théorème.

Exercice 7 :

Soient deux réels α et β ($\alpha<\beta$). On considère le $\mathbb{R}$-ev E des fonctions $[\alpha,\beta]\to\mathbb{R}$ *continues et affines par morceaux*. Si $a\in[\alpha,\beta]$, soit

$$f_a(x)=|x-a| \quad (x\in[\alpha,\beta]).$$

Montrer que la famille $(f_a)_{a\in[\alpha,\beta]}$ est *une base* du $\mathbb{R}$-ev E. ■

Montrons que si $a_0,a_1,\ldots,a_p$ est une famille d'éléments de $[\alpha,\beta]$ ($p\in\mathbb{N}^*$), $a=a_0<a_1<\ldots<a_p=b$, alors la famille $(f_{a_i})_{i\in[\![0,p]\!]}$ est libre.
Soit $(\lambda_i)_{i\in[\![0,p]\!]}$ est une famille de réels tels que :

$$\forall x\in[\alpha,\beta],\quad \sum_{i=0}^{p}\lambda_i\,|x-a_i|=0\ .$$

Alors, pour tout $j\in[\![1,p]\!]$, et pour tout $x\in[a_{j-1},a_j]$, on a :

$$\sum_{i=1}^{j-1}\lambda_i\,(x-a_i)-\sum_{i=j}^{p}\lambda_i\,(x-a_i)=0\ .$$

Nous en déduisons les égalités :

$$\lambda_0-\lambda_1-\lambda_2-\ldots-\lambda_{p-1}-\lambda_p=0$$
$$\lambda_0+\lambda_1-\lambda_2-\ldots-\lambda_{p-1}-\lambda_p=0$$

$$\begin{array}{ccccccc} \vdots & & \vdots & & \vdots & & \\ \lambda_0 & +\lambda_1 & +\lambda_2 & +\ldots & -\lambda_{p-1} & -\lambda_p & = 0 \\ \lambda_0 & +\lambda_1 & +\lambda_2 & +\ldots & +\lambda_{p-1} & -\lambda_p & = 0 \end{array}$$

En retranchant de chaque équation l'équation suivante, nous en déduisons $\lambda_1 = \ldots = \lambda_{p-1} = 0$, puis $\lambda_0 = \lambda_p$. Posons $\lambda = \lambda_0 = \lambda_p$, en reprenant la condition initiale, nous voyons que pour tout $x \in [\alpha, \beta]$, $\lambda(x-\alpha)+\lambda(\beta-x) = 0$, d'où $\lambda(\beta-\alpha) = 0$; donc $\lambda_0 = \lambda_1 = \ldots = \lambda_p = 0$. La famille $(f_{a_i})_{i\in[\![0,p]\!]}$ est par conséquent libre. Il est alors clair que toute sous-famille finie de la famille $(f_a)_{a\in[\alpha,\beta]}$ est libre, donc que cette famille est libre.

Soit f continue affine par morceaux sur $[\alpha, \beta]$; il existe un entier $p > 0$ et des éléments $a_0, a_1, \ldots, a_p$ de l'intervalle $[\alpha, \beta]$ tels que $\alpha = a_0 < a_1 < \ldots < a_p = b$, et tels que pour tout $i \in [\![1, p]\!]$, l'application f est affine sur l'intervalle $[a_{i-1}, a_i]$. Considérons le sous-$\mathbb{R}$-espace $E_{a_0,a_1,\ldots,a_p}$ de E, dont les éléments sont les applications affines par morceaux qui vérifient cette condition. Il est clair que l'application $f \mapsto (f(a_0), f(a_1), \ldots, f(a_p))$, $E_{a_0,a_1,\ldots,a_p} \to \mathbb{R}^{p+1}$ est un isomorphisme linéaire. L'espace $E_{a_0,a_1,\ldots,a_p}$ est donc de dimension $p+1$. La famille $(f_{a_i})_{i\in[\![0,p]\!]}$ est une famille libre dans cet espace $E_{a_0,a_1,\ldots,a_p}$ et le cardinal de son ensemble d'indices est $p+1$; c'est donc une base de cet espace. Comme $f \in E_{a_0,a_1,\ldots,a_p}$, cette application f est dans le sous-$\mathbb{R}$-espace engendré par la famille $(f_{a_i})_{i\in[\![0,p]\!]}$, donc dans le sous-$\mathbb{R}$-espace vectoriel engendré par la famille $(f_a)_{a\in[\alpha,\beta]}$.

La famille $(f_a)_{a\in[\alpha,\beta]}$ est donc une base du $\mathbb{R}$-espace vectoriel E.

§ VI.5 *LE CORPS DES NOMBRES COMPLEXES*

Exercice 7 :

> Soit $z = p + \mathrm{i}\,q$ donné, p et q réels. Peut-il être le produit de deux complexes dont l'un a une partie réelle donnée a et l'autre une partie imaginaire donnée b ? Discuter. ■

Soit $a + \mathrm{i}\,y$ le premier complexe et $x + \mathrm{i}\,b$ le second, où $x \in \mathbb{R}$ et $y \in \mathbb{R}$; ces complexes doivent vérifier la condition $(a + \mathrm{i}\,y)(x + \mathrm{i}\,b) = p + \mathrm{i}\,q$, ce qui équivaut aux deux égalités entre nombres réels :

$$\begin{aligned} a\,x - b\,y &= p \\ a\,b + x\,y &= q\,. \end{aligned}$$

Si $a = 0$ ou $b = 0$, la résolution se fait sans difficulté. Supposons $a \neq 0$ et $b \neq 0$; en posant $X = ax$ et $Y = -by$ les conditions ci-dessus deviennent :

$$X + Y = p$$
$$XY = a^2 b^2 - abq = ab(ab - q) .$$

Il y a donc des solutions réelles si, et seulement si $p^2 \geqslant 4ab(ab - q)$.
Si $p^2 = 4ab(ab - q)$, il y a un seul couple solution :

$$(x, y) = (p/2a, -p/2b) .$$

Si $p^2 > 4ab(ab - q)$, posons $\Delta = p^2 - 4ab(ab - q)$; il y a deux couples solutions :

$$(x, y) = \left(\frac{p + \sqrt{\Delta}}{2a}, \frac{\sqrt{\Delta} - p}{2b}\right) \quad \text{et} \quad (x, y) = \left(\frac{p - \sqrt{\Delta}}{2a}, -\frac{p + \sqrt{\Delta}}{2b}\right) .$$

Exercice 10 :

Déterminer $z \in \mathbb{C}^*$ pour que $z, \dfrac{1}{z}$ et $1 - z$ aient le même module. ■

Il est clair que z et $1/z$ ont même module si, et seulement si, $|z| = 1$.
On voit donc que $z, 1/z$ et $1 - z$ ont même module si, et seulement si, $|z| = |1 - z| = 1$. Posons $z = x + iy$, où $(x, y) \in \mathbb{R}^2$, ces conditions s'écrivent :

$$x^2 + y^2 = 1 \quad \text{et} \quad (x - 1)^2 + y^2 = 1 .$$

En remplaçant la deuxième équation par la différence des deux équations, nous obtenons les conditions équivalentes :

$$x^2 + y^2 = 1 \quad \text{et} \quad 2x - 1 = 0 .$$

Il y a donc deux solutions :

$$z = \frac{1 + i\sqrt{3}}{2} = -j^2 \quad \text{et} \quad z = \frac{1 - i\sqrt{3}}{2} = -j .$$

Ces nombres complexes sont les intersections du cercle de centre 0 et de rayon 1, avec le cercle de centre 1 et de rayon 1.

§ VI.6 *RACINES CARRÉES D'UN NOMBRE COMPLEXE*

Exercice 6 :

> Condition sur le paramètre a pour que l'équation $z + \bar{z}^2 = a$ admette une racine réelle. Si cette condition est réalisée, résoudre l'équation. ■

Le paramètre a vérifie la condition si, et seulement si, l'équation $x^2+x-a = 0$ a une solution réelle ; donc si, et seulement si, $a \in \mathbb{R}$, et $1+4a \geqslant 0$, soit $a \geqslant -1/4$.

Supposons cette condition réalisée, écrivons $z = x + \mathrm{i}y$, où $(x,y) \in \mathbb{R}^2$; comme $z^2 = x^2-y^2+2\mathrm{i}xy$, le nombre complexe z est solution de l'équation $z + \bar{z}^2 = a$ si, et seulement si, les deux équations réelles suivantes sont vérifiées :

$$x + x^2 - y^2 = a \quad \text{et} \quad y - 2xy = 0 .$$

Ce système équivaut à :

$$y = 0 \quad \text{et} \quad x^2 + x - a = 0$$

ou

$$x = \frac{1}{2} \quad \text{et} \quad y^2 = \frac{3}{4} - a .$$

Si $a \geqslant 3/4$, il n'y a que les deux solutions réelles, si $3/4 > a \geqslant -1/4$, il y en plus deux solutions non réelles.

Exercice 9 :

> Comment faut-il choisir z pour que les images des nombres z, z^2 et z^4 soient alignées ? ■

On voit que $z^2 = z$ si, et seulement si, $z = 0$ ou $z = 1$; dans ce cas les images des complexes z, z^2, z^4 sont alignées. Si $z \neq 0$ et $z \neq 1$, alors les images de z, z^2, z^4 sont alignées si, et seulement si $\dfrac{z^4 - z^2}{z^2 - z} \in \mathbb{R}$, soit si, et seulement si, $z(z+1) \in \mathbb{R}$. On voit donc que dans tous les cas les images des nombres z, z^2, z^4 sont alignées si, et seulement si, $z(z+1) \in \mathbb{R}$.

On observe que $z(z+1) = (z+1/2)^2 - 1/4$, et donc que la condition précédente s'écrit aussi $(z+1/2)^2 \in \mathbb{R}$. Les nombres complexes dont le carré est réel sont les nombres réels et les imaginaires purs. L'alignement est donc vérifié si, et seulement si, ou bien z est réel (et z, z^2, z^4 sont sur la droite réelle), ou bien $\mathrm{Re}(z) = -1/2$.

§ VI.7 *NOMBRES COMPLEXES DE MODULE 1*

Exercice 2 :

Soit des réels $a_1, a_2, \ldots, a_n$ tels que tous les $\operatorname{tg} a_k$ $(1 \leqslant k \leqslant n)$ et $\operatorname{tg}(a_1 + \ldots + a_n)$ soient définis. On pose $u_k = \operatorname{tg} a_k$. Pour $p \in [\![1, n]\!]$, soit

$$\sigma_p = \sum_{j_1 < j_2 < \ldots < j_p} u_{j_1} u_{j_2} \ldots u_{j_p} .$$

Démontrer :

$$\operatorname{tg}(a_1 + a_2 + \ldots + a_n) = \frac{\sigma_1 - \sigma_3 + \ldots + (-1)^q \sigma_{2q+1} + \ldots}{1 - \sigma_2 + \ldots + (-1)^r \sigma_{2r} + \ldots} . \blacksquare$$

On vérifie que pour $k \in [\![1, n]\!]$,

$$\frac{1 + \mathrm{i}\, u_k}{1 - \mathrm{i}\, u_k} = \frac{\cos a_k + \mathrm{i} \sin a_k}{\cos a_k - \mathrm{i} \sin a_k} = \mathrm{e}^{2\mathrm{i}\, a_k} ,$$

d'où :

$$\mathrm{e}^{2\mathrm{i}\,(a_1 + a_2 + \ldots + a_n)} = \prod_{k=1}^{n} \frac{1 + \mathrm{i}\, u_k}{1 - \mathrm{i}\, u_k} .$$

Posons $s = a_1 + a_2 + \ldots + a_n$ et $U = \operatorname{tg} s$. En utilisant la formule donnant le développement d'un produit de sommes, démontrée dans la résolution de l'exercice 9 du §III.4 (formule du crible), nous obtenons :

$$\mathrm{e}^{2\mathrm{i}\, s} = \frac{\displaystyle\sum_{p=0}^{n} \mathrm{i}^{\,p}\, \sigma_p}{\displaystyle\sum_{p=0}^{n} (-\mathrm{i})^p \sigma_p} .$$

Notons :

$$A = \sum_{r \in \mathbb{N},\, 2r \leqslant n} (-1)^r \sigma_{2r} = 1 - \sigma_2 + \ldots + (-1)^r \sigma_{2r} + \ldots$$

et

$$B = \sum_{q \in \mathbb{N},\, 2q+1 \leqslant n} (-1)^q \sigma_{2q+1} = \sigma_1 - \sigma_3 + \ldots + (-1)^q \sigma_{2q+1} + \ldots ,$$

on voit que :

$$\frac{1 + \mathrm{i}\, U}{1 - \mathrm{i}\, U} = \mathrm{e}^{2\mathrm{i}\, s} = \frac{A + \mathrm{i}\, B}{A - \mathrm{i}\, B} .$$

Cette égalité implique $(1 + \mathrm{i}\, U)(A - \mathrm{i}\, B) = (1 - \mathrm{i}\, U)(A + \mathrm{i}\, B)$, soit $B = AU$. Comme A et B ne sont pas tous les deux nuls, et que U existe, nous en déduisons $A \neq 0$ et $U = \operatorname{tg}(a_1 + \ldots + a_n) = \dfrac{B}{A}$, ce qu'il fallait

Exercice 3 :

Soit $x \in \mathbb{R}$ et $n \in \mathbb{N}^*$ tels que $\cos(2^k x) \neq 0$ pour tout $k \in [\![0, n-1]\!]$. Exprimer sous forme simple

$$S_n = \sum_{k=1}^{n} \frac{1}{2^k \cos x \cos 2x \dots \cos(2^{k-1}x)} \cdot \blacksquare$$

Cherchons à écrire le terme :

$$u_k = \frac{1}{2^k \cos x \cos 2x \dots \cos(2^{k-1}x)} ,$$

pour $k \geqslant 2$, sous la forme :

$$u_k = \frac{a_{k-1}}{2^{k-1} \cos x \cos 2x \dots \cos(2^{k-2}x)} - \frac{a_k}{2^k \cos x \cos 2x \dots \cos(2^{k-1}x)} ;$$

on voit qu'il suffit que $2\cos(2^{k-1}x)\, a_{k-1} - a_k = 1$.

Cette condition est satisfaite si on pose pour tout $h \geqslant 1$, $a_h = \cos(2^h x)$. On vérifie aussi que :

$$u_1 = \frac{1}{2\cos x} = \frac{2\cos^2 x - \cos 2x}{2\cos x} = \cos x - \frac{a_1}{2\cos x} .$$

Nous en déduisons que pour tout $n \in \mathbb{N}^*$:

$$S_n = \left(\cos x - \frac{a_1}{2\cos x}\right) + \left(\frac{a_1}{2\cos x} - \frac{a_2}{2^2 \cos x \cos 2x}\right) + \dots +$$
$$+ \left(\frac{a_{n-1}}{2^{n-1} \cos x \cos 2x \dots \cos(2^{n-2}x)} - \frac{a_n}{2^n \cos x \cos 2x \dots \cos(2^{n-1}x)}\right) ,$$

d'où :

$$S_n = \cos x - \frac{\cos(2^n x)}{2^n \cos x \cos 2x \dots \cos(2^{n-1}x)} .$$

Exercice 8 :

Exprimer simplement $S_n = \sum_{k=1}^{n} \frac{1}{\cos kx \cos(k+1)x} \cdot \blacksquare$

On suppose ici que pour tout $k \in [\![1, n+1]\!]$, $\cos kx \neq 0$. On vérifie que pour tout $k \in [\![1, n]\!]$:

$$\operatorname{tg}(k+1)x - \operatorname{tg} kx = \frac{\sin(k+1)x}{\cos(k+1)x} - \frac{\sin kx}{\cos kx} = \frac{\sin x}{\cos(k+1)x}$$

Nous en déduisons que :

$$S_n \sin x = (\mathrm{tg}2x - \mathrm{tg}\, x) + \ldots + (\mathrm{tg}(n+1)x - \mathrm{tg}\, nx) = \mathrm{tg}(n+1)x - \mathrm{tg}\, x \ .$$

Si $\sin x \neq 0$, nous obtenons :

$$S_n = \frac{\mathrm{tg}\,(n+1)x - \mathrm{tg}\, x}{\sin x} \ .$$

Si $\sin x = 0$, pour tout $h \in \mathbb{Z}$, $\sin hx = 0$, d'où pour tout $k \in \mathbb{N}$:

$$\cos x = \cos(k+1)x \cos kx + \sin(k+1)x \sin kx = \cos(k+1)x \cos kx \ ;$$

dans ce cas nous obtenons :

$$S_n = \frac{n}{\cos x} \ .$$

Exercice 9 :

Prouver que $1 + \dfrac{1}{\cos 2x} = \dfrac{\mathrm{tg}\, 2x}{\mathrm{tg}\, x}$ et en déduire une expression de :

$$P_n = \prod_{k=0}^{n} \left(1 + \frac{1}{\cos(2^k x)}\right) . \blacksquare$$

On voit que pour tout $y \in \mathbb{R}$ tel que $\cos y \neq 0$, $\sin y \neq 0$, et $\cos 2y \neq 0$:

$$1 + \frac{1}{\cos 2y} = \frac{2\cos^2 y}{\cos 2y} = \frac{2 \cos y \sin y \ \cos y}{\cos 2y \ \sin y} = \frac{\mathrm{tg}2y}{\mathrm{tg}\, y} \ .$$

Nous supposerons que pour tout $k \in [\![0, n]\!]$, $\cos(2^k x) \neq 0$.
Si $\cos(x/2) = 0$, alors $\cos x = -1$, donc $P_n = 0$.
Si $\sin(x/2) = 0$, alors on voit que pour tout $k \in [\![0, n]\!]$, $\cos(2^k x) = 1$, et donc que $P_n = 2^{n+1}$.
Supposons que $\cos(x/2) \neq 0$ et $\sin(x/2) \neq 0$; on voit que pour tout $k \in [\![0, n]\!]$, $\sin(2^k x) \neq 0$ (puisque $\sin(2^k x) = 2\sin(2^{k-1}x)\cos(2^{k-1}x)$). En utilisant la formule démontrée ci-dessus, nous obtenons :

$$P_n = \frac{\mathrm{tg}\, x}{\mathrm{tg}(x/2)} \frac{\mathrm{tg}\, 2x}{\mathrm{tg}\, x} \cdots \frac{\mathrm{tg}\, 2^n x}{\mathrm{tg}\, 2^{n-1} x} = \frac{\mathrm{tg}\, 2^n x}{\mathrm{tg}(x/2)} \ .$$

§ VI.8 *ARGUMENTS D'UN NOMBRE COMPLEXE; RACINES n-ièmes*

Exercice 11 :

Trouver 3 nombres de module 1 dont la somme et le produit sont égaux à 1 . ■

Cherchons une condition nécessaire.
Puisque ces nombres complexes z_1, z_2, z_3 sont de module 1 :

$$1 = \overline{z_1} + \overline{z_2} + \overline{z_3} = \frac{1}{z_1} + \frac{1}{z_2} + \frac{1}{z_3} = \frac{z_2\,z_3 + z_1\,z_3 + z_1\,z_2}{z_1\,z_2\,z_3} \ .$$

Nous en déduisons :

$$z_1 + z_2 + z_3 = 1$$
$$z_2\,z_3 + z_1\,z_3 + z_1\,z_2 = 1$$
$$z_1\,z_2\,z_3 = 1 \ ,$$

d'où :

$$(\mathrm{X} - z_1)(\mathrm{X} - z_2)(\mathrm{X} - z_3) = \mathrm{X}^3 - \mathrm{X}^2 + \mathrm{X} - 1 = (\mathrm{X} - 1)(\mathrm{X}^2 + 1) \ .$$

On voit donc qu'à l'ordre près, $(z_1, z_2, z_3) = (1, \mathrm{i}, -\mathrm{i})$.

Les trois nombres complexes 1 , i et $-\mathrm{i}$, conviennent puisqu'ils sont de module 1, que $1 + \mathrm{i} - \mathrm{i} = 1$, et que $1 \cdot \mathrm{i} \cdot (-\mathrm{i}) = 1$. Le triplet $(1, \mathrm{i}, -\mathrm{i})$ est donc, à l'ordre près, la seule solution. Il y a donc en tout 6 solutions.

Exercice 12 :

Résoudre le système à deux inconnues *réelles* :
$x^6 - 15\,x^4y^2 + 15\,x^2y^4 - y^6 = 1$ et $3\,x^5y - 10\,x^3y^3 + 3\,xy^5 = 0$.
■

Comme x et y sont des inconnues réelles, nous pouvons écrire ce système sous la forme équivalente :

$$(x^6 - 15\,x^4y^2 + 15\,x^2y^4 - y^6) + 2\mathrm{i}\,(3\,x^5y - 10\,x^3y^3 + 3\,xy^5) = 1 \ ,$$

soit encore :

$$x^6 + 6\,x^5(\mathrm{i}\,y) + 15\,x^4\,(\mathrm{i}\,y)^2 + 20\,x^3(\mathrm{i}\,y)^3 + 15\,x^2(\mathrm{i}\,y)^4 + 6\,x(\mathrm{i}\,y)^5 + (\mathrm{i}\,y)^6 = 1 \ .$$

Le système est donc équivalent à l'équation $(x + \mathrm{i}\,y)^6 = 1$. Les solutions sont donc les couples (x_k, y_k) , pour $k \in [\![0, 5]\!]$, où :

$$x_k = \cos\left(\frac{k\,\pi}{3}\right) \quad \text{et} \quad y_k = \sin\left(\frac{k\,\pi}{3}\right) \ .$$

Exercice 13 :

Résoudre le système à deux inconnues *complexes* : $(1+t)^n = (1-t)^n$ et $z^2+t^2=1$, où $n \in \mathbb{N}^*$ est donné. ■

Résolvons d'abord l'équation $(1+t)^n = (1-t)^n$, où $t \in \mathbb{C}$. Il est clair que le complexe t vérifie cette condition si, et seulement si, il existe un nombre complexe u tel que $u^n = 1$ et $1+t = u(1-t)$, donc si, et seulement si, il existe $k \in [\![0, n-1]\!]$, tel que :

$$1+t = \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}}(1-t) \quad \text{soit} \quad (1+\mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}})t = \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}} - 1 \ ,$$

soit enfin : $t\cos(\frac{k\pi}{n}) = \mathrm{i}\sin(\frac{k\pi}{n})$.

Si n est impair, pour tout $k \in [\![0, n-1]\!]$, $\cos(\frac{k\pi}{n}) \neq 0$, et l'équation a n solutions : les nombres $\mathrm{i}\,\mathrm{tg}\left(\frac{k\pi}{n}\right)$, où $k \in [\![0, n-1]\!]$.
Si n est pair, $n = 2p$, il n'y a pas de solution correspondant à la valeur $k = p$, car $\cos(\frac{p\pi}{n}) = 0$ et $\sin(\frac{p\pi}{n}) \neq 0$; mais à tout $k \in [\![0, n-1]\!] \setminus \{p\}$, correspond la solution $\mathrm{i}\,\mathrm{tg}\left(\frac{k\pi}{n}\right)$; il y a donc dans ce cas $n-1$ solutions.

Pour tout t donné solution de l'équation, donc de la forme $\mathrm{i}\,\mathrm{tg}\left(\frac{k\pi}{n}\right)$ où $k \in [\![0, n-1]\!] \setminus \{n/2\}$, z vérifie la deuxième équation si, et seulement si $z^2 = 1 - t^2 = 1 + \mathrm{tg}^2(\frac{k\pi}{n}) = \dfrac{1}{\cos^2(\frac{k\pi}{n})}$, donc si, et seulement si $z = \dfrac{1}{\cos(\frac{k\pi}{n})}$ ou $z = -\dfrac{1}{\cos(\frac{k\pi}{n})}$.

Exercice 18 :

Si G est un groupe, on note $\widehat{G}$ l'ensemble des homomorphismes de groupes $G \to \mathbb{U}$, muni de sa structure naturelle de groupe. Ce groupe est dit groupe des *caractères* du groupe G.
Pour chaque $\lambda \in \mathbb{R}$, on considère l'élément f_λ de $\widehat{\mathbb{Q}}$, groupe des caractères du groupe additif $\mathbb{Q}$, défini par :

$$(\forall x \in \mathbb{Q})\ f_\lambda(x) = \exp(\mathrm{i}\lambda x) .$$

Etudier cet homomorphisme du groupe $(\mathbb{R}, +)$ dans le groupe $\widehat{\mathbb{Q}}$. ■

a) Montrons que l'homomorphisme de groupes $\lambda \mapsto f_\lambda$, $\varphi : \mathbb{R} \to \widehat{\mathbb{Q}}$, est injectif.

Soit $\lambda \in \mathbb{R}$ tel que $f_\lambda = 1$, c'est-à-dire tel que pour tout rationnel r, $\exp(\mathrm{i}\lambda r) = 1$. Cette égalité est vérifiée en particulier pour

$\lambda \in 2\pi\mathbb{Z}$, nous poserons $\lambda = 2k\pi$, où $k \in \mathbb{Z}$; mais elle est aussi vérifiée pour tout rationnel de la forme $1/n$, où $n \in \mathbb{N}^*$, donc $2k\pi/n \in 2\pi\mathbb{Z}$, soit $n \mid k$. L'entier k est par conséquent divisible par tout entier $n > 0$; il est clair que cela n'est possible que si $k = 0$. Nous avons démontré que le noyau de l'homomorphisme de groupes $\lambda \mapsto f_\lambda$ est réduit à $\{0\}$, cet homomorphisme est donc injectif.

b) Montrons maintenant que l'homomorphisme $\lambda \mapsto f_\lambda$, $\varphi : \mathbb{R} \to \widehat{\mathbb{Q}}$ n'est pas surjectif.

Un caractère étrange, φ.
Soit $B = \{r \in \mathbb{Q} \mid \exists k \in \mathbb{N}\ 2^k r \in \mathbb{Z}\}$, c'est-à-dire l'ensemble des rationnels 2-adiques. La partie B de $\mathbb{Q}$ est un sous-groupe additif du groupe $\mathbb{Q}$. Posons pour $b \in B$:

$$\varphi(b) = \prod_{k=0}^{\infty} \exp\left(2\pi \mathrm{i}\, 2^k b\right) \ ;$$

pour $b \in B$ donné, pour k assez grand $2^k b \in \mathbb{Z}$, donc $\exp\left(2\pi \mathrm{i}\, 2^k b\right) = 1$; le produit est donc en fait fini. On voit facilement que $\varphi : B \to \mathbb{U}$ est un homomorphisme de groupes, donc un élément de $\widehat{B}$. Mais il n'est pas évident qu'on puisse étendre cet homomorphisme de groupes défini sur B, en un homomorphisme de groupes défini sur $\mathbb{Q}$ (à la différence de ce qui se passe dans les espaces vectoriels). Observons que $\mathbb{Z} \subset \mathrm{Ker}\,(\varphi)$; on peut donc factoriser l'homomorphisme φ pour obtenir un homomorphisme $\widetilde{\varphi} : B/\mathbb{Z} \to \mathbb{U}$.

Un supplémentaire de $B/\mathbb{Z}$ dans $\mathbb{Q}/\mathbb{Z}$.
Soit A l'ensemble des rationnels qui peuvent s'écrire avec un dénominateur impair. Il est clair qu'il s'agit d'un sous-groupe additif de $\mathbb{Q}$ qui contient le sous-groupe $\mathbb{Z}$. Soit $r = p/q$ un rationnel, où $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$, posons $q = 2^k q_1$, où $k \in \mathbb{N}$ et q_1 est un entier impair ; comme q_1 et 2^k sont premiers entre eux, il existe $(u, v) \in \mathbb{Z}^2$ tels que $u2^k + vq_1 = 1$; nous voyons alors que :

$$r = \frac{p}{q} = \frac{u\,2^k p + v\,q_1 p}{2^k q_1} = \frac{up}{q_1} + \frac{vp}{2^k} \in A + B \ .$$

Nous en déduisons $A + B = \mathbb{Q}$, mais la somme n'est pas directe car ces sous-groupes contiennent tous les deux $\mathbb{Z}$. Plus précisément, supposons $r \in A \cap B$, le dénominateur de l'écriture irréductible de ce rationnel doit être impair et aussi une puissance de 2 : ce ne peut être que 1 ; nous en déduisons $A \cap B = \mathbb{Z}$. Il est alors clair que :

$$\mathbb{Q}/\mathbb{Z} = A/\mathbb{Z} \oplus B/\mathbb{Z} \ .$$

Notons p_B la projection sur $B/\mathbb{Z}$ dans cette somme directe (c'est un homomorphisme de groupes).

L'extension de φ à $\mathbb{Q}$.
Considérons maintenant l'homomorphisme de groupes $\psi = \overline{\varphi} \circ p_B \circ \pi$ (π est l'homomorphisme canonique $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$), du groupe additif $\mathbb{Q}$ vers le groupe multiplicatif $\mathbb{U}$. L'homomorphisme ψ est un élément de $\widehat{\mathbb{Q}}$. Si $b \in B$, comme $\pi(b) \in B/\mathbb{Z}$, $p_B(\pi(b)) = \pi(b)$, donc $\psi(b) = \varphi(b)$; l'homomorphisme ψ est donc une extension à $\mathbb{Q}$ de l'homomorphisme φ défini sur le sous-groupe B. Remarquons que $\mathbb{Z} \subset \mathrm{Ker}\,(\psi)$.

Conclusion.
Supposons qu'il existe un réel λ tel que $\psi = f_\lambda$, c'est-à-dire tel que pour tout rationnel r, $\psi(r) = \exp(\mathrm{i}\lambda r)$; en particulier, pour $r = 1$, donc il existe un entier n tel que $\lambda = 2\pi n$. Mais c'est vrai aussi pour tous les nombres binaires 2^{-p}, où $p \in \mathbb{N}$; donc pour tout $p \in \mathbb{N}$:

$$\exp\left(\frac{2\pi \mathrm{i}\, n}{2^p}\right) = \prod_{k=0}^{\infty} \exp\left(\frac{2\pi \mathrm{i}\, 2^k}{2^p}\right) = \exp\left(2\pi \mathrm{i}\, 2^{-p} \sum_{k=0}^{p-1} 2^k\right) .$$

Nous en déduisons que pour tout $p \in \mathbb{N}$, $n \equiv 1+2+2^2+\ldots+2^{p-1} \mod (2^p)$.
Cela est évidemment impossible, car l'écriture binaire du nombre n ne pourrait pas être finie.
L'homomorphisme $\lambda \mapsto f_\lambda$ n'est donc pas surjectif.

Exercice 19 :

> Montrer que les groupes abéliens $\widehat{\mathbb{Q}_+^*}$ et $(\mathbb{R}/2\pi\mathbb{Z})^{\mathbb{N}}$ sont isomorphes. ■

Montrons d'abord que les groupes $\mathbb{Q}_+^*$ et $\mathbb{Z}^{(\mathbb{N})}$ sont isomorphes.
Notons $(p_i)_{i\in\mathbb{N}}$ la suite croissante des nombres premiers. A une suite $(n_i)_{i\in\mathbb{N}}$ d'entiers relatifs telle que l'ensemble $\{i \in \mathbb{N} \mid n_i \neq 0\}$ soit fini, faisons correspondre le rationnel > 0 :

$$\Phi\left((n_i)_{i\in\mathbb{N}}\right) = \prod_{i\in\mathbb{N}} p_i^{n_i} ,$$

ce qui a bien un sens car le produit est fini. Il est clair que l'application Φ ainsi définie est un homomorphisme de groupes. Cet homomorphisme est surjectif, car son image est un sous-groupe qui contient les entiers > 0 (existence d'une décomposition en produit de facteurs premiers pour les entiers > 0), donc tous les quotients d'entiers > 0. Montrons qu'il est injectif. Si $(n_i)_{i\in\mathbb{N}} \in \mathrm{Ker}\,(\Phi)$, notons $I = \{i \in \mathbb{N} \mid n_i > 0\}$, et $J = \{i \in \mathbb{N} \mid n_i < 0\}$, ensembles tous les deux finis. On voit que :

$$\prod_{i\in I} p_i^{n_i} = \prod_{j\in J} p_j^{-n_j} .$$

Comme I et J sont disjoints, ce n'est possible que si $I = J = \emptyset$; nous en déduisons que la suite $(n_i)_{i\in\mathbb{N}}$ est nécessairement nulle. Le noyau de Φ est réduit à $\{0\}$, l'homomorphisme Φ est donc injectif. A tout rationnel r on peut donc, par l'homomorphisme réciproque, faire correspondre une suite élément de $\mathbb{Z}^{(\mathbb{N})}$. Nous noterons :

$$r = \prod_{i\in\mathbb{N}} p_i^{\nu_i(r)} .$$

Remarquons que pour tout $i \in \mathbb{N}$ et pour tous rationnels $r > 0$ et $r' > 0$, $\nu_i(r + r') = \nu_i(r) + \nu_i(r')$.

Soit Θ l'application qui à un caractère φ du groupe $\mathbb{Q}_+^*$ fait correspondre la suite $\varphi(p_i)_{i\in\mathbb{N}}$ élément de $\mathbb{U}^{\mathbb{N}}$; c'est un homomorphisme du groupe $\widehat{\mathbb{Q}_+^*}$ vers le groupe $\mathbb{U}^{\mathbb{N}}$ puisque pour tout $i \in \mathbb{N}$, et pour tous caractères φ et ψ, on a par définition : $(\varphi \times \psi)(p_i) = \varphi(p_i)\,\psi(p_i)$.
Si pour tout $i \in \mathbb{N}$, $\varphi(p_i) = 1$, alors pour tout rationnel $r > 0$:

$$\varphi(r) = \varphi\left(\prod_{i\in\mathbb{N}} p_i^{\nu_i(r)}\right) = \prod_{i\in\mathbb{N}} (\varphi(p_i))^{\nu_i(r)} = 1 .$$

L'homomorphisme Θ est donc injectif.
Soit $(u_i)_{i\in\mathbb{N}}$ une suite d'éléments de $\mathbb{U}$, définissons le caractère φ en posant :

$$\varphi(r) = \prod_{i\in\mathbb{N}} u_i^{\nu_i(r)} ,$$

ce qui a bien un sens car $\{i \in \mathbb{N} \mid \nu_i(r) \neq 0\}$ est fini. C'est bien un homomorphisme de groupes car pour tout $i \in \mathbb{N}$, et tous rationnels r et r', $\nu_i(r + r') = \nu_i(r) + \nu_i(r')$; on vérifie facilement que pour tout $j \in \mathbb{N}$, $\varphi(p_j) = u_j$. L'homomorphisme Θ est donc surjectif.

Les groupes $\widehat{\mathbb{Q}_+^*}$ et $\mathbb{U}^{\mathbb{N}}$ sont donc isomorphes. Comme les groupes $\mathbb{R}/_{2\pi\mathbb{Z}}$ et $\mathbb{U}$ sont isomorphes, on voit que les groupes $\widehat{\mathbb{Q}_+^*}$ et $\left(\mathbb{R}/_{2\pi\mathbb{Z}}\right)^{\mathbb{N}}$ sont isomorphes, ce qu'il fallait démontrer.

§ VI.9 *NOMBRES COMPLEXES ET GÉOMÉTRIE*

Exercice 4 :

Soit l'équation $z^2 - 2z\,e^{i\theta} + 1 = 0$ où θ est un paramètre réel, et où l'inconnue est $z \in \mathbb{C}$. Résoudre cette équation. Quel est le lieu géométrique des racines dans le plan d'Ar

lorsque θ décrit $\mathbb{R}$? ■

L'équation s'écrit $(z-\mathrm{e}^{\mathrm{i}\,\theta})^2 = e^{2\,\mathrm{i}\,\theta} - 1 = 2\mathrm{i}\,e^{\mathrm{i}\,\theta}\sin(\theta) = 2e^{\mathrm{i}\,(\theta+\pi/2)}\sin(\theta)$.
Si $\sin(\theta) \geqslant 0$, les solutions sont $z = \mathrm{e}^{\mathrm{i}\,\theta} \pm \sqrt{2}\mathrm{e}^{\mathrm{i}\,\pi/4}\mathrm{e}^{\mathrm{i}\,\theta/2}\sqrt{\sin(\theta)}$ soit encore $z = \mathrm{e}^{\mathrm{i}\,\theta} \pm (1+\mathrm{i}\,)\mathrm{e}^{\mathrm{i}\,\theta/2}\sqrt{\sin(\theta)}$.
Si $\sin(\theta) < 0$, les solutions sont $z = \mathrm{e}^{\mathrm{i}\,\theta} \pm \sqrt{2}\mathrm{e}^{-\mathrm{i}\,\pi/4}\mathrm{e}^{\mathrm{i}\,\theta/2}\sqrt{-\sin(\theta)}$ soit encore $z = \mathrm{e}^{\mathrm{i}\,\theta} \pm (1-\mathrm{i}\,)\mathrm{e}^{\mathrm{i}\,\theta/2}\sqrt{-\sin(\theta)}$.

Un nombre complexe z est dans l'ensemble des racines si, et seulement si, il existe un réel θ tel que $z^2 - 2\,z\,\mathrm{e}^{\mathrm{i}\,\theta} + 1 = 0$, ce qui est équivalent à la condition $z \neq 0$ et $\left|\frac{z^2+1}{2\,z}\right| = 1$. Cette condition s'écrit encore $\left|z^2+1\right| = 2\,|z|$. Posons $z = x + \mathrm{i}\,y$, où x et y sont réels. D'après ce qui précède, le lieu géométrique des solutions est l'ensemble des points dont les coordonnées (x, y) vérifient la condition :

$$(x^2 - y^2 + 1)^2 + 4\,x^2\,y^2 = 4(x^2 + y^2)\ ,$$

soit après développement et simplification :

$$(x^2 + y^2)^2 + 1 - 2x^2 - 6y^2 = 0\ .$$

Or :

$$\begin{aligned}(x^2 + y^2)^2 + 1 - 2x^2 - 6y^2 &= (x^2 + y^2)^2 - 2\,(x^2 + y^2) + 1 - 4\,y^2 = \\ &= (x^2 + y^2 - 1)^2 - 4\,y^2 = (x^2 + y^2 - 2\,y - 1)\,(x^2 + y^2 + 2\,y - 1) = \\ &= \left(x^2 + (y-1)^2 - 2\right)\left(x^2 + (y+1)^2 - 2\right)\ .\end{aligned}$$

Le lieu géométrique des racines est donc la réunion du cercle de centre i et de rayon $\sqrt{2}$ et du cercle de centre $-\mathrm{i}$ et de rayon $\sqrt{2}$. Ces deux cercles se coupent aux points d'affixes 1 et -1.

Exercice 5 :

Soit a, b, c trois points non alignés dans $\mathbb{C}$. Calculer en fonction de a, b, c le centre du cercle circonscrit, l'orthocentre, le centre du cercle inscrit, et les centres des cercles exinscrits au triangle a, b, c. ■

Détermination du centre du cercle circonscrit.
Le complexe z est sur la médiatrice de (a, b) si, et seulement si :

$$|z-a|^2 = |z-b|^2\ , \quad \text{soit} \quad z\,\bar{z} - \bar{a}\,z - a\,\bar{z} + a\,\bar{a} = z\,\bar{z} - \bar{b}\,z - b\,\bar{z} + b\,\bar{b}\ .$$

Cette condition s'écrit aussi :

$$(1) \qquad (\bar{b} - \bar{a})\,z + (b-a)\,\bar{z} = b\,\bar{b} - a\,\bar{a}\ .$$

De manière analogue, le complexe z se trouve sur la médiatrice de (a,c) si, et seulement si :

$$(2) \qquad (\bar{c}-\bar{a})\,z+(c-a)\,\bar{z}=c\,\bar{c}-a\,\bar{a}\ .$$

Comme les points (a,b,c) ne sont pas alignés, la médiatrice de (a,b) et la médiatrice de (a,c) se coupent en un seul point z_0, centre du cercle circonscrit, qu'on obtient en multipliant l'équation (1) par $(c-a)$, l'équation (2) par $(b-a)$, et en faisant la différence :

$$z_0=\frac{(c-a)(b\,\bar{b}-a\,\bar{a})-(b-a)(c\,\bar{c}-a\,\bar{a})}{(c-a)(\bar{b}-\bar{a})-(b-a)(\bar{c}-\bar{a})}\ .$$

En développant nous obtenons l'expression suivante :

$$z_0=\frac{(b-c)\,a\,\bar{a}+(c-a)\,b\,\bar{b}+(a-b)\,c\,\bar{c}}{(\bar{b}\,c-\bar{c}\,b)+(\bar{c}\,a-\bar{a}\,c)+(\bar{a}\,b-\bar{b}\,a)}\ .$$

Dans cette expression, le numérateur et le dénominateur sont invariants par les cycles d'ordre 3 sur les lettres a,b,c, et sont transformés en leurs opposés par transposition de deux lettres. On retrouve bien sûr l'invariance par permutation sur a,b,c, du centre du cercle circonscrit.

Détermination de l'orthocentre.
Nous pouvons utiliser ici la formule $\overrightarrow{OH}=3\overrightarrow{OG}$, où O est le centre du cercle circonscrit, H l'orthocentre et G l'isobarycentre d'un triangle. L'orthocentre H affecté du coefficient 1, est donc le barycentre de $(O,-2)$, $(G,3)$. Nous obtenons par conséquent :

$$z_H=-2\,z_O+3\,\frac{a+b+c}{3}=a+b+c-2\,z_0\ .$$

Détermination des centres des cercles inscrits et exinscrits.
Notons $l_a=|b-c|$, $l_b=|c-a|$ et $l_c=|a-b|$ les longueurs des côtés du triangle. Nous savons que si I est le centre du cercle inscrit, $(I,l_a+l_b+l_c)$ est barycentre de (a,l_a), (b,l_b), (c,l_c). Nous obtenons donc ;

$$z_I=\frac{|b-c|\ a+|c-a|\ b+|a-b|\ c}{|b-c|+|c-a|+|a-b|}\ .$$

Si J est le centre du cercle exinscrit qui est sur la bissectrice intérieure en a, alors $(I,-l_a+l_b+l_c)$ est barycentre de $(a,-l_a)$, (b,l_b), (c,l_c). Nous obtenons donc :

$$z_J=\frac{-|b-c|\ a+|c-a|\ b+|a-b|\ c}{|c-a|+|a-b|-|b-c|}\ .$$

On obtient de manière analogue les affixes des centres des deux autres cercles exinscrits.

§ VI.10 *NOMBRES COMPLEXES ET SIMILITUDES*

Exercice 1 :

Quels sont les sous-groupes finis du groupe $\mathcal{S}_+$? du groupe $\mathcal{S}$?
■

Montrons le lemme suivant :

Lemme :

Soit E un espace affine sur le corps K de caractéristique 0. Si G est un sous-groupe fini du groupe affine de E, G a un point fixe, c'est-à-dire il existe $M_0 \in E$ tel que pour tout $g \in G$, $g(M_0) = M_0$. ■

Soit $M \in E$, posons :

$$M_0 = \frac{1}{n} \sum_{g \in G} g(M) \ ,$$

où $n = \text{card}\,(G)$; M_0 est donc l'isobarycentre des images de M par les éléments du groupe G. Si $\gamma \in G$, cette application affine conserve le barycentre, donc :

$$\gamma(M_0) = \frac{1}{n} \sum_{g \in G} \gamma \circ g(M) \ .$$

Comme $\gamma \circ g$ décrit G quand g décrit G, nous voyons que :

$$\gamma(M_0) = \frac{1}{n} \sum_{g' \in G} g'(M) = M_0 \ .$$

Le point M_0 est donc invariant par tous les éléments du groupe fini G.

Remarquons que l'application $g \mapsto \vec{g}$, $G \to \text{GL}(\vec{E})$ est alors un homomorphisme injectif de groupes. Le groupe G est donc isomorphe à un sous-groupe fini du groupe $\text{GL}(\vec{E})$. Fin du lemme.

Si G est un sous-groupe fini du groupe $\mathcal{S}_+$, il existe d'après le lemme un complexe z_0 tel que pour tout $s \in G$, $s(z_0) = z_0$. L'application $g \mapsto \vec{g}$, induit un isomorphisme entre G et un sous-groupe fini du groupe $\vec{\mathcal{S}}_+$, lui-même isomorphe au groupe $(\mathbb{C}^*, \times)$. On sait qu'un sous-groupe fini du groupe $(\mathbb{C}^*, \times)$ est cyclique, engendré par le complexe $\exp(2\,i$

est le cardinal du groupe. Si $n = \mathrm{card}\,(G)$, et que z_0 est point fixe pour G, le groupe G est nécessairement le sous-groupe engendré par l'isométrie directe :

$$r_{z_0,n} : z \mapsto z_0 + \exp(2\pi\,\mathrm{i}/n)(z - z_0) .$$

Nous pouvons remarquer que si G_0, de point fixe z_0 et G_1 de point fixe z_1 sont des sous-groupes finis de $\mathcal{S}_+$ même cardinal n, alors il sont conjugués ; en effet si T est la translation $T(z) = z - z_0 + z_1$ (pour $z \in \mathbb{C}$), on vérifie que pour tout $z \in \mathbb{C}$:

$$\begin{aligned} r_{z_1,n} \circ T(z) &= z_1 + \exp(2\pi\,\mathrm{i}/n)(z - z_0 + z_1 - z_1) = \\ &= z_1 - z_0 + z_0 + \exp(2\pi\,\mathrm{i}/n)(z - z_0) = T \circ r_{z_0,n}(z) . \end{aligned}$$

Remarquons qu'il existe des sous-groupes finis de $\mathcal{S}$, par exemple, pour tout $n \in \mathbb{N}^*$ le sous-groupe engendré par $r_{0,n}$ et la conjugaison c (cf. §V.2 exercice 6*c*)). Nous noterons G_n ce groupe (de cardinal $2n$). Nous allons démontrer que tout sous-groupe fini de $\mathcal{S}$ qui contient au moins une similitude indirecte est conjugué, dans le groupe $\mathcal{S}$, de l'un de ces sous-groupes.

Soit G un sous-groupe fini du groupe $\mathcal{S}$ qui contient au moins une similitude indirecte S. D'après le lemme, il existe un complexe z_0 invariant par tous les éléments de G. Nous pouvons appliquer ce qui a été dit ci-dessus au groupe $G \cap \mathcal{S}_+$. Si $n = \mathrm{card}\,(G \cap \mathcal{S}_+)$, le groupe $G \cap \mathcal{S}_+$ est le sous-groupe engendré par l'isométrie directe $r_{z_0,n}$. Comme S^2 est un élément de ce groupe, c'est une isométrie directe, donc si $\lambda > 0$ est le rapport réel de la similitude S, $\lambda^2 = 1$, donc $\lambda = 1$, et puisque S a un point fixe, c'est une symétrie orthogonale par rapport à une droite D (Théorème VI.10.7). Si S' est une autre similitude indirecte élément de G, alors $S^{-1} \circ S' \in G \cap \mathcal{S}_+$, donc $S' \in \{S\} \circ (G \cap \mathcal{S}_+)$; comme $\{S\} \circ (G \cap \mathcal{S}_+) \subset G$, on voit que le groupe G est la réunion du sous-groupe $G \cap \mathcal{S}_+$ engendré par $r_{z_0,n}$, et de l'ensemble $\{S\} \circ (G \cap \mathcal{S}_+)$ composé de n symétries orthogonales par rapport à des droites. Ces droites forment un faisceau régulier, en effet, si la droite D est dirigée par le complexe $\exp(\mathrm{i}\theta/2)$, alors pour tout $z \in \mathbb{C}$, $S(z) = z_0 + \exp(\mathrm{i}\theta)(\overline{z - z_0})$. Les autres similitudes indirectes du groupe sont les similitudes $z \mapsto z_0 + \exp\mathrm{i}(\theta - 2k\pi/n)(\overline{z - z_0})$, où $k \in [\![0, n-1]\!]$, ce sont donc les symétries par rapport aux droites passant par z_0 et dirigées par les nombres complexes $\exp\mathrm{i}(\theta/2 - k\pi/n)$, où $k \in [\![0, n-1]\!]$.

Considérons la similitude $f : z \mapsto z_0 + \exp(\mathrm{i}\theta/2)\,z$. En notant toujours c la conjugaison dans $\mathbb{C}$, on voit que $f^{-1} \circ S \circ f = c$ et que $f^{-1} \circ r_{z_0,n} \circ f = r_{0,n}$. Les sous-groupes G et $G_{0,n}$ sont donc conjugués dans le groupe $\mathcal{S}$.

Exercice 2 :

‖ On note $\mathcal{T}$ le groupe des translations de $\mathbb{C}$.

a) Montrer que si G est un sous-groupe de $\mathcal{S}_+$ tel que $G \cap \mathcal{T} = \{\mathrm{Id}_{\mathbb{C}}\}$, alors G est abélien.

b) Si G est un sous-groupe de $\mathcal{S}$, on note G_{z_0} le *stabilisateur* de z_0 dans G (c'est-à-dire $G_{z_0} = \{f \in G \mid f(z_0) = z_0\}$). Vérifier que $(\mathcal{S}_+)_{z_0}$ est isomorphe à $\overrightarrow{\mathcal{S}}_+$, et que $\mathcal{S}_{z_0}$ est isomorphe à $\overrightarrow{\mathcal{S}}$, pour tout $z_0 \in \mathbb{C}$.

c) Si G est un *sous-groupe abélien* du groupe $\mathcal{S}_+$, prouver qu'il existe $z_0 \in \mathbb{C}$ tel que $G \subset (\mathcal{S}_+)_{z_0}$, ou bien que $G \subset \mathcal{T}$.

d) Chercher les couples d'isométries de $\mathbb{C}$ *permutables*. En déduire les sous-groupes abéliens de $\mathrm{Is}(\mathbb{C})$, puis de $\mathcal{S}$. ■

a) Remarquons que le groupe $\overrightarrow{\mathcal{S}}_+$, qui est isomorphe au groupe $(\mathbb{C}^*, \times)$, est abélien. Soient f et g deux éléments de G, comme $\overrightarrow{f \circ g \circ f^{-1} \circ g^{-1}} = \overrightarrow{f} \circ \overrightarrow{g} \circ \overrightarrow{f}^{-1} \circ \overrightarrow{g}^{-1} = \mathrm{Id}_{\mathbb{C}}$, la similitude directe $f \circ g \circ f^{-1} \circ g^{-1}$ est une translation ; c'est donc un élément de $G \cap \mathcal{T} = \{\mathrm{Id}_{\mathbb{C}}\}$. Nous en déduisons que $f \circ g \circ f^{-1} \circ g^{-1} = \mathrm{Id}_{\mathbb{C}}$, et donc que $f \circ g = g \circ f$. Le sous-groupe G est donc abélien.

b) De manière générale, la restriction à G_{z_0} de l'homomorphisme de groupes $g \mapsto \overrightarrow{g}$, $\mathcal{S} \to \overrightarrow{\mathcal{S}}$, est un homomorphisme injectif. Le groupe G_{z_0} est donc toujours isomorphe à un sous-groupe du groupe $\overrightarrow{G}$. Nous devons démontrer que dans le cas où $G = \mathcal{S}$, ou $G = \mathcal{S}_+$, cet homomorphisme est surjectif. Or l'application $z \mapsto u\,z$, où $u \in \mathbb{C}^*$, est l'application linéaire associée à la similitude $z \mapsto z_0 + u(z - z_0)$ qui laisse z_0 invariant, et l'application $z \mapsto \bar{z}$ est l'application linéaire associée à la similitude indirecte $z \mapsto z_0 + \overline{z - z_0}$ qui laisse aussi z_0 invariant. Si $G = \mathcal{S}_+$, le sous-groupe image de G_{z_0} par $g \mapsto \overrightarrow{g}$ est donc bien $\overrightarrow{\mathcal{S}}_+$, et si $G = \mathcal{S}$, le sous-groupe image de G_{z_0} est bien $\overrightarrow{\mathcal{S}}$.

c) Montrons que si deux endomorphismes f et g d'un ensemble X commutent, l'ensemble des points fixes de l'un est stable par l'autre. En effet si $x \in X$ est tel que $f(x) = x$, alors $g(x) = g(f(x)) = f(g(x))$, donc $g(x)$ est aussi point fixe de f. Si f a un seul point fixe, alors ce point fixe est aussi point fixe de g.

Soit G un sous-groupe abélien de $\mathcal{S}_+$, soit il est inclus dans le groupe des translations $\mathcal{T}$, soit il contient une similitude directe f qui r

translation. On sait que f a un point fixe z_0 et un seul ; par conséquent, si g est un autre élément de G, g commutant avec f, $g(z_0)$ est un point fixe de f, donc $g(z_0) = z_0$. Nous en déduisons que dans ce cas $G \subset (\mathcal{S}_+)_{z_0}$.

d) 1) Déterminons l'ensemble $\mathcal{C}_r$ des isométries de $\mathbb{C}$ qui commutent avec une rotation r de centre z_0 (c'est un sous-groupe).
Soit $f \in \mathcal{C}_r$, nous savons (cf. question précédente) que f admet z_0 pour point fixe ; l'isométrie f est donc soit une rotation de centre z_0 (ou l'identité), soit une symétrie orthogonale par rapport à une droite D qui contient z_0 ; écrivons alors $r = S_{D'} \circ S_D$, où D' est une droite qui passe par z_0 ; on voit que $S_{D'}$ et S_D commutent, donc $r = S_D \circ S_{D'} = S_{D'} \circ S_D = r^{-1}$; l'isométrie r est donc dans ce cas nécessairement la symétrie par rapport au point z_0 (on a exclu le cas $r = \mathrm{Id}_{\mathbb{C}}$).
Le groupe des isométries qui commutent avec r est soit $(\mathrm{Is}_+(\mathbb{C}))_{z_0}$ si r n'est pas la symétrie par rapport au point z_0, soit le groupe $(\mathrm{Is}(\mathbb{C}))_{z_0}$, dans le cas contraire.

2) Déterminons le sous-groupe $\mathcal{C}_{T_{\vec{u}}}$ des isométries de $\mathbb{C}$ qui commutent avec la translation $T_{\vec{u}}$, $\vec{u} \neq \vec{0}$.
De manière générale, si E est un espace affine sur le corps K, f un automorphisme affine de E, et $T_{\vec{v}}$ la translation de vecteur $\vec{v} \in \overrightarrow{E}$, on vérifie :

$$f \circ T_{\vec{v}} \circ f^{-1} = T_{\vec{f}(\vec{v})} .$$

Une application affine f et une translation $T_{\vec{u}}$ commutent si, et seulement si, le vecteur $\vec{u}$ est invariant par l'application linéaire associée à f.
Les isométries vectorielles directes différentes de l'identité n'admettent aucun vecteur non nul invariant ; une isométrie vectorielle indirecte admet le vecteur non nul $\vec{u}$ comme vecteur invariant si, et seulement si, c'est une symétrie par rapport à la droite engendrée par ce vecteur. Le sous-groupe $\mathcal{C}_{T_{\vec{u}}}$ a donc pour éléments les translations quelconques, et les isométries indirectes de la forme $S_D \circ T_{\vec{v}}$, où D est une droite dirigée par $\vec{u}$, et $\vec{v} \in \overrightarrow{E}$ (une telle isométrie peut s'écire $S_D \circ T_{\vec{v}'}$ où $\vec{v}' \in \overrightarrow{D}$).

3) Déterminons le sous-groupe $\mathcal{C}_{S_D}$ des isométries de $\mathbb{C}$ qui commutent avec S_D, symétrie orthogonale par rapport à la droite D.
Si f est une isométrie de $\mathbb{C}$, on sait que :

$$f \circ S_D \circ f^{-1} = S_{f(D)} .$$

L'isométrie f commute avec S_D si, et seulement si $D = f(D)$. Déterminons plus précisément cet ensemble d'isométries. Notons $\vec{u}$ un vecteur directeur de la droite D. Si $D = f(D)$, la restriction de f à D est une isométrie de la droite, donc soit une symétrie par rapport à un point

une translation d'un vecteur $\vec{v} \in \overrightarrow{D}$. Dans le premier cas, z_0 est point fixe de f et $\overrightarrow{f}(\vec{v}) = -\vec{v}$; l'isométrie f est nécessairement soit la symétrie par rapport à la droite Δ qui coupe orthogonalement D en z_0 si elle est indirecte, soit la symétrie par rapport au point z_0 si elle est directe. Dans le deuxième cas, $T_{-\vec{v}} \circ f$ est une isométrie qui laisse la droite D invariante point par point ; c'est donc soit l'identité si elle est directe, et alors $f = T_{\vec{v}}$, soit la symétrie orthogonale par rapport à la droite D, et alors $f = T_{\vec{v}} \circ S_D$. Réciproquement les symétries par rapport à des points de la droite D, les translations de vecteur $\vec{v} \in \overrightarrow{D}$, les symétries orthogonales par rapport à des droites orthogonales à D, et les isométries indirectes qui sont composées de la symétrie par rapport à la droite D et d'une translation de vecteur $\vec{v} \in \overrightarrow{D}$, laissent la droite D stable, donc commutent avec S_D. Ces isométries sont par conséquent les éléments de $\mathscr{C}_{S_D}$.

4) Déterminons le sous-groupe $\mathscr{C}_U$ des isométries de $\mathbb{C}$ qui commutent avec l'isométrie $U = S_D \circ T_{\vec{u}}$, où D est une droite et $\vec{u}$ un vecteur directeur de cette droite (donc $\neq \vec{0}$).
Si f est une isométrie de $\mathbb{C}$, on vérifie que :

$$f \circ S_D \circ T_{\vec{u}} \circ f^{-1} = f \circ S_D \circ f^{-1} \circ f \circ T_{\vec{u}} \circ f^{-1} = S_{f(D)} \circ T_{\vec{f}(\vec{u})} .$$

Comme $\vec{f}(\vec{u})$ dirige la droite $f(D)$, il y a unicité de la droite et du vecteur ; l'isométrie f commute donc avec U si, et seulement si $D = f(D)$ et $\vec{f}(\vec{u}) = \vec{u}$. Comme dans le cas précédent, les translations de vecteur $\vec{v} \in \overrightarrow{D}$, et les composés $S_D \circ T_{\vec{v}}$ où $\vec{v} \in \overrightarrow{D}$, commutent avec l'isométrie indirecte U, mais il n'y en a pas d'autres.

5) Cherchons maintenant tous les sous-groupes abéliens de $\mathrm{Is}_{\mathbb{C}}$.
Soit G un sous-groupe abélien de $\mathrm{Is}_{\mathbb{C}}$;

α) Soit G contient une rotation de centre z_0 qui n'est pas la symétrie de centre z_0 ; il est clair d'après le 1), que $G \subset (\mathrm{Is}_+(\mathbb{C}))_{z_0}$. Cette condition est suffisante pour que le groupe G soit abélien.

β) Soit G contient une symétrie par rapport à un point z_0, mais aucune rotation qui ne soit pas une symétrie point. D'après 1), le groupe G ne peut alors contenir, hormis la symétrie par rapport à z_0, que des symétries par rapport à des droites qui passent par z_0 ; mais si S_D est dans le groupe G, le groupe G ne peut pas contenir d'autre symétrie (par rapport à une droite) que la symétrie par rapport à la droite Δ qui coupe orthogonalement D en z_0, sinon le groupe G contiendrait une rotation de centre z_0 différente de la symétrie de centre z_0. Le sous-groupe G est donc dans ce cas nécessairement inclus dans l'un des groupes $\{\mathrm{Id}, S_{z_0}, S_D, S_\Delta\}$, où $z_0 \in \mathbb{C}$, D

des droites orthogonales qui passent par z_0. Un tel sous-groupe étant abélien, cette condition est suffisante pour que G soit abélien.

γ) Soit G contient une isométrie indirecte U de la forme $S_D \circ T_{\vec{u}}$, où $\vec{u} \in \overrightarrow{D}$, et $\vec{u} \neq \vec{0}$. D'après le 4), on peut affirmer que G est inclus dans le sous-groupe $\mathcal{C}_U$ qui est la réunion de l'ensemble des translations de vecteur $\vec{v} \in \overrightarrow{D}$, et de l'ensemble des isométries indirectes de la forme $S_D \circ T_{\vec{v}}$, où $\vec{v} \in \overrightarrow{D}$. Comme un tel sous-groupe est abélien, la condition est suffisante pour que G soit abélien.

δ) Soit G ne contient que des translations et des symétries par rapport à des droites, et au moins une symétrie par rapport à une droite D. Si G contient la symétrie S_Δ, alors il contient l'isométrie directe $S_D \circ S_\Delta$; la droite Δ est nécessairement parallèle à D, sinon G contiendrait une rotation ; mais comme S_D et S_Δ doivent commuter, la translation $S_D \circ S_\Delta$ doit être involutive, donc nulle, d'où $D = \Delta$. Si $T_{\vec{v}}$ est une translation élément de G, $T_{\vec{v}} \circ S_D$ est une isométrie indirecte élément de G, donc égale à S_D ; nous en déduisons que $\vec{v} = 0$. Le groupe G est donc dans ce cas nécessairement inclus dans le sous-groupe $\{\mathrm{Id}, S_D\}$. Un tel sous-groupe étant abélien, c'est une condition suffisante pour que G soit abélien.

ε) Soit G ne contient que des translations ; il est alors inclus dans le sous-groupe $\mathcal{T}$ des translations, ce qui est une condition suffisante.

Remarquons enfin que si $z_0 \in \mathbb{C}$, et que G est un groupe abélien inclus dans $(\mathrm{Is}(\mathbb{C}))_{z_0}$, alors soit $G \subset (\mathrm{Is}_+(\mathbb{C}))_{z_0}$, soit G est inclus dans un sous-groupe de la forme $\{\mathrm{Id}, S_{z_0}, S_D, S_\Delta\}$, où D et Δ sont des droites qui se coupent orthogonalement en z_0.

6) Cherchons maintenant tous les sous-groupes abéliens de $\mathcal{S}$.
Soit G un sous-groupe abélien de $\mathcal{S}$.

α) Soit G contient une similitude directe ou indirecte s de centre z_0, c'est-à-dire ayant z_0 comme seul point fixe. Tous les éléments de G admettent z_0 pour point fixe ; le sous-groupe G est donc un sous-groupe abélien du groupe $\mathcal{S}_{z_0}$. Soit $\psi : \mathcal{S}_{z_0} \to \mathbb{R}_+^*$, l'homomorphisme de groupes qui à une similitude fait correspondre son rapport réel ; pour $s \in \mathcal{S}_{z_0}$, posons $\varphi(s) = h_{z_0,\psi(s)^{-1}} \circ s$; on voit que cette application est un homomorphisme de groupes de $\mathcal{S}_{z_0}$ vers $(\mathrm{Is}(\mathbb{C}))_{z_0}$; on peut aussi écrire $s = h_{z_0,\psi(s)} \circ \varphi(s)$ (produit commutatif). Il est clair que deux éléments de $\mathcal{S}_{z_0}$ commutent si, et seulement si, leurs images par φ commutent. Le groupe G est donc abélien, si, et seulement si, il est inclus dans l'image réciproque par φ d'un sous-groupe abélien de $(\mathrm{Is}(\mathbb{C}))_{z_0}$. Nous en déduisons que, soit le groupe G est inclus dans le groupe abélien $(\mathcal{S}_+)_{z_0}$, soit G est inclus dans le sous-groupe abélien de $\mathcal{S}_{z_0}$ engendré par les homothéties de centre z_0 et de

et les symétries par rapport à deux droites qui se coupent orthogonalement en z_0 ; on peut aussi considérer qu'un tel groupe est engendré par la symétrie autour d'une droite passant par z_0, et les homothéties de rapport $\neq 0$ de centre z_0.

β) Soit G ne contient aucune similitude à centre, mais dans ce cas il ne contient que des translations ou des similitudes indirectes qui sont composées d'une symétrie orthogonale par rapport à une droite D et d'une translation $T_{\vec{v}}$, où $\vec{v} \in \overrightarrow{D}$. Dans ce cas le sous-groupe G ne contient donc que des isométries. Les différentes possibilités sont décrites dans 5) γ, δ, ε.

§ VI.11 *NOMBRES COMPLEXES, DROITES ET CERCLES*

Exercice 1 :

Soit a, b, c trois points dans le plan d'Argand-Cauchy, non alignés, et $\theta \in \mathbb{R} \setminus \pi\mathbb{Z}$. Par $z \in \mathbb{C}$, on mène les trois droites $\Delta_1, \Delta_2, \Delta_3$ telles que

$$\widehat{(\Delta_1, D(b,c))} = \widehat{(\Delta_2, D(c,a))} = \widehat{(\Delta_3, D(a,b))} = \theta \mod(\pi),$$

qui rencontrent respectivement $D(b,c)$, $D(c,a)$ et $D(a,b)$ en α, β, γ. Trouver l'ensemble des $z \in \mathbb{C}$ tels que α, β, γ soient alignés. ■

Si z est confondu avec l'un des sommets du triangle, par exemple si $z = a$, alors β et γ sont confondus avec a, donc α, β et γ sont alignés. Inversement, si deux des points α, β ou γ sont confondus, on voit que z est confondu avec l'un des sommets du triangle. Nous excluons ce cas dans la suite.
Soit C_3 le cercle qui est la réunion de la paire $\{z, c\}$ et de l'ensemble des points ζ tels que $\widehat{(D(z,\zeta), D(c,\zeta))} = \theta \mod(\pi)$.
On voit que $\alpha \in C_3$, car soit $\alpha = z$ ou $\alpha = c$, soit dans le cas contraire :

$$\widehat{(D(\alpha,z), D(\alpha,c))} = \widehat{(\Delta_1, D(b,c))} = \theta \mod(\pi) .$$

De même $\beta \in C_3$, car soit $\beta = z$ ou $\beta = c$, soit dans le cas contraire :

$$\widehat{(D(\beta,z), D(\beta,c))} = \widehat{(\Delta_2, D(a,c))} = \theta \mod(\pi) .$$

Comme α, β, γ sont distincts, on peut supposer par exemple $z \neq \alpha$. Les points α, β, z, c sont sur C_3.
Si $\beta \neq c$,

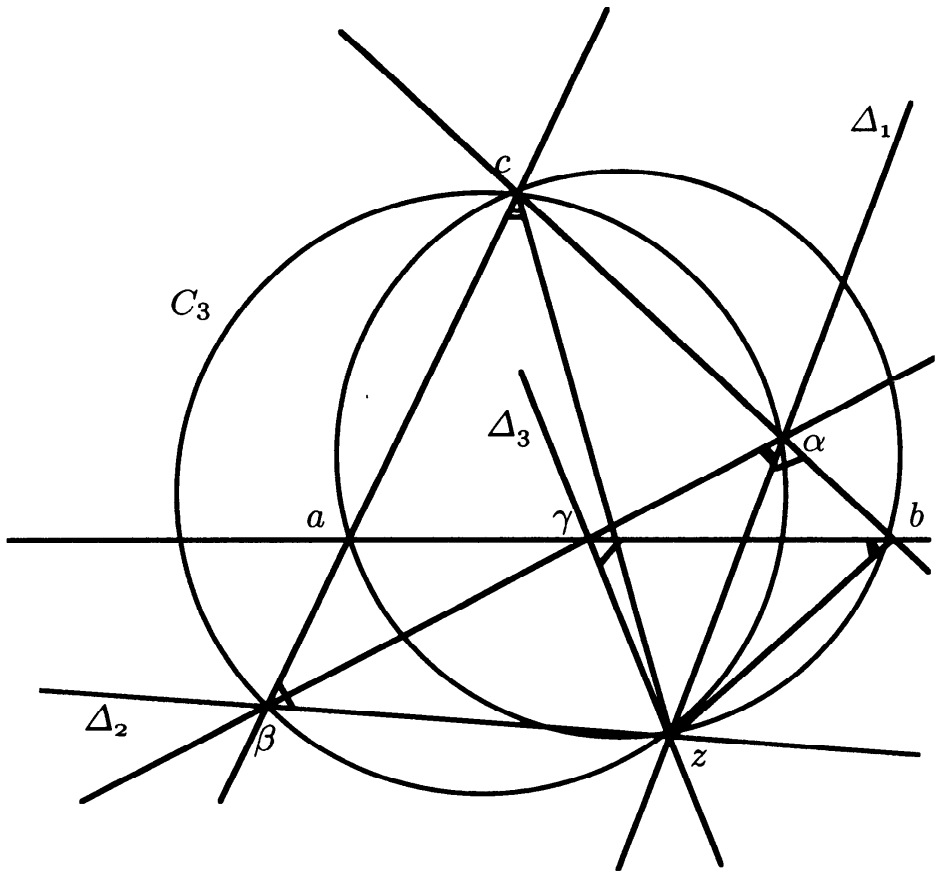
$$\widehat{(D(\alpha,\beta), D(\alpha,z))} = \widehat{(D(c,\beta), D(c,z))} = \widehat{(D(c,a), D(c,z))}$$

Si $\beta = c$, alors $\alpha \neq c$ et,

$$(\widehat{D(\alpha,\beta), D(\alpha,z)}) = (\widehat{D(\alpha,c), D(\alpha,z)}) = (\widehat{D(b,c), \Delta_1}) =$$
$$= \theta = (\widehat{D(c,a), \Delta_2}) = (\widehat{D(c,a), D(c,z)}) \mod(\pi) .$$

De manière analogue, dans tous les cas,

$$(\widehat{D(\alpha,\gamma), D(\alpha,z)}) = (\widehat{D(b,a), D(b,z)}) \mod(\pi) .$$



Nous en déduisons que :

$$(\widehat{D(\alpha,\beta), D(\alpha,\gamma)}) = (\widehat{D(c,a), D(c,z)}) - (\widehat{D(b,a), D(b,z)}) =$$
$$= (\widehat{D(c,a), D(b,a)}) + (\widehat{D(b,a), D(c,z)}) -$$
$$- (\widehat{D(b,a), D(c,z)}) - (\widehat{D(c,z), D(b,z)}) =$$
$$= (\widehat{D(c,a), D(b,a)}) - (\widehat{D(c,z), D(b,z)}) \mod(\pi) .$$

Les points α, β, γ sont donc alignés, si et seulement si $(\widehat{D(c,a), D(b,a)}) = (\widehat{D(c,z), D(b,z)}) \mod(\pi)$, soit si, et seulement si, le point z est sur le cercle circonscrit au triangle de sommets a, b, c.

En conclusion, en tenant compte du cas où deux des points α, β, γ sont confondus et z est l'un des points a, b, c, les points α, β, γ sont alignés si, et seulement si, z est sur le cercle circonscrit au triangle de sommets a, b, c.

Exercice 2 :

> On donne deux cercles de rayons distincts, $\mathscr{C}$ et $\mathscr{C}'$, dans le plan D'Argand-Chauchy. Trouver toutes les similitudes directes $f \in \mathcal{S}_+$ telles que $f(\mathscr{C}) = \mathscr{C}'$. Trouver l'ensemble des centres de ces similitudes. ■

Soient z_O le centre de $\mathscr{C}$ et $z_{O'}$ le centre de $\mathscr{C}'$, R le rayon de $\mathscr{C}$ et R' le rayon de $\mathscr{C}'$. Soit $T : z \mapsto z - z_O + z_{O'}$ la translation qui transforme z_O en $z_{O'}$, et h l'homothétie de centre z_O et de rapport R'/R. On voit que la similitude directe $s_0 = T \circ h$ transforme le cercle $\mathscr{C}$ en le cercle $\mathscr{C}'$. Une similitude directe s vérifie la condition de l'énoncé si, et seulement si, $s(\mathscr{C}) = \mathscr{C}' = s_0(\mathscr{C})$, soit si, et seulement si, $s_0^{-1} \circ s(\mathscr{C}) = \mathscr{C}$. Le rapport de la similitude $s_0^{-1} \circ s$ est donc nécessairement 1, et cette similitude doit laisser le point z_O invariant. La similitude directe $s_0^{-1} \circ s$ est donc nécessairement une rotation r de centre z_O (ou l'identité) ; cette condition est visiblement suffisante. L'ensemble des similitudes directes s telles que $s(\mathscr{C}) = \mathscr{C}'$, est donc l'ensemble des similitudes qui s'écrivent $s = s_0 \circ r$, où r est une rotation de centre z_O (ou l'identité).

On voit que si l'isométrie directe r de centre z_O est associée au nombre complexe $u \in \mathbb{U}$, alors la similitude $s = T \circ h \circ r$ est l'application

$$s_u : z \mapsto z_{O'} + \frac{R'}{R}\, u\,(z - z_O) .$$

L'ensemble des similitudes directes s telles que $s(\mathscr{C}) = \mathscr{C}'$ est donc l'ensemble des similitudes s_u, où $u \in \mathbb{U}$.

Comme $R \neq R'$, pour tout $u \in \mathbb{U}$ la similitude s_u est à centre, et son centre c_u est l'image de u par une homographie dont le domaine de définition contient $\mathbb{U}$. L'ensemble des centres des similitudes s_u est donc un cercle. Précisons ce cercle. On a :

$$c_u = z_{O'} + \frac{R'}{R}\, u\,(c_u - z_O) .$$

Nous en déduisons que c est l'un des centres de ces similitudes si, et seulement si :

$$\frac{R(c - z_{O'})}{R'(c - z_O)} \in \mathbb{U} \quad \text{soit} \quad \left|\frac{(c - z_{O'})}{(c - z_O)}\right| = \frac{R'}{R} .$$

L'ensemble des centres des similitudes s telles que $s(\mathscr{C}) = \mathscr{C}'$ est donc le cercle (dit d'Apollonius) qui est l'ensemble des complexes c tels que le rapport des distances de c aux centres des cercles $\mathscr{C}'$ et $\mathscr{C}$, est égal au rapport des rayons des cercles.

Chapitre VII

POLYNÔMES SUR UN CORPS COMMUTATIF

§ VII.1 *POLYNÔMES À UNE INDÉTERMINÉE*

Exercice 4 :

> Soit $\mathscr{A}$ la K-algèbre $K^{[\mathbb{Z}]}$ du groupe $\mathbb{Z}$ (cf. §VI.4).
>
> *a*) Expliquer pourquoi on peut décrire $\mathscr{A}$ comme l'ensemble des expressions $\sum_{k\in\mathbb{Z}} a_k X^k$, où $(a_k)_{k\in\mathbb{Z}}$ est une suite d'éléments de K à support fini, et où $X = (\ldots 0,0,1,0,0,\ldots)$, l'indice du terme non nul étant 1.
>
> *b*) Montrer que $\mathscr{A}$ et $K[X]$ ne sont pas des K-algèbres isomorphes.
>
> *c*) Montrer que $\mathscr{A}$ et $K[X]$ ne sont pas des *anneaux* isomorphes.
>
> ■

a) Reprenons les notations générales de l'exemple 6 du §VI.4. Nous noterons additivement la loi du monoïde M. On vérifie que pour tout λ et $\mu \in K^{(M)}$, $e_\lambda * e_\mu = e_{\lambda+\mu}$. En effet, $e_\lambda = \sum_{i\in M} e_\lambda(i)\, e_i$, et $e_\mu = \sum_{j\in M} e_\mu(j)\, e_j$, donc pour tout $k \in M$, $(e_\lambda * e_\mu)(k) = \sum_{i+j=k} e_\lambda(i)\, e_\mu(j)$. Si $k \neq \lambda+\mu$, et que $i+j=k$, alors $i \neq \lambda$ ou $j \neq \mu$, donc $e_\lambda(i)\, e_\mu(j) = 0$; dans ce cas $(e_\lambda * e_\mu)(k) = 0$. Si $k = \lambda+\mu$, et que $i+j = \lambda+\mu$, alors $e_\lambda(i)\, e_\mu(j) = 0$ sauf si $i = \lambda$ et $j = \mu$, auquel cas ce produit vaut 1 ; donc $(e_\lambda * e_\mu)(\lambda+\mu) = 1$. Nous en déduisons $e_\lambda * e_\mu = e_{\lambda+\mu}$.

On démontre aussi facilement, comme dans le cas particulier où $M = \mathbb{N}$, que la loi $*$ est associative, que si 0 est élément neutre du monoïde M, l'élément e_0 est neutre pour la loi $*$, et donc que $K^{(M)}$ est une K-algèbre associative et unitaire.

Dans le cas particulier de l'exercice, $M = \mathbb{Z}$, et $e_1 = X$. On voit que pour tout $k \in \mathbb{Z}$, e_k est inversible dans la K-algèbre $K^{[\mathbb{Z}]}$, d

puisque $e_{-k} * e_k = e_0$. L'application $k \mapsto e_k$ est donc un homomorphisme de groupes, du groupe $(\mathbb{Z}, +)$ vers le groupe des éléments inversibles de la K-algèbre $K^{[\mathbb{Z}]}$; nous en déduisons que pour tout $k \in \mathbb{Z}$, $e_k = e_1^k = X^k$. En conclusion :

$$\sum_{k\in\mathbb{Z}} a_k X^k = \sum_{k\in\mathbb{Z}} a_k e_k = (a_k)_{k\in\mathbb{Z}} ,$$

pour tout élément $(a_k)_{k\in\mathbb{Z}}$ de $K^{(\mathbb{Z})}$.

b) Soit φ un homomorphisme de K-algèbres, de $\mathscr{A}$ vers $K[X]$. Alors $\varphi(1) = 1$, et pour tout $k \in \mathbb{Z}$, $\varphi(X^{-k})\,\varphi(X^k) = \varphi(1) = 1$. Les polynômes $\varphi(X^k)$ sont donc, pour tout $k \in \mathbb{Z}$, inversibles, donc constants. Il est alors clair que l'homomorphisme de K-algèbres φ, est nécessairement à valeurs dans la sous-K-algèbre des polynômes constants, et ne peut donc être un isomorphisme de K-algèbres. Les K-algèbres $\mathscr{A}$ et $K[X]$ ne sont donc pas isomorphes.

c) Soit φ un homomorphisme d'anneaux, de $\mathscr{A}$ vers $K[X]$. Pour tout scalaire $\lambda \in K$, $\lambda \neq 0$, comme $(\lambda e_k) * (\lambda^{-1} e_{-k}) = e_0$, le polynôme $\varphi(\lambda e_k)$ est inversible, donc constant. L'homomorphisme d'anneaux φ est donc nécessairement à valeurs dans le sous-anneau des polynômes constants, et ne peut être un isomorphisme. Les anneaux $\mathscr{A}$ et $K[X]$ ne sont donc pas isomorphes.

Exercice 5 :

> Dans la K-algèbre $K[X]$, on considère la sous-K-algèbre $\mathscr{A}$ engendrée par X^2 et X^3, notée $\mathscr{A} = K[X^2, X^3]$. Montrer que $K[X]$ et $\mathscr{A}$ ne sont pas des K-algèbres isomorphes. ■

Supposons que φ soit un isomorphisme de K-algèbres, $\varphi : K[X] \mapsto \mathscr{A}$. Posons $A = \varphi(X)$. Pour tout polynôme $P \in K[X]$, on voit que $\varphi(P(X)) = P(\varphi(X)) = P(A)$. Comme l'application φ est surjective, il existe deux polynômes P et Q dans $K[X]$ tels que $X^2 = P(A)$ et $X^3 = Q(A)$. Cela implique $A \neq 0$, et $2 = \deg(P(A)) = \deg(P) \times \deg(A)$, d'où $\deg(A) \mid 2$; de même, $\deg(A) \mid 3$; le polynôme A est donc nécessairement de degré 1, de la forme $A = a + bX$ $(b \neq 0)$. On voit alors que pour tout $P \in K[X]$, $P = P((A-a)/b) \in \mathscr{A}$. Nous en déduisons que s'il existait un isomorphisme de K-algèbres $\varphi : K[X] \mapsto \mathscr{A}$, alors on aurait $K[X] = K[X^2, X^3]$.

Montrons que l'égalité ci-dessus est fausse, et par conséquent que les algèbres $\mathscr{A}$ et $K[X]$ ne sont pas isomorphes. Introduisons par exemple l'ensemble $\mathscr{B} = \{P \in K[X] \mid P'(0) = 0\}$. On voit facilement que $\mathscr{B}$ est une sous-K-algèbre qui contient les polynômes X^2 et X^3, donc la so

$\mathcal{A}$. La sous-K-algèbre $\mathcal{B}$ étant strictement incluse dans $K[X]$ ($X \notin \mathcal{B}$), la sous-K-algèbre $\mathcal{A}$ est strictement incluse dans $K[X]$, ce qu'il fallait démontrer.

Exercice 6 :

Soient K et L deux corps commutatifs. Si les *anneaux* $K[X]$ et $L[X]$ sont isomorphes, alors les corps K et L sont isomorphes.
■

Soit $\Phi : K[X] \to L[X]$ un isomorphisme d'anneaux. Posons pour tout $\lambda \in K$, $\varphi(\lambda) = \Phi(\lambda \cdot 1_{K[X]})$, où $1_{K[X]}$ désigne le polynôme constant de valeur 1_K, élément de $K[X]$. On voit que φ est un homomorphisme injectif d'anneaux, du corps K dans l'anneau $L[X]$; l'image de K par φ est un sous-anneau de l'anneau $L[X]$ qui est un corps ; cette image est donc constituée de $\varphi(0_K) = 0_{L[X]}$, et d'éléments inversibles dans l'anneau $L[X]$, donc de polynômes constants. Posons pour tout $\lambda \in K$, $\varphi(\lambda) = f(\lambda) \cdot 1_{L[X]}$; il est clair qu'on définit ainsi une application $f : K \to L$ qui est un homomorphisme injectif d'anneaux.

Si $\mu \in L$, $\Phi^{-1}(\mu \cdot 1_{L[X]})$ est soit nul si $\mu = 0$, soit inversible si $\mu \neq 0$, et est donc dans tous les cas un polynôme constant $\lambda \cdot 1_{K[X]}$. On voit que $\varphi(\lambda) = \mu \cdot 1_{L[X]}$, d'où $f(\lambda) = \mu$. L'application f est donc un isomorphisme du corps K sur le corps L. Les corps K et L sont donc isomorphes.

§ VII.2 *L'ANNEAU EUCLIDIEN K[X]*

Exercice 1 :

Soit $P \in K[X]$ et b, c deux entiers naturels premiers entre eux. Démontrer que $(P^b - 1)(P^c - 1)$ divise $(P - 1)(P^{bc} - 1)$.
■

Pour tout $n \in \mathbb{N}^*$, notons A_n le polynôme $X^{n-1} + \ldots + X + 1$ ($A_1 = 1$), de telle sorte que $X^n - 1 = (X - 1) A_n$. Pour tout polynôme P, et m et k entiers > 0, $P^{mk} - 1 = (P^k)^m - 1 = (P^k - 1) A_m(P^k)$. On déduit que si n et k sont des entiers > 0 et que k divise n, alors le polynôme $P^k - 1$ divise le polynôme $P^n - 1$.

Montrons que si b et c sont des entiers > 0 et que $\text{pgcd}(b, c) = d$, alors le polynôme $P^d - 1$ est un pgcd des polynômes $P^b - 1$ et $P^c - 1$.

Il existe $(n, m) \in \mathbb{Z}^2$ tel que $mb - nc = d$. Si (m_0, n_0) est une solution particulière, où $(m_0, n_0) \in \mathbb{Z}^2$, alors pour tout $k \in \mathbb{Z}$, le c

$k\,c, n_0 + k\,b)$ est aussi solution. Comme $b > 0$ et $c > 0$, il est clair qu'on peut trouver des entiers $m > 0$ et $n > 0$ tels que $m\,b - n\,c = d$.
En utilisant de tels entiers, on obtient :

$$P^{m\,b} - 1 = P^{n\,c+d} - 1 = P^{n\,c+d} - P^d + P^d - 1 = P^d\,(P^{n\,c} - 1) + P^d - 1\ ,$$

donc :

$$(P^b - 1)\,A_m(P^b) - (P^c - 1)\,P^d\,A_n(P^c) = P^d - 1\ .$$

Tout diviseur commun de $P^b - 1$ et de $P^c - 1$ divise $P^d - 1$, et inversement, d'après la remarque initiale, $P^d - 1$ divise $P^b - 1$ et $P^c - 1$. Le polynôme $P^d - 1$ est donc bien un pgcd des polynômes $P^b - 1$ et $P^c - 1$.

En particulier, si b et c sont des entiers > 0 premiers entre eux, alors le polynôme $P - 1$ est un pgcd des polynômes $P^b - 1$ et $P^c - 1$

Si $P = 1$, ou si $b = 0$ ou $c = 0$, la propriété à démontrer est vraie. Nous supposerons dans la suite $P \neq 1$, $b > 0$ et $c > 0$, et b et c premiers entre eux. Posons $P^b - 1 = (P - 1)B$ et $P^c - 1 = (P - 1)C$ (ce qui est possible car $P \neq 1$). D'après ce qui précède, les polynômes B et C sont premiers entre eux. Posons aussi $P^{bc} - 1 = (P - 1)D$. Comme $P^b - 1$ divise $P^{bc} - 1$, c'est-à-dire $(P - 1)B$ divise $(P - 1)D$, nous voyons que B divise D ; de même C divise D et puisque B et C sont premiers entre eux, BC divise D. Finalement $(P^b - 1)(P^c - 1) = (P - 1)^2BC$ divise $(P - 1)^2D = (P - 1)(P^{bc} - 1)$, ce qu'il fallait démontrer.

Exercice 2 :

On donne $K = \mathbb{Z}/_{5\,\mathbb{Z}}$. Effectuer la division euclidienne de $A = \bar{2}\,X^3 + \bar{3}\,X^2 + \bar{1}$ par $B = \bar{1}\,X^2 + \bar{2}\,X + \bar{3}$. ■

Comme le coefficient dominant du diviseur est $\bar{1}$, on peut faire la division euclidienne comme si l'anneau de base était $\mathbb{Z}$. On pourra ensuite remplacer les entiers par leurs classes modulo 5.
On pose l'opération sans oublier de faire figurer le monôme $0\,X$ dans l'écriture du dividende.

$$\begin{array}{rrr|l} 2X^3 & +3X^2 & +0X\ +1 & X^2\ +2X+3 \\ \cline{4-4} -X^2 & -6X & +1 & 2X\ -1 \\ & -4X & +4 & \end{array}$$

Comme $-\bar{4} = \bar{1}$, nous pouvons en déduire l'égalité :

$$\bar{2}\,X^3 + \bar{3}\,X^2 + \bar{1} = (\bar{2}\,X - \bar{1})(X^2 + \bar{2}\,X + \bar{3}) + X - \bar{1}$$

Exercice 5 :

Soit L un sous-anneau du corps K. On suppose l'anneau $L[X]$ principal. Démontrer que L est un sous-corps de K. ■

Soit $l \in L$, $l \neq 0$, montrons que l est inversible dans L, ou encore que l'inverse de l dans le corps K est dans L.

Soit P un pgcd dans l'anneau principal $L[X]$, du polynôme X et du polynôme constant $l \cdot 1_{L[X]}$. Puisque P divise un polynôme constant, c'est un polynôme constant de valeur $p \in L$. Comme le polynôme $P = p \cdot 1_{L[X]}$ divise dans $L[X]$ le polynôme X, on voit que p divise dans l'anneau L le coefficient dominant de X, c'est-à-dire 1 ; l'élément p de l'anneau L est donc inversible dans L. Les polynômes $l \cdot 1_{L[X]}$ et X sont donc premiers entre eux dans l'anneau $L[X]$. D'après le théorème de Bézout, il existe deux polynômes A et B, éléments de $L[X]$, tels que :

$$A(X) \times (l \cdot 1_{L[X]}) + B(X) \times X = 1_{L[X]} .$$

En remplaçant dans cette égalité X par 0, on obtient $A(0) \times l = 1$. Comme $A \in L[X]$, on voit que $A(0) \in L$; l'élément l est donc inversible dans l'anneau L, ce qu'il fallait démontrer.

Exercice 7 :

Soit $m_1, m_2, \ldots, m_k$ des naturels $\geqslant 1$. Montrer que le pgcd normalisé des polynômes $(X^{m_i} - 1)_{1 \leqslant i \leqslant k}$ est $X^d - 1$, où $d = \text{pgcd}\,(m_1, m_2, \ldots, m_k)$. ■

D'après l'exercice 1, si P est un polynôme et b et c des entiers > 0, le polynôme $P^{\text{pgcd}(b,c)} - 1$ est un pgcd des polynômes $P^b - 1$ et $P^c - 1$. Soit P un polynôme non constant normalisé, montrons par récurrence sur l'entier $k \geqslant 1$ que si $m_1, m_2, \ldots, m_k$ sont des entiers naturels, alors le polynôme $P^{\text{pgcd}(m_1, m_2, \ldots, m_k)} - 1$ est le pgcd des polynômes $(P^{m_1} - 1)$, $(P^{m_2} - 1), \ldots, (P^{m_k} - 1)$.
La proposition est vraie pour $k = 1$ et $k = 2$, puisque $P^{\text{pgcd}(b,c)} - 1$ est le pgcd normalisé de $P^b - 1$ et de $P^c - 1$. Supposons cette propriété vraie pour k, et montrons qu'elle est vraie pour $k + 1$. Soient $m_1, m_2, \ldots, m_k, m_{k+1}$ des entiers naturels ; posons :

$$d_k = \text{pgcd}\,(m_1, m_2, \ldots, m_k) \quad \text{et} \quad D_k = \text{pgcd}\,((P^{m_1} - 1), \ldots, (P^{m_k} - 1)) .$$

On sait que :

$$D_{k+1} = \text{pgcd}\,((P^{m_1} - 1), \ldots, (P^{m_k} - 1), (P^{m_{k+1}} - 1)) =$$
$$= \text{pgcd}\,(D_k, (P^{m_{k+1}} - 1)) ,$$

d'où en utilisant l'hypothèse de récurrence :

$$D_{k+1} = \operatorname{pgcd}\left((P^{d_k} - 1), (P^{m_{k+1}} - 1)\right) = P^{\operatorname{pgcd}(d_k, m_{k+1})} - 1 \ .$$

Comme $d_{k+1} = \operatorname{pgcd}(m_1, \ldots, m_k, m_{k+1}) = \operatorname{pgcd}(d_k, m_{k+1})$ (associativité du pgcd), on voit finalement que :

$$D_{k+1} = P^{d_{k+1}} - 1 \ .$$

La propriété est donc démontrée par récurrence.

Cette propriété est en particulier vraie dans le cas où $P = X$.

Exercice 10 :

Soit $r_1, r_2, \ldots, r_k$ des naturels tels que $0 \leqslant r_1 < r_2 < \ldots < r_k \leqslant n-1$ où n est un entier $\geqslant 2$. On donne dans $\mathbb{N}$ des nombres $m_1, m_2, \ldots, m_k$ tels que $m_i \equiv r_i \bmod (n)$ pour $1 \leqslant i \leqslant k$. Montrer que le reste dans la division euclidienne du polynôme $X^{m_1} + X^{m_2} + \ldots + X^{m_k}$ par $X^n - 1$ dans $K[X]$, est $X^{r_1} + X^{r_2} + \ldots + X^{r_k}$ et calculer le quotient. ■

Posons pour $i \in [\![1, k]\!]$, $m_i = d_i\, n + r_i$ (divisions euclidiennes). On voit que pour tout $i \in [\![1, k]\!]$:

$$X^{m_i} = X^{d_i n + r_i} = X^{r_i} + (X^{d_i n} - 1)X^{r_i} = X^{r_i} + X^{r_i}(X^n - 1)\left(\sum_{j=0}^{d_i - 1} X^{j n}\right) \ ,$$

la dernière somme étant par convention nulle si $d_i = 0$. Nous en déduisons l'égalité :

$$\sum_{i=1}^{k} X^{m_i} = \sum_{i=1}^{k} X^{r_i} + (X^n - 1)\sum_{i=1}^{k} X^{r_i}\left(\sum_{j=0}^{d_i - 1} X^{j n}\right) \ .$$

Comme le degré du polynôme $X^{r_1} + \ldots + X^{r_k}$ est $r_k < n$, ce polynôme est le reste dans la division euclidienne du polynôme $X^{m_1} + X^{m_2} + \ldots + X^{m_k}$ par $X^n - 1$, et le quotient est le polynôme :

$$Q = \sum_{i=1}^{k} X^{r_i}\left(\sum_{j=0}^{d_i - 1} X^{j n}\right) \ .$$

Exercice 11 :

Soit q et m dans $\mathbb{N}^*$. Trouver une condition

suffisante pour que $1+X^m+X^{2m}+\ldots+X^{qm}$ soit divisible par $1+X+X^2+\ldots+X^q$ dans $K[X]$. ■

On voit que $1+X+X^2+\ldots+X^q$ divise $1+X^m+X^{2m}+\ldots+X^{qm}$ si, et seulement si,

$$(X^m-1)(X-1)(1+X+\ldots+X^q)\,|\,(X-1)(X^m-1)(1+X^m+\ldots+X^{qm})\,,$$

soit si, et seulement si, $(X^m-1)(X^{q+1}-1)\,|\,(X-1)(X^{(q+1)m}-1)$. D'après l'exercice 1, c'est vrai si les entiers $(q+1)$ et m sont premiers entre eux. Montrons qu'en général cette condition est aussi nécessaire. Nous utiliserons le lemme suivant :

Lemme :

Soit $P\in K[X]$, non constant, et b,c dans $\mathbb{N}^*$, si le polynôme $(P^b-1)(P^c-1)$ divise $(P-1)(P^{bc}-1)$ et que b ou c n'est pas divisible dans $\mathbb{Z}$ par la caractéristique du corps K, alors b et c sont premiers entre eux. ■

Si $(P^b-1)(P^c-1)$ divise $(P-1)(P^{bc}-1)$, alors (P^c-1) divise le polynôme $(P-1)(1+P^b+P^{2b}+\ldots+P^{(c-1)b})$. Supposons que l'entier $d>0$ divise b et c, les polynômes (P^b-1) et (P^c-1) sont divisibles par (P^d-1). Nous pouvons donc écrire modulo le polynôme (P^d-1), c'est-à-dire dans l'anneau quotient, les égalités $P^c=1$ et $P^b=1$, d'où :

$$0=(P-1)\underbrace{(1+1+\ldots+1)}_{c\text{ fois}}\,.$$

Cela signifie que (P^d-1) divise $c(P-1)$, ce qui n'est possible, si $c\cdot 1_K\neq 0$, que si $d=1$. Nous pouvons obtenir le même résultat si $b\cdot 1_K\neq 0$. Le lemme est donc démontré.

Nous pouvons remarquer que si K est un corps de caractéristique $p>0$ premier, alors $(P^p-1)^p=P^{p\times p}-1$ dans $K[X]$ (puisque $\binom{p}{k}$ est divisible par p si $0<k<p$), et donc que $(P^p-1)(P^p-1)$ divise le polynôme $(P-1)(P^{p\times p}-1)$. On a ici un exemple où $(P^b-1)(P^c-1)$ divise $(P-1)(P^{bc}-1)$ et p divise à la fois b et c ; b et c ne sont pas premiers entre eux.
Fin du lemme.

D'après ce lemme, nous pouvons dire que si les entiers $q+1$ et m ne sont pas tous les deux divisibles par la caractéristique du corps K, alors $1+X+\ldots+X^q$ divise le polynôme $1+X^m+\ldots+X^{qm}$, si, et seulement si, les entiers $q+1$ et m sont premiers entre eux. Remarquons que si $q=1$, $m=2$ et que la caractéristique du corps est 2, $q+1=m=2$, mais $(1+X)$ divise $(1+X)^2=1+X^2$.

§ VII.3 *L'ANNEAU FACTORIEL K[X]*

Exercice 3 :

On considère le sous-anneau $\mathbb{Z}[X]$ de l'anneau $\mathbb{Q}[X]$.

a) Si p est un nombre premier dans $\mathbb{Z}$, vérifier que p est élément irréductible de $\mathbb{Z}[X]$ mais non de $\mathbb{Q}[X]$, et que pX est irréductible dans $\mathbb{Q}[X]$ mais non dans $\mathbb{Z}[X]$.

b) Soit $F \in \mathbb{Z}[X]\backslash\{0\}$ et $\mathscr{C}(F)$ le pgcd dans $\mathbb{Z}$ de ses coefficients (appelé le *contenu* de F). F est dit *primitif* ssi $\mathscr{C}(F) = 1$ (par exemple tout polynôme normalisé est primitif). Montrer que si F et G sont primitifs, alors FG l'est aussi (théorème dû à Gauss). En déduire que si F et G sont dans $\mathbb{Z}[X] \setminus \{0\}$, $\mathscr{C}(FG) = \mathscr{C}(F)\mathscr{C}(G)$.

c) Soit $F \in \mathbb{Z}[X] \setminus \{0\}$ *non constant*. Montrer l'équivalence : F est irréductible dans $\mathbb{Z}[X]$ ssi F est primitif dans $\mathbb{Z}[X]$ et irréductible dans $\mathbb{Q}[X]$.

d) Quels sont les éléments inversibles de l'anneau $\mathbb{Z}[X]$? Montrer que $\mathbb{Z}[X]$ est factoriel. ■

a) L'entier p premier est inversible dans l'anneau $\mathbb{Q}$, donc le polynôme constant $p\cdot 1$ est inversible dans l'anneau $\mathbb{Q}[X]$; il n'est donc pas irréductible dans cet anneau.
Si A et B sont deux éléments de $\mathbb{Z}[X]$ tels que $p \cdot 1 = A \times B$, alors A et B sont nécessairement constants ; posons $A = a \cdot 1$, $a \in \mathbb{Z}$, et $B = b \cdot 1$, $b \in \mathbb{Z}$, comme $p = ab$ et que p est premier, alors a ou b est inversible dans $\mathbb{Z}$, donc A ou B est inversible dans $\mathbb{Z}[X]$. Puisque d'autre part le polynôme constant $p \cdot 1$ n'est pas inversible dans l'anneau $\mathbb{Z}[X]$ (sinon p le serait dans $\mathbb{Z}$), il est irréductible dans cet anneau.
Le polynôme pX n'est pas irréductible dans $\mathbb{Z}[X]$, car $p \cdot 1$ et X sont irréductibles dans $\mathbb{Z}[X]$. Mais ce polynôme est irréductible dans $\mathbb{Q}[X]$, car il est, dans $\mathbb{Q}[X]$, associé au polynôme irréductible X.

b) Supposons que le polynôme FG ne soit pas primitif. Il existe alors un nombre premier p qui divise tous les coefficients de FG. Nous pouvons donc écrire dans l'anneau $\mathbb{Z}/_{p\mathbb{Z}}[X]$, en remplaçant les entiers coefficients des polynômes par leurs classes, que $\bar{F}\bar{G} = 0$. Comme l'anneau $\mathbb{Z}/_{p\mathbb{Z}}$ est un corps, l'anneau $\mathbb{Z}/_{p\mathbb{Z}}[X]$ est intègre ; nous pouvons donc en déduire que $\bar{F} = 0$ ou $\bar{G} = 0$. Cela signifie que ou bien p divise tous les c

F, ou bien p divise tous les coefficients de G ; l'un des polynômes F ou G n'est donc pas primitif. On voit par conséquent que si les polynômes F et G sont primitifs, alors le polynôme FG est primitif.

Soient F et G des polynômes non nuls éléments de $\mathbb{Z}[X]$, en divisant tous les coefficients des polynômes par leur pgcd, on peut écrire $F = \mathscr{C}(F)F_1$ et $G = \mathscr{C}(G)G_1$, où F_1 et G_1 sont des éléments primitifs de $\mathbb{Z}[X]$. Donc $FG = \mathscr{C}(F)\mathscr{C}(G)F_1G_1$. Comme le pgcd des coefficients du polynôme F_1G_1 est 1, le pgcd des coefficients du polynôme FG est $\mathscr{C}(F)\mathscr{C}(G)$, c'est-à-dire $\mathscr{C}(FG) = \mathscr{C}(F)\mathscr{C}(G)$.

c) Soit F, non constant, irréductible dans $\mathbb{Z}[X]$, il n'est pas nul et on peut l'écrire $F = \mathscr{C}(F)F_1$ où F_1 est un élément primitif de $\mathbb{Z}[X]$. Comme F est non constant, F_1 est non constant, donc non inversible, ni dans $\mathbb{Q}[X]$, ni dans $\mathbb{Z}[X]$; nous en déduisons que le polynôme (constant) $\mathscr{C}(F)$ est inversible dans $\mathbb{Z}[X]$, donc que $\mathscr{C}(F) = 1$. Le polynôme F est donc nécessairement primitif.
Supposons que $F = A \times B$, où A et B sont dans $\mathbb{Q}[X]$. On peut trouver des entiers naturels a et b non nuls tels que les polynômes $A' = aA$ et $B' = bB$ soient à coefficients entiers. Ecrivons maintenant $A' = \mathscr{C}(A')A'_1$ et $B' = \mathscr{C}(B')B'_1$ où A'_1 et B'_1 sont des éléments primitifs de $\mathbb{Z}[X]$. On voit que $abF = A'B' = \mathscr{C}(A')\mathscr{C}(B')A'_1B'_1$, d'où, en prenant les contenus, $ab = \mathscr{C}(A')\mathscr{C}(B')$. Nous en déduisons l'égalité $F = A'_1B'_1$, factorisation de F dans $\mathbb{Z}[X]$. Comme F est irréductible dans $\mathbb{Z}[X]$, ceci implique que A'_1 ou B'_1 est inversible dans $\mathbb{Z}[X]$, donc (au moins) constant. Il est alors clair que A ou B est constant, donc inversible dans $\mathbb{Q}[X]$. Le polynôme non constant F est donc irréductible dans $\mathbb{Q}[X]$.

Réciproquement, montrons que si F est primitif dans $\mathbb{Z}[X]$ et irréductible dans $\mathbb{Q}[X]$ (donc non constant), il est irréductible dans $\mathbb{Z}[X]$.
Le polynôme F n'est évidemment pas inversible dans $\mathbb{Z}[X]$, et s'il s'écrit $F = AB$, où A et B sont des polynômes à coefficients entiers, alors, puisqu'il est irréductible dans $\mathbb{Q}[X]$, l'un des polynômes A ou B est inversible dans $\mathbb{Q}[X]$, donc constant. Supposons par exemple $A = a \cdot 1$, où $a \in \mathbb{Z}$, alors $F = aB$, donc $1 = \mathscr{C}(F) = a\mathscr{C}(B)$. L'entier a est donc inversible dans l'anneau $\mathbb{Z}$, et le polynôme $A = a \cdot 1$ est inversible dans l'anneau $\mathbb{Z}[X]$. Le polynôme F est donc irréductible dans l'anneau $\mathbb{Z}[X]$.

d) Les éléments inversibles dans l'anneau $\mathbb{Z}[X]$ sont les polynômes constants, inversibles dans $\mathbb{Z}$, donc les polynômes 1 et -1. Les polynômes irréductibles dans $\mathbb{Z}[X]$ sont, d'après ce qui précède, les polynômes constants de la forme $p \cdot 1$, où p est un élément irréductible de l'anneau $\mathbb{Z}$ (donc premier ou opposé d'un nombre premier), et les polynômes primitifs dans $\mathbb{Z}[X]$ qui sont irréductibles dans $\mathbb{Q}[X]$.

Soit F un polynôme primitif dans $\mathbb{Z}[X]$, montrons qu'il est produit de polynômes irréductibles dans $\mathbb{Z}[X]$. Comme l'anneau $\mathbb{Q}[X]$ est principal, il est factoriel, il existe donc un entier k et, dans l'anneau $\mathbb{Q}[X]$, des polynômes irréductibles $(P_i)_{i\in[\![1,k]\!]}$, tels que $F = \prod_{i=1}^{k} P_i$. Pour tout $i \in [\![1,k]\!]$, il existe un entier $q_i > 0$ tel que le polynôme $P_i' = q_i P_i$ soit à coefficients entiers ; le polynôme P_i' est irréductible dans $\mathbb{Q}[X]$. Notons encore $P_i' = \mathscr{C}(P_i')A_i$, où A_i est un élément primitif de $\mathbb{Z}[X]$, qui est irréductible dans $\mathbb{Q}[X]$, donc, d'après ce qui précède, aussi dans $\mathbb{Z}[X]$. Nous pouvons écrire :

$$\left(\prod_{i=1}^{k} q_i\right) F = \prod_{i=1}^{k} P_i' = \left(\prod_{i=1}^{k} \mathscr{C}(P_i')\right) \prod_{i=1}^{k} A_i \ .$$

Comme les polynômes $\prod_{i=1}^{k} A_i$ et F sont primitifs, on voit que :

$$\prod_{i=1}^{k} q_i = \prod_{i=1}^{k} \mathscr{C}(P_i') \quad \text{d'où} \quad F = \prod_{i=1}^{k} A_i \ .$$

Soit F un polynôme non nul dans l'anneau $\mathbb{Z}[X]$, écrivons $F = \mathscr{C}(F)\, F_1$, où F_1 est un polynôme primitif. Le polynôme F_1 peut s'écrire comme produit de polynômes primitifs et irréductibles dans $\mathbb{Z}[X]$; l'entier $\mathscr{C}(F)$ peut s'écrire comme produit de nombres irréductibles dans l'anneau $\mathbb{Z}$, le polynôme constant $\mathscr{C}(F)\cdot 1$ peut donc s'écrire comme produit d'éléments irréductibles (constants) de l'anneau $\mathbb{Z}[X]$. Le polynôme F peut donc s'écrire comme produit d'éléments irréductibles dans l'anneau $\mathbb{Z}[X]$.

Soit A un anneau intègre, et P et Q deux polynômes non nuls dans $A[X]$, nous dirons que P et Q sont A-associés s'il existe un scalaire $\lambda \in A$ inversible dans A, tel que $Q = \lambda \cdot P$; on définit ainsi une relation d'équivalence sur l'ensemble des polynômes non nuls à coefficients dans A.
Soit $\mathscr{P}$ l'ensemble des nombres entiers premiers, $\mathscr{P}'$ l'ensemble des polynômes $p\cdot 1$ où $p \in \mathscr{P}$, et $\mathscr{S}$ l'ensemble des polynômes non constants et irréductibles dans $\mathbb{Z}[X]$ dont le coefficient dominant est positif. Montrons que $\mathscr{P}' \cup \mathscr{S}$ est un système de représentants de l'ensemble des polynômes irréductibles dans $\mathbb{Z}[X]$ pour la relation $\mathbb{Z}$-associé.
Si P est irréductible dans $\mathbb{Z}[X]$; soit il est constant de la forme $a\cdot 1$, où a est irréductible dans $\mathbb{Z}$, dans ce cas $|a|$ est premier et P est $\mathbb{Z}$-associé à $|a|\cdot 1$ élément de $\mathscr{P}'$; soit c'est un polynôme non constant irréductible dans $\mathbb{Q}[X]$ et primitif, dans ce cas, si ε est le signe de son coefficient dominant ($\varepsilon \in \{-1,1\}$), P est $\mathbb{Z}$-associé à l'élément εP de $\mathscr{S}$.
Deux éléments de $\mathscr{P}'$ différents ne sont évidemment pas $\mathbb{Z}$-associés, et un élément de $\mathscr{P}'$ et un élément de $\mathscr{S}$ non plus. Soient P et Q

de $\mathcal{S}$, s'ils sont $\mathbb{Z}$-associés, ils sont égaux ou opposés, mais comme leurs coefficients dominants sont positifs, ils sont égaux. L'ensemble $\mathcal{P} \cup \mathcal{S}$ est donc bien un système de représentants de l'ensemble des polynômes irréductibles dans $\mathbb{Z}[X]$ pour la relation $\mathbb{Z}$-associé. D'après ce qui précède pour tout polynôme non nul $P \in \mathbb{Z}[X]$, il existe un signe $\varepsilon \in \{-1, 1\}$, une suite $(\nu_p)_{p\in\mathcal{P}}$ appartenant à $\mathcal{P}^{(\mathbb{N})}$, une suite $(\mu_R)_{R\in\mathcal{S}}$ appartenant à $\mathcal{S}^{(\mathbb{N})}$, telles que :

$$P = \varepsilon \prod_{p\in\mathcal{P}} p^{\nu_p} \prod_{R\in\mathcal{S}} R^{\mu_R} .$$

Démontrons maintenant que le triplet (ε, μ, ν) est unique, le polynôme non nul P étant donné, ce qui démontrera que l'anneau $\mathbb{Z}[X]$ est factoriel.
Le signe ε est uniquement déterminé par P car c'est le signe de son coefficient dominant. Le produit $\prod_{p\in\mathcal{P}} p^{\nu_p}$ est uniquement déterminé par P car c'est son contenu (puisque les polynômes $R \in \mathcal{S}$ sont primitifs), donc la famille $(\nu_p)_{p\in\mathcal{P}}$ est uniquement déterminée par P. Enfin, si R et R' sont deux éléments de $\mathcal{S}$ différents, ils ne sont pas $\mathbb{Z}$-associés, mais pas non plus $\mathbb{Q}$-associés. En effet, s'ils sont $\mathbb{Q}$-associés, alors $R = (p/q)R'$, où p et q sont des entiers > 0 (parce que les coefficients dominants de R et R' sont > 0), mais $qR = pR'$, donc $q = \mathcal{C}(qR) = \mathcal{C}(pR') = p$, et $R = R'$.
Comme les polynômes $R \in \mathcal{S}$ sont irréductibles dans $\mathbb{Q}[X]$, deux à deux non $\mathbb{Q}$-associés, et que l'anneau $\mathbb{Q}[X]$ est factoriel, la famille $(\mu_R)_{R\in\mathcal{S}}$ est uniquement déterminée par P.
Cela termine la démonstration du fait que l'anneau $\mathbb{Z}[X]$ est factoriel.

Exercice 4 :

Soit p un nombre premier dans $\mathbb{Z}$ et C un polynôme de $\mathbb{Z}[X]$ de degré $\geqslant 2$, $X^n + c_{n-1}X^{n-1} + \ldots + c_0$ tel que

$$c_i \equiv 0 \mod(p) \text{ pour } 0 \leqslant i \leqslant n-1 \text{ et } c_0 \not\equiv 0 \mod(p^2) .$$

a) Démontrer que C est irréductible dans $\mathbb{Z}[X]$.

b) En déduire que C est irréductible dans $\mathbb{Q}[X]$ en se servant de l'exercice 3.

c) Soit p un nombre premier dans $\mathbb{Z}$. Montrer que le polynôme Φ défini par $\Phi = X^{p-1} + X^{p-2} + \ldots + 1$ est irréductible dans $\mathbb{Q}[X]$.

d) Si $\alpha \in \mathbb{N}^*$ et p premier dans $\mathbb{Z}$, prouver de la même façon que le polynôme

$$\Psi = X^{p^{\alpha-1}(p-1)} + X^{p^{\alpha-1}(p-2)} + \ldots + 1$$

est irréductible dans $\mathbb{Q}[X]$.

e) Soit $n \in \mathbb{N}^*$. Trouver des nombres entiers $a \in \mathbb{Z}^*$ tels que $X^n - a$ soit irréductible dans $\mathbb{Q}[X]$. ■

a) Nous ne supposerons pas dans cette question que le coefficient dominant c_n de C soit 1, mais nous supposerons que les coefficients de C sont premiers entre eux dans leur ensemble, ce qui implique que c_n est premier avec p. Supposons que $C = A \times B$, où A et B sont dans $\mathbb{Z}[X]$. En remplaçant dans cette égalité les coefficients entiers des polynômes par leurs classes modulo p, on obtient l'égalité $\bar{C} = \bar{A} \times \bar{B}$ dans l'anneau $\mathbb{Z}/_{p\mathbb{Z}}[X]$. Mais ici $\bar{C} = \overline{c_n} X^n$, et comme le polynôme X est irréductible dans l'anneau $\mathbb{Z}/_{p\mathbb{Z}}[X]$, $\bar{A}$ et $\bar{B}$ sont des monômes. Posons $\bar{A} = \lambda X^a$ et $\bar{B} = \mu X^b$, où a et b sont des entiers ; on voit que $a + b = n$. Si a' est le degré du polynôme A, et b' le degré du polynôme B, alors $a' \geqslant a$ et $b' \geqslant b$, mais comme $a' + b' = n$, nécessairement $a' = a$ et $b' = b$. Cela signifie que les coefficients des polynômes A et B, sauf les coefficients dominants, sont divisibles par p. Si les polynômes A et B étaient tous les deux non constants, alors $A(0)$ et $B(0)$ seraient divisibles par p, et comme $C(0) = A(0) \times B(0)$, le coefficient c_0 de C serait divisible par p^2, ce qui est contraire à l'hypothèse. L'un des polynômes A ou B est donc constant, et en tant qu'entier divise tous les coefficients de C. Comme les coefficients de C sont premiers entre eux dans leur ensemble, on en déduit que ce polynôme est constant et inversible dans l'anneau $\mathbb{Z}[X]$. Le polynôme C est donc irréductible dans $\mathbb{Z}[X]$.

b) Comme le polynôme C n'est pas constant et est irréductible dans $\mathbb{Z}[X]$, il est irréductible dans $\mathbb{Q}[X]$ (exercice 3, *c*)).

c) On vérifie que $(X - 1)\Phi = X^p - 1$, donc :

$$X\,\Phi(X+1) = (X+1)^p - 1 = X^p + \binom{p}{1} X^{p-1} + \ldots + \binom{p}{p-1} X + 1 - 1 ,$$

d'où :

$$\Phi(X+1) = X^{p-1} + \binom{p}{1} X^{p-2} + \ldots + \binom{p}{p-2} X + \binom{p}{p-1} .$$

Le polynôme $\Phi(X + 1)$ vérifie visiblement le critère d'Eisenstein (voir *a*)), et est donc irréductible dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$. Il en est de même pour le polynôme Φ, puisque si $\Phi = A \times B$, où A et B sont dans $\mathbb{Z}[X]$, alors $\Phi(X+1) = A(X+1) \times B(X+1)$, donc $A(X+1)$ ou $B(X+1)$ est inversible dans $\mathbb{Z}[X]$; l'un des polynômes A ou B est donc inversible dans $\mathbb{Z}[X]$.

d) Montrons par récurrence que pour tout entier $k \geqslant 1$, on a, dans l'anneau $\mathbb{Z}/_{p\mathbb{Z}}[X]$, l'égalité :

$$X^{p^k} - 1 = (X - 1)^{p^k} .$$

On sait que cette égalité est vraie pour $k = 1$. Supposons la vraie pour k, alors :

$$X^{p^{k+1}} - 1 = (X^p)^{p^k} - 1 = (X^p - 1)^{p^k} = (X-1)^{p \cdot p^k} = (X-1)^{p^{k+1}} .$$

L'égalité est donc vraie pour $k+1$.
L'égalité est donc vraie par récurrence pour tout entier $k \geqslant 1$.

On vérifie que dans $\mathbb{Z}[X]$:

$$\left(X^{p^{\alpha-1}} - 1\right) \Psi = \left(X^{p^{\alpha-1}}\right)^p - 1 = X^{p^\alpha} - 1 .$$

En remplaçant dans cette égalité les coefficients entiers des polynômes par leurs classes modulo p, et en utilisant l'identité démontrée ci-dessus, on trouve l'égalité :

$$\left(X^{p^{\alpha-1}} - 1\right) \overline{\Psi} = (X-1)^{p^{\alpha-1}} \overline{\Psi} = X^{p^\alpha} - 1 = (X-1)^{p^\alpha} ,$$

d'où (puisque $\mathbb{Z}/_{p\mathbb{Z}}[X]$ est un anneau intègre) :

$$\overline{\Psi} = (X-1)^{p^\alpha - p^{\alpha-1}} = (X-1)^{p^{\alpha-1}(p-1)} .$$

Nous en déduisons que :

$$\overline{\Psi}(X+1) = X^{p^{\alpha-1}(p-1)} = \overline{\Psi(X+1)} .$$

Les coefficients du polynôme $\Psi(X+1)$, qui est de degré $p^{\alpha-1}(p-1)$, sont donc tous divisibles par p, sauf le coefficient dominant. Le coefficient c_0 de ce polynôme est $\Psi(1) = p$, qui n'est pas divisible par p^2. Le polynôme $\Psi(X+1)$ est donc, d'après le critère d'Eisenstein, irréductible dans $\mathbb{Z}[X]$, et dans $\mathbb{Q}[X]$. Il en est de même pour le polynôme Ψ.

e) S'il existe un nombre premier p qui divise a mais dont le carré ne divise pas a, alors, d'après le critère d'Eisenstein, le polynôme $X^n - a$ est irréductible dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$.

Exercice 9 :

a) Factoriser le polynôme $X^4 - X^2 + 1$ sur le corps $\mathbb{Z}/_{11\mathbb{Z}}$.

b) Factoriser le polynôme $X^5 + X + 1$ sur le corps des rationnels.

c) Montrer que les polynômes $X^4 + X + 1$ et $X^6 + X^2 + 1$ sont irréductibles dans $\mathbb{Q}[X]$. ■

Remarquons d'abord que si K est un corps et $P \in K[X]$ est non nul de degré 2 ou 3, il est irréductible dans $K[X]$ si, et seulement si, il n'a pas de zéro dans le corps. En effet, toute factorisation non triviale de P contient nécessairement un polynôme de degré 1. Ce résultat ne s'étend évidemment pas à des polynômes de degré > 3.

a) Nous pouvons utiliser ici une méthode analogue à la méthode de factorisation des polynômes bicarrés dans $\mathbb{R}[X]$. Etablissons la liste des carrés dans le corps $\mathbb{Z}/_{11\,\mathbb{Z}}$.

élément	:	0	1	2	3	4	5
carré	:	0	1	4	9	5	3

Puisque le discriminant du polynôme $Y^2 - Y + 1$ est $-3 = 8$, qui n'est pas un carré, on essaye l'autre méthode :

$$(1) \qquad X^4 - X^2 + 1 = (X^2+1)^2 - 3X^2 = (X^2+1)^2 - 25X^2 = \\ = (X^2 - 5X + 1)(X^2 + 5X + 1)\ .$$

On voit que $X^2 - 5X + 1 = X^2 + 6X + 1 = (X+3)^2 - 8$, et $X^2 + 5X + 1 = X^2 - 6X + 1 = (X-3)^2 - 8$; comme 8 n'est pas un carré dans le corps $\mathbb{Z}/_{11\,\mathbb{Z}}$, ces deux polynômes n'ont pas de zéros dans le corps, et sont donc irréductibles. Nous avons donc obtenu avec (1), une factorisation en produit de facteurs irréductibles du polynôme $X^4 - X^2 + 1$ sur le corps $\mathbb{Z}/_{11\,\mathbb{Z}}$.

Nous utiliserons dans la suite le lemme suivant :

Lemme :

> Si $P \in \mathbb{Z}[X]$ est un polynôme normalisé, ses zéros rationnels sont entiers, et divisent $P(0)$. ■

Posons $P = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$, où $a_{n-1}, \ldots, a_1, a_0$ sont des entiers relatifs. Supposons que le rationnel $r = p/q$, où $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ et p premier avec q, soit zéro de P, nous pouvons alors écrire, après multiplication par q^n :

$$p^n + a_{n-1}p^{n-1}q + \ldots + a_1 p q^{n-1} + a_0 q^n = 0\ ,$$

d'où $q \mid p^n$. Comme q est premier avec p, donc avec p^n, nous en déduisons que $q = 1$ (puisque $q > 0$). Le rationnel r est donc entier, $r = p$, et on voit que p divise a_0. Remarquons que cette propriété permet de chercher les zéros rationnels d'un polynôme normalisé à coefficients entiers, dans un ensemble fini de cardinal assez petit.
Fin du lemme

b) En regardant bien, on voit que le polynôme X^5+X+1 admet comme zéro le complexe j , racine troisième de 1, cela suggère qu'il est divisible par le polynôme X^2+X+1 . En effet :

$$X^5+X+1=(X^3-1)X^2+X^2+X+1=$$
$$=(X^2+X+1)(1+(X-1)X^2)=(X^2+X+1)(X^3-X^2+1)\ .$$

D'après le lemme, ces deux polynômes ne peuvent avoir comme zéros rationnels que 1 ou -1 . Ils n'ont donc pas de zéros rationnels et sont par conséquent irréductibles dans $\mathbb{Q}[X]$. Nous avons bien obtenu une factorisation du polynôme X^5+X+1 en produit de facteurs irréductibles dans $\mathbb{Q}[X]$.

c) Supposons que le polynôme X^4+X+1 ne soit pas irréductible dans $\mathbb{Q}[X]$. Ce polynôme n'a aucun zéro rationnel car ceux-ci ne peuvent être que 1 ou -1 , il se factorise donc, dans $\mathbb{Q}[X]$, en un produit de deux polynômes de degré 2, qu'on peut supposer normalisés. Posons :

$$X^4+X+1=(X^2+aX+b)(X^2+cX+d)\ ,$$

où a,b,c,d sont des rationnels. Il est clair que $a+c=0$ et $bd=1$ (d'où $b\neq 0$), nous pouvons donc écrire :

$$X^4+X+1=(X^2+aX+b)(X^2-aX+\frac{1}{b})=$$
$$=X^4+\big(b+\frac{1}{b}-a^2\big)X^2+a\big(\frac{1}{b}-b\big)X+1\ .$$

Nous obtenons les relations :

$$a^2=b+\frac{1}{b}\quad\text{et}\quad a\big(\frac{1}{b}-b\big)=1\ ,$$

d'où :

$$a^6=a^2(b+1/b)^2=a^2(b^2+1/b^2+2)=4a^2+a^2(b^2+1/b^2-2)=4a^2+1\ .$$

Cela est impossible, car le polynôme X^6-4X^2-1 , ne peut avoir comme zéros rationnels que 1 ou -1 , qui ne sont pas des zéros.
Le polynôme X^4+X+1 est donc irréductible dans $\mathbb{Q}[X]$.

Dans ce qui suit "irréductible" signifiera "irréductible dans $\mathbb{Q}[X]$ ".
Remarquons que le polynôme $A=X^3+X+1$ n'a pas de zéro rationnel, et est donc irréductible (il est de degré 3). Le polynôme $P=X^6+X^2+1=A(X^2)$ n'a donc pas non plus de zéro rationnel mais cela ne suffit évidemment pas à prouver qu'il est irréductible. Supposons que P ne soit pas

Soit R un diviseur irréductible de P.
1) Le polynôme R n'est ni de degré 1 ni de degré 5, sinon P aurait un zéro rationnel.
2) Supposons que R soit pair. Il existe alors un polynôme $R_1 \in \mathbb{Q}[X]$, non constant, de degré < 3, tel que $R(X) = R_1(X^2)$, et comme $R_1(X^2)$ divise $P = A(X^2)$, il est clair que R_1 divise A dans $\mathbb{Q}[X]$, ce qui est impossible puisque A est irréductible. Les diviseurs irréductibles de P ne sont donc pas pairs.
3) Le polynôme R n'est évidemment pas impair, car $P(0) \neq 0$.

Soit R un diviseur de P, irréductible, normalisé, et de plus petit degré possible. Soit d le degré de R. On voit que $2d \leqslant 6$, donc $d \leqslant 3$, et par conséquent $d = 2$ ou $d = 3$.
Si $d = 2$, $R(X)$ et $R(-X)$ sont deux polynômes irréductibles de degré 2 normalisés, et non associés, sinon ils seraient égaux, ce qui est exclu d'après 2). Le produit $R(X)\,R(-X)$, de degré 4, divise P, et le quotient exact est un polynôme pair de degré 2, ce qui est impossible d'après 1) et 2).
Si $d = 3$, $R(X)$ et $-R(-X)$ sont deux polynômes irréductibles de degré 3, normalisés, non associés, sinon ils seraient égaux et R serait impair, ce qui est impossible d'après 3). Le produit $-R(X)\,R(-X)$, de degré 6, divise P. Ces deux polynômes sont donc associés, et par conséquent égaux puisqu'ils sont normalisés. Il existe donc des rationnels (a, b, c) tels que :

$$X^6 + X^2 + 1 = (X^3 + a\,X^2 + b\,X + c)\,(X^3 - a\,X^2 + b\,X - c)\ ,$$

ce qui est impossible car on devrait avoir $c^2 = -1$ et $c \in \mathbb{Q}$.

Le polynôme $P = X^6 + X^2 + 1$ est donc irréductible dans $\mathbb{Q}[X]$.

Exercice 10 :

> Soit $c > 0$ fixé et n dans $\mathbb{N}^*$. Montrer que l'ensemble des polynômes de $\mathbb{Q}[X]$: $F = X^n + r_1\,X^{n-1} + \ldots + r_n$, qui sont irréductibles dans $\mathbb{Q}[X]$ et tels que $|r_i| \leqslant c$ pour tout i est *infini*. ■

Nous utiliserons ici la variante du théorème d'Eisenstein, démontrée dans la résolution de l'exercice 4 *a*).
Soit $k \in \mathbb{N}$, alors le polynôme : $P_k = (2k+1)\,X^n + 2$, vérifie le critère : les coefficients sont premiers entre eux dans leur ensemble, tous les coefficients sauf le coefficient dominant sont divisibles par 2, nombre premier, et la valeur en zéro n'est pas divisible par 2^2. Le polynôme P_k est donc irréductible dans $\mathbb{Z}[X]$. Comme il est aussi non constant, il est irréductible dans $\mathbb{Q}[X]$ (cf. exercice 3 *c*)). Le polynôme :

$$Q_k = X^n + \frac{2}{2k+1}\ ,$$

qui lui est associé dans $\mathbb{Q}[X]$, est donc irréductible dans $\mathbb{Q}[X]$. Un nombre $c > 0$ étant donné, le polynôme Q_k vérifie les conditions de l'énoncé pourvu que $2k + 1 \geqslant 2/c$. L'ensemble des polynômes qui vérifient les conditions de l'énoncé est donc infini.

§ VII.4 *FONCTIONS POLYNÔMES, RACINES*

Exercice 2 :

> Soit K un corps commutatif et soit $P \in K[X]$
>
> *a*) Montrer que l'application $K[X] \to K[X]$, $F \mapsto F \circ P$ est un *automorphisme* de la K-algèbre $K[X]$ si, et seulement si, $\deg(P) = 1$.
>
> *b*) Montrer que les automorphismes de la K-algèbre $K[X]$ sont précisément ceux définis au *a*). Ces automorphismes forment un groupe que l'on définira de manière simple. ■

a) On sait que l'homorphisme $\Phi_P : F \mapsto F \circ P$ est injectif si, et seulement si, $\deg(P) \geqslant 1$ (§VII.4 Exemple 2). Si F est un élément non nul de $K[X]$, on voit facilement que $\deg(F \circ P) = \deg(F)\deg(P)$. Supposons que l'homomorphisme Φ_P soit surjectif, en particulier, comme il existe un polynôme F tel que $F \circ P = X$, on voit que $\deg(P) \mid 1$, et donc $\deg(P) = 1$.
Inversement, montrons que si P est de la forme $b + a\,X$, où a et b sont des éléments de K, $a \neq 0$, l'homomorphisme Φ_P est bijectif. Posons $Q = (X - b)/a$, on voit que $P \circ Q = a\,Q + b = X$, et que $Q \circ P = X$. Pour tout polynôme F, on a donc :

$$\Phi_P \circ \Phi_Q(F) = (F \circ Q) \circ P = F \circ (Q \circ P) = F(X) = F\ ,$$

et de même :

$$\Phi_Q \circ \Phi_P(F) = (F \circ P) \circ Q = F \circ (P \circ Q) = F(X) = F\ .$$

Les endomorphismes de K-algèbres Φ_P et Φ_Q sont donc bijectifs réciproques l'un de l'autre, et sont donc des automorphismes.

b) Supposons que Φ soit un endomorphisme de la K-algèbre $K[X]$ et posons $\Phi(X) = P$. Pour tout polynôme $F = \sum_{k=0}^{n} a_n\,X^n$,

$$\Phi(F) = \Phi\left(\sum_{k=0}^{n} a_k\,X^k\right) = \sum_{k=0}^{n} a_k\,(\Phi(X))^k = \sum_{k=0}^{n} a_k\,P^k = F \circ P$$

Nous en déduisons $\Phi = \Phi_P$, où $P = \Phi(X)$.
Les automorphismes de la K-algèbre $K[X]$, sont donc les automorphismes Φ_P, où P est un polynôme de degré 1.
Pour tous polynômes P, Q dans $K[X]$, on a pour tout polynôme F :

$$\Phi_P \circ \Phi_Q(F) = (F \circ Q) \circ P = F \circ (Q \circ P) = \Phi_{Q \circ P}(F) ,$$

d'où $\Phi_P \circ \Phi_Q = \Phi_{Q \circ P}$. L'application $P \mapsto \Phi_P$ est donc un isomorphisme entre le groupe des polynômes de degré 1 muni de la loi interne $(P, Q) \mapsto Q \circ P$ et le groupe des automorphismes de la K-algèbre $K[X]$.

Exercice 4 :

a) Résoudre dans $\mathbb{C}[X]$ l'équation $P^2 + Q^2 = R^2$, où les polynômes inconnus P, Q, R sont non nuls.
b) Si $n \geqslant 3$ montrer que l'équation $P^n + Q^n = R^n$ (où P, Q et R sont dans $\mathbb{C}[X] \setminus \{0\}$) n'admet que les solutions de la forme $P = \lambda D, Q = \mu D, R = \nu D$, où $D \in \mathbb{C}[X] \setminus \{0\}$ et λ, μ, ν sont des éléments de $\mathbb{C}^*$ vérifiant $\lambda^n + \mu^n = \nu^n$. ■

a) Supposons que les polynômes P, Q, R soient non nuls et vérifient l'équation $P^2 + Q^2 = R^2$. Soit $D = \text{pgcd}(P, Q, R)$, c'est un polynôme non nul et normalisé. Posons $P = D P_1$, $Q = D Q_1$, et $R = D R_1$; les polynômes P_1, Q_1, R_1 sont premiers entre eux dans leur ensemble et vérifient l'équation. Ecrivons $Q_1^2 = R_1^2 - P_1^2 = (R_1 - P_1)(R_1 + P_1)$. Les polynômes $R_1 - P_1$ et $R_1 + P_1$ sont non nuls et premiers entre eux, car si un polynôme irréductible les divisait tous les deux, il diviserait Q_1^2, donc Q_1, et P_1 et R_1. En utilisant la décomposition des polynômes en produits de facteurs irréductibles, on voit facilement que ces polynômes sont proportionnels à des carrés de polynômes, donc sont des carrés de polynômes (le corps $\mathbb{C}$ est algébriquement clos). Il existe par conséquent deux polynômes A et B, non nuls et premiers entre eux tels que :

$$A^2 = R_1 - P_1 , \quad B^2 = R_1 + P_1 , \quad Q_1^2 = A^2 B^2 .$$

En remplaçant éventuellement A par $-A$, nous en déduisons finalement qu'il existe deux polynômes A et B non nuls premiers entre eux (et tels que $A^2 \neq B^2$ et $A^2 \neq -B^2$) tels que :

$$P = D \frac{B^2 - A^2}{2} , \quad Q = D A B , \quad R = D \frac{B^2 + A^2}{2} .$$

Inversement, si D est un polynôme non nul, et A, B deux polynômes non nuls et premiers entre eux (et, s'ils sont tous les deux consta

$A^2 \neq B^2$ et $A^2 \neq -B^2$), le triplet défini ci-dessus est bien solution de l'équation puisque :

$$D^2\left(\frac{B^2-A^2}{2}\right)^2 + D^2\,A^2\,B^2 = D^2\left(\frac{B^2+A^2}{2}\right)^2 .$$

Nous avons donc résolu l'équation, au sens où nous avons paramétré l'ensemble des solutions. Remarquons que le paramétrage est presque injectif. En effet, si A et B sont premiers entre eux, alors A^2 est premier avec B^2, donc A^2-B^2 et A^2+B^2 sont premiers entre eux. Le polynôme D est donc nécessairement $\operatorname{pgcd}(P,Q,R)$. D'où $A^2=(R-P)/D$ et $B^2=(P+R)/D$ et $A\,B=Q/D$. Le couple (A,B) est donc déterminé au signe près.

b) Montrons par récurrence sur $k \in \mathbb{N}$ la proposition suivante : si P, Q, R sont des polynômes de degrés $\leqslant k$, premiers entre eux et tels qu'il existe des scalaires a,b,c tous non nuls vérifiant $a\,P^n+b\,Q^n+c\,R^n=0$, alors ces polynômes sont constants. La proposition est évidente si $k=0$. Supposons qu'elle soit vraie pour $k-1$. Soient P, Q, R trois polynômes premiers entre eux, de degrés $\leqslant k$, pour lesquels il existe (a,b,c) scalaires tous non nuls tels que $a\,P^n+b\,Q^n+c\,R^n=0$. Soit $z \in \mathbb{C}$ tel que $z^n=-c/b$, on peut écrire :

$$(-a/b)\,P^n = Q^n + c/b\,R^n = Q^n - (zR)^n = \prod_{u\in\mu_n} (Q - u\,z\,R) ,$$

où μ_n désigne l'ensemble des racines n-ièmes de 1. Les polynômes $Q-u\,z\,R$ sont premiers entre eux deux à deux, car si un polynôme irréductible en divisait deux différents il diviserait Q, R et P. En utilisant la décomposition en facteurs premiers, on voit facilement que comme leur produit est proportionnel à la puissance n d'un polynôme, chacun d'eux est proportionnel à la puissance n d'un polynôme, donc est une puissance n d'un polynôme ($\mathbb{C}$ est algébriquement clos). Soit r un générateur du groupe μ_n, on a au moins (puisque $n \geqslant 3$) trois polynômes P_0, P_1, P_2, premiers entre eux deux à deux tels que :

$$Q - zR = P_0^n , \quad Q - r\,zR = P_1^n , \quad Q - r^2 z\,R = P_2^n .$$

On voit que les polynômes P_0^n, P_1^n, P_2^n sont $\mathbb{C}$-liés, et plus précisément que :

$$\begin{aligned}(r^2-r)P_0^n + (1-r^2)P_1^n + (r-1)P_2^n &= \\ = (r^2-r)(Q-zR) + (1-r^2)(Q-r\,zR) + (r-1)(Q-r^2zR) &= 0 .\end{aligned}$$

Les coefficients $(r^2-r),(1-r^2),(r-1)$ sont tous non nuls, et les degrés des polynômes P_0,P_1,P_2 sont évidemment $<k$; nous pouvons donc déduire de l'hypothèse de récurrence que ces polynômes sont constants. L

$Q - zR$ et $Q - rzR$ sont constants, et par conséquent les polynômes Q, R, et enfin P, sont constants. Cela achève la démonstration par récurrence.

Soient P, Q, R trois polynômes non nuls tels que $P^n + Q^n - R^n = 0$; notons D leur pgcd (qui n'est pas nul) et posons $P = D\,P_1$, $Q = D\,Q_1$ et $R = D\,R_1$. Les polynômes P_1, Q_1, R_1 sont premiers entre eux et vérifient la relation $P_1^n + Q_1^n - R_1^n = 0$; d'après la proposition démontrée ci-dessus, ces polynômes sont nécessairement constants. Il existe donc un polynôme D non nul, et des complexes non nuls λ, μ, ν, tels que $P = \lambda D$, $Q = \mu D$ et $R = \nu D$. Un tel triplet est solution de l'équation si, et seulement si $\lambda^n + \mu^n = \nu^n$.

Exercice 5 :

> On suppose le corps K *fini*, de cardinal q ; on considère l'homomorphisme naturel de K-algèbres $f : K[X] \to \mathcal{F}(K)$, $F \mapsto \widetilde{F}$.
>
> *a*) En utilisant le polynôme d'interpolation de Lagrange, montrer que f est surjectif, autrement dit que toute application de K dans K est une fonction polynomiale.
>
> *b*) Montrer que l'idéal $\mathrm{Ker}\,(f)$ est engendré par
>
> $$\prod_{x \in K} (X - x) = X^q - X\,. \blacksquare$$

a) Soit une application quelconque $\varphi : K \to K$. Notons $a_1, a_2, \ldots, a_q$ les éléments du corps K. D'après le théorème VII.4.3, il existe un et un seul polynôme $\Lambda \in K[X]$ de degré $\leqslant q - 1$ tel que pour tout $i \in [\![1, q]\!]$, $\Lambda(a_i) = \varphi(a_i)$. L'application polynomiale $\widetilde{\Lambda}$ coïncide donc avec l'application φ. L'homomorphisme de K-algèbres f est donc surjectif.

b) Un polynôme $F \in K[X]$ est dans le noyau de l'homomorphisme de K-algèbres f si, et seulement si, en notant toujours $a_1, a_2, \ldots, a_q$ les éléments de K, pour tout $i \in [\![1, q]\!]$, $F(a_i) = 0$. Le polynôme nul étant la solution dans $K_{q-1}[X]$, d'après la partie (II) du théorème VII.4.3, le noyau de f est l'ensemble des polynômes $G\,P$, où $G \in K[X]$ et où P désigne le polynôme $P = (X - a_1)(X - a_2)\ldots(X - a_q)$; l'ensemble de ces polynômes est donc l'idéal engendré par le polynôme $P = \prod_{x \in K} (X - x)$.

Soit $Q = X^q - X$; montrons que l'application polynomiale $\widetilde{Q}$ est identiquement nulle sur K. Si $k \in K^*$, k est inversible et sa période multiplicative divise le cardinal du groupe $(K^*, \times)$; ce cardinal étant $q - 1$, nous en déduisons $k^{q-1} = 1$ puis $k^q = k$; comme $Q(0) = 0$, on voit donc que $\widetilde{Q} = 0$. Le polynôme Q est par conséquent divisible par le p

mais comme ils sont tous les deux normalisés et de degré q, ces polynômes sont égaux. L'idéal $\mathrm{Ker}\,(f)$ est donc engendré par le polynôme $X^q - X$.

Exercice 6 :

On prend $K = \mathbb{Q}$. Soit $a_1, a_2, \ldots, a_n$ des entiers rationnels distincts. Démontrer que le polynôme

$$(X - a_1)(X - a_2)\ldots(X - a_n) - 1$$

est irréductible dans l'anneau $\mathbb{Z}[X]$, donc (cf. exercice 3 du §VII.3) irréductible aussi dans $\mathbb{Q}[X]$. ■

Supposons $P = (X-a_1)(X-a_2)\ldots(X-a_n)-1 = A\,B$, où A et B sont des éléments de $\mathbb{Z}[X]$. Pour tout $i \in [\![1, n]\!]$, $P(a_i) = -1 = A(a_i)\,B(a_i)$; comme $A(a_i)$ et $B(a_i)$ sont des entiers, ils sont dans $\{-1, +1\}$, et par conséquent $A(a_i) = -B(a_i)$. Si l'un des polynômes A ou B n'est pas constant, alors les polynômes A et $-B$, considérés comme éléments de $\mathbb{Q}[X]$, sont de degrés $\leqslant n-1$ et coïncident en n éléments du corps, donc sont identiques ; cela est impossible car le produit des coefficients dominants des polynômes A et B doit être 1. L'un des polynômes A ou B est donc constant, de valeur entière et inversible dans $\mathbb{Z}$; ce polynôme est donc inversible dans $\mathbb{Z}[X]$. Le polynôme P est donc irréductible dans $\mathbb{Z}[X]$, et comme il n'est pas constant, irréductible aussi dans $\mathbb{Q}[X]$.

Exercice 13 :

Opérateur de différence. Le corps de base est $\mathbb{C}$. Soit τ l'endomorphisme du $\mathbb{C}$-ev $\mathbb{C}[X]$ qui envoie le polynôme $F \in \mathbb{C}[X]$ sur $F(X+1)$. On note Id l'opérateur identique de $\mathbb{C}[X]$ et on pose $\Delta = \tau - \mathrm{Id}$.

a) Vérifier que, pour tout $n \in \mathbb{N}^*$, Δ envoie $\mathbb{C}_n[X]$ dans $\mathbb{C}_{n-1}[X]$. Préciser la valeur de $\Delta^{<n>}(F)$ pour $F \in \mathbb{C}_n[X]$. On raisonnera dans la $\mathbb{C}$-algèbre $\mathrm{Hom}_{\mathbb{C}}(\mathbb{C}[X])$.

b) En déduire les identités

$$\sum_{k=0}^{n}(-1)^k \binom{n}{k} (X-k)^p = \begin{cases} 0 & \text{si } n > p \\ n\,! & \text{si } n = p \end{cases}$$

c) A partir de l'identité

$$\sum_{k=0}^{n}(-1)^{k+n} \binom{n}{k} k^n = n\,!\,,$$

qui est une conséquence de *b*), démontrer que le théorème de Fermat IV.4.5 entraîne le théorème de Wilson IV.4.6. ■

a) Soit $p \in \mathbb{N}^*$, on voit que

$$\Delta(X^p) = (X+1)^p - X^p = \sum_{k=0}^{p-1} \binom{p}{k} X^k \in \mathbb{C}_{p-1}[X] .$$

Il est donc clair que Δ envoie $\mathbb{C}_n[X]$ dans $\mathbb{C}_{n-1}[X]$. On vérifie que pour tout $p \in \mathbb{N}^*$, le monôme de plus haut degré dans $\Delta(X^p)$ est $p\,X^{p-1}$. On voit facilement que si $F = a_n X^n + \ldots + a_0$, alors $\Delta^{<n>}(F) = n!\,a_n$.

b) Les opérateurs τ et Id, éléments de $\mathrm{Hom}_{\mathbb{C}}(\mathbb{C}[X])$, commutent ; on peut donc utiliser la formule du binôme de Newton pour développer la puissance (au sens de la composition) $\Delta^{<n>} = (\tau - \mathrm{Id})^{<n>}$. En appliquant cette égalité à $F = a_n X^n + \ldots + a_0$ on trouve :

$$n!\,a_n = \Delta^{<n>}(F) = \sum_{k=0}^{n} \binom{n}{k} (-1)^k \tau^{<n-k>}(F) =$$

$$= \sum_{k=0}^{n} \binom{n}{k} (-1)^k F(X+n-k) .$$

En remplaçant dans cette égalité X par $X-n$, on obtient :

$$n!\,a_n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k F(X-k) .$$

On obtient le résultat demandé en posant $F = X^p$, où $p \leqslant n$.

c) En remplaçant X par 0 dans l'identité obtenue pour $p = n$ dans la question précédente, on obtient pour tout $n \in \mathbb{N}^*$:

$$n! = \sum_{k=0}^{n} \binom{n}{k} (-1)^k (-k)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^{k+n} k^n ,$$

d'où, en remplaçant n par $n-1$, pour tout $n \geqslant 2$:

$$(n-1)! = \sum_{k=0}^{n-1} \binom{n-1}{k} (-1)^{k+n-1} k^{n-1} = \sum_{k=1}^{n-1} \binom{n-1}{k} (-1)^{k+n-1} k^{n-1}$$

Supposons que pour tout entier $k \in [\![1, n-1]\!]$, on ait $k^{n-1} \equiv 1 \bmod (n)$ (petit théorème de Fermat), alors n est premier avec tout élément $k \in [\![1, n-1]\!]$, donc n est premier, et :

$$(n-1)\,! \equiv \sum_{k=1}^{n-1} \binom{n-1}{k} (-1)^{k+n-1} \equiv \sum_{k=1}^{n-1} \binom{n-1}{k} (-1)^{n-1-k} \equiv$$
$$\equiv (1-1)^{n-1} - (-1)^{n-1} \equiv (-1)^n \mod (n) \ .$$

Comme n est premier impair, ou $n = 2$, on en déduit le théorème de Wilson.

Exercice 24 :

Déterminer tous les polynômes $P \in \mathbb{C}[X]$ tels que
$$P(X^2) = P(X)\,P(X-1)\,. \blacksquare$$

Supposons que $P \in \mathbb{C}[X]$ soit un polynôme non nul qui vérifie cette condition.
Si $\alpha \in \mathbb{C}$ est un zéro de P, comme $P(\alpha^2) = P(\alpha)P(\alpha-1) = 0$, α^2 est un zéro de P ; on voit alors que pour tout $n \in \mathbb{N}$, α^{2^n} est un zéro de P. Comme l'ensemble des zéros de P est fini, l'application $n \mapsto \alpha^{2^n}$ est non injective, il existe donc deux entiers distincts n et m tels que $\alpha^{2^n} = \alpha^{2^m}$; supposons $n > m$, α vérifie l'égalité $\alpha^{2^m}(\alpha^{2^n - 2^m} - 1) = 0$. Nous pouvons déduire de ce qui précède qu'un zéro de P est nécessairement soit 0 soit un complexe de module 1.
Soit α un zéro de P, comme $P((\alpha+1)^2) = P(\alpha+1)\,P(\alpha) = 0$, $(\alpha+1)^2$ est un zéro de P ; nous pouvons en déduire que soit $\alpha = -1$, soit $|\alpha+1| = 1$. On voit alors que 1 ne peut pas être zéro de P ; comme $P(1) = P(1)\,P(0)$, 0 n'est pas un zéro de P, et comme $P(0) = P(0)\,P(-1)$, -1 n'est pas non plus zéro de P.
On déduit de ce qui précède que si α est un zéro de P, alors $|\alpha| = 1$ et $|\alpha+1| = 1$. Il est géométriquement clair que les zéros de P ne peuvent être que j et j^2, racines cubiques de 1, et par conséquent, puisque d'autre part le coefficient dominant de P est nécessairement 1, que le polynôme P est nécessairement de la forme $P = (X-\mathrm{j})^a\,(X-\mathrm{j}^2)^b$, où a et b sont des entiers naturels.
Les entiers naturels a et b étant donnés, le polynôme $P = (X-\mathrm{j})^a\,(X-\mathrm{j}^2)^b$ vérifie la condition de l'énoncé si, et seulement si :

$$(X^2-\mathrm{j})^a\,(X^2-\mathrm{j}^2)^b = (X-\mathrm{j})^a\,(X-\mathrm{j}^2)^b\,(X-1-\mathrm{j})^a(X-1-\mathrm{j}^2)^b \ .$$

En utilisant les égalités $1+\mathrm{j}+\mathrm{j}^2 = 0$, et $\mathrm{j} = \mathrm{j}^4$, on obtient la condition nécessaire et suffisante :

$$(X-\mathrm{j}^2)^a\,(X+\mathrm{j}^2)^a\,(X-\mathrm{j})^b\,(X+\mathrm{j})^b = (X-\mathrm{j})^a\,(X-\mathrm{j}^2)^b\,(X+\mathrm{j}$$

soit après simplification :

$$(X - \mathrm{j}^2)^a (X - \mathrm{j})^b = (X - \mathrm{j})^a (X - \mathrm{j}^2)^b .$$

Comme $\mathrm{j} \neq \mathrm{j}^2$, cette condition est réalisée si, et seulement si, $a = b$.

Les polynômes $P \in \mathbb{C}[X]$ tels que $P(X^2) = P(X)\,P(X+1)$ sont donc les puissances entières du polynôme $1 + X + X^2$, et le polynôme nul.

§ VII.5 *RACINES D'UN POLYNÔME. FORMULE DE TAYLOR*

Exercice 6 :

Le corps de base est de caractéristique nulle. On donne des entiers $n \geqslant 2$, $p \geqslant 2$ et $(n_i)_{1 \leqslant i \leqslant p}$ tels que $\sum_{i=1}^{p} n_i = n$, ainsi que des éléments $a_1, a_2, \ldots, a_p$ de K distincts. Pour chaque $i \in [\![1, p]\!]$, soit $\Phi_i(X) = \prod_{j \neq i} (X - a_j)^{n_j}$.

a) Montrer que les $(X - a_i)^k \Phi_i$ $(0 \leqslant k \leqslant n_i - 1)$ forment une base du K-ev U_i des $F \in K_{(n-1)}[X]$ tels que $F^{(\nu)}(a_j) = 0$ pour tout $j \neq i$ et tout $\nu \leqslant n_j - 1$.

b) On donne une famille $(b_{i,k})_{i \in [\![1,p]\!],\, k \in [\![1, n_i - 1]\!]}$ d'éléments de K. Montrer qu'il existe un, et un seul, polynôme $F \in K_{(n-1)}[X]$ tel que $F^{(\nu)}(a_j) = b_{j,\nu}$ pour $j \in [\![1, p]\!]$ et $\nu \leqslant n_j - 1$.

Que retrouve-t-on pour tous les n_i égaux à 1 ? Expliciter le résultat pour tous les n_i égaux à 2 (Formule de Hermite). ■

a) L'espace U_i est l'espace des polynômes qui admettent chacun des a_j, où $j \neq i$, comme zéro a un ordre multiplicité $\geqslant n_j$, et dont le degré est $\leqslant n-1$ (U_i contient aussi le polynôme nul). C'est donc le sous-K-ev des polynômes divisibles par Φ_i, et dont le degré est $\leqslant n-1$. Comme $\deg(\Phi_i) = \sum_{j \neq i} n_j = n - n_i$, l'espace U_i est le sous-K-ev des polynômes qui s'écrivent $A\Phi$, où $A \in K_{n_i - 1}[X]$. La famille $((X - a_i)^k)_{k \in [\![0, n_i - 1]\!]}$ étant une base du sous-K-ev $K_{n_i - 1}[X]$, il est clair que la famille $((X - a_i)^k \Phi_i)_{k \in [\![0, n_i - 1]\!]}$ est une base du sous-K-ev U_i ; ce sous-espace est donc de dimension n_i.

Pour $i \in [\![1, p]\!]$, notons E_i le sous-K-ev de l'espace $K_{n-1}[X]$, constitué par les polynômes divisibles par $(X - a_i)^{n_i}$. L'espace $U_i \cap E_i$ est le sous-K-ev de $K_{n-1}[X]$ constitué par les polynômes divisibles par $\prod_{j=}^{p} (X - a_j)^{n_i}$

polynôme de degré n ; on voit donc que $U_i \cap E_i = \{0\}$. D'autre part, pour tout $j \neq i$, $U_j \subset E_i$, donc $\underset{j\neq i}{+} U_j \subset E_i$. Il est donc clair que les sous-K-ev U_i, où $i \in [\![1,p]\!]$, sont en somme directe. Comme pour tout $i \in [\![1,p]\!]$, $\dim(U_i) = n_i$, et que $\sum_{i=1}^{p} n_i = n$, on voit que :

$$K_{n-1}[X] = \bigoplus_{i=1}^{p} U_i ,$$

et donc que la famille $((X-a_i)^k \Phi_i)_{i\in[\![1,p]\!],\, k\in[\![0,n_i-1]\!]}$, est une base du K-ev $K_{n-1}[X]$.

b) Considérons l'application K-linéaire qui à un élément F de $K_{n-1}[X]$ fait correspondre la famille $(F^{(\nu)}(a_j))_{j\in[\![1,p]\!],\, \nu\in[\![0,n_j-1]\!]}$, élément d'un K-espace vectoriel de dimension $\sum_{i=1}^{p} n_i = n$. Cette application est injective car si pour tout $j \in [\![1,p]\!]$ et, pour j donné pour tout $\nu \in [\![0,n_j-1]\!]$, $F^{(\nu)}(a_j) = 0$, alors F est nul ou admet tous les a_j, où $j \in [\![1,p]\!]$, comme zéro à un ordre de multiplicité $\geqslant n_j$, donc est de degré $\geqslant n$. Comme la dimension de l'espace de départ est égale à la dimension de l'espace d'arrivée, cette application linéaire est bijective, ce qu'il fallait démontrer.

Si tous les n_i sont égaux à 1, on retrouve le théorème VII.4.3 (polynôme d'interpolation de Lagrange).
Si tous les n_i sont égaux à 2, posons pour tout $i \in [\![1,p]\!]$ et pour tout $k \in \{0,1\}$, $A_{i,k} = (X-a_i)^k \Phi_i$. D'après ce qui a été démontré dans la question *a*), la famille $(A_{i,k})_{i\in[\![1,p]\!],\, k\in\{0,1\}}$ est une base du K-espace $K_{n-1}[X]$ (remarquons que $n = 2p$).
Soit $i \in [\![1,p]\!]$ et $k \in \{0,1\}$. On voit que pour tout $j \neq i$ et pour tout $\nu \in \{0,1\}$, $A_{i,k}^{(\nu)}(a_j) = 0$. Comme $A_{i,k} = (X-a_i)^k \Phi_i$, on obtient $A_{i,0}(a_i) = \Phi_i(a_i)$, $A_{i,1}(a_i) = 0$, $A'_{i,0}(a_i) = \Phi'_i(a_i)$, $A'_{i,1}(a_i) = \Phi_i(a_i)$. Exhibons maintenant deux polynômes $B_{i,0}$ et $B_{i,1}$ qui engendrent le même sous-espace que $A_{i,0}$ et $A_{i,1}$, mais tels que $B_{i,0}(a_i) = 1$, $B'_{i,0}(a_i) = 0$, $B_{i,1}(a_i) = 0$ et $B'_{i,1}(a_i) = 1$. Il suffit de poser $B_{i,1} = (1/\alpha_i)A_{i,1}$, et $B_{i,0} = (1/\alpha_i)A_{i,0} - (\beta_i/\alpha_i^2)A_{i,1}$, où $\alpha_i = \Phi_i(a_i)$ et $\beta_i = \Phi'_i(a_i)$; en résumé :

$$B_{i,0} = \frac{\Phi_i(a_i) - \Phi'_i(a_i)\,(X-a_i)}{\Phi_i^2(a_i)}\Phi_i \qquad B_{i,1} = \frac{X-a_i}{\Phi_i(a_i)}\,\Phi_i .$$

On voit que le polynôme :

$$F = \sum_{i\in[\![1,p]\!],\, k\in\{0,1\}} b_{i,k}\, B_{i,k} ,$$

est tel que pour tout $j \in [\![1,p]\!]$ et tout $\nu \in \{0,1\}$, $F^{(\nu)}(a_j) = b_{j,\nu}$.

Exercice 9 :

Déterminer les polynômes P solutions des équations différentielles suivantes :

a) $(1-X)P'(X) - P(X) = X^n$.

b) $X(X-1)P' + P^2 - (2X+1)P + 2X = 0$.

c) $XP'' - (X+m)P' + nP = 0$ (avec $m \in \mathbb{N}^*$, $n \in \mathbb{N}^*$).

d) $X(X+1)P'' + (X+2)P' - P = 0$.

e) $(1+X^2)P'' - (2X+1)P' + 2P = 0$. ■

Nous supposerons que le corps de base, K, est de caractéristique 0.

a) L'équation s'écrit $P' - (XP)' = X^n$. Le polynôme P est donc solution si, et seulement si, il existe un scalaire $a \in K$ tel que :

$$(1-X)P = \frac{X^{n+1} + a}{n+1}.$$

Le scalaire a étant nécessairement -1, l'équation a une et une seule solution :

$$P = -\frac{1 + X + X^2 + \ldots + X^n}{n+1}.$$

b) Supposons que le polynôme $P \neq 0$ de degré p soit solution de l'équation (0 n'est pas solution). On voit que le polynôme $(2X+1)P - X(X-1)P' - 2X$ est de degré $\leqslant p+1$, et puisque c'est P^2 on en déduit $2p \leqslant p+1$, soit $p \leqslant 1$. Posons $P = a + bX$, où $(a,b) \in K$, le polynôme P est solution de l'équation si, et seulement si :

$$bX(X-1) + (a+bX)^2 - (2X+1)(a+bX) + 2X = 0.$$

On trouve facilement les conditions :

$$b^2 - b = 0 \quad 2ab - 2a - 2b + 2 = 0 \quad a^2 - a = 0,$$

ce qui s'écrit encore :

$$b(b-1) = 0 \quad (a-1)(b-1) = 0 \quad a(a-1) = 0.$$

Le scalaire a est 0 ou 1, si c'est 0, alors $b = 1$, si c'est 1, alors $b = 0$ ou $b = 1$. L'équation différentielle a donc trois solutions : X, 1 e

c) Supposons que le polynôme non nul P de degré p soit solution. L'équation s'écrit aussi $n\,P - X\,P' = m\,P' - X\,P''$, le polynôme $n\,P - X\,P'$ est donc dans le sous-K-espace $K_{p-1}[X]$. Nous en déduisons que si $a \neq 0$ est le coefficient dominant du polynôme P, $na - pa = 0$, d'où $n = p$. Un polynôme solution de l'équation est donc soit nul soit exactement de degré n.

Le polynôme $P = \sum_{k=0}^{n} a_k\,X^k$ est solution si, et seulement si :

$$n\sum_{k=0}^{n} a_k\,X^k - \sum_{k=1}^{n} k\,a_k\,X^k = m\sum_{k=1}^{n} k\,a_k\,X^{k-1} - \sum_{k=2}^{n} k(k-1)\,a_k\,X^{k-1}\ .$$

Cette condition s'écrit :

$$\sum_{k=0}^{n-1}(n-k)\,a_k\,X^k = \sum_{k=1}^{n} k(m-k+1)\,a_k\,X^{k-1} = \sum_{h=0}^{n-1}(h+1)(m-h)a_{h+1}\,X^h\ ,$$

elle est donc équivalente à la condition :

$$(\forall k \in [\![0, n-1]\!]) \quad (n-k)\,a_k = (k+1)(m-k)\,a_{k+1}\ .$$

Le polynôme P est donc déterminé par son coefficient dominant a_n ; l'ensemble des solutions est un sous-K-espace de dimension 1. On obtient :

$$a_{n-1} = \frac{n\,(m-n+1)}{1}\,a_n\ , \quad a_{n-2} = \frac{(n-1)\,(m-n+2)}{2}\,a_{n-1}\ ,$$

etc., d'où pour tout $k \in [\![1, n]\!]$:

$$a_{n-k} = \frac{n\,(n-1)\ldots(n-k+1)\,(m-n+1)\ldots(m-n+k)}{1\ldots k}\,a_n\ ,$$

Soit encore pour tout $i \in [\![0, n-1]\!]$:

$$(1) \qquad a_i = \binom{n}{i}\,(m-n+1)\,(m-n+2)\ldots(m-i)\,a_n\ .$$

Supposons $m \in [\![0, n-1]\!]$; il est clair que $a_m = 0$, et que tous les coefficients a_i, pour $i \in [\![0, m]\!]$ sont aussi nuls ; et si $i \in [\![m+1, n-1]\!]$ (ce qui implique $n - m - 1 > 0$) on a :

$$a_i = \binom{n}{i}(-1)^{n-i}(i-m)\ldots(n-m-1)\,a_n = \binom{n}{i}(-1)^{n-i}\frac{(n-m-1)\,!}{(i-}$$

Cette égalité est vraie aussi si $i = n$.
Supposons $m \geqslant n$. L'égalité (1) s'écrit alors pour tout $i \in [\![0, n-1]\!]$:

$$a_i = \binom{n}{i} \frac{(m-i)!}{(m-n)!} a_n \ .$$

Cette égalité est vraie aussi si $i = n$.

d) Soit $P = a_p X^p + \ldots + a_0$, où $a_p \in K \setminus \{0\}$, un polynôme non nul de degré $p \geqslant 2$. Le coefficient du monôme de degré p dans le polynôme $X(X+1)P'' + (X+2)P' - P$ est $\big(p(p-1) + p - 1\big) a_p = (p^2 - 1) a_p \neq 0$. Les solutions de l'équation sont donc nécessairement de degré $\leqslant 1$.
Le polynôme $a + bX$, où $(a, b) \in K^2$ est solution si, et seulement si :

$$b(X+2) = a + bX \ .$$

Les solutions de l'équation sont donc les polynômes de la forme $b(X+2)$, où $b \in K$.

e) Soit $P = a_p X^p + \ldots + a_0$, où $a_p \in K \setminus \{0\}$, un polynôme non nul de degré $p \geqslant 2$. Le coefficient du monôme de degré p dans le polynôme $(1+X^2)P'' - (2X+1)P' + 2P$ est $\big(p(p-1) - 2p + 2\big) a_p = (p^2 - 3p + 2) a_p = (p-1)(p-2) a_p$. Les solutions de l'équation sont donc nécessairement de degré $\leqslant 2$.
Le polynôme $a + bX + cX^2$, où $(a, b, c) \in K^3$ est solution si, et seulement si :

$$2c(1+X^2) - (2X+1)(b+2cX) + 2(a+bX+cX^2) = 0 \ ,$$

soit si, et seulement si :

$$2c - 4c + 2c = 0 \quad -2b - 2c + 2b = 0 \quad 2c - b + 2a = 0 \ .$$

Les solutions de l'équation sont donc les polynômes de la forme $a(1+2X)$, où $a \in K$.

Exercice 10 :

Un calcul des polynômes de Tchebychev

On reprend les notations de l'exercice 8 du §VII.4, c'est-à-dire que pour tout $n \in \mathbb{N}$, T_n et U_n sont les polynômes à coefficients réels tels que pour tout $\theta \in \mathbb{R}$:

$$T_n(\cos\theta) = \cos(n\theta) \qquad \text{et} \qquad \sin\theta \, U_n(\cos\theta) = \sin(n+1)\theta \ .$$

a) Démontrer que, pour n fixé $\geqslant 2$, le polynôme T_n satisfait l'équation différentielle

$$(1-X^2)\,T_n''(X) - X\,T_n'(X) + n^2 T_n(X) = 0$$

(on suppose connues les dérivées des fonctions élémentaires utilisées en Analyse). Déduire de là des relations de récurrence entre les coefficients de T_n. Calculer $T_n(0)$ et $T_n'(0)$ et en déduire l'expression exacte de chaque coefficient.

b) Montrer que le polynôme U_n vérifie l'équation différentielle

$$(1-X^2)\,U_n''(X) - 3\,X\,U_n'(X) + n(n+2)\,U_n(X) = 0\,.$$

Par une méthode analogue trouver l'expression de U_n. ■

a) En dérivant l'égalité $T_n(\cos\theta) = \cos(n\,\theta)$ vraie pour tout $\theta \in \mathbb{R}$, on trouve :

$$(\forall \theta \in \mathbb{R}) \quad \sin\theta\, T_n'(\cos\theta) = n \sin n\,\theta\,.$$

En dérivant encore une fois on obtient :

$$(\forall \theta \in \mathbb{R}) \quad \cos\theta\, T_n'(\cos\theta) - \sin^2\theta T_n''(\cos\theta) = n^2 \cos n\,\theta = n^2\, T_n(\cos\theta)\,.$$

Nous pouvons en déduire l'égalité :

$$(\forall x \in [-1,1]) \quad x\,T_n'(x) - (1-x^2)\,T_n''(x) - n^2\,T_n(x) = 0\,.$$

Le polynôme T_n vérifie donc l'équation différentielle :

$$(1-X^2)\,T_n''(X) - X\,T_n'(X) + n^2 T_n(X) = 0\,.$$

On peut établir à l'aide de cette équation différentielle que le degré du polynôme T_n est nécessairement n. En effet, s'il est de degré p et de coefficient dominant $a \neq 0$, on trouve la condition $a\left(n^2 - p - p(p-1)\right) = a\,(n^2 - p^2) = 0$. L'entier $n \geqslant 2$ étant donné, posons $T_n = \sum_{k=0}^{n} a_k\,X^k$. L'équation différentielle que vérifie T_n s'écrit aussi :

$$T_n'' = X^2\,T_n''(X) + X\,T_n'(X) - n^2 T_n(X)\,,$$

soit :

$$\sum_{k=2}^{n} k(k-1)\,a_k\,X^{k-2} = \sum_{k=2}^{n} k(k-1)\,a_k\,X^k + \sum_{k=1}^{n} k\,a_k\,X^k - n^2 \sum_{k=0}^{n} a_k\,X^k\,.$$

En posant $h = k-2$ dans la première somme, et en ramenant l'indice de début de chacune des sommes de droite à 0, on obtient :

$$\sum_{h=0}^{n-2} (h+2)(h+1)\,a_{h+2}\,X^h = \sum_{k=0}^{n} (k^2 - n^2)\,a_k\,X^k\,.$$

Cette égalité équivaut aux conditions $a_{n-1} = 0$ et :

$$(\forall k \in [\![0, n-2]\!]) \quad (k+2)(k+1)\, a_{k+2} = (k^2 - n^2)\, a_k = -(n-k)(n+k) a_k \ .$$

Nous voyons que pour tout $p \in \mathbb{N}$ tel que $n - (2p+1) \geqslant 0$, $a_{n-(2p+1)} = 0$, et que les coefficients a_{n-2p}, peuvent être déterminés par récurrence à partir de la valeur de a_n. On voit que :

$$a_{n-2} = -\frac{n(n-1)}{2 \cdot 2(n-1)}\, a_n \quad , \quad a_{n-4} = -\frac{(n-2)(n-3)}{4 \cdot 2(n-2)}\, a_{n-2} \ ,$$

etc., de telle sorte que pour p entier tel que $n - 2p \geqslant 0$:

$$a_{n-2p} = (-1)^p \frac{n(n-1)\dots(n-2p+1)}{2^{2p} \times 1 \cdot 2 \dots p \times (n-1)\dots(n-p)}\, a_n \ ,$$

soit encore :

$$a_{n-2p} = (-1)^p\, n\, \frac{(n-p-1)!}{2^{2p}\,(n-2p)!\,p!}\, a_n \ .$$

Déterminons maintenant les coefficients a_0 et a_1.
Nous utiliserons les égalités :

$$a_0 = T_n(0) = T_n(\cos(\pi/2)) = \cos n\,(\pi/2) \ ,$$

et :

$$a_1 = T_n'(0) = T_n'(\cos(\pi/2)) = n \frac{\sin n\,(\pi/2)}{\sin(\pi/2)} \ .$$

Si n est pair, $n = 2q$, alors $a_0 = (-1)^q$ et $a_1 = 0$ (ce qui était prévu) ; on trouve :

$$(-1)^q = a_{2q-2q} = (-1)^q 2q \frac{(q-1)\,!}{2^{2q}\,q\,!}\, a_{2q} = (-1)^q \frac{2\, a_{2q}}{2^{2q}} \ ,$$

d'où $a_{2q} = 2^{2q-1} = 2^{n-1}$.
Si n est impair, $n = 2q+1$, alors $a_0 = 0$ et $a_1 = (-1)^q\,(2q+1)$; on trouve :

$$(-1)^q(2q+1) = a_{2q+1-2q} = (-1)^q(2q+1) \frac{q!}{2^{2q}\,1!\,q!}\, a_{2q+1} = (-1)^q \frac{2q+1}{2^{2q}}\, a_{2q+1},$$

d'où $a_{2q+1} = 2^{2q} = 2^{n-1}$.
Nous obtenons donc, pour tout p entier tel que $n - 2p \geqslant 0$, l'égalité :

$$a_{n-2p} = (-1)^p\, n\, 2^{n-1}\, \frac{(n-p-1)!}{2^{2p}\,(n-2p)!\,p!} \ .$$

En particulier (si $n \geqslant 2$) :

$$a_{n-2} = -\frac{n(n-1)}{4(n-1)}\, a_n = -n\, 2^{n-3} .$$

Les autres coefficients sont nuls.

b) En dérivant l'égalité $\sin\theta\, U_n(\cos\theta) = \sin(n+1)\,\theta$, vraie pour tout $\theta \in \mathbb{R}$, on trouve :

$$(\forall \theta \in \mathbb{R}) \quad \cos\theta\, U_n(\cos\theta) - \sin^2\theta\, U_n'(\cos\theta) = (n+1)\,\cos(n+1)\,\theta .$$

En dérivant encore une fois on obtient :

$$(\forall \theta \in \mathbb{R})$$
$$-\sin\theta\, U_n(\cos\theta) - 3\,\sin\theta\,\cos\theta\, U_n'(\cos\theta) + \sin^3\theta\, U_n''(\cos\theta) =$$
$$= -(n+1)^2\,\sin(n+1)\,\theta = -(n+1)^2\,\sin\theta\, U_n(\cos\theta) .$$

Nous pouvons en déduire l'égalité :

$$(\forall x \in]0,1[) \quad -U_n(x) - 3\,x\,U_n'(x) + (1-x^2)\,U_n''(x) + (n+1)^2\,U_n(x) = 0 .$$

Le polynôme U_n vérifie donc l'équation différentielle :

$$(1-X^2)\,U_n''(X) - 3X\,U_n'(X) + n(n+2)\,U_n(X) = 0 .$$

On peut établir à l'aide de cette équation différentielle que le degré du polynôme U_n est nécessairement n. En effet, s'il est de degré p et de coefficient dominant $a \neq 0$, on trouve la condition :

$$a\,(n(n+2) - 3p - p(p-1)) = a\,\big(n(n+2) - p(p+2)\big) = 0 .$$

L'entier $n \geqslant 2$ étant donné, posons $U_n = \sum_{k=0}^{n} a_k\, X^k$. L'équation différentielle que vérifie U_n s'écrit aussi :

$$U_n'' = X^2\, U_n''(X) + 3X\, U_n'(X) - n(n+2)U_n(X) ,$$

soit :

$$\sum_{k=2}^{n} k(k-1)\, a_k\, X^{k-2} = \sum_{k=2}^{n} k(k-1)\, a_k\, X^k + 3\sum_{k=1}^{n} k\, a_k\, X^k - n(n+2)\sum_{k=0}^{n} a_k\, X^k .$$

En posant $h = k-2$ dans la première somme, et en ramenant l'indice de début de chacune des sommes de droite à 0, on obtient :

$$\sum_{h=0}^{n-2} (h+2)(h+1)\, a_{h+2}\, X^h = \sum_{k=0}^{n} \big(k(k+2) - n(n+2)\big)\, a_k\, X^k$$

Cette égalité équivaut aux conditions $a_{n-1} = 0$ et $(\forall k \in [\![0, n-2]\!])$:

$$(k+2)(k+1)\,a_{k+2} = -(n(n+2) - k(k+2))\,a_k = -(n-k)(n+k+2)\,a_k \ .$$

Nous voyons que pour tout $p \in \mathbb{N}$ tel que $n-(2p+1) \geqslant 0$, $a_{n-(2p+1)} = 0$, et que les coefficients a_{n-2p}, peuvent être déterminés par récurrence à partir de la valeur de a_n. On voit que :

$$a_{n-2} = -\frac{n(n-1)}{2 \cdot 2n}\,a_n \quad , \quad a_{n-4} = -\frac{(n-2)(n-3)}{4 \cdot 2(n-1)}\,a_{n-2} \ ,$$

etc., de telle sorte que pour p entier tel que $n - 2p \geqslant 0$:

$$a_{n-2p} = (-1)^p \frac{n(n-1)\ldots(n-2p+1)}{2^{2p} \times 1 \cdot 2 \ldots p \times n\,(n-1)\ldots(n-p+1)}\,a_n \ ,$$

soit encore :

$$a_{n-2p} = (-1)^p \frac{(n-p)!}{2^{2p}\,(n-2p)!\,p!}\,a_n \ .$$

Déterminons maintenant les coefficients a_0 et a_1.
Nous utiliserons les égalités :

$$a_0 = U_n(0) = U_n(\cos(\pi/2)) = \frac{\sin(n+1)\,\pi/2}{\sin \pi/2} = \sin(n+1)\,\pi/2 \ ,$$

et :

$$a_1 = U_n'(0) = U_n'(\cos \pi/2) \ ;$$

comme :

$$(\forall \theta \in \mathbb{R}) \quad \cos\theta\, U_n(\cos\theta) - \sin^2\theta\, U_n'(\cos\theta) = (n+1)\,\cos(n+1)\,\theta \ ,$$

en particulier pour $\theta = \pi/2$, nous trouvons :

$$a_1 = -(n+1)\,\cos(n+1)\pi/2 \ .$$

Si n est pair, $n = 2q$, alors $a_0 = (-1)^q$ et $a_1 = 0$ (ce qui était prévu) ; on trouve :

$$(-1)^q = a_{2q-2q} = (-1)^q \frac{q\,!}{2^{2q}\,q\,!}\,a_{2q} = (-1)^q \frac{a_{2q}}{2^{2q}} \ ,$$

d'où $a_{2q} = 2^{2q} = 2^n$.
Si n est impair, $n = 2q+1$, alors $a_0 = 0$ et $a_1 = (-1)^q\,(2q+2)$; on trouve :

$$(-1)^q\,(2q+2) = a_{2q+1-2q} = (-1)^q \frac{(q+1)\,!}{2^{2q}\,1!\,q\,!}\,a_{2q+1} = (-1)^q \frac{q+1}{2}$$

d'où $a_{2q+1} = 2^{2q+1} = 2^n$.
Nous obtenons donc, pour tout p entier tel que $n - 2p \geqslant 0$, l'égalité :

$$a_{n-2p} = (-1)^p \, 2^n \, \frac{(n-p)!}{2^{2p}\,(n-2p)!\,p!} \ .$$

Les autres coefficients sont nuls.

Nous aurions pu trouver plus vite ce résultat en remarquant que pour tout $n \in \mathbb{N}$:

$$T'_{n+1}(X) = (n+1)\,U_n(X) \ .$$

Exercice 11 :

Soit $n \in \mathbb{N}^*$ et $T_n \in \mathbb{C}[X]$ le n-ième polynôme de Tchebychev de première espèce défini dans l'exercice précédent. On observera d'abord que $T_p \circ T_q = T_{pq}$ pour tous p et q dans $\mathbb{N}$.

a) Montrer que T_n et $-T_n$ sont les seules solutions polynomiales non constantes de l'équation différentielle

$$(1 - X^2)\,Y'^2 - n^2\,(1 - Y^2) = 0 \ .$$

b) Soit $n \geqslant 2$, montrer que les seuls polynômes non constants $P \in \mathbb{C}[X]$ tels que $P \circ T_n = T_n \circ P$ sont si n est pair les T_k , $k \in \mathbb{N}^*$, et si n est impair les polynômes εT_k , où $\varepsilon = \pm 1$, et $k \in \mathbb{N}^*$. ■

On vérifie que pour tous p et q entiers, pour tout $\theta \in \mathbb{R}$:

$$T_p(T_q(\cos\theta)) = T_p(\cos q\theta) = \cos pq\theta = T_{pq}(\cos\theta) \ .$$

Nous pouvons en déduire que les polynômes $T_p \circ T_q$ et T_{pq} sont identiques.

a) Supposons que le polynôme P non constant soit solution de l'équation différentielle de l'énoncé ; en dérivant on obtient la relation :

$$-2X\,P'^2 + 2\,(1 - X^2)P'\,P'' + 2n^2\,P\,P' = 0 \ ,$$

et par conséquent :

$$(1 - X^2)\,P'' - X\,P' + n^2\,P = 0 \ .$$

D'après les résultats trouvés lors de la résolution de l'exercice précédent, les solutions polynomiales de cette équation différentielle sont proportionnelles à T_n . Il existe donc un scalaire $\lambda \in \mathbb{C}$ tel que $P = \lambda T_n$.

Si P est de cette forme alors le polynôme $(1-X^2)P'^2 - n^2(1-P^2)$ a une dérivée nulle, donc est constant ; sa valeur en 1 est $-n^2(1-\lambda^2 T_n^2(1))$, et comme $T_n(1) = T_n(\cos 0) = \cos 0 = 1$, cette valeur est nulle si, et seulement si, $\lambda^2 = 1$. Le polynôme λT_n est donc solution de l'équation différentielle de l'énoncé si, et seulement si, $\lambda = \pm 1$. Les solutions polynomiales non constantes de cette équation sont donc bien T_n et $-T_n$.

b) De la résolution de l'exercice précédent, nous utiliserons le fait que pour tout n entier, $n \geqslant 2$, le polynôme T_n est de la forme $T_n = a_n X^n - b_n X^{n-2} + \ldots$, où a_n et b_n sont des scalaires non nuls ($a_n = 2^{n-1}$ et $b_n = n\,2^{n-3}$).
Soit P un polynôme non constant de degré $p \geqslant 1$ tel que $P \circ T_n = T_n \circ P$. Posons $P = \lambda T_p + Q$, où $\lambda \in \mathbb{C}^*$, et $Q \in \mathbb{C}_{p-1}[X]$. La condition s'écrit :

$$\lambda T_p \circ T_n + Q \circ T_n = T_n \circ (\lambda T_p + Q)\ . \tag{1}$$

Nous voulons d'abord démontrer par l'absurde que $Q = 0$.

Supposons que Q soit non nul de degré $q < p$. En utilisant la formule de Taylor, la condition (1) s'écrit sous la forme :

$$\lambda T_p \circ T_n + Q \circ T_n = T_n(\lambda T_p) + \sum_{h=1}^{n} \frac{Q^h}{h!} T_n^{(h)}(\lambda T_p)\ .$$

Comme pour tout $h \in [\![1, n]\!]$, le polynôme $Q^h T_n^{(h)}(\lambda T_p)$ est de degré $q\,h + (n-h)\,p = n\,p - h(p-q)$, le degré du polynôme

$$A = \sum_{h=1}^{n} \frac{Q^h}{h!} T_n^{(h)}(\lambda T_p)\ ,$$

est $n\,p - (p-q)$.
Le degré du polynôme $B = Q \circ T_n$ est $q\,n$, et comme $q\,n < n\,p - (p-q)$, puisque $(p-q) < n\,(p-q)$, le degré du polynôme $A - B$ est $n\,p - (p-q)$.
Comme

$$T_p(T_n) = T_{np} = T_n(T_p) = a_n\,T_p^n - b_n\,T_p^{n-2} + \ldots\ ,$$

on voit que :

$$T_n(\lambda T_p) = a_n\,\lambda^n\,T_p^n - b_n\,\lambda^{n-2}\,T_p^{n-2} + \ldots\ ,$$

et donc que le polynôme $C = T_n(\lambda T_p) - \lambda^n\,T_{pn}$ est de degré $\leqslant p(n-2)$.
La condition s'écrit maintenant :

$$\lambda T_{pn} + B = C + \lambda^n\,T_{pn} + A\ .$$

Comme $\deg(C) \leqslant p(n-2) < np-(p-q)$, puisque $0 < p+q$, on en déduit finalement que le polynôme $(\lambda - \lambda^n)T_{pn}$ est de degré $np-(q-p)$, ce qui est évidemment impossible. Le polynôme Q est donc nécessairement nul, et le polynôme P est nécessairement de la forme λT_p.

La condition (1) s'écrit alors :

$$\lambda T_p \circ T_n = \lambda T_n(T_p) = T_n(\lambda T_p)\ , \tag{2}$$

soit :

$$\lambda a_n T_p^n - \lambda b_n T_p^{n-2} + \ldots = a_n \lambda^n T_p^n - b_n \lambda^{n-2} T_p^{n-2} + \ldots\ .$$

Par égalité des coefficients dominants, on trouve d'abord que $\lambda = \lambda^n$, puis que $\lambda = \lambda^{n-2}$; on voit donc que nécessairement $\lambda^2 = 1$.
En conclusion, si P est un polynôme non constant de degré p tel que $P \circ T_n = T_n \circ P$, alors $P = \varepsilon T_p$, où $\epsilon \in \{-1,+1\}$.

Le polynôme $P = \varepsilon T_p$, où $\epsilon \in \{-1,+1\}$, vérifie la condition (2) si, et seulement si, $\varepsilon T_n(T_p) = T_n(\varepsilon T_p)$. Si n est pair alors T_n est pair, et $T_n(\varepsilon T_p) = T_n(T_p) = T_{np}$; dans ce cas la seule solution de degré p est T_p. Si n est impair, alors T_n est impair, et $T_n(\varepsilon T_p) = \varepsilon T_n(T_p) = \varepsilon T_{np}$; dans ce cas les solutions de degré p sont les polynômes T_p et $-T_p$.
L'ensemble des polynômes non constants P tels que $P \circ T_n = T_n \circ P$ est donc,
- si n est pair l'ensemble des polynômes T_p, où $p \in \mathbb{N}^*$;
- si n est impair l'ensemble des polynômes εT_p, où $p \in \mathbb{N}^*$, et $\varepsilon \in \{-1,+1\}$.

Autre solution. Nous utiliserons la notion d'indice d'une fraction rationnelle non constante $F \in \mathbb{C}(X)$, notion abordée dans l'exercice 6 du § VIII.3.
Soit P un polynôme non constant de degré $p \geqslant 1$ tel que $P \circ T_n = T_n \circ P$.
En dérivant cette identité nous obtenons :

$$(P' \circ T_n)\, T_n' = (T_n' \circ P)\, P'\ .$$

Or $T_n'^2 (1-X^2) = n^2 (1-T_n^2)$, donc :

$$(P' \circ T_n)^2\, T_n'^2 = (P' \circ T_n)^2\, \frac{n^2(1-T_n^2)}{1-X^2} =$$

$$= (T_n' \circ P)^2\, P'^2 = \frac{n^2\left(1-(T_n \circ P)^2\right)}{1-P^2}\, P'^2\ ,$$

d'où

$$\frac{(P' \circ T_n)^2 (1-T_n^2)}{1-(T_n \circ P)^2} = \frac{P'^2 (1-X^2)}{1-P^2}\ . \tag{1}$$

Comme $T_n \circ P = P \circ T_n$, l'égalité (1) s'écrit sous la forme (2) $F \circ T_n = F$, où F est la fraction rationnelle non nulle :

$$F = \frac{P'^2 (1 - X^2)}{1 - P^2} .$$

Supposons que la fraction rationnelle F ne soit pas constante, et notons k son indice ($k > 0$). Le polynôme T_n est de degré n, donc d'indice n en tant que fraction rationnelle. L'indice de $F \circ T_n = F$ est donc $kn = k$, ce qui est contradictoire ($n \geqslant 2$). La fraction rationnelle F est donc constante, sa valeur constante étant nécessairement p^2. On voit donc que le polynôme P vérifie la condition différentielle :

$$(1 - X^2) P'^2 - p^2 (1 - P^2) = 0 .$$

On a vu dans le *a*) que les seules solutions polynomiales de cette équation différentielle sont T_p et $-T_p$. Nous arrivons donc à la même conclusion que par la méthode précédente.

Exercice 22 :

Soit $P \in \mathbb{Z}[X]$ un polynôme de degré $\geqslant 1$ et $n \in \mathbb{Z}$. On pose $m = P(n)$.

a) Montrer que pour tout $k \in \mathbb{Z}$, $P(n + km)$ est divisible par m.

b) Montrer qu'il n'existe pas de polynôme non constant $P \in \mathbb{Z}[X]$ tel que pour tout $n \in \mathbb{Z}$, $|P(n)|$ soit premier.

c) Vérifier cependant que $n^2 - n + 41$ prend des valeurs premières pour $0 \leqslant n \leqslant 40$ et $n^2 - 79n + 1601$ pour $0 \leqslant n \leqslant 79$. ■

a) Il est clair que si P est un polynôme à coefficients entiers, il "conserve les congruences", c'est-à-dire que si n_1 et n_2 sont deux entiers tels que $n_1 \equiv n_2 \bmod (d)$, où $d \in \mathbb{N}$, alors $P(n_1) \equiv P(n_2) \bmod (d)$.
Nous en déduisons ici que $P(n + k\,m) \equiv P(n) \equiv m \equiv 0 \bmod (m)$, soit m divise $P(n + k\,m)$ (y compris si $m = 0$).

b) Remarquons que si le polynôme $Q \in \mathbb{Z}[X]$ n'est pas "constant" l'application polynomiale associée, de $\mathbb{Z}$ dans $\mathbb{Z}$, n'est pas constante.
Supposons que $P \in \mathbb{Z}[X]$ soit un polynôme non constant tel que pour tout $n \in \mathbb{Z}$, $|P(n)|$ soit premier. Soit $n \in \mathbb{N}$, on pose $m = P(n)$ ($|m|$ est premier). Comme le polynôme $P^2(n + mX)$ n'est pas constant ($m \neq 0$), il existe un entier $k \in \mathbb{Z}$, tel que $P^2(n + m\,k) \neq m^2$. Or $m \mid P(n + k\,m)$, et $|m|$ et $|P(n + k\,m)|$ sont premiers, donc $|m| = |P(n + k\,m)|$.

contradiction.
Il n'y a donc pas de polynôme non constant $P \in \mathbb{Z}[X]$ tel que pour tout $n \in \mathbb{Z}$, $|P(n)|$ soit premier.

c) Les nombres de la forme $n^2 - n + 41$, où $0 \leqslant n \leqslant 40$, sont minorés par 41 et majorés par $40^2 - 40 + 41 = 1601$. Si l'un de ces nombres n'était pas premier, il serait divisible par un nombre premier p tel que $p^2 \leqslant 1601$. Les diviseurs premiers possibles sont $3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37$ (l'entier $n(n-1)+41$ est impair). Si on démontre que l'équation $x^2 - x + 41 = 0$ n'a pas de racine dans le corps $\mathbb{Z}/p\mathbb{Z}$, où p est l'un de ces nombres premiers, alors il n'y aura pas d'entier n tel que $n^2 - n + 41$ soit divisible par l'un de ces nombres premiers. On pourra en déduire que les nombres $n^2 - n + 41$, où $0 \leqslant n \leqslant 40$, sont tous premiers.
Le polynôme $X^2 - X + 41$ a un zéro dans le corps $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, son discriminant $D = 1 - 4 \cdot 41 = -163$ est un carré dans ce corps. Nous sommes donc ramenés à calculer les résidus quadratiques de cet entier, modulo les nombres premiers énumérés ci-dessus.

Modulo 3 : $-163 \equiv -1$, D n'est pas un carré (carrés $0, 1$) ;
Modulo 5 : $-163 \equiv 2$, D n'est pas un carré, (carrés $0, 1, 4$) ;
Modulo 7 : $-163 \equiv -2$, D n'est pas un carré, (carrés $0, 1, 4, 2$).

On pourrait faire toutes les vérifications nécessaires à la main, mais le calcul serait assez long. Nous pouvons utiliser le critère d'Euler, cf. §VII.5 Exemple 3. On sait que $x \in \mathbb{Z}/p\mathbb{Z}$, $x \neq 0$, est un carré si, et seulement si la période multiplicative de x divise $(p-1)/2$; il suffit donc de calculer $(-163)^{(p-1)/2}$ modulo p, p premier : -163 ne sera pas un carré modulo p, si, et seulement si, le résultat est -1.

Modulo 11 : $-163 \equiv 2$, $2^5 \equiv 32 \equiv -1$;
Modulo 13 : $-163 \equiv 6$, $6^6 \equiv 6^2 \cdot 6^4 \equiv (-3) \cdot 9 \equiv -27 \equiv -1$;
Modulo 17 : $-163 \equiv 7$, $7^2 \equiv -2$, $7^4 \equiv 4$, $7^8 \equiv 16 \equiv -1$;
Modulo 19 : $-163 \equiv 8$, $8^2 \equiv 7$, $8^4 \equiv 11$, $8^8 \equiv 7$, $8^9 \equiv 56 \equiv -1$;
Modulo 23 : $-163 \equiv -2$, $(-2)^8 \equiv 256 \equiv 3$,
$(-2)^{11} \equiv -2^3 \cdot 2^8 \equiv -24 \equiv -1$;
Modulo 29 : $-163 \equiv 11$, $11^2 \equiv 5$, $11^4 \equiv -4$, $11^8 \equiv 16$,
$11^{14} \equiv 11^2 \cdot 11^4 \cdot 11^8 \equiv -320 \equiv -1$;
Modulo 31 : $-163 \equiv -8$, $8^2 \equiv 2$, $8^4 \equiv 4$, $8^8 \equiv 16$,
$(-8)^{15} \equiv -8^1 \cdot 8^2 \cdot 8^4 \cdot 8^8 \equiv -8 \cdot 2 \cdot 4 \cdot 16 \equiv -1$;
Modulo 37 : $-163 \equiv -15$, $15^2 \equiv 3$, $15^4 \equiv 9$, $15^8 \equiv 7$, $15^{16} \equiv 12$,
$(-15)^{18} \equiv 15^2 \cdot 15^{16} \equiv 3 \cdot 12 \equiv -1$.

Nous pouvons en déduire que pour toutes les valeurs de n entre 0 et 40, le nombre $n^2 - n + 41$ est premier (pour $n = 41$, il admet 41 c

premier).

Posons $P = X^2 - X + 41$ et $Q = X^2 - 79X + 1601$. On peut remarquer que :

$$Q = X^2 - 80X + X + 40^2 + 1 = (40 - X)^2 - (40 - X) + 41 = P(40 - X) .$$

L'ensemble des valeurs prises par le polynôme Q sur l'intervalle des entiers $[\![0, 79]\!]$ est donc l'ensemble des valeurs prises par le polynôme P sur l'intervalle des entiers $[\![-39, 40]\!]$. Or $P = X(X-1)+41$, donc $P(1-X) = (1 - X)(-X) + 41 = P(X)$; l'ensemble des valeurs prises par le polynôme P sur l'intervalle des entiers $[\![-39, 0]\!]$ est donc identique à l'ensemble des valeurs prises par ce polynôme sur l'intervalle des entiers $[\![1, 40]\!]$. Nous en déduisons donc que l'ensemble des valeurs prises par le polynôme Q sur l'intervalle des entiers $[\![0, 79]\!]$ est identique à l'ensemble des valeurs prises par le polynôme P sur l'intervalle des entiers $[\![0, 40]\!]$ et ne comporte donc que des nombres premiers.

Exercice 23 :

(Polynômes d'Euler) : K est de caractéristique nulle. Montrer qu'il existe un polynôme $P \in K[X]$ et un seul vérifiant

(1) $$P(X + 1) + P(X) = 2X^n \quad (n \in \mathbb{N}) .$$

Soit E_n le polynôme correspondant. Trouver une relation simple entre E'_n et E_{n-1}. Développer $E_n(X + 1)$ sous la forme $\sum a_p E_p(X)$ et en déduire une relation de récurrence entre E_n et les précédents. Expliciter E_n pour $n \in [\![0, 5]\!]$. Démontrer que

$$E_n(1 - X) = (-1)^n E_n(X) . \blacksquare$$

Soit $P \in K[X]$ un polynôme non nul de degré p, on voit que le polynôme $P(X + 1) + P(X)$ est non nul de degré p. Nous pouvons en déduire qu'une solution de l'équation (1) est nécessairement non nulle de degré n, et que l'application K-linéaire $P \mapsto P(X + 1) + P(X)$ est injective. Comme la restriction de cette application à $K_n[X]$ définit un endomorphisme de ce K-ev de dimension finie $n+1$, cette restriction est surjective. Il y a donc un et un seul polynôme solution de (1), et il est de degré n.

Pour tout $n \in \mathbb{N}^*$, en dérivant l'égalité :

$$E_n(X + 1) + E_n(X) = 2X^n ,$$

on trouve :

$$E'_n(X + 1) + E'_n(X) = 2nX^{n-1} .$$

Par unicité, nous en déduisons $(1/n)E'_n = E_{n-1}$, soit $E'_n = n\,E_{n-1}$. On voit aussi par récurrence que pour tout $k \in [\![0, n]\!]$:

$$E_n^{(k)} = n\,(n-1)\dots(n-k+1)\,E_{n-k} = \frac{n\,!}{(n-k)!}E_{n-k}\ .$$

En appliquant la formule de Taylor, on trouve que pour tout $n \in \mathbb{N}$:

$$E_n(X+1) = E_n(X) + \sum_{k=1}^{n} \frac{1}{k\,!}E_n^{(k)} = E_n + \sum_{k=1}^{n} \binom{n}{k} E_{n-k}\ ,$$

d'où :

$$2\,X^n - E_n(X) = E_n + \sum_{k=1}^{n} \binom{n}{k} E_{n-k}\ ,$$

soit enfin :

$$E_n = X^n - \frac{1}{2}\sum_{k=1}^{n} \binom{n}{k} E_{n-k}\ .$$

Il est clair que $E_0 = 1$; en utilisant la formule de récurrence trouvée ci-dessus on trouve $E_1 = X-(1/2)$, $E_2 = X^2-(1/2)\big(2(X-1/2)+1\big) = X^2-X$. Pour calculer E_3, E_4 et E_5, nous pouvons utiliser la relation $E'_n = n\,E_{n-1}$, cela permet de déterminer E_n à une constante près, la constante étant elle-même déterminée par la relation $E_n(1) + E_n(0) = 0$ (pour $n > 0$).

$E'_3 = 3\,X^2 - 3\,X$, $E_3 = X^3 - (3/2)X^2 + a$, $1 - (3/2) + 2a = 0$, $a = 1/4$;
d'où $E_3 = X^3 - (3/2)X^2 + 1/4$.

$E'_4 = 4\,X^3 - 6\,X^2 + 1$, $E_4 = X^4 - 2\,X^3 + X + a$, $1 - 2 + 1 + 2a = 0$, $a = 0$;
d'où $E_4 = X^4 - 2\,X^3 + X$.

$E'_5 = 5\,X^4 - 10\,X^3 + 5\,X$, $E_5 = X^5 - (5/2)X^4 + (5/2)X^2 + a$,
$1 - 5/2 + 5/2 + 2a = 0$, $a = -1/2$;
d'où $E_5 = X^5 - (5/2)X^4 + (5/2)X^2 - 1/2$.

Pour tout $n \in \mathbb{N}$ posons $F_n(X) = (-1)^n\,E_n(1-X)$; on voit que :

$$\begin{aligned} F_n(X+1) + F_n(X) &= (-1)^n\,\big(E_n(-X) + E_n(1+(-X))\big) = \\ &= (-1)^n\,2(-X)^n = 2\,X^n\ . \end{aligned}$$

Par unicité nous en déduisons $E_n = F_n = (-1)^n\,E_n(1-X)$.
Remarquons que cela implique que pour n pair, $E_n(0) = E_n(1)$; comme $E_n(1) + E_n(0) = 2 \cdot 0^n = 0$ (pour $n > 0$), on en déduit que pour tout n pair > 0, $E_n(0) = E_n(1) = 0$.

§ VII.6 *FACTORISATION DANS* $\mathbb{R}[X]$

Exercice 2 :

Décomposer dans $\mathbb{R}[X]$ le polynôme $F_n = X^{2^n}+1$, où $n \in \mathbb{N}^*$, et en déduire des expressions par radicaux des nombres $\cos \frac{k\pi}{2^n}$, $0 \leqslant k \leqslant 2^{n+1}-1$. ■

Les polynômes F_n, où $n \in \mathbb{N}^*$, n'ont pas de zéros réels ; leurs décompositions en produits de facteurs irréductibles dans $\mathbb{R}[X]$ ne comportent donc que des polynômes irréductibles de degré 2.
Les zéros complexes du polynôme F_n sont tous simples, ce sont les nombres $z_{n,k} = \exp(\mathrm{i}\,\theta_{n,k})$, où $\theta_{n,k} = (-\pi + 2k\pi)/2^n$, $k \in [\![1, 2^{n-1}]\!]$, et les complexes conjugués. Donc :

$$X^{2^n}+1 = \prod_{k=1}^{2^{n-1}} (X - z_{n,k})(X - \bar{z}_{n,k}) = \prod_{k=1}^{2^{n-1}} (X^2 - 2\cos\theta_{n,k}\, X + 1) \,.$$

On obtient ainsi la décomposition en facteurs irréductibles dans $\mathbb{R}[X]$ du polynôme $X^{2^n}+1$.

Le polynôme $F_1 = X^2+1$ est irréductible.
Décomposons d'une autre manière le polynôme F_2 :

$$F_2 = X^4+1 = (X^2+1)^2 - 2X^2 = (X^2 - \sqrt{2}\,X + 1)(X^2 + \sqrt{2}\,X + 1) \,.$$

Par identification, et comme $\cos\pi/4 > \cos 3\pi/4$, nous obtenons $\cos\pi/4 = \sqrt{2}/2$, et $\cos 3\pi/4 = -\sqrt{2}/2$.
De manière analogue :

$$\begin{aligned} F_3 = X^8+1 &= (X^2)^4+1 = (X^4 - \sqrt{2}\,X^2 + 1)(X^4 + \sqrt{2}\,X^2 + 1) = \\ &= \big((X^2+1)^2 - (2+\sqrt{2})X^2\big)\big((X^2+1)^2 - (2-\sqrt{2})X^2\big) = \\ &= \left(X^2 - \sqrt{2+\sqrt{2}}\,X + 1\right)\left(X^2 + \sqrt{2+\sqrt{2}}\,X + 1\right) \times \\ &\qquad \left(X^2 - \sqrt{2-\sqrt{2}}\,X + 1\right)\left(X^2 + \sqrt{2-\sqrt{2}}\,X + 1\right) \,. \end{aligned}$$

Par identification, et comme $\cos\pi/8 > \cos 3\pi/8 > \cos 5\pi/8 > \cos 7\pi/8$, on obtient :

$$\cos\pi/8 = \frac{\sqrt{2+\sqrt{2}}}{2} \quad , \quad \cos 3\pi/8 = \frac{\sqrt{2-\sqrt{2}}}{2} \,,$$

$$\cos 5\pi/8 = -\frac{\sqrt{2-\sqrt{2}}}{2} \quad , \quad \cos 7\pi/8 = -\frac{\sqrt{2+\sqrt{2}}}{2}$$

Supposons avoir obtenu la décomposition de F_n dans $\mathbb{R}[X]$ ($n \in \mathbb{N}^*$), sous la forme :

$$F_n = \prod_{k=1}^{2^{n-1}} (X^2 - 2\,a_{n,k}\,X + 1)\ ,$$

où $(a_{n,k})$, pour $k \in [\![1, 2^{n-1}]\!]$, est une suite décroissante de réels dans l'intervalle $]-1, 1[$ (le discriminant de chaque facteur est < 0), chacun de ces réels étant exprimé à l'aide de nombres rationnels et de racines carrées. Par identification avec la décomposition précédemment trouvée, et comme la suite $(\cos\theta_{n,k})$, $k \in [\![1, 2^{n-1}]\!]$, est strictement décroissante, on voit que pour tout $k \in [\![1, 2^{n-1}]\!]$, $\cos\theta_{n,k} = a_{n,k}$.

Nous pouvons en déduire la décomposition de F_{n+1} ; en effet :

$$F_{n+1}(X) = F_n(X^2) =$$

$$= \prod_{k=1}^{2^{n-1}} (X^4 - 2\,a_{n,k}\,X^2 + 1) = \prod_{k=1}^{2^{n-1}} \left((X^2+1)^2 - 2(1+a_{n,k})\,X^2\right)$$

$$= \prod_{k=1}^{2^{n-1}} \left(X^2 + \sqrt{2(1+a_{n,k})}\,X + 1\right) \prod_{k=1}^{2^{n-1}} \left(X^2 - \sqrt{2(1+a_{n,k})}\,X + 1\right)\ .$$

Nous obtenons :

$$a_{n+1,k} = \sqrt{\frac{1+a_{n,k}}{2}} \quad (k \in [\![1, 2^{n-1}]\!])\ ,$$

et :

$$a_{n+1,k} = -\sqrt{\frac{1+a_{n,2^n-k+1}}{2}} \quad (k \in [\![2^{n-1}+1, 2^n]\!])\ .$$

La suite obtenue ainsi, $(a_{n+1,k})$, où $k \in [\![1, 2^n]\!]$, est bien une suite strictement décroissante de nombres exprimés à l'aide de rationnels et de racines carrées.

On peut donc trouver par récurrence une expression par radicaux des nombres $\cos\frac{k\,\pi}{2^n}$, $0 \leqslant k \leqslant 2^{n+1} - 1$.

Exercice 3 :

On donne un entier $n \geqslant 3$ et on cherche la forme d'un polynôme normalisé de degré 3, $X^3 + a\,X^2 + b\,X + c \in \mathbb{R}[X]$ qui divise $X^n - 1$.

a) Montrer que si n est impair les polynômes cher

$X^3 - u\,X^2 + u\,X - 1$, avec

$$u = 1 + 2\cos\frac{2k\pi}{n} \quad \text{et} \quad k \in \left[\!\left[1, \frac{n-1}{2}\right]\!\right].$$

b) Montrer que si n est pair, les polynômes cherchés sont $X^3 - v\,X^2 + \varepsilon\,v\,X - \varepsilon$, avec

$$\varepsilon \in \{-1, 1\} \quad \text{et} \quad v = \varepsilon + 2\cos\frac{2k\pi}{n} \quad , \quad k \in \left[\!\left[1, \frac{n}{2} - 1\right]\!\right]. \blacksquare$$

a) Posons $n = 2p + 1$, $p \in \mathbb{N}^*$. Soit $P = X^3 + a\,X^2 + b\,X + c$ un polynôme dans $\mathbb{R}[X]$ qui divise $X^{2p+1} - 1$. Comme le polynôme P a au moins un zéro réel, celui-ci ne peut être que le seul zéro réel du polynôme $X^{2p+1} - 1$, soit 1. Nous pouvons en déduire que le polynôme P divise le polynôme $X^{2p+1} - 1$, si, et seulement si, il est le produit de $(X - 1)$ par l'un des facteurs irréductibles normalisés de degré 2 du polynôme $X^{2p+1} - 1$.

Les zéros complexes du polynôme $X^{2p+1} - 1$ sont au nombre de $2p + 1$, tous simples ; ce sont 1, les nombres $z_k = \exp \mathrm{i}\,\theta_k$, où $\theta_k = 2k\pi/(2p + 1)$, $k \in [\![1, p]\!]$, et les complexes conjugués. Nous obtenons par conséquent :

$$X^{2p+1} - 1 = (X-1)\prod_{k=1}^{p}(X - z_k)(X - \bar{z}_k) = (X-1)\prod_{k=1}^{p}(X^2 - 2\cos\theta_k\,X + 1).$$

Les polynômes de degré 3 cherchés sont donc les polynômes de la forme :

$$\begin{aligned} P &= (X-1)\left(X^2 - 2\cos\theta_k\,X + 1\right) = \\ &= X^3 - (1 + 2\cos\theta_k)\,X^2 + (1 + 2\cos\theta_k)\,X - 1 \quad (k \in [\![1, p]\!]), \end{aligned}$$

Ce qu'il fallait démontrer puisque :

$$\cos\theta_k = \cos\frac{2k\pi}{2p+1} = \cos\frac{2k\pi}{n} \quad (k \in [\![1, p]\!]).$$

b) Posons $n = 2p$, $p \geqslant 2$. Soit $P = X^3 + a\,X^2 + b\,X + c$ un polynôme élément de $\mathbb{R}[X]$, qui divise $X^{2p} - 1$. Les zéros complexes du polynôme P sont donc tous simples, au nombre de 3 ; l'un de ces zéros est réel et il ne peut être que l'un des zéros réels du polynôme $X^{2p} - 1$, soit -1 ou $+1$. Il est clair que le polynôme P ne peut pas avoir 3 zéros réels, il est donc nécessairement le produit de $(X - 1)$ ou de $(X + 1)$, par l'un des facteurs irréductibles normalisés de degré 2 du polynôme $X^{2p} - 1$. Cette condition est évidement suffisante.

Les zéros complexes du polynôme $X^{2p}-1$ sont les nombres -1, $+1$, les complexes $z_k = \exp i\theta_k$, $\theta_k = k\pi/p$, $k \in [\![1, p-1]\!]$, et les complexes conjugués. Nous obtenons par conséquent :

$$X^{2p}-1 = (X-1)(X+1)\prod_{k=1}^{p-1}(X-z_k)(X-\bar{z}_k) =$$
$$= (X-1)(X+1)\prod_{k=1}^{p-1}(X^2-2\cos\theta_k X+1)\ .$$

Les polynômes de degré 3 cherchés sont donc les polynômes de la forme :

$$P = (X-1)\left(X^2-2\cos\theta_k X+1\right) =$$
$$= X^3-(1+2\cos\theta_k)X^2+(1+2\cos\theta_k)X-1\ ,$$

ou :

$$P = (X+1)\left(X^2-2\cos\theta_k X+1\right) =$$
$$= X^3-(2\cos\theta_k-1)X^2-(2\cos\theta_k-1)X+1\ .$$

Ce qu'il fallait démontrer puisque :

$$\cos\theta_k = \cos\frac{k\pi}{p} = \cos\frac{2k\pi}{n} \quad k \in [\![1, p-1]\!]\ .$$

Exercice 4 :

Soit $(a,b) \in \mathbb{R}^2 \setminus \{(0,0)\}$ et $\lambda \in \mathbb{R}^*$. On se propose de chercher la décomposition dans $\mathbb{R}[X]$ du polynôme $F = (X^2+a^2)^2 + \lambda^2(X+b)^2$. Soit $t \in \mathbb{R}$; on pose

$$G_t(X) = (X^2+a^2+t)^2 - F(X)\ .$$

Chercher $t \neq 0$ pour que le trinôme G_t ait un discriminant nul dans $\mathbb{R}[X]$, et en déduire la factorisation cherchée (méthode de Ferrari). ■

Nous supposerons que $b \neq 0$, sinon F est un polynôme bicarré dont les factorisations sont connues.

Calculons les coefficients du polynôme G_t :

$$G_t(X) = (X^2+a^2+t)^2 - (X^2+a^2)^2 - \lambda^2(X+b)^2 =$$
$$= 2t(X^2+a^2) + t^2 - \lambda^2(X+b)^2 =$$
$$= (2t-\lambda^2)X^2 - 2b\lambda^2 X + t^2 + 2ta^2 - \lambda^2 b^2$$

Posons alors :

$$\Delta_t = b^2\lambda^4 - (2t - \lambda^2)(t^2 + 2ta^2 - \lambda^2 b^2) .$$

Si $\Delta_t = 0$, alors $(2t - \lambda^2) \neq 0$ (sinon $b^2\lambda^4 = 0$), le polynôme G_t est de degré 2, de discriminant nul. Cherchons une valeur réelle non nulle de t telle que $\Delta_t = 0$.

On obtient :

$$\Delta_t = \lambda^2 (t^2 + 2ta^2) - 2t (t^2 + 2ta^2 - \lambda^2 b^2) ,$$

soit pour $t \neq 0$:

$$\frac{\Delta_t}{t} = -2t^2 + (\lambda^2 - 4a^2)t + 2\lambda^2(a^2 + b^2) = Q(t) .$$

Le polynôme $Q(t)$, de degré 2, a des zéros réels non nuls et de signes opposés car $\lambda^2 (a^2 + b^2) > 0$. Le discriminant du polynôme Q est :

$$D = (\lambda^2 - 4a^2)^2 + 16\lambda^2(a^2 + b^2) = (\lambda^2 + 4a^2)^2 + 16\lambda^2 b^2 > 0 .$$

Comme la valeur de Δ_t pour $t = \lambda^2/2$ est $b^2\lambda^4$, on voit que :

$$Q(\lambda^2/2) = 2b^2\lambda^2 > 0 .$$

Nous pouvons en déduire que si t_1 est le zéro > 0 du polynôme Q, alors $t_1 > \lambda^2/2$, soit encore $2t_1 - \lambda^2 > 0$. La valeur explicite de t_1 est :

$$t_1 = \frac{(\lambda^2 - 4a^2) + \sqrt{(\lambda^2 + 4a^2)^2 + 16\lambda^2 b^2}}{4} \quad (> \lambda^2/2) .$$

Pour cette valeur de t, le polynôme G_t s'écrit :

$$G_{t_1}(X) = (2t_1 - \lambda^2)(X - \mu)^2 ,$$

où μ est le zéro double de ce polynôme de degré 2, soit :

$$\mu = \frac{b\lambda^2}{2t_1 - \lambda^2} .$$

Nous obtenons alors :

$$F(X) = (X^2 + a^2 + t_1)^2 - (2t_1 - \lambda^2)(X - \mu)^2 ,$$

et comme $2t_1 - \lambda^2 > 0$, nous en déduisons la factorisation :

$$F(X) = \left(X^2 + \sqrt{2t_1 - \lambda^2}\,(X - \mu) + a^2 + t_1\right)\left(X^2 - \sqrt{2t_1 - \lambda^2}\,(X -\right.$$

Comme le polynôme F n'a pas de zéro réel, et que ces deux polynômes du second degré sont distincts, il s'agit bien là de la décomposition dans $\mathbb{R}[X]$ du polynôme F en produit de facteurs irréductibles normalisés.

Exercice 6 :

Factoriser dans $\mathbb{R}[X]$: $16\,X^5 - 20\,X^3 + 5\,X - 1$ et
$X^5 - 13\,X^4 + 67\,X^3 - 171\,X^2 + 216\,X - 108$
sachant qu'il admettent des racines multiples. ■

a) Utilisons l'algorithme d'Euclide pour calculer le pgcd des polynômes $P = 16\,X^5 - 20\,X^3 + 5\,X - 1$ et du polynôme dérivée $P' = 80\,X^4 - 60\,X^2 + 5 = 5\,(16\,X^4 - 12\,X^2 + 1)$. On divise P par $P'/5$.

$$\begin{array}{rrrrrr|l} 16X^5 & +0X^4 & -20X^3 & +0X^2 & +5X & +1 & 16X^4 - 12X^2 + 1 \\ \cline{7-7} & & -8X^3 & & +4X & -1 & X \end{array}$$

$$\begin{array}{rrrrrr|l} 16X^4 & +0X^3 & -12X^2 & +0X & +1 & & 8X^3 - 4X + 1 \\ \cline{6-6} & & -4X^2 & -2X & +1 & & 2X \end{array}$$

$$\begin{array}{rrrrr|l} 8X^3 & +0X^2 & -4X & +1 & & 4X^2 + 2X - 1 \\ \cline{5-5} & -4X^2 & -2X & +1 & & 2X - 1 \\ & & & 0 & & \end{array}$$

Le pgcd cherché est, à un scalaire près, $4X^2 + 2X - 1$, le dernier reste non nul. Il est facile de voir que ce polynôme a deux zéros réels distincts, qui sont donc chacun zéro double de P. Le polynôme P est donc divisible par $(4X^2 + 2X - 1)^2$. Calculons les quotients.

$$\begin{array}{rrrrrr|l} 16X^5 & +0X^4 & -20X^3 & +0X^2 & +5X & -1 & 4X^2 + 2X - 1 \\ \cline{7-7} & -8X^4 & -16X^3 & +0X^2 & +5X & -1 & 4X^3 - 2X^2 - 3X + 1 \\ \cline{7-7} & & -12X^3 & -2X^2 & +5X & -1 & \\ & & & & 4X^2 & +2X \quad -1 & \\ & & & & & 0 & \end{array}$$

$$\begin{array}{rrrr|l} 4X^3 & -2X^2 & -3X & +1 & 4X^2 + 2X - 1 \\ \cline{5-5} & -4X^2 & -2X & +1 & X - 1 \\ & & & 0 & \end{array}$$

Nous en déduisons finalement :

$$16X^5 - 20X^3 + 5X - 1 = (X-1)(4X^2 + 2X - 1)^2 \ ;$$

mais ceci n'est pas la factorisation car le polynôme $4X^2 + 2X - 1$ n'est pas irréductible ; on obtiendra une décomposition en produit de facteurs irréductibles en utilisant l'égalité ;

$$4X^2 + 2X - 1 = (2X + 1/2)^2 - 5/4 = \left(2X + \frac{1+\sqrt{5}}{2}\right)\left(2X + \frac{1-\sqrt{5}}{2}\right) \ .$$

b) Nous pourrions utiliser le même algorithme mais on peut simplifier le polynôme en cherchant ses zéros rationnels. Comme le polynôme :

$$P = X^5 - 13\,X^4 + 67\,X^3 - 171\,X^2 + 216\,X - 108$$

est normalisé, ses zéros rationnels sont entiers et divisent $108 = 4 \cdot 27$. D'autre part il est clair que ce sont des nombres > 0. Utilisons le schéma de Hörner pour calculer la valeur de P en 1.

						|1
1	−13	67	−171	216	−108	
1	−12	55	−116	100	−8	

Le nombre 1 n'est donc pas zéro du polynôme P. Essayons avec 2.

						|2
1	−13	67	−171	216	−108	
1	−11	45	−81	54	0	
1	−9	27	−27	0		
1	−7	13	−1			

On a donc l'égalité :

$$P = X^5 - 13X^4 + 67X^3 - 171X^2 + 216X - 108 = (X-2)^2(X^3 - 9X^2 + 27X - 27),$$

et on voit que :

$$P = (X-2)^2(X-3)^3 \ .$$

Exercice 7 :

Soit $F \in \mathbb{R}[X]$; on identifie F avec la fonction polynomiale $\mathbb{R} \to \mathbb{R}$ qu'il définit :

a) Pour que $F(\mathbb{R}) \subset \mathbb{R}_+$, il faut et il suffit qu'il existe A et B dans $\mathbb{R}[X]$ tels que $F = A^2 + B^2$.

b) Supposons de plus que F est **pair** ; si $F(\mathbb{R}) \subset \mathbb{R}_+$, alors il existe A et B dans $\mathbb{R}[X]$ tels que

$$F = A^2(X^2) + X^2\,B^2(X^2)\,.$$

c) Si $F(\mathbb{R}_+) \subset \mathbb{R}_+$, il existe A et B dans $\mathbb{R}[X]$ tels que

$$F = A^2(X) + X\,B^2(X)\,.\ \blacksquare$$

a) Il est clair que la condition est suffisante ; montrons qu'elle est nécessaire. Remarquons d'abord deux propriétés qui éclairent le problème.

1) L'ensemble des polynômes qui s'écrivent comme somme de deux carrés de polynômes est stable par la multiplication ; c'est une conséquence de l'égalité :

$$(A^2 + B^2)(A'^2 + B'^2) = (AA' - BB')^2 + (AB' + A'B)^2\ ,$$

où A, B, A', B' sont des polynômes à coefficients réels.

2) Si P est un polynôme normalisé de degré 2, irréductible dans $\mathbb{R}[X]$, il s'écrit sous la forme $P = X^2 - 2p\,X + q$, où p et q sont des réels tels que $p^2 - q < 0$; on peut écrire $P = (X-p)^2 + (\sqrt{q-p^2})^2$. Le polynôme P est donc somme de deux carrés.

Si $G \in \mathbb{R}[X]$ est normalisé et n'a aucun zéro réel, il est produit de polynômes de degré 2 normalisés et irréductibles dans $\mathbb{R}[X]$. Il s'écrit donc comme somme de deux carrés de polynômes à coefficients réels (vrai aussi si $G = 1$).

Supposons que le polynôme $F \in \mathbb{R}[X]$ soit tel que $F(\mathbb{R}) \subset \mathbb{R}_+$.
Soit α un zéro réel d'ordre k de F , posons $F = (X-\alpha)^k Q$, où $Q \in \mathbb{R}[X]$ ($Q(\alpha) \neq 0$) . Nous voulons démontrer que k est nécessairement pair. Il existe deux réels u et v , $u < \alpha < v$, tels que l'intervalle $[u, v]$ ne contienne aucun zéro du polynôme Q . Le polynôme Q garde donc sur cet intervalle un signe constant. On peut le démontrer en utilisant la décomposition en facteurs irréductibles de Q dans $\mathbb{R}[X]$: tous les facteurs irréductibles de Q gardent un signe constant sur cet intervalle. Si k était impair, le polynôme F ne pourrait pas être > 0 à la fois sur l'intervalle $[u, \alpha[$, et sur l'intervalle $]\alpha, v]$; l'entier k est donc pair.
Le coefficient dominant du polynôme F est > 0 , car il est du signe de $F(x)$ pour tout x réel strictement plus grand que le plus grand des zéros de F ; c'est donc un carré dans $\mathbb{R}$. Il existe donc deux polynômes, U et G dans $\mathbb{R}[X]$, tels que $F = U^2\,G$, le polynôme G étant normalisé et n'ayant aucun zéro réel.
D'après ce qui précède, il existe deux polynômes A et B dans $\mathbb{R}[X]$ tels que $G = A^2 + B^2$, d'où $F = (UA)^2 + (UB)^2$. Le polynôme F est donc somme de deux carrés de polynômes à coefficients réels, ce qu'il fallait démontrer.

b) Notons $\mathcal{P}$ l'ensemble des polynômes à coefficients réels qui peuvent s'écrire sous la forme $A^2(X^2) + X^2 B^2(X^2)$, où A et B sont dans $\mathbb{R}[X]$. Montrons que $\mathcal{P}$ est stable par la multiplication. En effet, si A, A', B, B' sont des éléments de $\mathbb{R}[X]$, en posant $Y = X^2$:

$$(A^2(Y) + YB^2(Y))(A'^2(Y) + YB'^2(Y)) =$$
$$= \big(A(Y)A'(Y) - YB(Y)B'(Y)\big)^2 + Y\big(A(Y)B'(Y) + A'(Y)B(Y)\big)^2 .$$

Notons $\mathcal{Q}$ l'ensemble des éléments F de $\mathbb{R}[X]$, pairs et tels que $F(\mathbb{R}) \subset \mathbb{R}_+$; il est clair que c'est aussi une partie de $\mathbb{R}[X]$ stable par la multiplication, qui contient $\mathcal{P}$. Démontrons par récurrence l'inclusion opposée.

Pour $p \in \mathbb{N}$, notons $\mathcal{H}_p$ la propriété suivante : $\mathbb{R}_p[X] \cap \mathcal{Q} \subset \mathcal{P}$. La propriété $\mathcal{H}_0$ est vraie, car si F est un polynôme constant élément de $\mathcal{Q}$, alors il existe $a \in \mathbb{R}$ tel que $F = a^2$, et $F = a^2 + 0\,X^2 \in \mathcal{P}$. Supposons que $\mathcal{H}_p$ soit vraie et démontrons qu'alors $\mathcal{H}_{p+1}$ l'est aussi.
Soit $F \in \mathbb{R}_{p+1}[X] \cap \mathcal{Q}$. Si F est divisible par un polynôme D non constant élément de $\mathcal{P}$, alors le quotient Q est dans $\mathcal{Q} \cap \mathbb{R}_p[X]$; d'après l'hypothèse de récurrence, $Q \in \mathcal{P}$, et puisque $\mathcal{P}$ est stable par la multiplication $F \in \mathcal{P}$. Il suffit donc de démontrer qu'on peut toujours trouver un tel diviseur de F.
Si F a un zéro réel α d'ordre $k > 0$, alors (cf. *a*)) k est pair, $k = 2q$; si $\alpha = 0$, F divisible par $X^{2q} \in \mathcal{P}$, si $\alpha \neq 0$, $-\alpha$ est, par parité, zéro de F d'ordre $2q$, donc F est divisible par le polynôme :

$$D = (X - \alpha)^{2q}(X + \alpha)^{2q} = (X^2 - \alpha^2)^{2q} \in \mathcal{P} ;$$

Si F n'a aucun zéro réel, il est divisible par un facteur de degré 2 normalisé, irréductible dans $\mathbb{R}[X]$, de la forme $X^2 - 2pX + q$, où p et q sont des réels tels que $p^2 < q$; si $p = 0$, alors F est divisible par $D = X^2 + q \in \mathcal{P}$ ($q > 0$) ; si $p \neq 0$, le polynôme F est aussi divisible, par parité, par le polynôme $X^2 + 2pX + q$, donc par le polynôme :

$$D = (X^2 - 2pX + q)(X^2 + 2pX + q) = (X^2 + q)^2 - 4p^2X^2 =$$
$$= (X^2 - q)^2 + 4(q - p^2)X^2 \in \mathcal{P} \quad (q - p^2 > 0) .$$

Nous voyons donc que dans tous les cas, $F \in \mathcal{P}$.

La propriété $\mathcal{H}_p$ est donc vraie pour tout entier p. Nous en déduisons $\mathcal{Q} \subset \mathcal{P}$, donc finalement $\mathcal{P} = \mathcal{Q}$, ce qu'il fallait démontrer.

c) Soit $F \in \mathbb{R}[X]$ tels que $F(\mathbb{R}_+) \subset \mathbb{R}_+$; posons $G(X) = F(X^2)$. Il est clair que G est un polynôme pair et que $G(\mathbb{R}) \subset \mathbb{R}_+$, don

il existe deux polynômes A et B dans $\mathbb{R}[X]$ tel que $F(X^2) = A^2(X^2) + X^2B^2(X^2)$. Nous en déduisons $F(X) = A^2(X) + XB^2(X)$, ce qu'il fallait démontrer.

§ VII.7 *CONGRUENCES DANS K[X] ANNEAUX QUOTIENTS*

Exercice 2 :

Soit P un polynôme non constant de $\mathbb{C}[X]$ tel que $P(0) \neq 0$ et ayant toutes ses racines *distinctes*. Montrer qu'il existe $A \in \mathbb{C}[X]$ tel que $A^2 \equiv X \bmod (P)$. ■

Notons n le degré de P, et $\alpha_1, \alpha_2, \ldots, \alpha_n$ les zéros de P. Choisissons des complexes $\beta_1, \beta_2, \ldots, \beta_n$ tels que pour tout $i \in [\![1, n]\!]$, $\beta_i^2 = \alpha_i$; les complexes $\beta_1, \beta_2, \ldots, \beta_n$ sont évidemment distincts. Soit A le polynôme élément de $\mathbb{C}_{n-1}[X]$ tel que pour tout $i \in [\![1, n]\!]$, $A(\alpha_i) = \beta_i$ (polynôme d'interpolation de Lagrange). On voit que les polynômes A^2 et X coïncident en tout α_i, pour $i \in [\![1, n]\!]$. Nous pouvons en déduire que $A^2 - X$ est divisible par $\prod_{i=1}^{n} (X - \alpha_i)$, donc par P. Cela s'écrit aussi :

$$A^2(X) \equiv X \mod (P) .$$

Exercice 4 :

Soit $P \in K[X]$. Démontrer que le polynôme $P(P(X)) - X$ est divisible par $P(X) - X$. ■

Posons $Q = P(X) - X$. Si A et B dans $K[X]$ sont congrus modulo Q, alors pour tout entier n, $A^n \equiv B^n \bmod (Q)$; on voit donc que pour tout polynôme $R \in K[X]$, $R(A) \equiv R(B) \bmod (Q)$. En particulier comme $P \equiv X \bmod (Q)$, nous pouvons écrire :

$$P(P(X)) \equiv P(X) \equiv X \mod (Q) ,$$

ce qu'il fallait démontrer.

Exercice 6 :

Chercher le polynôme minimal P du nombre algébrique $a = \sqrt[3]{2} + \sqrt[3]{4}$. Exprimer ensuite toutes les racines de P en fonction de $\sqrt[3]{2}$, de j et de $\bar{\text{j}}$. ■

Notons $\alpha = \sqrt[3]{2}$ et $\beta = \sqrt[3]{4}$, de telle sorte que $a = \alpha + \beta$. On remarque que $\alpha\beta = \sqrt[3]{8} = 2$ et que $a^3 = \alpha^3 + \beta^3 + 3\alpha\beta(\alpha + \beta) = 6 + 6a$. Le réel a est donc zéro du polynôme à coefficients entiers $P = X^3 - 6(X + 1)$.
Supposons que le polynôme P ait un zéro rationnel p/q, où $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$, p et q premiers entre eux ; alors $p^3 = 6(pq^2 + q^3)$, $q^2 \mid p^3$, donc $q = 1$; d'où $p^3 = 6(p+1)$, mais comme p est premier avec $p+1$, $p^3 \mid 6$, et $6 \mid p^3$, ce qui est impossible.
Comme le polynôme P est de degré 3 et n'a pas de zéros rationnel, il est irréductible dans $\mathbb{Q}[X]$; c'est donc le polynôme minimal du nombre algébrique a.

Posons $\alpha' = \mathrm{j}\alpha$ et $\beta' = \bar{\mathrm{j}}\beta$, on voit que $\alpha'^3 = \alpha^3 = 2$, $\beta'^3 = \beta^3 = 4$, et $\alpha'\beta' = \alpha\beta = 2$. Soit $a' = \alpha' + \beta'$, $a'^3 = \alpha'^3 + \beta'^3 + 3\alpha'\beta'(\alpha' + \beta') = 6 + 6a'$. Le complexe $\mathrm{j}\alpha + \bar{\mathrm{j}}\beta$ est donc zéro du polynôme P, et il en est de même pour le complexe conjugué $\bar{\mathrm{j}}\alpha + \mathrm{j}\beta$. Les complexes $\alpha + \beta$, $\mathrm{j}\alpha + \bar{\mathrm{j}}\beta$, $\bar{\mathrm{j}}\alpha + \mathrm{j}\beta$ étant distincts, ce sont les zéros de P.

Chapitre VIII

FRACTIONS RATIONNELLES. NOTIONS SUR LES SÉRIES FORMELLES

§ VIII.1 *LE CORPS K(X)*

Exercice 1 :

Le corps de base est $\mathbb{C}$. Suivant les valeurs de m et n dans $\mathbb{N}^*$, et de $\lambda \in \mathbb{C}$, donner la forme irréductible de la fraction rationnelle $\dfrac{X^m + \lambda^m}{X^n + \lambda^n} \in \mathbb{C}(X)$. ■

Nous supposerons $\lambda \neq 0$; il est alors clair qu'on peut se ramener au cas $\lambda = 1$, ce que nous supposerons par la suite. Il s'agit ici de calculer le pgcd des polynômes $X^n + 1$ et $X^m + 1$. Posons $n = 2^k n'$ et $m = 2^h m'$, où n' et m' sont des entiers impairs.
Supposons $h \neq k$, par exemple $h > k$. Si les polynômes $X^n + 1$ et $X^m + 1$ avaient un zéro commun z, alors on aurait $z^{n'm} = (-1)^{n'} = -1$, mais aussi $z^{n'm} = z^{2^{h-k} n m'} = (-1)^{2^{h-k} m'} = 1$. Les deux polynômes sont donc premiers entre eux, et la fraction rationnelle de l'énoncé est sous forme irréductible.

Supposons $h = k$. Nous pouvons alors écrire :

$$X^n + 1 = \left(X^{2^k}\right)^{n'} - (-1)^{n'} \quad \text{et} \quad X^m + 1 = \left(X^{2^k}\right)^{m'} - (-1)^{m'},$$

soit $X^n + 1 = P(X^{2^k})$ et $X^m + 1 = Q(X^{2^k})$, où $P = X^{n'} - (-1)^{n'}$ et $Q = X^{m'} - (-1)^{m'}$. Or on sait que le pgcd des polynômes P et Q est le polynôme $D = X^{d'} - (-1)^{d'}$, où $d' = \text{pgcd}\,(n', m')$ (§VII.2, Exercice 7). Démontrons que le pgcd des polynômes $P(X^{2^k})$ et $Q(X^{2^k})$ est bien, comme on s'y attend, $D(X^{2^k})$. Soient P_1 et Q_1 les polynômes tels que $P = D\,P_1$ et $Q = D\,Q_1$; les polynômes P_1 et Q_1 sont premiers entre eux, et il existe par conséquent deux polynômes A et B tels que $A\,P_1 + B\,Q_1 = 1$; on voit que $A(R)\,P_1(R) + B(R)\,Q_1(R) = 1$ pour tout $R \in \mathbb{C}[X]$; le pgcd des polynômes $P(R) = D(R)\,P_1(R)$ et $Q(R) = D(R)\,Q_1(R)$ est

en particulier dans le cas où $R = X^{2^k}$. En conclusion le pgcd des polynômes $X^n + 1$ et $X^m + 1$ est, dans ce cas, $X^{2^k d'} - (-1)^{d'} = X^d + 1$, où $d = \text{pgcd}(n, m)$.

Il reste à déterminer, dans le cas où $h = k$, le quotient des polynômes $X^n + 1$ et $X^m + 1$ par $X^d + 1$. Posons $n = dn_1$ et $m = dm_1$; les entiers n_1 et m_1 sont impairs. On voit que :

$$\frac{X^n + 1}{X^d + 1} = \frac{X^{dn_1} - (-1)^{n_1}}{X^d - (-1)} = \sum_{j=0}^{n_1 - 1} (-1)^j X^{dj} ,$$

et de même :

$$\frac{X^m + 1}{X^d + 1} = \frac{X^{dm_1} - (-1)^{m_1}}{X^d - (-1)} = \sum_{i=0}^{m_1 - 1} (-1)^i X^{di} .$$

La forme irréductible de la fraction est donc :

$$\frac{X^m + 1}{X^n + 1} = \frac{\sum_{i=0}^{m_1 - 1} (-1)^i X^{di}}{\sum_{j=0}^{n_1 - 1} (-1)^j X^{dj}} .$$

Exercice 2 :

Le corps de base est $\mathbb{C}$. Suivant les valeurs de $n \in \mathbb{N}^*$, mettre sous forme irréductible la fraction

$$F = \frac{(X^{5n} + X^{2n} - 2)(X^3 + (2 - 4\lambda^2)X - 4\lambda)}{(X^3 - 1)(X^4 + 4)} . \blacksquare$$

Nous commencerons par réduire séparément les fractions :

$$A_n = \frac{X^{5n} + X^{2n} - 2}{X^3 - 1} ,$$

et :

$$B_\lambda = \frac{X^3 + (2 - 4\lambda^2)X - 4\lambda}{X^4 + 4} .$$

1) Réduction de la fraction rationnelle A_n.
On voit que 1 est toujours zéro du polynôme $X^{5n} + X^{2n} - 2$, et que j et j^2 sont zéros de ce polynôme si, et seulement si, $\mathrm{j}^{5n} + \mathrm{j}^{2n} - 2$

et seulement si, $2\mathrm{j}^{2n} = 2$, ou encore $3 \mid 2n$, soit $3 \mid n$.
On vérifie que :

$$X^{5n} + X^{2n} - 2 = X^{5n} - 1 + X^{2n} - 1 = (X-1)P_n$$

où :

$$P_n = \sum_{i=0}^{5n-1} X^i + \sum_{j=0}^{2n-1} X^j \ .$$

Si 3 ne divise pas n, la forme irréductible de la fraction rationnelle A_n est donc :

$$A_n = \frac{P_n}{1 + X + X^2} \ .$$

Si 3 divise n, posons $n = 3p$. On voit que :

$$X^{5n} + X^{2n} - 2 = X^{15p} - 1 + X^{6p} - 1 = (X^3)^{5p} - 1 + (X^3)^{2p} - 1 = (X^3 - 1)Q_p \ ,$$

où :

$$Q_p = \sum_{i=0}^{5p-1} X^{3i} + \sum_{j=0}^{2p-1} X^{3j} \ .$$

Dans ce cas, la fraction rationnelle A_n est le polynôme Q_p.

2) Réduction de la fraction rationnelle B_λ.
Remarquons que :

$$X^3 + (2 - 4\lambda^2)X - 4\lambda = (X - 2\lambda)(X^2 + 2\lambda X + 2) \ ,$$

d'où :

$$(1) \qquad B_\lambda = \frac{(X - 2\lambda)(X^2 + 2\lambda X + 2)}{X^4 + 4} \ .$$

En effectuant la division euclidienne du polynôme $X^4 + 4$ par le polynôme $X^2 + 2\lambda X + 2$, on trouve l'égalité :

$$(2) \quad X^4 + 4 = (X^2 + 2\lambda X + 2)(X^2 - 2\lambda X + 4\lambda^2 - 2) + 8(1 - \lambda^2)(\lambda X + 1) \ .$$

Cela nous amène à distinguer les cas suivants.

a) Si $\lambda = \varepsilon \in \{-1, 1\}$:

$$B_\lambda = \frac{X - 2\varepsilon}{X^2 - 2\varepsilon X + 2} \ .$$

Il s'agit bien d'une forme irréductible.

b) Si $\lambda \notin \{-1, 1\}$, on voit que les polynômes X^4+4 et $X^2+2\lambda X+2$ sont premiers entre eux, en effet, d'après l'égalité (2), c'est évident si $\lambda = 0$, et si $\lambda \neq 0$, un zéro commun de ces deux polynômes ne pourrait être que $-1/\lambda$, qui n'est pas zéro de $X^2 + 2\lambda X + 2$. L'égalité (1) donne donc la forme irréductible de la fraction rationnelle B_λ, sauf si 2λ est zéro du polynôme $X^4 + 4$. Dans ce cas $(2\lambda)^4 = -4$ et :

$$X^4 + 4 = X^4 - (2\lambda)^4 = (X - 2\lambda)(X^3 + 2\lambda X^2 + 4\lambda^2 X + 8\lambda^3) .$$

La forme irréductible de la fraction rationnelle B_λ est alors :

$$B_\lambda = \frac{X^2 + 2\lambda X + 2}{X^3 + 2\lambda X^2 + 4\lambda^2 X + 8\lambda^3} .$$

Comme :

$$\begin{aligned} X^4 + 4 &= (X^2 + 2)^2 - 4X^2 = \\ &= (X^2 - 2X + 2)(X^2 + 2X + 2) = \big((X-1)^2 + 1\big)\big((X+1)^2 + 1\big) , \end{aligned}$$

les zéros du polynôme $X^4 + 4$ sont $1+\mathrm{i}$, $1-\mathrm{i}$, $-1+\mathrm{i}$ et $-1-\mathrm{i}$.

3) Réduction de la fraction rationnelle $F = A_n \times B_\lambda$.
Remarquons que les polynômes $X^{5n} + X^{2n} - 2$ et $X^4 + 4$ n'ont pas de zéro commun, car si $z^4 = -4$ ($z \in \mathbb{C}$), alors $|z| = \sqrt{2}$, et $|z^{5n} + z^{2n}| \geqslant (\sqrt{2})^{5n} - 2^n > 4^n - 2^n \geqslant 2$ (puisque $n \geqslant 1$). Ces polynômes sont donc premiers entre eux, et tout diviseur de X^4+4 est premier avec tout diviseur de $X^{5n} + X^{2n} - 2$. Examinons les différents cas.

Si n est divisible par 3 ($n = 3p$).
Dans ce cas :

$$F = \frac{Q_p \times (X - 2\lambda)(X^2 + 2\lambda X + 2)}{X^4 + 4} .$$

Comme $X^4 + 4$ est premier avec le polynôme Q_p, on obtient la forme irréductible de F en multipliant par Q_p le numérateur de la forme irréductible de B_λ.

Si n n'est pas divisible par 3.
Dans ce cas :

$$F = \frac{P_n}{X^2 + X + 1} \times \frac{(X - 2\lambda)(X^2 + 2\lambda X + 2)}{X^4 + 4} .$$

a) Si $\lambda = \varepsilon \in \{-1, 1\}$:

$$F = \frac{P_n}{X^2 + X + 1} \times \frac{X - 2\varepsilon}{X^2 - 2\varepsilon X + 2} .$$

Comme 2ε n'est pas zéro du polynôme X^2+X+1, il s'agit d'une forme irréductible.

b) Si 2λ est l'un des zéros du polynôme X^4+4, alors 2λ est l'un des nombres $1+\mathrm{i}$, $1-\mathrm{i}$, $-1+\mathrm{i}$ ou $-1-\mathrm{i}$, donc $\lambda \notin \{-1,1\}$; par conséquent :

$$F = \frac{P_n}{X^2+X+1} \times \frac{X^2+2\lambda X+2}{X^3+2\lambda X^2+4\lambda^2 X+8\lambda^3} .$$

On vérifie assez facilement que ni j ni j^2 ne peuvent être zéros du polynôme $X^2+2\lambda X+2$. Il s'agit donc d'une forme irréductible.

c) Si $\lambda \notin \{-1,1\}$, et 2λ n'est pas zéro du polynôme X^4+4 :

$$F = \frac{P_n}{X^2+X+1} \times \frac{(X-2\lambda)(X^2+2\lambda X+2)}{X^4+4} .$$

Cette forme est irréductible, sauf si j ou j^2 est zéro du polynôme $(X-2\lambda)(X^2+2\lambda X+2)$.

d) Notons $\omega = \mathrm{j}$ ou j^2 suivant les cas. Le complexe ω est zéro du polynôme $(X-2\lambda)(X^2+2\lambda X+2)$ si, et seulement si, $2\lambda = \omega$, ou $\omega^2+2\lambda\omega+2=0$, soit :

$$\lambda = \frac{\omega}{2} \quad \text{ou} \quad \lambda = -\frac{2+\omega^2}{2\omega} = -\omega^2 - \frac{\omega}{2} = 1+\omega-\frac{\omega}{2} = 1+\frac{\omega}{2} .$$

On vérifie que dans les deux cas $\lambda \notin \{-1,1\}$ et 2λ n'est pas zéro du polynôme X^4+4.
Dans le premier cas :

$$F = \frac{P_n}{X-\omega^2} \times \frac{X^2+\omega X+2}{X^4+4} .$$

On voit qu'il s'agit d'une forme irréductible, car $\omega^4+\omega^3+2 = \omega+3 \neq 0$.

Dans le second, l'autre zéro du polynôme $X^2+2\lambda X+2$ étant $2/\omega = 2\omega^2$, on obtient :

$$F = \frac{P_n}{X-\omega^2} \times \frac{(X-2-\omega)(X-2\omega^2)}{X^4+4} .$$

Il est clair qu'il s'agit d'une forme irréductible.

Exercice 5 :

On suppose que K est le corps des fractions d'un anneau intègre A. Montrer que $K(X)$ est le corps des fractions de l'anneau $A[X]$. ■

Soit $F \in K(X)$, il existe P et Q dans $K[X]$, $Q \neq 0$, tels que $F = P/Q$. On peut trouver un élément $\lambda \in A$, $\lambda \neq 0$, et un élément $\mu \in A$, $\mu \neq 0$ tels que $P_1 = \lambda P \in A[X]$ et $Q_1 = \mu Q \in A[X]$. Nous pouvons alors écrire :

$$F = \frac{P}{Q} = \frac{\lambda \mu P}{\lambda \mu Q} = \frac{\mu P_1}{\lambda Q_1} .$$

Tout élément de $K(X)$ est donc quotient de deux éléments de $A[X]$ et est par conséquent dans le corps des fractions de cet anneau intègre. Comme l'inclusion opposée est évidente, il y a égalité.

Exercice 10 :

Soit F, $G_1, G_2, \ldots, G_n \in \mathbb{C}(X)$ avec $n \geqslant 1$. On suppose que :

$$F^n + G_1 F^{n-1} + \ldots + G_n = 0 .$$

Montrer que l'ensemble des pôles de F est contenu dans l'union des ensembles de pôles des G_i. ■

Posons $F = P/Q$, où P et Q sont des polynômes éléments de $\mathbb{C}[X]$, premiers entre eux, et $Q \neq 0$. Il est clair que :

$$P^n + G_1 P^{n-1} Q + \ldots + G_n Q^n = 0 .$$

S'il existait un pôle $z \in \mathbb{C}$ de la fraction rationnelle F qui ne soit pôle d'aucune des fractions G_i, où $i \in [\![1, n]\!]$, alors, comme $Q(z) = 0$, on pourrait écrire :

$$P^n(z) = P^n(z) + G_1(z) P^{n-1}(z) Q(z) + \ldots + G_n(z) Q^n(z) = 0 ,$$

d'où $P(z) = 0$; les polynômes P et Q seraient tous les deux divisibles par $(X - z)$, ce qui est en contradiction avec l'hypothèse qu'ils sont premiers entre eux. Nous pouvons en déduire que tout pôle de F est pôle d'au moins l'une des fractions rationnelles G_i, où $i \in [\![1, n]\!]$.

Exercice 12 :

Chercher $F \in K(X)$ telle que $F^2 = X$; conclure : $K(X)$ n'est jamais algébriquement clos. ■

Supposons $F^2 = X$ et posons $F = P/Q$, où P et Q sont des polynômes éléments de $\mathbb{C}[X]$, premiers entre eux et $Q \neq 0$. On voit que $P^2 = XQ^2$ donc $Q \mid P^2$; mais comme Q est aussi premier avec P^2, Q est inversible. La fraction rationnelle F est nécessairement un polynôme, mais cela est impossible car le carré d'un polynôme (non nul) est de degré pair. L'équation en F, $F^2 = X$, n'a donc pas de solution dans le corps $K(X)$; le corps $K(X)$ n'est donc pas algébriquement clos.

§ VIII.2 *DÉCOMPOSITION EN ÉLÉMENTS SIMPLES*

Exercice 1 :

Décomposer en éléments simples sur $\mathbb{C}$ les fractions rationnelles suivantes :

a) $F = \dfrac{1}{(X^2-1)^2}$.

b) $F = \dfrac{1}{(X-1)(X-2)\dots(X-n)}$, $n \in \mathbb{N}^*$.

c) $F = \dfrac{1}{(X-1)^2(X-2)^2\dots(X-n)^2}$, $n \in \mathbb{N}^*$.

d) $\dfrac{1}{T_n(X)}$ et $\dfrac{1}{U_n(X)}$, où T_n et U_n sont les polynômes de Tchebychev (cf. §VII.5 exercice 10).

e) $\dfrac{1}{E_n(X)}$ pour $n \in \{2,3,4,5\}$, où E_n est un polynôme d'Euler (cf. §VII.5 exercice 23).

f) $F = \dfrac{1}{X\prod_{i=1}^{n}(X^2-k^2)}$ *g)* $F = \dfrac{1}{(X+1)^7 - X^7 - 1}$. ■

a) En élevant au carré l'égalité :

$$\frac{1}{X^2-1} = \frac{1/2}{X-1} - \frac{1/2}{X+1}$$

nous obtenons :

$$\frac{1}{(X^2-1)^2} = \frac{1/4}{(X-1)^2} - \frac{1/2}{(X-1)(X+1)} + \frac{1/4}{(X+1)^2},$$

d'où :

$$\frac{1}{(X^2-1)^2} = \frac{1/4}{(X-1)^2} - \frac{1/4}{X-1} + \frac{1/4}{(X+1)^2} + \frac{1/4}{X+}$$

b) Posons $Q(X) = (X-1)(X-2)\dots(X-n)$; pour tout $i \in [\![1,n]\!]$, introduisons le polynôme Q_i tel que $Q = (X-i)\,Q_i$. Comme tous les pôles sont simples, et que la partie entière de la fraction rationnelle est nulle, nous pouvons écrire :

$$F = \frac{1}{(X-1)(X-2)\dots(X-n)} = \sum_{i=1}^{n} \frac{a_i}{X-i} ,$$

où pour tout $i \in [\![1,n]\!]$,

$$a_i = \frac{1}{Q_i(i)} = \frac{1}{(i-1)(i-2)\dots 1 \times (-1)(-2)\dots(i-n)} = \frac{(-1)^{n-i}}{(i-1)\,!\,(n-i)!} .$$

c) Nous reprenons les notations de la question précédente. La décomposition s'écrit ici :

$$F = \frac{1}{(X-1)^2(X-2)^2\dots(X-n)^2} = \sum_{i=1}^{n} \frac{b_i}{(X-i)^2} + \sum_{i=1}^{n} \frac{c_i}{(X-i)} ,$$

où pour tout $i \in [\![1,n]\!]$, $b_i = 1/Q_i^2(i) = a_i^2$, et c_i est un coefficient rationnel à déterminer.
Pour i fixé, multiplions l'égalité ci-dessus par $(X-i)^2$, nous obtenons une égalité de la forme ;

$$\frac{1}{Q_i^2(X)} = b_i + c_i(X-i) + (X-i)^2\,G_i(X) ,$$

où, pour $i \in [\![1,n]\!]$, G_i est une fraction rationnelle qui n'a pas le pôle i. Nous retrouvons naturellement $b_i = a_i^2$, et prenant la valeur en i de la dérivée, nous obtenons :

$$\frac{-2\,Q_i'(i)}{Q_i^3(i)} = c_i .$$

d)

1) Pour tout $\theta \in \mathbb{R}$, $\cos n\theta = T_n(\cos\theta)$, et on sait que T_n est de degré n. Les réels $x_k = \cos\left((\pi + 2k\pi)/2n\right)$, où $k \in [\![0, n-1]\!]$, sont n réels distincts, et sont visiblement tous zéros du polynôme T_n ; ils forment donc une numérotation des zéros de ce polynôme. Nous en déduisons que la fraction rationnelle $F = 1/T_n$ a n pôles simples et que, puisque sa partie entière est nulle, sa décomposition en éléments simples est de la forme :

$$\frac{1}{T_n(X)} = \sum_{k=0}^{n-1} \frac{a_k}{X - x_k} ,$$

où pour tout $k \in [\![0, n-1]\!]$,

$$a_k = \frac{1}{T_n'(x_k)} .$$

Nous obtenons facilement par dérivation :

$$(\forall \theta \in \mathbb{R}) \quad n \sin n\theta = \sin\theta \, T_n'(\cos\theta) .$$

Posons, pour $k \in [\![0, n-1]\!]$, $\theta_k = (\pi + 2k\pi)/2n$; nous obtenons $\sin n\theta_k = (-1)^k$, et comme $\sin\theta_k > 0$, $\sin\theta_k = \sqrt{1 - x_k^2}$. Nous en déduisons que pour tout $k \in [\![0, n-1]\!]$:

$$a_k = \frac{1}{T_n'(x_k)} = (-1)^k \frac{\sqrt{1 - x_k^2}}{n} .$$

2) Pour tout $\theta \in \mathbb{R}$, $\sin(n+1)\theta = \sin\theta \, U_n(\cos\theta)$, et on sait que U_n est de degré n. Pour $k \in [\![1, n]\!]$ posons $\theta_k = k\pi/(n+1)$; on voit que les réels $x_k = \cos\theta_k$, pour $k \in [\![1, n]\!]$, sont n zéros du polynôme U_n, et forment donc une numérotation des zéros de ce polynôme. La fraction rationnelle $F = 1/U_n$, de partie entière nulle, a donc n pôles simples ; sa décomposition en éléments simples est de la forme :

$$\frac{1}{U_n(X)} = \sum_{k=1}^{n} \frac{a_k}{X - x_k} ,$$

où pour tout $k \in [\![1, n]\!]$,

$$a_k = \frac{1}{U_n'(x_k)} .$$

Nous obtenons facilement par dérivation :

$$(\forall \theta \in \mathbb{R}) \quad (n+1)\cos(n+1)\theta = \cos\theta \, U_n(\cos\theta) - \sin^2\theta \, U_n'(\cos\theta) .$$

Pour $\theta = \theta_k$, où $k \in [\![1, n]\!]$, on obtient $\cos(n+1)\theta_k = \cos k\pi = (-1)^k$ et $U_n(\cos\theta_k) = 0$ (bien sûr !), d'où :

$$a_k = -\frac{\sin^2\theta_k}{(n+1)(-1)^k} = (-1)^{k+1} \frac{\sin^2\theta_k}{(n+1)} = (-1)^{k+1} \frac{1 - x_k^2}{n+1} .$$

e) Nous utiliserons les résultats de l'exercice 23 du §VII.5 ; en particulier, si $n > 0$ est pair, 0 et 1 sont des zéros de E_n, et si n est impair, $E_n(X) = -E_n(1 - X)$, donc $1/2$ est zéro de E_n.

1) Comme $E_2 = X^2 - X$, nous obtenons :

$$\frac{1}{E_2(X)} = \frac{1}{X(X-1)} = \frac{1}{(X-1)} - \frac{1}{X} .$$

2) On a vu que $E_3 = X^3 - (3/2)X^2 + 1/4 = (X - 1/2)(X^2 - X - 1/2)$. La décomposition en facteurs irréductibles du polynôme E_3 est donc :

$$E_3 = (X - 1/2)\big((X - 1/2)^2 - 3/4\big) =$$
$$= \left(X - \frac{1}{2}\right)\left(X - \frac{1+\sqrt{3}}{2}\right)\left(X - \frac{1-\sqrt{3}}{2}\right) .$$

Posons

$$\alpha = \frac{1+\sqrt{3}}{2} \quad \text{et} \quad \beta = \frac{1-\sqrt{3}}{2} ,$$

nous obtenons :

$$\frac{1}{E_3} = \frac{u}{X - 1/2} + \frac{a}{X - \alpha} + \frac{b}{X - \beta} ,$$

où :

$$u = \frac{1}{(1/2)^2 - 1/2 - 1/2} = -\frac{4}{3} ,$$

et

$$a = \frac{1}{E_3'(\alpha)} = \frac{1}{3\alpha^2 - 3\alpha} = \frac{2}{3} \qquad b = \frac{1}{E_3'(\beta)} = \frac{1}{3\beta^2 - 3\beta} = \frac{2}{3} .$$

En conclusion :

$$\frac{1}{E_3(X)} = -\frac{4/3}{X - 1/2} + \frac{2/3}{X - \frac{1+\sqrt{3}}{2}} + \frac{2/3}{X - \frac{1-\sqrt{3}}{2}} .$$

3) Nous avons obtenu $E_4 = X^4 - 2X^3 + X = X(X - 1)(X^2 - X - 1)$. La décomposition en facteurs irréductibles dans $\mathbb{C}[X]$ du polynôme E_4 est donc :

$$E_4 = X(X - 1)\big((X - 1/2)^2 - 5/4\big) =$$
$$= X(X - 1)\left(X - \frac{1+\sqrt{5}}{2}\right)\left(X - \frac{1-\sqrt{5}}{2}\right) .$$

Posons

$$\alpha = \frac{1+\sqrt{5}}{2} \quad \text{et} \quad \beta = \frac{1-\sqrt{5}}{2} .$$

En utilisant une identité de Bézout évidente, nous obtenons :

$$\frac{1}{E_4} = \frac{X(X-1) - (X^2 - X - 1)}{X(X-1)(X^2 - X - 1)} = \frac{1}{X^2 - X - 1} - \frac{1}{X(X-1)} .$$

On voit que :

$$\frac{1}{(X - \alpha)(X - \beta)} = \frac{1}{\alpha - \beta}\left(\frac{1}{X - \alpha} - \frac{1}{X - \beta}\right) .$$

En tenant compte des valeurs de α et β, on obtient finalement :

$$\frac{1}{E_4(X)} = \frac{1}{X} - \frac{1}{X-1} + \frac{1/\sqrt{5}}{X - \frac{1+\sqrt{5}}{2}} - \frac{1/\sqrt{5}}{X - \frac{1-\sqrt{5}}{2}} .$$

4) Nous avons obtenu $E_5 = X^5 - 5/2\,X^4 + 5/2\,X^2 - 1/2$. Puisque 5 est impair, $1/2$ est zéro de ce polynôme ; on obtient facilement par division euclidienne ou en utilisant le schéma de Hörner : $E_5 = (X-1/2)(X^4-2X^3-X^2+2\,X+1)$. Le polynôme E_5 peut s'exprimer comme un polynôme impair en $X - 1/2$, et son quotient par $X - 1/2$ est un polynôme du second degré en $(X - 1/2)^2$, donc aussi en $X(X-1)$; en identifiant on trouve :

$$X^4 - 2X^3 - X^2 + 2\,X + 1 = X^2(X-1)^2 - 2\,X(X-1) + 1 = \\ = \big(X(X-1) - 1\big)^2 = (X^2 - X - 1)^2 .$$

On voit aussi que :

$$X^2 - X - 1 = (X - 1/2)^2 - 5/4 = (X - \alpha)(X - \beta) ,$$

où :

$$\alpha = \frac{1+\sqrt{5}}{2} \quad \text{et} \quad \beta = \frac{1-\sqrt{5}}{2} .$$

La décomposition du polynôme E_5 en facteurs irréductibles dans $\mathbb{C}[X]$ est donc :

$$E_5(X) = (X - 1/2)(X - \alpha)^2(X - \beta)^2 .$$

La décomposition en éléments simples de la fraction rationnelle $1/E_5$, de partie entière nulle, est donc de la forme :

$$(1) \qquad \frac{1}{E_5(X)} = \frac{u}{X - 1/2} + \frac{a_1}{(X-\alpha)^2} + \frac{a_2}{X-\alpha} + \frac{b_1}{(X-\alpha)^2} + \frac{b_2}{X-\alpha} ,$$

où :

$$u = \frac{1}{((1/2)^2 - 1/2 - 1)^2} = \frac{16}{25} .$$

En multipliant l'égalité (1) par $(X-\alpha)^2$, on obtient une égalité de la forme :

$$F(X) = \frac{1}{(X - 1/2)(X-\beta)^2} = a_1 + a_2(X-\alpha) + (X-\alpha)^2\,G(X) ,$$

où G est une fraction rationnelle qui n'admet pas le pôle α. En prenant la valeur en α de la fraction rationnelle F on trouve :

$$a_1 = \frac{1}{(\alpha - 1/2)(\alpha-\beta)^2} = \frac{2}{5\sqrt{5}} \quad , \text{de même} \quad b_1 = -\frac{2}{5}$$

et en prenant la valeur en α de la dérivée logarithmique de F, on trouve :

$$\frac{F'(\alpha)}{F(\alpha)} = \frac{a_2}{a_1} = -\frac{1}{\alpha - 1/2} - \frac{2}{\alpha - \beta} = -\frac{1}{\sqrt{5}/2} - \frac{2}{\sqrt{5}} = -\frac{4}{\sqrt{5}} ;$$

on trouve ainsi la valeur de a_2, et de manière analogue la valeur de b_2 :

$$a_2 = -\frac{8}{25} \quad \text{et} \quad b_2 = -\frac{8}{25} .$$

Nous obtenons la décomposition :

$$\frac{25}{E_5(X)} = = \frac{16}{X - 1/2} + \frac{2\sqrt{5}}{\left(X - \frac{1+\sqrt{5}}{2}\right)^2} - \frac{8}{X - \frac{1+\sqrt{5}}{2}} - \frac{2\sqrt{5}}{\left(X - \frac{1-\sqrt{5}}{2}\right)^2} - \frac{8}{X - \frac{1-\sqrt{5}}{2}} .$$

f) Nous pouvons ici écrire :

$$F = \frac{1}{X \prod_{k=1}^{n} (X^2 - k^2)} = \frac{1}{\prod_{k=-n}^{n} (X - k)} .$$

La décomposition en éléments simples de la fraction rationnelle $1/F$ et donc de la forme :

$$F = \sum_{k=-n}^{n} \frac{a_k}{X - k} ,$$

où pour tout $i \in [\![-n, n]\!]$:

$$\frac{1}{a_i} = \prod_{k \in [\![-n,n]\!] \setminus \{i\}} (i - k) = = (i + n) \dots 1 \times (-1) \dots (i - n) = (-1)^{n-i} (n + i) ! (n - i) ! .$$

g) Décomposons d'abord le polynôme $P = (X + 1)^7 - X^7 - 1$ en produit de facteurs irréductibles dans $\mathbb{C}[X]$. On obtient :

$$P = (X + 1)^7 - X^7 - 1 = 7 X^6 + 21 X^5 + 35 X^4 + 35 X^3 + 21 X^2 + 7 X = = 7 X (X^5 + 3 X^4 + 5 X^3 + 5 X^2 + 3)$$

Un zéro évident du polynôme P est -1 ; des zéros un peu moins évidents sont j et j^2. Par division euclidienne par $X+1$, puis par X^2+X+1, on obtient l'égalité :

$$P = 7X(X+1)(X^2+X+1)^2 = 7X(X+1)(X-\mathrm{j})^2(X-\mathrm{j}^2)^2 .$$

Nous pouvons utiliser l'identité de Bézout $(X^2+X+1) - X(X+1) = 1$:

$$\begin{aligned}\frac{7}{P} &= \frac{1}{X(X+1)(X^2+X+1)} - \frac{1}{(X^2+X+1)^2} \\ &= \frac{1}{X(X+1)} - \frac{1}{X^2+X+1} - \frac{1}{(X^2+X+1)^2} \\ &= \frac{1}{X} - \frac{1}{X+1} - \frac{1}{X^2+X+1} - \frac{1}{(X^2+X+1)^2} ,\end{aligned}$$

ce qui est la décomposition en éléments simples dans $\mathbb{R}(X)$ de $7/P$.
Décomposons maintenant dans $\mathbb{C}(X)$ la fraction rationnelle :

$$\frac{1}{X^2+X+1} + \frac{1}{(X^2+X+1)^2} = \frac{X^2+X+2}{(X^2+X+1)^2} .$$

Sa décomposition est de la forme :

$$(1) \qquad \frac{X^2+X+2}{(X^2+X+1)^2} = \frac{a_1}{(X-\mathrm{j})^2} + \frac{a_2}{X-\mathrm{j}} + \frac{\bar{a}_1}{(X-\mathrm{j}^2)^2} + \frac{\bar{a}_2}{X-\mathrm{j}^2} .$$

En multipliant cette égalité par $(X-\mathrm{j})^2$, nous obtenons :

$$F = \frac{X^2+X+2}{(X-\mathrm{j}^2)^2} = a_1 + a_2(X-\mathrm{j}) + (X-\mathrm{j})^2 G(X) ,$$

où G est une fraction rationnelle qui n'a pas le pôle j. Nous obtenons :

$$a_1 = F(\mathrm{j}) = \frac{\mathrm{j}^2+\mathrm{j}+2}{(\mathrm{j}-\mathrm{j}^2)^2} = \frac{1}{(\mathrm{i}\sqrt{3})^2} = -\frac{1}{3} ,$$

et :

$$\frac{a_2}{a_1} = \frac{F'(\mathrm{j})}{F(\mathrm{j})} = \frac{2\mathrm{j}+1}{\mathrm{j}^2+\mathrm{j}+2} - 2\frac{1}{\mathrm{j}-\mathrm{j}^2} = \frac{\mathrm{i}\sqrt{3}}{1} - \frac{2}{\mathrm{i}\sqrt{3}} = \frac{5\mathrm{i}}{\sqrt{3}} ,$$

d'où :

$$a_2 = -\frac{5\mathrm{i}}{3\sqrt{3}} = -\frac{5\mathrm{i}\sqrt{3}}{9} .$$

Nous obtenons ainsi la décomposition de la fraction rationnelle $7/P$, en éléments simples dans $\mathbb{C}(X)$:

$$\begin{aligned}\frac{7}{P} &= \\ &= \frac{1}{X} - \frac{1}{(X+1)} + \frac{1/3}{(X-\mathrm{j})^2} + \frac{5\mathrm{i}\sqrt{3}/9}{X-\mathrm{j}} + \frac{1/3}{(X-\mathrm{j}^2)^2} - \frac{5\mathrm{i}\sqrt{3}/9}{\cdot}\end{aligned}$$

Exercice 3 :

Décomposer en éléments simples sur $\mathbb{R}$ les fractions rationnelles suivantes :

a) $F = \dfrac{1}{X^m(1-X)^n}$, $m \in \mathbb{N}^*, n \in \mathbb{N}^*$; *b)* $F = \dfrac{1}{(X^2-1)^n}$;

c) $F = \dfrac{X^4+1}{(X-1)(X^2-X+1)^n}$; *d)* $F = \dfrac{X^5-X^3-X^2}{X^2-1}$;

e) $F = \dfrac{4X^3}{(X^2+1)^2}$; *f)* $F = \dfrac{X^6-X^2+1}{(X-1)^3}$. ■

a) En dérivant $n-1$ fois l'égalité :

$$\frac{1}{1-X} = 1 + X + \ldots + X^{n+m-2} + \frac{X^{n+m-1}}{1-X} ,$$

on trouve :

$$\frac{(n-1)!}{(1-X)^n} = (n-1)! + \frac{n!}{1!}X + \ldots + \frac{(n+m-2)!}{(m-1)!}X^{m-1} + X^m G(X) ,$$

où G est une fraction rationnelle qui n'a que le pôle 1. Nous obtenons donc :

$$\frac{1}{X^m(1-X)^n} = \frac{\binom{n-1}{0}}{X^m} + \frac{\binom{n}{1}}{X^{m-1}} + \ldots + \frac{\binom{n+m-2}{m-1}}{X} + \frac{1}{(n-1)!}G(X) .$$

La partie polaire relative au pôle 0 dans la décomposition en éléments simples de F est donc :

$$F_0 = \frac{\binom{n-1}{0}}{X^m} + \frac{\binom{n}{1}}{X^{m-1}} + \ldots + \frac{\binom{n+m-2}{m-1}}{X} .$$

En remplaçant X par $(1-X)$ et en échangeant n et m on obtient la partie polaire relative au pôle 1 :

$$F_1 = \frac{\binom{m-1}{0}}{(1-X)^n} + \frac{\binom{m}{1}}{(1-X)^{n-1}} + \ldots + \frac{\binom{n+m-2}{n-1}}{1-X} .$$

Comme la fraction rationnelle F est de partie entière nulle et que son dénominateur est dissocié dans $\mathbb{R}[X]$, elle est somme de ses parties polaires, soit ici :

$$F = F_0 + F_1 .$$

b) Posons $Y = (X+1)/2$, on voit que :

$$\frac{1}{(X^2-1)^n} = \frac{1}{4^n Y^n (Y-1)^n} = \frac{(-1)^n}{4^n Y^n (1-Y)^n} .$$

D'après le a) :

$$\frac{1}{(X^2-1)^n} = \frac{(-1)^n}{4^n}\left(\sum_{i=0}^{n-1}\frac{\binom{n-1+i}{i}}{Y^{n-i}} + \sum_{j=0}^{n-1}\frac{\binom{n-1+j}{j}}{(1-Y)^{n-j}}\right) ,$$

soit finalement :

$$\frac{1}{(X^2-1)^n} = \frac{(-1)^n}{4^n}\left(\sum_{i=0}^{n-1}\frac{\binom{n-1+i}{i}2^{n-i}}{(X+1)^{n-i}} + \sum_{j=0}^{n-1}\frac{\binom{n-1+j}{j}2^{n-j}}{(1-X)^{n-j}}\right) .$$

c) Nous supposerons $n \geqslant 2$; la fraction rationnelle est alors de partie entière nulle. Il est clair que la partie polaire relative au pôle 1 est $F_1 = 2/(X-1)$. Comme le polynôme $X^2 - X + 1$ est irréductible sur $\mathbb{R}$, il ne reste dans la décomposition qu'une partie primaire, qui est :

$$R = F - F_1 = \\ = \frac{X^4+1}{(X-1)(X^2-X+1)^n} - \frac{2}{X-1} = \frac{X^4+1-2(X^2-X+1)^n}{(X-1)(X^2-X+1)^n} .$$

Nous pouvons écrire :

$$R = \frac{X^4-1-2\big((X^2-X+1)^n-1\big)}{(X-1)(X^2-X+1)^n} = \\ = \frac{(X-1)(X+1)(X^2+1) - 2(X^2-X)\sum_{i=0}^{n-1}(X^2-X+1)^i}{(X-1)(X^2-X+1)^n} ,$$

soit, après simplification :

$$R = \frac{(X+1)(X^2+1)}{(X^2-X+1)^n} - 2\sum_{i=0}^{n-1}\frac{X}{(X^2-X+1)^{n-i}} .$$

De l'égalité :

$$(X+1)(X^2+1) = (X^2-X+1)(X+2) + 2X - 1 ,$$

obtenue par division euclidienne, nous déduisons :

$$R = \frac{2X-1}{(X^2-X+1)^n} + \frac{X+2}{(X^2-X+1)^{n-1}} - 2\sum_{i=0}^{n-1}\frac{X}{(X^2-X}$$

La décomposition en éléments simples de F sur $\mathbb{R}$ est donc :

$$F = \frac{2}{X-1} - \frac{1}{(X^2-X+1)^n} + \frac{2-X}{(X^2-X+1)^{n-1}} - 2\sum_{i=2}^{n-1} \frac{X}{(X^2-X+1)^{n-i}} \cdot$$

d) On observe que :

$$F = \frac{X^5 - X^3 - X^2}{X^2-1} = \frac{X^3(X^2-1) - (X^2-1) - 1}{X^2-1} =$$
$$= X^3 - 1 + \frac{1/2}{X+1} - \frac{1/2}{X-1} ,$$

ce qui est la décomposition en éléments simples sur $\mathbb{R}$ de la fraction rationnelle F.

e) On obtient facilement la décomposition cherchée en remarquant que :

$$F = \frac{4X^3}{(X^2+1)^2} = \frac{4X(X^2+1) - 4X}{(X^2+1)^2} = \frac{4X}{X^2+1} - \frac{4X}{(X^2+1)^2} \cdot$$

f) En posant $Y = X - 1$ on obtient :

$$F = \frac{X^6 - X^2 + 1}{(X-1)^3} = \frac{(Y+1)^6 - (Y+1)^2 + 1}{Y^3} =$$
$$= Y^3 + 6Y^2 + 15Y + 20 + \frac{15-1}{Y} + \frac{6-2}{Y^2} + \frac{1-1+1}{Y^3}$$
$$= P(X) + \frac{14}{X-1} + \frac{4}{(X-1)^2} + \frac{1}{(X-1)^3} ,$$

où le polynôme P est la partie entière de la fraction rationnelle F. D'après le calcul ci-dessus :

$$P = (X-1)^3 + 6(X-1)^2 + 15(X-1) + 20 = X^3 + 3X^2 + 6X + 10 .$$

Exercice 5 :

Décomposer en éléments simples sur $K = \mathbb{Z}/5\mathbb{Z}$ les fractions rationnelles suivantes :

a) $\dfrac{X - \bar{1}}{(X+\bar{1})^2(X+\bar{2})}$; *b*) $\dfrac{\bar{1}}{(X^2+\bar{1})(X^2+\bar{2})}$;

c) $\dfrac{X-\bar{2}}{(X^2+\bar{4})(X^2+\bar{3})}$; *d)* $\dfrac{\bar{4}X+\bar{2}}{X^3+\bar{2}X^2+\bar{4}X+\bar{3}}$;
et décomposer $\dfrac{\bar{2}X^5+\bar{3}X^3+\bar{6}X^2+\bar{4}}{(X^2+\bar{1})^2}$ sur $\mathbb{Z}/7\mathbb{Z}$. ■

Les carrés dans le corps $\mathbb{Z}/5\mathbb{Z}$ sont $\bar{0},\bar{1},\bar{4}$. Comme sur tout corps, un polynôme du second degré qui n'a pas de zéro est irréductible.

a) La décomposition de la fraction rationnelle est de la forme :

$$\frac{X-\bar{1}}{(X+\bar{1})^2(X+\bar{2})}=\frac{a}{(X+\bar{1})^2}+\frac{b}{X+\bar{1}}+\frac{c}{X+\bar{2}}\ ,$$

où a,b,c sont des éléments de $\mathbb{Z}/5\mathbb{Z}$ à déterminer. Nous obtenons par les méthodes usuelles :

$$a=\frac{-\bar{2}}{\bar{1}}=\bar{3}\quad\text{et}\quad c=\frac{-\bar{3}}{\bar{1}}=\bar{2}\ .$$

Pour déterminer b, nous pouvons prendre la valeur en $\bar{0}$:

$$\frac{-\bar{1}}{\bar{2}}=\frac{\bar{4}}{\bar{2}}=\bar{2}=\bar{3}+b+\frac{\bar{2}}{\bar{2}}\quad\text{soit}\quad b=\bar{3}\ .$$

La décomposition en éléments simples de la fraction rationnelle est donc :

$$\frac{X-\bar{1}}{(X+\bar{1})^2(X+\bar{2})}=\frac{\bar{3}}{(X+\bar{1})^2}+\frac{\bar{3}}{X+\bar{1}}+\frac{\bar{2}}{X+\bar{2}}\ .$$

b) On voit que $-\bar{1}=\bar{4}$ est un carré, et que $-\bar{2}=\bar{3}$ n'en est pas un. La factorisation en produit de facteurs irréductibles du dénominateur est donc :

$$(X-\bar{2})(X+\bar{2})(X^2+\bar{2})\ .$$

Nous obtenons :

$$\frac{\bar{1}}{(X^2+\bar{1})(X^2+\bar{2})}=\frac{\bar{1}}{X^2-\bar{4}}-\frac{\bar{1}}{X^2+\bar{2}}=\frac{\bar{1}}{X+\bar{2}}-\frac{\bar{1}}{X-\bar{2}}-\frac{\bar{1}}{X^2+\bar{2}}\ .$$

c) On voit que $-\bar{4}=\bar{1}$ est un carré, alors que $-\bar{3}=\bar{2}$ n'en est pas un. La décomposition en facteurs irréductibles du dénominateur est donc :

$$(X^2+\bar{4})(X^2+\bar{3})=(X-\bar{1})(X+\bar{1})(X^2+\bar{3})\ .$$

Nous obtenons :

$$\frac{X-\bar{2}}{(X^2+\bar{4})(X^2+\bar{3})} = (X-\bar{2})\left(\frac{1}{X^2+\bar{3}} - \frac{1}{X^2+\bar{4}}\right) = \frac{X-\bar{2}}{X^2+\bar{3}} - \frac{X-\bar{2}}{X^2+\bar{4}} .$$

La première fraction est un élément simple. Pour la deuxième on trouve facilement en utilisant les méthodes usuelles :

$$\frac{\bar{2}-X}{X^2-\bar{1}} = \frac{\bar{3}}{X-\bar{1}} + \frac{\bar{1}}{X+\bar{1}} .$$

La décomposition en éléments simples de la fraction est donc :

$$\frac{X-\bar{2}}{(X^2+\bar{4})(X^2+\bar{3})} = \frac{X-\bar{2}}{X^2+\bar{3}} + \frac{\bar{3}}{X-\bar{1}} + \frac{\bar{1}}{X+\bar{1}} .$$

d) On voit facilement que $\bar{1}$ est zéro du dénominateur ; on obtient :

$$X^3+\bar{2}X^2+\bar{4}X+\bar{3} = (X-\bar{1})(X^2+\bar{3}X+\bar{2}) = (X-\bar{1})(X+\bar{1})(X+\bar{2}) .$$

La décomposition de la fraction rationnelle de l'énoncé est donc de la forme :

$$\frac{\bar{4}X+\bar{2}}{X^3+\bar{2}X^2+\bar{4}X+\bar{3}} = \frac{a}{X-\bar{1}} + \frac{b}{X+\bar{1}} + \frac{c}{X+\bar{2}} ,$$

où a, b, c sont des éléments de $\mathbb{Z}/5\mathbb{Z}$. On obtient par la méthode des résidus :

$$a = \frac{\bar{6}}{\bar{6}} = \bar{1} , \quad b = \frac{-\bar{2}}{-\bar{2}} = \bar{1} , \quad c = \frac{-\bar{6}}{\bar{3}} = -\bar{2} = \bar{3} .$$

Nous obtenons par conséquent la factorisation :

$$\frac{\bar{4}X+\bar{2}}{X^3+\bar{2}X^2+\bar{4}X+\bar{3}} = \frac{\bar{1}}{X-\bar{1}} + \frac{\bar{1}}{X+\bar{1}} + \frac{\bar{3}}{X+\bar{2}} .$$

e) Les carrés modulo 7 sont $0, 1, 4, 2$; nous en déduisons que $-\bar{1}$ n'est pas un carré et que le polynôme $X^2+\bar{1}$ est irréductible. Pour décomposer la fraction rationnelle :

$$F = \frac{\bar{2}X^5+\bar{3}X^3+\bar{6}X^2+\bar{4}}{(X^2+\bar{1})^2} ,$$

en éléments simples sur le corps $\mathbb{Z}/7\mathbb{Z}$, nous utiliserons la méthode des divisions euclidiennes successives, puisque le dénominateur n'a qu'un seul facteur irréductible.

$$\begin{array}{rrrrr|l} 2X^5 & +0X^4 & +3X^3 & +6X^2 & +0\,X\ +4 & X^2+1 \\ \cline{6-6} & & X^3 & +6X^2 & +0X\ +4 & 2X^3+X+6 \\ & & & +6X^2 & -X\ +4 & \\ & & & & -X\ -2 & \end{array}$$

$$\begin{array}{rrrr|l} 2X^3 & +0X^2 & +\ X & +6 & X^2+1 \\ \cline{5-5} & & -X & +6 & 2X \end{array}$$

Nous en déduisons la décomposition en éléments simples de la fraction rationnelle F :

$$F = \bar{2}\,X + \frac{\bar{6}-X}{X^2+\bar{1}} - \frac{X+\bar{2}}{(X^2+1)^2}\ .$$

Exercice 7 :

Réduire au même dénominateur et simplifier les fractions suivantes ($n \in \mathbb{N}, n \geqslant 2$) :

a) $F = \displaystyle\sum_{\zeta\in\mu_n} \frac{1}{X-\zeta}$; *b)* $F = \displaystyle\sum_{\zeta\in\mu_n} \frac{1}{(X-\zeta)^2}$;

c) $F = \displaystyle\sum_{\zeta\in\mu_n} \frac{\zeta^k(X-\omega)}{(X-\zeta)^2}$, avec $\omega = \mathrm{e}^{\mathrm{i}\,\pi/n}$ et $k \in \mathbb{N}$. ■

a) On sait que

$$\prod_{\zeta\in\mu_n} (X-\zeta) = X^n - 1\ .$$

La dérivée logarithmique du produit étant la somme des dérivées logarithmiques, nous obtenons pour tout $n \in \mathbb{N}^*$:

$$\frac{n\,X^{n-1}}{X^n-1} = \sum_{\zeta\in\mu_n} \frac{1}{X-\zeta}\ .$$

Cette fraction n'est pas simplifiable car le polynôme X^n-1 est premier avec son polynôme dérivé (tous ses zéros sont simples).

b) En dérivant l'égalité trouvée dans le *a)*, on obtient pour tout $n \geqslant 2$:

$$\frac{n(n-1)X^{n-2}(X^n-1) - n^2X^{2n-2}}{(X^n-1)^2} = -\sum_{\zeta\in\mu_n} \frac{1}{(X-\zeta)^2}\ .$$

D'où l'égalité :

$$\sum_{\zeta\in\mu_n} \frac{1}{(X-\zeta)^2} = \frac{nX^{n-2}(X^n+n-1)}{(X^n-1)^2} \cdot$$

L'ensemble des zéros du dénominateur est μ_n, et en $\zeta \in \mu_n$ le numérateur vaut $n\,\zeta^{n-2}(1+n-1) = n^2\zeta^{-2} \neq 0$. Cette fraction rationnelle est donc sous forme irréductible.

c) Pour tout $k \in \mathbb{N}$ nous pouvons écrire :

$$F_k = (X-\omega) \sum_{\zeta\in\mu_n} \frac{\zeta^k}{(X-\zeta)^2} \cdot$$

Soit $P \in \mathbb{C}_{n-1}[X]$, la fraction rationnelle $P/(X^n-1)$ est de partie entière nulle et sa décomposition en éléments simples sur $\mathbb{C}$ est de la forme :

$$\frac{P}{X^n-1} = \sum_{\zeta\in\mu_n} \frac{a_\zeta}{X-\zeta} \,, \tag{1}$$

où, d'après le théorème VIII.2.2, pour tout $\zeta \in \mu_n$:

$$a_\zeta = \frac{P(\zeta)}{n\,\zeta^{n-1}} = \frac{1}{n}\zeta\,P(\zeta) \,.$$

En dérivant l'égalité (1), nous obtenons :

$$\frac{(X^n-1)P' - n\,X^{n-1}\,P}{(X^n-1)^2} = -\sum_{\zeta\in\mu_n} \frac{a_\zeta}{(X-\zeta)^2} \,,$$

d'où finalement :

$$\sum_{\zeta\in\mu_n} \frac{\zeta\,P(\zeta)}{(X-\zeta)^2} = \frac{n^2\,X^{n-1}\,P - n\,(X^n-1)P'}{(X^n-1)^2} \cdot \tag{2}$$

La fraction rationnelle F_k ne dépend que de la classe de l'entier k modulo n. Soit $k_1 \in [\![1,n]\!]$ tel que $k \equiv k_1 \bmod (n)$, nous pouvons utiliser l'égalité (2) avec le polynôme $P = X^{k_1-1}$ (puisque $0 \leqslant k_1 - 1 \leqslant n-1$) ; nous obtenons,
si $k_1 \geqslant 2$:

$$\sum_{\zeta\in\mu_n} \frac{\zeta^k}{(X-\zeta)^2} = \sum_{\zeta\in\mu_n} \frac{\zeta^{k_1}}{(X-\zeta)^2} =$$

$$= \frac{n^2\,X^{n-1}\,X^{k_1-1} - n(k_1-1)\,(X^n-1)X^{k_1-2}}{(X^n-1)^2}$$

$$= \frac{n(n-k_1+1)\,X^{n+k_1-2} + n(k_1-1)X^{k_1-2}}{(X^n-1)^2}$$

Dans le cas particulier où $k_1 = 1$, on voit que $P = 1$ et $P' = 0$, on obtient :

$$\sum_{\zeta \in \mu_n} \frac{\zeta}{(X-\zeta)^2} = \frac{n^2 X^{n-1}}{(X^n-1)^2} .$$

D'où si $k_1 > 1$:

$$F_k = (X-\omega)\, \frac{n(n-k_1+1)\, X^{n+k_1-2} + n(k_1-1)X^{k_1-2}}{(X^n-1)^2} ,$$

et si $k_1 = 1$:

$$F_k = (X-\omega)\, \frac{n^2 X^{n-1}}{(X^n-1)^2} .$$

Dans les deux cas la fraction obtenue n'est pas simplifiable puisque $\omega \notin \mu_n$ ($\omega^n = -1$), et qu'en $\zeta \in \mu_n$, le numérateur de la fraction est, dans les deux cas, $n^2 (\zeta - \omega)\, \zeta^{k_1-2} \neq 0$.

§ VIII.3 *FONCTIONS RATIONNELLES. DÉRIVATION*

Exercice 2 :

On se place dans le plan d'Argand-Cauchy. Soit $F \in \mathbb{C}[X]$ un polynôme non constant.

a) Si toutes les racines de F sont dans un même demi-plan ouvert $\mathcal{H}$ de $\mathbb{C}$, les racines de F' appartiennent à $\mathcal{H}$.

b) Si toutes les racines de F sont dans un même demi-plan fermé de frontière Δ, et si F' a des racines sur Δ, alors F a des racines sur Δ.

c) Si les racines de F sont dans un polygone convexe fermé de $\mathbb{C}$, celles de F' y sont aussi.

d) Si les racines de F sont *simples* et ont pour images les sommets d'un polygone convexe, les racines de F' sont à *l'intérieur* de ce polygone. ■

Posons :

$$F(X) = \prod_{i=1}^{k} (X - z_i)^{n_i} ,$$

où $(z_1, z_2, \ldots, z_k)$ sont les k zéros de F (2 à 2 distincts) et $n_1, n_2, \ldots, n_k$ leurs ordres respectifs, tous entiers > 0. Nous obtenons facile

logarithmique) :

$$\frac{F'}{F} = \sum_{i=1}^{k} \frac{n_i}{X - z_i} \cdot$$

Si $z \in \mathbb{C}$ est un zéro de F' qui n'est pas zéro de F, nous obtenons :

$$0 = \sum_{i=1}^{k} \frac{n_i}{z - z_i} = \sum_{i=1}^{k} \frac{n_i}{|z - z_i|^2} \overline{(z - z_i)} ,$$

soit encore en prenant le conjugué :

$$0 = \sum_{i=1}^{k} \frac{n_i}{|z - z_i|^2} (z - z_i) .$$

Pour tout $i \in [\![1, k]\!]$ posons $t_i = n_i / |z - z_i|^2$; ce sont des réels > 0. Notons $s = \sum_{i=1}^{k} t_i$, on voit que :

$$s \cdot z = \sum_{i=1}^{k} t_i z_i .$$

Cela signifie que tout zéro de F' qui n'est pas un zéro de F, est barycentre à coefficients > 0 des zéros de F. Pour tout $i \in [\![1, k]\!]$ posons $\alpha_i = t_i / s$, on obtient :

$$z = \sum_{i=1}^{k} \alpha_i z_i \quad \text{et} \quad \sum_{i=1}^{k} \alpha_i = 1 .$$

Les propositions de l'énoncé découlent de cette remarque. Nous utiliserons dans ce qui suit les notations introduites ici.

a) Soit φ une forme affine sur le $\mathbb{R}$-espace affine $\mathbb{C}$ telle que

$$\mathcal{H} = \{z \in \mathbb{C} \mid \varphi(z) > 0\} ;$$

Pour tout $i \in [\![1, k]\!]$, $z_i \in \mathcal{H}$ donc $\varphi(z_i) > 0$. Soit z un zéro de F', si c'est un zéro de F alors $z \in \mathcal{H}$; si ce n'est pas un zéro de F, en utilisant les notations introduites ci-dessus, on obtient :

$$\varphi(z) = \sum_{i=1}^{k} \alpha_i \varphi(z_i) > 0 ,$$

donc $z \in \mathcal{H}$.

b) Si aucun zéro de F n'était sur Δ, les zéros de F seraient tous dans un demi-plan ouvert $\mathcal{H}$ de frontière Δ, et tous les zéros de F' seraient dans le demi-plan ouvert $\mathcal{H}$, ce qui contredit l'hypothèse. Donc F a des zéros sur Δ.

c) De manière plus générale, les convexes étant stables par barycentres à coefficients positifs, si les zéros de F sont dans un convexe, les zéros de F' y sont aussi.

d) Nous allons démontrer, sans supposer que les zéros de F sont simples, que si les zéros de F sont dans un convexe $\mathcal{C}$, et qu'ils ne sont pas alignés, alors les zéros de F' qui ne sont pas zéros de F sont dans l'intérieur de $\mathcal{C}$. Si les zéros de F sont simples, aucun zéro de F' n'est zéro de F. Nous utiliserons le lemme géométrique et topologique suivant :

Lemme :

> Soient E et F des $\mathbb{R}$-espaces affines de dimension finie ; une application affine surjective $\varphi : E \to F$ est ouverte. ■

Soit S une variété affine de E telle que $\overrightarrow{S} \bigoplus \mathrm{Ker}\,\overrightarrow{\varphi} = \overrightarrow{E}$, et p la projection affine sur S parallèlement à $\mathrm{Ker}\,\overrightarrow{\varphi}$. On voit que $\varphi = \varphi_{|S} \circ p$; la projection affine p est ouverte et $\varphi_{|S}$ est un isomorphisme affine $S \to F$, donc un homéomorphisme. Nous en déduisons que φ est ouverte.

Considérons maintenant le $\mathbb{R}$-espace affine H, dont les éléments sont les k-uplets de réels dont la somme est 1. Si les zéros de F, que nous avons notés $z_1, z_2, \ldots, z_k$, ne sont pas alignés, l'application

$$\varphi : H \to \mathbb{C} \quad , \quad (\alpha_1, \alpha_2, \ldots, \alpha_k) \mapsto \alpha_1 z_1 + \ldots + \alpha_k z_k \ ,$$

est affine surjective, donc ouverte.
Soit H_+, l'ensemble des éléments de H constitués de réels $\geqslant 0$; comme φ est affine et que $\mathcal{C}$ est un convexe contenant les zéros de F, $\varphi(H_+) \subset \mathcal{C}$.
Soit H_+^* l'ensemble des éléments de H constitués de réels > 0, c'est un ouvert de H inclus dans H_+, donc $\varphi(H_+^*)$ est un ouvert de $\mathbb{C}$ inclus dans $\mathcal{C}$, donc dans l'intérieur de $\mathcal{C}$.
Les zéros de F' qui ne sont pas zéros de F, sont dans $\varphi(H_+^*)$, donc dans l'intérieur de $\mathcal{C}$.

Nous en déduisons en particulier que si les zéros de F sont les sommets d'un polygone convexe $\mathcal{C}$ (donc non alignés), les zéros de F' qui ne sont pas zéros de F, sont dans l'intérieur de $\mathcal{C}$.

Exercice 3 :

Trouver tous les couples (F, G) d'éléments *non constants* de $\mathbb{C}(X)$ tels que $F \circ G \in \mathbb{C}[X]$. ■

Supposons que F et G soient des éléments de $\mathbb{C}(X)$ non constants tels que $F \circ G$ soit un polynôme P. Soit $F = U/V$ et $G = A/B$ des formes irréductibles de F et de G. Par définition :

$$P(X)\,V(G(X)) = U(G(X)) \ . \tag{1}$$

Soit a un pôle de F, c'est-à-dire un zéro de V (s'il en existe). Supposons que le polynôme $A(X) - a\,B(X)$ ne soit pas constant ; comme le corps $\mathbb{C}$ est algébriquement clos, il a au moins un zéro z, et $B(z) \neq 0$ sinon $A(z) = 0$ et $B(z) = 0$, ce qui est exclu puisque A et B sont premiers entre eux ; nous voyons que $a = G(z)$, d'où $V(a) = 0$ et $P(z)\,V(a) = U(a) = 0$; cela est contradictoire puisque U et V sont premiers entre eux. Nous en déduisons que si a est un zéro de V, alors le polynôme $A - a\,B$ est constant.

Supposons que F ait au moins deux pôles distincts, a et a'. Les polynômes $A - a\,B$ et $A - a'B$ seraient constants, le polynôme $(a - a')\,B$ serait constant. On voit donc que les polynômes A et B seraient constants et la fraction rationnelle G serait constante, ce qui est en contradiction avec l'hypothèse. Nous en déduisons que soit la fraction rationnelle F est un polynôme, soit elle a un pôle unique.

Supposons que F soit un polynôme (non constant). Posons :

$$F = \sum_{i=0}^{n} u_i\,X^i \ ,$$

où $n > 0$ et $u_n \neq 0$. Par définition de P :

$$P = \sum_{i=0}^{n} u_i\,\frac{A^i}{B^i} \quad \text{soit} \quad P\,B^n = \sum_{i=0}^{n-1} u_i\,A^i\,B^{n-i} + u_n\,A^n \ .$$

On voit que B divise A^n, alors que A et B sont premiers entre eux. Le polynôme B est donc constant, et la fraction rationnelle G est un polynôme.
Inversement si F et G sont des polynômes, $F \circ G$ est un polynôme.

Supposons maintenant que F a un pôle unique a. Nous avons vu que le polynôme $A - a\,B$ est constant, posons $b = A - a\,B$, où $b \in \mathbb{C}$, $b \neq 0$. On voit que G est de la forme :

$$G = \frac{A}{B} = a + \frac{b}{B} \ .$$

La fraction rationnelle F s'écrit sous la forme :

$$F = \frac{U(X)}{(X-a)^k} ,$$

où $k \in \mathbb{N}^*$ et $U \in \mathbb{C}[X]$. La condition $F \circ G = P \in \mathbb{C}[X]$ devient alors :

$$B^k U\left(a + \frac{b}{B}\right) = b^k P .$$

Posons :

$$U = \sum_{i=0}^{n} u_i X^i ,$$

où $n \geqslant 0$ et $u_n \neq 0$. Supposons $n > k$, on peut alors écrire :

$$B^n U\left(a + \frac{b}{B}\right) = b^k B^{n-k} P ,$$

soit :

$$\sum_{i=0}^{n-1} u_i (aB+b)^i B^{n-i} + u_n (aB+b)^n = b^k P B^{n-k} .$$

Nous en déduisons $B \,|\, (aB+b)^n$, donc $B \,|\, b^n$. Le polynôme B devrait donc être constant, ce qui est impossible puisque G n'est pas constante. Nous obtenons finalement la condition nécessaire suivante (dans le cas où on suppose que F a au moins un pôle) :
La fraction rationnelle G est de la forme :

$$G = a + \frac{b}{B} ,$$

où $a \in \mathbb{C}$, $b \in \mathbb{C}$, $b \neq 0$, B est un polynôme non constant ; et la fraction rationnelle F est de la forme :

$$F = \frac{U(X)}{(X-a)^k} ,$$

où $k \in \mathbb{N}^*$ et U est un polynôme non nul de degré $n \leqslant k$.
Cette condition est suffisante, car si elle est réalisée :

$$F \circ G = \frac{U(a+b/B)}{(b/B)^k} = \frac{1}{b^k} B^k U(a+b/B) .$$

Il est clair que puisque $n = \deg(U) \leqslant k$, on obtient bien ainsi un polynôme.

Exercice 6 :

‖ On prend $K = \mathbb{C}$.

a) Soit $G \in \mathbb{C}(X)$ une fraction non constante. Pour tout $t \in \mathbb{C}$, on note $G^{-1}(t)$ l'ensemble des $z \in \mathbb{C}$ tels que G est définie en z et $G(z) = t$. Montrer que pour tout $t \in \mathbb{C}$, l'ensemble $G^{-1}(t)$ est fini, et qu'il existe un entier $\nu > 0$ tel que pour tout $t \in \mathbb{C}$, $\text{card}\left(G^{-1}(t)\right) \leqslant \nu$, l'ensemble $\mathcal{S}_G = \left\{t \in \mathbb{C} \,|\, \text{card}\left(G^{-1}(t)\right) < \nu\right\}$ étant fini. L'entier ν sera appelé *indice* de G.

b) Montrer que $G \in \mathbb{C}(X)$, non constante, est d'indice 1 si, et seulement si, elle est *homographique*.

c) Soit $G \in \mathbb{C}(X)$ non constante, montrer que l'isomorphisme $F \mapsto F(G)$ de $\mathbb{C}(X)$ dans $\mathbb{C}(X)$ est un automorphisme si, et seulement si, G est homographique.

d) Montrer que les automorphismes de la $\mathbb{C}$-algèbre $\mathbb{C}(X)$ sont exclusivement ceux trouvés en *c*). ■

a) Soit $G = P/Q$, où P et Q sont des éléments de $\mathbb{C}[X]$, une forme irréductible de la fraction rationnelle G. Pour tout $t \in \mathbb{C}$, l'ensemble $G^{-1}(t)$ est exactement l'ensemble des zéros du polynôme $P - tQ$; en effet si G est définie en z et $G(z) = t$, alors $P(z) = tQ(z)$, et si $P(z) - tQ(z) = 0$, alors $Q(z) \neq 0$, sinon on aurait $P(z) = Q(z) = 0$ (ce qui est exclu puisque P et Q sont premiers entre eux), donc G est définie en z et $G(z) = t$. Pour tout $t \in \mathbb{C}$, le polynôme $P - tQ$ est non nul (sinon G serait constante), de degré majoré par $\nu = \sup(\deg(P), \deg(Q))$, donc $G^{-1}(t)$ est fini de cardinal majoré par ν ($\nu > 0$).

Le polynôme $P'Q - PQ'$ est non nul, sinon, comme Q est premier avec P, le polynôme Q diviserait Q', ce qui est impossible ($Q \neq 0$). L'ensemble M des zéros de ce polynôme est donc fini. Notons $G(M)$ l'ensemble des images par G des éléments de M en lesquels G est définie. Si pour $t \in \mathbb{C}$, le polynôme $P - tQ$ a un zéro multiple z, alors $P(z) - tQ(z) = 0$ et $P'(z) - tQ'(z) = 0$, d'où $P'(z)Q(z) - P(z)Q'(z) = 0$, soit $z \in M$ et $t \in G(M)$. Nous voyons donc que pour tout t, si $t \notin G(M)$ le polynôme $P - tQ$ n'a que des zéros simples, et a donc un nombre de zéros égal à son degré.

Supposons $\deg(P) > \deg(Q)$. Le polynôme $P - tQ$ est pour tout $t \in \mathbb{C}$ de degré $\nu = \deg(P)$, et pour tout t n'appartenant pas à l'ensemble fini $G(M)$, le nombre de ses zéros est égal à son degré, soit ν. L'ensemble $G^{-1}(t)$ est donc toujours fini de cardinal majoré par ν, ce cardinal étant exactement ν sauf si t est dans un ensemble fini inclus dans $G(M)$.
Supposons $\deg(P) < \deg(Q)$. Le polynôme $P - tQ$ est pour tout $t \in \mathbb{C}\backslash\{0\}$ de degré $\nu = \deg(Q)$, et pour $t = 0$ de degré $< \nu$. Si $t \neq 0$ et $t \notin G(M)$, ce polynôme n'a que des zéros simples, et en a exactement ν

$G^{-1}(t)$ est donc toujours fini de cardinal majoré par ν, ce cardinal étant exactement ν sauf si t est dans un ensemble fini inclus dans $\{0\} \cup G(M)$. Supposons $\deg(P) = \deg(Q)$. Le polynôme $P - tQ$ est de degré $\nu = \deg(P) = \deg(Q)$, sauf pour la valeur t_0 égale au rapport des coefficients dominants de P et de Q, valeur pour laquelle son degré est $< \nu$. On voit que l'ensemble $G^{-1}(t)$ est toujours fini de cardinal $\leqslant \nu$, et que ce cardinal est exactement ν, sauf si t est dans un ensemble fini inclus dans l'ensemble fini $\{t_0\} \cup G(M)$.

Nous déduisons de ce qui précède que l'indice de la fraction non constante $G = P/Q$ (forme irréductible) est l'entier $\sup(\deg(P), \deg(Q))$.

b) Une fraction rationnelle G non constante est donc d'indice 1 si, et seulement si, elle peut s'exprimer comme quotient de deux polynômes de degrés $\leqslant 1$, non tous les deux constants, c'est-à-dire si, et seulement si, c'est une fraction rationnelle homographique.

c) Montrons que si F et G sont des fractions rationnelles non constantes, $F \circ G$ est une fraction rationnelle non constante dont l'indice est le produit de l'indice de F par l'indice de G.

Soit μ l'indice de F et ν l'indice de G. Soit E l'ensemble fini $S_F \cup F(S_G)$, si $t \notin E$, il y a exactement μ complexes $y_1, y_2, \ldots, y_\mu$ distincts tels que F est défini en y et $F(y) = t$, et, comme aucun de ces nombres n'est dans S_G, pour tout $i \in [\![1, \mu]\!]$, il y a exactement ν complexes z tels que G est défini en z et $G(z) = y_i$; il y a donc, pour tout $t \notin E$, $\mu\nu$ complexes z tels que $F \circ G$ est défini en z et $F(G(z)) = t$. La fraction rationnelle $F \circ G$ n'est donc pas constante, et son indice est $\mu\nu$.

Si G est une homographie, on voit facilement qu'elle a une réciproque, H telle que $G \circ H = X$ et $H \circ G = X$ (voir exercice 5). Les isomorphismes $F \mapsto F(G)$ et $F \mapsto F(H)$ sont alors réciproques l'un de l'autre, puisque pour toute fraction rationnelle F, $F \circ G \circ H = F \circ X = F$, et $F \circ H \circ G = F \circ X = F$. Ces isomorphismes sont donc des automorphismes de l'algèbre $\mathbb{C}(X)$.
Si $F \mapsto F(G)$ est un automorphisme de l'algèbre $\mathbb{C}(X)$, G n'est pas constante et il existe une fraction rationnelle F, nécessairement non constante, telle que $F \circ G = X$. Si ν est l'indice de G et μ est l'indice de F, alors, d'après ce qui précède, $\mu\nu = 1$. Nous en déduisons que nécessairement $\nu = 1$ et donc que la fraction rationnelle G est une homographie.
L'isomorphisme d'algèbres $F \mapsto F(G)$ est donc un automorphisme si, et seulement si, G est une fraction rationnelle homographique.

d) Soit Φ un automorphisme de la $\mathbb{C}$-algèbre $\mathbb{C}(X)$, posons $\Phi(X) = G$. Pour tout polynôme $P \in \mathbb{C}[X]$, $P = \sum_{n\in\mathbb{N}} a_n X^n$, comme Φ est un homomorphisme d'algèbres :

$$\Phi(P) = \Phi\left(\sum_{n\in\mathbb{N}} a_n X^n\right) = \sum_{n\in\mathbb{N}} a_n \left(\Phi(X)\right)^n = P(G) .$$

Pour toute fraction rationnelle F de représentant irréductible $F = P/Q$, où P et Q sont des polynômes :

$$\Phi(F) = \Phi(P)/\Phi(Q) = P(G)/Q(G) = F(G) .$$

Les automorphismes de l'algèbre $\mathbb{C}(X)$ sont donc tous de la forme $F \mapsto F(G)$, où G est une fraction rationnelle, homographique d'après *c*).

Exercice 7 :

Soit A, B, $y_1, y_2, \ldots, y_N$, $c_1, c_2, \ldots, c_N$ des réels, les c_k non nuls, $y_1 < y_2 < \ldots < y_N$ ($N \in \mathbb{N}^*$). On considère la fraction $F \in \mathbb{R}(X)$ donnée par :

$$F = AX + B - \sum_{k=1}^{N} \frac{c_k}{X - y_k} .$$

Montrer que, pour que F possède $N+1$ zéros réels simples et *entrelacés* avec les pôles y_k, il faut et il suffit que A et les c_k soient tous de même signe. ■

Supposons que A et les réels c_k, où $k \in [\![1, N]\!]$ soient tous de même signe, par exemple tous > 0. Il est clair que la fonction rationnelle $x \mapsto F(x)$ est strictement croissante sur chacun des intervalles inclus dans son domaine de définition, c'est-à-dire sur les intervalles $]-\infty, y_1[$, $]y_1, y_2[, \ldots,]y_{N-1}, y_N[$, et $]y_N, +\infty[$.
Comme $F(x) \underset{x\to-\infty}{\longrightarrow} -\infty$ et $F(x) \underset{x\to y_1^-}{\longrightarrow} +\infty$, F a exactement 1 zéro réel sur l'intervalle $]-\infty, y_1[$.
Pour tout $k \in [\![1, N-1]\!]$, $F(x) \underset{x\to y_k^+}{\longrightarrow} -\infty$ et $F(x) \underset{x\to y_{k+1}^-}{\longrightarrow} +\infty$; la fraction rationnelle F a donc exactement 1 zéro réel sur chacun de ces $N-1$ intervalles.
Comme $F(x) \underset{x\to+\infty}{\longrightarrow} +\infty$ et $F(x) \underset{x\to y_N^+}{\longrightarrow} -\infty$, F a exactement 1 zéro réel sur l'intervalle $]y_N, +\infty[$.
Le nombre de zéros réels de la fraction rationnelle F est donc

$N+1$, et ces zéros sont entrelacés avec les y_k. Ces zéros sont tous simples car le numérateur d'un représentant irréductible de la fraction F est un polynôme de degré $\leqslant N+1$; s'il a $N+1$ zéros, c'est qu'il est de degré $N+1$ et que tous ses zéros sont réels et simples.

Supposons que la fraction rationnelle F ait $N+1$ zéros réels tous simples entrelacés avec les y_k. Elle a donc un zéro x_0 dans l'intervalle $]-\infty, y_1[$, un zéro x_k dans chaque intervalle $]y_k, y_{k+1}[$, où $k \in [\![1, N-1]\!]$, et un zéro x_N dans l'intervalle $]y_N, +\infty[$. Supposons que pour un entier $k \in [\![1, N-1]\!]$, les signes de c_k et c_{k+1} soient opposés, c_{k+1} de signe ε $(\in \{-1, +1\})$ et c_k de signe $-\varepsilon$. On voit que $F(x) \underset{x \to y_k^+}{\longrightarrow} \varepsilon\infty$, et que $F(x) \underset{x \to y_{k+1}^-}{\longrightarrow} \varepsilon\infty$. Mais F prend en $x_k \in]y_k, y_{k+1}[$ la valeur 0, et $F'(x_k) \neq 0$, puisque x_k est un zéro simple de F. Il y a donc à droite ou à gauche de x_k dans l'intervalle $]y_k, y_{k+1}[$, des réels x en lesquels $F(x)$ est du signe opposé à ε ; il existe donc dans cet intervalle au moins un autre zéro de F, ce qui est contradictoire. Les réels c_k sont donc tous de même signe ε. Supposons que A soit du signe opposé à ε ; on voit qu'alors $F(x) \underset{x \to -\infty}{\longrightarrow} \varepsilon\infty$, et que $F(x) \underset{x \to y_1^-}{\longrightarrow} \varepsilon\infty$; or F prend la valeur 0 sur l'intervalle $]-\infty, y_1[$ en x_0 et $F'(x_0) \neq 0$; on en déduit comme ci-dessus que F prend au moins une autre fois la valeur 0 dans cet intervalle, ce qui est contraire aux hypothèses. Le nombre A est donc nécessairement du même signe que les réels c_k.

L'équivalence des deux propositions est donc démontrée.

Exercice 9 :

> Le corps de base est $\mathbb{C}$. On donne $F \in \mathbb{C}(X)$ non constante. On suppose trouvé $k \in \mathbb{N}^*$ tel que $F(\zeta X) = F(X)$ pour tout $\zeta \in \mu_k$. Prouver qu'il existe $G \in \mathbb{C}(X)$ telle que $F(X) = G(X^k)$. ■

Soit $P \in \mathbb{C}[X]$, montrons qu'il existe un polynôme P_1 tel que :

$$\sum_{\zeta \in \mu_k} P(\zeta X) = P_1(X^k) .$$

Pour tout entier n, posons :

$$s_n = \sum_{\zeta \in \mu_k} \zeta^n .$$

Soit α est un générateur du groupe μ_k, on peut aussi écrire :

$$s_n = \sum_{i=0}^{k-1} \alpha^{in} = \begin{cases} \frac{\alpha^{kn}-1}{\alpha^n-1} = 0 \text{ si } n \not\equiv 0 \bmod (k) \\ k \qquad \text{si } n \equiv 0 \bmod (k) \end{cases}$$

Nous en déduisons, en posant $P = \sum_{n\in\mathbb{N}} a_n X^n$:

$$\sum_{\zeta\in\mu_k} P(\zeta X) = \sum_{n\in\mathbb{N}} a_n s_n X^n = \sum_{i\in\mathbb{N}} k\, a_{ik} X^{ik} .$$

On obtient donc le résultat annoncé en posant :

$$P_1 = \sum_{i\in\mathbb{N}} a_{ik} X^i .$$

Supposons maintenant que $F \in \mathbb{C}(X)$ soit telle que $F(\zeta X) = F(X)$ pour tout $\zeta \in \mu_k$ ($k \in \mathbb{N}^*$). Posons $F = P/Q$, où P et Q sont dans $\mathbb{C}[X]$, $Q \neq 0$ et P et Q premiers entre eux. Pour tout $\zeta \in \mu_k$:

$$F(X)Q(\zeta X) = F(\zeta X)Q(\zeta X) = P(\zeta X) ,$$

d'où :

$$F(X) \sum_{\zeta\in\mu_k} Q(\zeta X) = \sum_{\zeta\in\mu_k} P(\zeta X) ,$$

soit encore, en introduisant les polynômes P_1 et Q_1 tels que :

$$\sum_{\zeta\in\mu_k} P(\zeta X) = P_1(X^k) \quad \text{et} \quad \sum_{\zeta\in\mu_k} Q(\zeta X) = Q_1(X^k) ,$$

$$F(X)\, Q_1(X^k) = P_1(X^k) .$$

Les polynômes Q_1 et P_1 ne sont pas tous les deux nuls, sinon, comme $P_1(0) = k\,P(0)$ et que de même $Q_1(0) = k\,Q(0)$, les polynômes P et Q seraient tous les deux divisibles par X donc non premiers entre eux. Le polynôme Q_1 n'est donc pas nul, et on obtient finalement :

$$F(X) = \frac{P_1(X^k)}{Q_1(X^k)} .$$

Il existe donc bien une fraction rationnelle G telle que $F = G(X^k)$.

Exercice 12 :

Le corps de base est $\mathbb{C}$. Soit Γ l'ensemble des six homographies suivantes :

$$e = X, \quad f_1 = \frac{1}{X}, \quad f_2 = 1 - X,$$

$$f_3 = \frac{1}{1-X}, \quad f_4 = 1 - \frac{1}{X}, \quad f_5 = \frac{X}{X-1}$$

a) Montrer que Γ est un sous-groupe du groupe $\mathrm{PGL}(\mathbb{C})$ défini dans l'exercice 5, et que ce groupe est isomorphe à $\mathfrak{S}_3$.
b) On identifie Γ à un groupe de bijections de $\widetilde{\mathbb{C}}$ dans $\widetilde{\mathbb{C}}$ (cf. exercice 5). Trouver les groupes d'isotropie des divers $z \in \widetilde{\mathbb{C}}$. Etudier la figure formée par les points fixes des f_k $(1 \leqslant k \leqslant 5)$.
c) Montrer que toutes les Γ-orbites de $\widetilde{\mathbb{C}}$ ont 6 éléments, sauf un nombre fini d'entre elles que l'on précisera.
d) Soit $\Phi = X^2 - X + 1$, $\Psi = (X+1)(2X-1)(X-2)$ et $\Lambda = \dfrac{\Phi^3}{\Psi^2}$. Démontrer que $\Lambda \circ F = \Lambda$ pour toute $F \in \Gamma$.
e) Soit $\Theta \in \mathbb{C}(X)$ telle que $\Theta \circ F = \Theta$ pour toute $F \in \Gamma$. Montrer qu'il existe $G \in \mathbb{C}(X)$ telle que $\Theta = G \circ \Lambda$. ■

a) On remarque que $f_4 = f_2 \circ f_1$ et que $f_3 = f_1 \circ f_2$. On voit aussi que f_5 peut s'écrire :

$$f_5 = \frac{1}{1 - \dfrac{1}{X}},$$

et donc que $f_5 = f_1 \circ f_2 \circ f_1$ ou encore $f_5 = f_1 \circ f_2 \circ f_1^{-1}$, puisque f_1 est d'ordre 2. Les éléments f_1, f_2 et f_5 sont donc d'ordre 2. Les éléments f_3 et f_4 sont par conséquent inverses l'un de l'autre. Ce sont des éléments d'ordre 3 puisque :

$$f_3 \circ f_3 = \frac{1}{1 - \dfrac{1}{1-X}} = \frac{X}{X-1} = f_4 .$$

Les éléments de l'ensemble Γ peuvent s'écrire sous la forme : e, f_1, $f_2 = f_4 \circ f_1 = f_3^{-1} \circ f_1$, f_3, $f_4 = f_3^{-1}$, $f_5 = f_1 \circ f_2 \circ f_1 = f_3 \circ f_1$; comme f_1 est d'ordre 2 et que f_3 est d'ordre 3, on voit que $\Gamma = \left\{ f_3^i \circ f_1^j,\ (i,j) \in \mathbb{Z}^2 \right\}$.
On peut remarquer la relation de conjugaison :

$$f_1 \circ f_3 \circ f_1^{-1} = f_1 \circ f_1 \circ f_2 \circ f_1 = f_2 \circ f_1 = f_3^{-1} .$$

Nous en déduisons que pour tout entier p :

$$f_1 \circ f_3^p \circ f_1^{-1} = f_3^{-p} ,$$

et, puisque f_1 est involutive, que pour tous entiers p et q :

$$f_1^q \circ f_3^p \circ f_1^{-q} = f_3^{(-1)^q p} \quad \text{soit} \quad f_1^q \circ f_3^p = f_3^{(-1)^q p} \circ f_1^q$$

L'ensemble Γ, non vide, est bien un sous-groupe, puisque pour tous entiers p, q, r, s, on a :

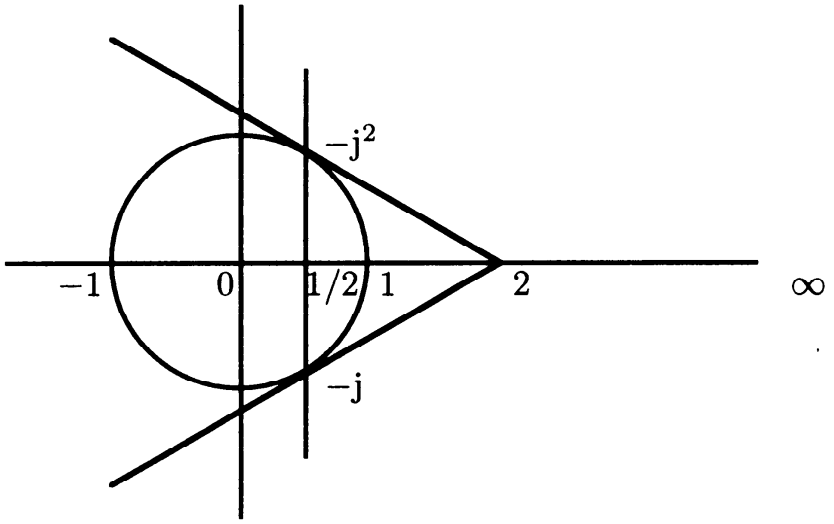
$$(f_3^p \circ f_1^q) \circ (f_3^r \circ f_1^s)^{-1} = f_3^p \circ f_1^{q-s} \circ f_3^{-r} = f_3^{p-(-1)^{q-s}r} \circ f_1^{q-s} .$$

Ce groupe a 6 éléments, 3 éléments d'ordre 2, 2 éléments d'ordre 3, et n'est pas abélien ; il est donc isomorphe au groupe $\mathfrak{S}_3$ (cf. §V.4 exercice 6).

b) c) Notons E_k l'ensemble des points fixes de f_k, où $1 \leqslant k \leqslant 5$, on trouve facilement que :

$$E_1 = \{-1, 1\}, \quad E_2 = \{1/2, \infty\}, \quad E_3 = E_4 = \{-\mathrm{j}, -\mathrm{j}^2\}, \quad E_5 = \{2, 0\} .$$

Si $z \in \widetilde{\mathbb{C}}$ n'est dans aucun de ces ensembles, son groupe d'isotropie est réduit à $\{e\}$ et son orbite a 6 éléments. Le groupe d'isotropie des éléments de E_k, où $k \in \{1, 2, 5\}$, est $\{e, f_k\}$; on constate que ces éléments sont dans deux orbites de cardinal 3 : $\{1, 0, \infty\}$ et $\{-1, 1/2, 2\}$. Le groupe d'isotropie des éléments de $E_3 = E_4$ est le sous-groupe $\{e, f_3, f_4\}$; ces éléments forment une seule orbite de cardinal 2.



d) Comme f_1 et f_2 engendrent le groupe Γ, une fraction rationnelle Θ est telle que $\Theta \circ F = \Theta$ pour tout élément F de Γ si, et seulement si, $\Theta \circ f_1 = \Theta$ et $\Theta \circ f_2 = \Theta$. Vérifions que c'est le cas pour la fraction rationnelle Λ. On constate que :

$$\Phi(1/X) = \frac{1}{X^2} - \frac{1}{X} + 1 = \frac{\Phi(X)}{X^2} ,$$

et que :

$$\Psi(1/X) = \frac{(1+X)(2-X)(1-2X)}{X^3} = \frac{\Psi(X)}{X^3} .$$

Par conséquent :

$$\Lambda(1/X) = \frac{\Phi^3(X)}{X^6}\frac{X^6}{\Psi^2(X)} = \Lambda(X) \ .$$

D'autre part, en remarquant que $\Phi = 1 - X(1-X)$:

$$\Phi(1-X) = 1 - (1-X)X = \Phi(X) \ ,$$

et :

$$\Psi(1-X) = (2-X)(1-2X)(-1-X) = -\Psi(X) \ .$$

Par conséquent :

$$\Lambda(1-X) = \frac{\Phi^3(1-X)}{\Psi^2(1-X)} = \frac{\Phi^3(X)}{\Psi^2(X)} = \Lambda(X) \ .$$

On a donc bien $\Lambda \circ F = \Lambda$ pour tout élément F de Γ.

e) Notons I_Γ l'ensemble des fractions rationnelles invariantes sous l'action du groupe Γ. Il est clair que toute fraction rationnelle qui peut s'écrire sous la forme $G \circ \Lambda$ est dans I_Γ. Montrons l'inclusion opposée.

Soit $\Theta \in I_\Gamma$, on a :

$$\Theta(X) = \frac{1}{6}\left(\Theta(f_0(X)) + \ldots + \Theta(f_5(X))\right) \ .$$

On voit que si $X_1, \ldots, X_6$ sont 6 indéterminées sur le corps $\mathbb{C}$, la fraction rationnelle $\Theta(X_1) + \ldots + \Theta(X_6)$ est symétrique et s'exprime par conséquent comme une fraction rationnelle à coefficients dans $\mathbb{C}$ en les polynômes symétriques élémentaires en $(X_1, \ldots, X_6)$. On voit donc que Θ est une fraction rationnelle à coefficients dans $\mathbb{C}$ en les polynômes symétriques élémentaires en $f_0(X)$, $f_1(X)$, $\ldots$, $f_5(X)$.

Ces polynômes symétriques élémentaires sont les éléments du corps $\mathbb{C}(X)$ qui sont les coefficients du polynôme $P(Z)$ (à coefficients dans le corps $K(X)$) :

$$P = (Z-X)\left(Z-\frac{1}{X}\right)(Z-(1-X))\times \left(Z-1+\frac{1}{X}\right)\left(Z-\frac{1}{1-X}\right)\left(Z-\frac{X}{X-1}\right) \ .$$

On voit facilement que la somme des zéros est 3, et comme le polynôme P est réciproque (et que $P(1) \neq 0$ et $P(-1) \neq 0$), il est de la forme :

$$P = Z^6 - 3Z^5 + \alpha Z^4 + \beta Z^3 + \alpha Z^2 - 3Z + 1 \ .$$

On voit aussi que $P(Z) = P(1-Z)$, donc $P(0) = P(1)$. Cela nous donne la relation :

$$1 - 3 + \alpha + \beta + \alpha - 3 + 1 = 1 \quad \text{soit} \quad 2\alpha + \beta = 5 \ .$$

Le polynôme P est donc de la forme :

$$P = Z^6 - 3\,Z^5 + \alpha\,Z^4 + (5 - 2\alpha)\,Z^3 + \alpha\,Z^2 - 3\,Z + 1 \ .$$

Comme X est un zéro de P, nous en déduisons :

$$0 = X^6 - 3\,X^5 + \alpha\,X^4 + (5 - 2\alpha)\,X^3 + \alpha\,X^2 - 3\,X + 1 \ ,$$

d'où la valeur de α :

$$\alpha = -\frac{X^6 - 3\,X^5 + 5\,X^3 - 3\,X + 1}{X^4 - 2\,X^3 + X^2} \ .$$

Ce qui précède prouve que les fractions rationnelles éléments de I_Γ sont des fractions rationnelles en $\alpha \in \mathbb{C}(X)$. La fraction rationnelle Λ est élément de I_Γ et est par conséquent une fraction rationnelle en α, mais comme son indice est aussi 6, elle s'exprime sous la forme $H(\alpha)$ où H est une homographie (voir exercice 6). Les éléments de I_Γ sont donc aussi des fractions rationnelles en Λ, ce qu'il fallait démontrer.

Le calcul montre que :

$$s_2 = 2\,\frac{(X^2 - X + 1)^3}{X^2(1 - X)^2} - 3 \quad \text{et} \quad \alpha = 6 - \frac{(X^2 - X + 1)^3}{X^2(1 - X)^2} \ ,$$

et que :

$$\Psi^2 = 4\,(X^2 - X + 1)^3 - 27\,X^2(1 - X)^2 \ ,$$

d'où :

$$\frac{1}{\Lambda} = \frac{\Psi^2}{\Phi^3} = 4 - 27\,\frac{X^2(1 - X)^2}{(X^2 - X + 1)^3} = 4 - \frac{27}{6 - \alpha} \ .$$

§ VIII.5 *APPLICATIONS DES SÉRIES FORMELLES*

Exercice 3 :

Développer en série formelle les fonctions rationnelles suivantes, le corps de base étant $\mathbb{C}$:

a) $F = \dfrac{1}{1 + X + X^2 + \ldots + X^{n-1}}$ $(n \in \mathbb{N},\ n \geqslant 2$

b) $F = \dfrac{1}{(1-aX)^p(1-bX)^q}$, $a \neq b$, $(p,q) \in \mathbb{N}^{*2}$.

c) $F = \dfrac{1}{(1-X^p)(1-X^q)}$ avec p et q premiers entre eux (cf. §VIII.5 exemple 2). ■

a) On peut écrire :

$$F = \frac{1-X}{1-X^n} = (1-X)\left(\sum_{k\in\mathbb{N}} X^{kn}\right) = \sum_{k\in\mathbb{N}} (X^{kn} - X^{kn+1}) ,$$

Posons :

$$F = \sum_{m\in\mathbb{N}} a_m X^m ,$$

on voit que si $m \equiv 0 \bmod(n)$, alors $a_m = 1$, si $m \equiv 1 \bmod(n)$, alors $a_m = -1$, et sinon $a_m = 0$.

b) Nous pouvons utiliser le théorème VIII.5.3 pour obtenir :

$$\frac{1}{(1-aX)^p} = \sum_{i\in\mathbb{N}} \binom{i+p-1}{i} a^i X^i ,$$

et :

$$\frac{1}{(1-bX)^q} = \sum_{j\in\mathbb{N}} \binom{j+q-1}{j} b^j X^j .$$

Nous obtenons donc :

$$F = \left(\sum_{i\in\mathbb{N}} \binom{i+p-1}{i} a^i X^i\right)\left(\sum_{j\in\mathbb{N}} \binom{j+q-1}{j} b^j X^j\right) =$$

$$= \sum_{k\in\mathbb{N}} \left(\sum_{i+j=k} \binom{i+p-1}{i}\binom{j+q-1}{j} a^i b^j\right) X^k .$$

c) En utilisant les égalités :

$$\frac{1}{1-X^p} = \sum_{h\in\mathbb{N}} X^{hp} ,$$

et :

$$\frac{1}{1-X^q} = \sum_{k\in\mathbb{N}} X^{kq} ,$$

on trouve l'expression :

$$F = \left(\sum_{h\in\mathbb{N}} X^{hp}\right)\left(\sum_{k\in\mathbb{N}} X^{kq}\right) = \sum_{n\in\mathbb{N}} c_n X^n ,$$

où pour tout $n \in \mathbb{N}$,

$$c_n = \sum_{hp+kq=n} 1 = \operatorname{card}\left(\{(h,k) \in \mathbb{N}^2 \mid hp+kq=n\}\right) .$$

On pourrait décomposer la fraction rationnelle F en éléments simples pour trouver une autre expression de ces coefficients, comme cela a été fait dans l'exemple 2 (§VIII.5). Nous pouvons aussi déterminer ces nombres en poursuivant la méthode utilisée dans l'exercice 18 du §IV.2. Soient deux entiers naturels u et v tels que :

$$up - vq = 1 .$$

Nous avions établi que c_n est le nombre d'entiers λ dans l'intervalle :

$$I_n = \left[\frac{vn}{p} , \frac{un}{q}\right] .$$

Le nombre d'entiers λ tels que $0 \leqslant \lambda \leqslant un/q$ est évidemment $\lfloor un/q \rfloor + 1$ (partie entière). Un entier λ vérifie $0 \leqslant \lambda < vn/p$ si, et seulement si, $-vn/p < -\lambda \leqslant 0$, soit si, et seulement si, $\lfloor -vn/p \rfloor < -\lambda \leqslant 0$; le nombre de ces entiers est donc $-\lfloor -vn/p \rfloor$. Le nombre d'entiers dans l'intervalle I_n est donc :

$$c_n = \lfloor un/q \rfloor + 1 + \lfloor -vn/p \rfloor .$$

On vérifie à l'aide de cette formule que pour tout $k \in \mathbb{N}$:

$$c_{n+kpq} = c_n + ukp - vkq = c_n + k .$$

Il suffit donc de déterminer les coefficients c_n pour $n \in [\![0, pq-1]\!]$.
Pour $p = 3, q = 2$, on trouve $3 - 2 = 1$, on peut donc choisir $u = v = 1$, et

$$c_n = \lfloor n/2 \rfloor + 1 + \lfloor -n/3 \rfloor .$$

On établit facilement :

$$c_0 = 1,\ c_1 = 0,\ c_2 = 1,\ c_3 = 1,\ c_4 = 1,\ c_5 = 1 .$$

Il semble dans cet exemple que c_n et c_{n+1} ne peuvent différer que d'au plus 1. Démontrons que cette propriété est vraie quels que soient p

> 0 premiers entre eux (y compris si $p = q = 1$), et pour tout $n \in \mathbb{N}$.
Remarquons d'abord qu'on peut trouver v tel que $0 \leqslant v < p$, et qu'alors $1 \leqslant up = 1 + vq \leqslant (p-1)q + 1 \leqslant pq$, donc $0 < u \leqslant q$. On a :

$$I_{n+1} = \left(I_n \cup \left]\frac{un}{q}, \frac{un}{q} + \frac{u}{q}\right]\right) \setminus \left[\frac{vn}{p}, \frac{vn}{p} + \frac{v}{p}\right[.$$

Les intervalles :

$$\left]\frac{un}{q}, \frac{un}{q} + \frac{u}{q}\right] \quad \text{et} \quad \left[\frac{vn}{p}, \frac{vn}{p} + \frac{v}{p}\right[,$$

sont de longueurs $\leqslant 1$, et ne contiennent chacun qu'au plus un entier. On voit donc que c_n et c_{n+1} ne peuvent différer que d'au plus 1.

Exercice 4 :

> *a*) Soit $k \in \mathbb{N}^*$. Montrer que si $S \in \mathbb{C}[[X]]$ est une série donnée *de valuation nulle*, il existe exactement k éléments $T \in \mathbb{C}[[X]]$ tels que $T^k = S$. On commencera par traiter le cas où $S = 1 + X$.
> *b*) Soit $A \in \mathbb{C}[[X]]$, $B \in \mathbb{C}[[X]]$, a et b les termes constants de A et B. Montrer que si $a^2 - 4b \neq 0$, alors l'équation $T^2 + AT + B = 0$ où la série inconnue $T \in \mathbb{C}[[X]]$ possède exactement deux solutions. ■

a) Soit $\mathcal{T}$ l'ensemble des solutions. Considérons l'application $\varphi : \mathcal{T} \to \mathbb{C}$, $T \mapsto T(0)$. Notons $s = S(0)$; on voit que l'application φ est à valeurs dans l'ensemble des solutions complexes de l'équation $t^k = s$, équation qui a k solutions, toutes non nulles puisque $s \neq 0$.
Montrons que φ est injective. Des moyens assez élémentaires suffisent. Si T_1 et T_2 sont telles que $T_1^k = T_2^k = S$ et $T_1(0) = T_2(0) = t$, alors :

$$T_1^k - T_2^k = (T_1 - T_2)(T_1^{k-1} + T_1^{k-2}T_2 + \ldots + T_1 T_2^{k-2} + T_2^{k-1}) = 0 .$$

Le deuxième facteur n'est pas nul puisque son terme constant est $k\,t^{k-1}$, nous pouvons en déduire, puisque $\mathbb{C}[[X]]$ est un anneau intègre, que $T_1 = T_2$.
Montrons que l'application φ est surjective. Soit $t \in \mathbb{C}$ tel que $t^k = s$. Notons :

$$R_k = \sum_{n \geqslant 0} \binom{1/k}{n} X^n = (1 + X)^{1/k} .$$

Le point (II) du théorème VIII.5.4 permet d'affirmer que :

$$(R_k(X))^k = (1 + X)^{k \times 1/k} = (1 + X) .$$

Nous pouvons dans cette identité substituer $s^{-1}S - 1$, qui est de valuation $\geqslant 1$, à X (voir définition VIII.4.4). Nous obtenons l'égalité :

$$\big(R_k(s^{-1}S - 1)\big)^k = 1 + (s^{-1}S - 1) = s^{-1}S \ ,$$

d'où :

$$\big(t\, R_k(s^{-1}S - 1)\big)^k = t^k\, s^{-1}S = S \ .$$

On vérifie facilement que le terme constant de la solution trouvée est bien t.

Le nombre de solutions de l'équation de l'énoncé est donc exactement k.

b) L'équation s'écrit :

$$(2T + A)^2 = A^2 - 4B \ .$$

Le terme constant de la série formelle $A^2 - 4B$ est $a^2 - 4b \neq 0$; cette série formelle est donc de valuation nulle. D'après *a*), il existe exactement deux séries formelles solutions de l'équation.

Exercice 7 (nombre d'*involutions* dans $\mathfrak{S}_n$). **:**

> Pour $n \in \mathbb{N}$, soit u_n le nombre de permutations σ dans $\mathfrak{S}_n$ telles que $\sigma^2 = \mathrm{Id}$. On pose $u_0 = u_1 = 1$.
>
> *a*) Montrer : $(\forall n \geqslant 2)\ u_n = u_{n-1} + (n-1)u_{n-2}$.
>
> *b*) On considère la série formelle $S = \sum_{n \geqslant 0} \dfrac{u_n}{n!} X^n \in \mathbb{C}[[X]]$.
>
> Montrer que $S' - (1 + X)S = 0$ et en déduire que $S = \exp\left(X + \dfrac{X^2}{2}\right)$. En déduire l'expression de u_n. ■

a) L'ensemble I des involutions dans $\mathfrak{S}_n$ est partagé en I_1, ensemble des involutions $\sigma \in \mathfrak{S}_n$ telles que $\sigma(n) = n$ et I_2, ensemble des involutions $\sigma \in \mathfrak{S}_n$ telles que $\sigma(n) \neq n$. Il est clair que I_1 est en bijection avec l'ensemble des involutions dans $\mathfrak{S}_{n-1}$, et est par conséquent de cardinal u_{n-1}. Pour tout $k \in [\![1, n-1]\!]$ notons $I_{2,k}$ l'ensemble des involutions $\sigma \in I_2$ telles que $\sigma(n) = k$. On voit que $(I_{2,k})_{k \in [\![1,n-1]\!]}$ est un partage de I_2. Soit $k \in [\![1, n-1]\!]$, une permutation $\sigma \in \mathfrak{S}_n$ est dans $I_{2,k}$ si, et seulement si, elle est involutive et $\sigma(n) = k$; nous en déduisons que σ est involutive, que $\sigma(n) = k$ et que $\sigma(k) = n$. On voit donc que $I_{2,k}$ est en bijection avec l'ensemble des involutions de l'ensemble $[\![1, n-1]\!] \setminus \{k\}$, qui est de cardinal u_{n-2}. Le cardinal de I_2 est donc $(n-1)u_{n-2}$. Nous en déduisons finalement :

$$(\forall n \geqslant 2) \quad u_n = u_{n-1} + (n-1)u_{n-2} \ .$$

b) Posons pour tout $n \in \mathbb{N}$, $v_n = \dfrac{u_n}{n!}$. On voit que $v_0 = v_1 = 1$, et que pour tout $n \geqslant 1$:

$$(n+1)v_{n+1} = \frac{u_{n+1}}{n!} = \frac{u_n}{n!} + \frac{n\,u_{n-1}}{n!} = v_n + v_{n-1} .$$

Nous en déduisons :

$$(1+X)S = (1+X)\sum_{n\geqslant 0} v_n X^n = \sum_{n\geqslant 0} v_n X^n + \sum_{n\geqslant 1} v_{n-1} X^n =$$
$$= v_0 + \sum_{n\geqslant 1}(v_n + v_{n-1})X^n = v_0 + \sum_{n\geqslant 1}(n+1)v_{n+1}X^n .$$

Comme $v_0 = v_1 = 1$, on trouve finalement :

$$(1+X)S = \sum_{n\geqslant 0}(n+1)v_{n+1}X^n = S' .$$

Considérons la série formelle :

$$F = \exp\left(-X - \frac{X^2}{2}\right) S ;$$

En dérivant on trouve :

$$F' = \left(S' - (1+X)S\right) \exp\left(-X - \frac{X^2}{2}\right) = 0 .$$

La série formelle F est donc réduite à son terme constant qui est 1. Nous en déduisons que :

$$S = \exp\left(X + \frac{X^2}{2}\right) = \exp(X) \exp\left(\frac{X^2}{2}\right) .$$

Cela nous permet de trouver une autre expression des nombres u_n. En effet :

$$S = \left(\sum_{p\geqslant 0} \frac{X^p}{p!}\right)\left(\sum_{q\geqslant 0} \frac{X^{2q}}{2^q\, q!}\right) = \sum_{n\geqslant 0}\left(\sum_{p+2q=n} \frac{1}{p!\, q!\, 2^q}\right) X^n .$$

Nous en déduisons que pour tout entier n :

$$u_n = \sum_{p+2q=n} \frac{n!}{p!\, q!\, 2^q} .$$

Exercice 10 :

Pour $n \geqslant 1$, soit S_n le nombre des permutations du groupe alterné $\mathfrak{A}_n$ dont le nombre de points fixes est *pair*, et U_n le nombre de dérangements dans $\mathfrak{A}_n$. On convient que $U_0 = 1$, $S_0 = 1$. Soit $\Phi_1 = \sum_{p\geqslant 0} \frac{U_p}{p!} X^p \in \mathbb{C}[[X]]$ et $\Psi_1 = \sum_{p\geqslant 0} \frac{S_p}{p!} X^p \in \mathbb{C}[[X]]$.

On note aussi T_n le nombre des $\sigma \in \mathfrak{S}_n \setminus \mathfrak{A}_n$ dont le nombre de points fixes est impair, et A_p le nombre de dérangements dans $\mathfrak{S}_p \setminus \mathfrak{A}_p$. On convient $A_0 = 0$, $T_0 = 0$. Soit $\Phi_2 = \sum_{p\geqslant 0} \frac{A_p}{p!} X^p \in \mathbb{C}[[X]]$ et $\Psi_2 = \sum_{p\geqslant 0} \frac{T_p}{p!} X^p \in \mathbb{C}[[X]]$. Montrer que

$$\Phi_1 = \frac{1}{2}\frac{2-X^2}{1-X}\exp(-X), \quad \Psi_1 = \frac{1}{4}\frac{2-X^2}{1-X}(1+\exp(-2X)),$$
$$\Phi_2 = \frac{1}{2}\frac{X^2}{1-X}\exp(-X), \quad \Psi_2 = \frac{1}{4}\frac{X^2}{1-X}(1-\exp(-2X)).$$

En déduire U_n, S_n, T_n, A_n. ■

Déterminons d'abord le nombre U_n des dérangements dans $\mathfrak{A}_n$.
Le nombre de permutions paires dans $\mathfrak{A}_n$ qui ont exactement k points fixes est $\binom{n}{k} U_{n-k}$; en effet, une permutation paire qui a k points fixes induit sur l'ensemble de ses points non invariants (de cardinal $n-k$) une permutation paire qui est un dérangement ; cette égalité est vraie aussi dans le cas où $k = n$, puisqu'il y a une seule permutation qui a n points fixes : l'identité. En classant les permutations paires suivant leur nombre de points fixes, on trouve donc l'égalité, pour tout entier $n \geqslant 2$:

$$\frac{n!}{2} = U_n + \binom{n}{1} U_{n-1} + \ldots + \binom{n}{n-1} U_1 + \binom{n}{n} U_0 .$$

Posons pour tout $n \in \mathbb{N}$, $u_n = U_n/n!$; on voit que $u_0 = 1$, et comme il est clair que $U_1 = 0$, on en déduit $u_1 = 0$. D'autre part pour tout $n \geqslant 2$:

$$\frac{1}{2} = u_n + \frac{1}{1!} u_{n-1} + \ldots + \frac{1}{(n-1)!} u_1 + \frac{1}{n!} u_0 .$$

On reconnaît ci-dessus les coefficients de la série formelle $\exp(X)\,\Phi_1(X)$, à partir du rang $n = 2$. Nous voyons donc que :

$$\exp(X)\,\Phi_1(X) = u_0 + \left(\frac{u_0}{1!} + \frac{u_1}{0!}\right) X + \frac{1}{2} X^2 + \ldots + \frac{1}{2} X^n$$

soit, puisque $u_0 = 1$ et $u_1 = 0$:

$$\exp(X)\,\Phi_1(X) = \frac{1}{2}(1+X) + \frac{1}{2}(1+X+X^2+\ldots) = \\ = \frac{1}{2}(1+X) + \frac{1}{2}\frac{1}{1-X} = \frac{1}{2}\frac{2-X^2}{1-X}\ .$$

Nous en déduisons finalement que :

$$\Phi_1(X) = \frac{1}{2}\frac{\exp(-X)}{1-X} + \frac{1}{2}(1+X)\exp(-X) = \frac{1}{2}\frac{2-X^2}{1-X}\exp(-X)\ .$$

Si on note D_n le nombre de dérangements dans $\mathfrak{S}_n$, on sait que (cf. exemple 3) :

$$\frac{\exp(-X)}{1-X} = \sum_{n\geqslant 0}\frac{D_n}{n!}X^n = \sum_{n\geqslant 0}\left(\sum_{p=0}^{n}\frac{(-1)^p}{p!}\right)X^n\ .$$

Il est clair que pour tout $n \in \mathbb{N}$, $U_n + A_n = D_n$; on voit donc que :

$$\Phi_2(X) = \frac{1}{2}\frac{\exp(-X)}{1-X} - \frac{1}{2}(1+X)\exp(-X) = \frac{1}{2}\frac{X^2}{1-X}\exp(-X)\ .$$

On constate que :

$$(1+X)\exp(-X) = (1+X)\sum_{n\in\mathbb{N}}\frac{(-1)^n}{n!}X^n = \\ = \sum_{n\geqslant 0}\frac{(-1)^n}{n!}X^n + \sum_{n\geqslant 0}\frac{(-1)^n}{n!}X^{n+1} = \\ = 1 + \sum_{n\geqslant 1}(-1)^{n-1}\left(\frac{1}{(n-1)!} - \frac{1}{n!}\right)X^n = \sum_{n\geqslant 0}(-1)^{n-1}\frac{n-1}{n!}X^n\ .$$

Nous en déduisons que pour tout $n \in \mathbb{N}$:

$$U_n = \frac{1}{2}D_n - (-1)^n\frac{n-1}{2} \quad \text{et} \quad A_n = \frac{1}{2}D_n + (-1)^n\frac{n-1}{2}\ .$$

Etudions maintenant les nombres S_n.
Pour $n \in \mathbb{N}$ notons R_n le nombre des permutations paires qui ont un nombre impair de points fixes ($R_0 = 0$). On voit que pour tout $n \in \mathbb{N}$, $S_n + R_n$ est le nombre de permutations paires, soit, si $n \geqslant 2$:

$$S_n + R_n = \frac{n!}{2}\ ,$$

et :

$$S_0 + R_0 = S_1 + R_1 = 1\ .$$

Introduisons pour tout $n \in \mathbb{N}$ les nombres $s_n = S_n/n!$ et $r_n = R_n/n!$. Nous voyons que :

$$\sum_{n\in\mathbb{N}}(s_n + r_n)X^n = \frac{1}{2}(1+X) + \frac{1}{2}\frac{1}{1-X} = \frac{1}{2}\frac{2-X^2}{1-X} .$$

En classant les permutations paires qui ont un nombre pair de points fixes suivant le nombre de leurs points fixes, on trouve que pour tout $n \in \mathbb{N}$:

$$S_n = \binom{n}{0}U_n + \binom{n}{2}U_{n-2}\dots ,$$

et en classant les permutations paires qui ont un nombre impair de points fixes :

$$R_n = \binom{n}{1}U_{n-1} + \binom{n}{3}U_{n-3} + \dots .$$

Nous en déduisons que pour tout $n \in \mathbb{N}$:

$$S_n - R_n = \binom{n}{0}U_n - \binom{n}{1}U_{n-1} + \binom{n}{2}U_{n-2} - \dots (-1)^n\binom{n}{n}U_0 ,$$

d'où pour tout $n \in \mathbb{N}$:

$$s_n - r_n = \sum_{p=0}^{n}\frac{(-1)^p}{p!}U_{n-p} .$$

On reconnaît les coefficients de la série formelle $\Phi_1(X)\exp(-X)$; on voit alors que :

$$\begin{aligned}\Psi_1(X) = \sum_{n\in\mathbb{N}}\frac{s_n + r_n + s_n - r_n}{2}X^n &= \frac{1}{4}\frac{2-X^2}{1-X} + \frac{1}{2}\Phi_1(X)\exp(-X) = \\ &= \frac{1}{4}\frac{2-X^2}{1-X}\left(1+\exp(-2X)\right) = \\ &= \frac{1}{4}\left(1 + X + \frac{1}{1-X}\right)\left(1+\exp(-2X)\right) .\end{aligned}$$

L'étude des nombres T_n est analogue, mais les valeurs initiales diffèrent. Pour $n \in \mathbb{N}$ notons Q_n le nombre des permutations impaires qui ont un nombre pair de points fixes ($Q_0 = 0$). On voit que pour tout $n \in \mathbb{N}$, $T_n + Q_n$ est le nombre de permutations impaires, soit, si $n \geqslant 2$:

$$T_n + Q_n = \frac{n!}{2} ,$$

et :

$$T_0 + Q_0 = T_1 + Q_1 = 0 .$$

Introduisons pour tout $n \in \mathbb{N}$ les nombres $t_n = T_n/n!$ et $q_n = Q_n/n!$. Nous voyons que :

$$\sum_{n\in\mathbb{N}} (t_n + q_n)X^n = -\frac{1}{2}(1+X) + \frac{1}{2}\frac{1}{1-X} = \frac{1}{2}\frac{X^2}{1-X} .$$

En classant les permutations impaires qui ont un nombre pair de points fixes suivant le nombre de leurs points fixes, on trouve que pour tout $n \in \mathbb{N}$:

$$Q_n = \binom{n}{0} A_n + \binom{n}{2} A_{n-2} \dots ,$$

et en classant les permutations impaires qui ont un nombre impair de points fixes :

$$T_n = \binom{n}{1} A_{n-1} + \binom{n}{3} A_{n-3} + \dots .$$

Nous en déduisons que pour tout $n \in \mathbb{N}$:

$$Q_n - T_n = \binom{n}{0} A_n - \binom{n}{1} A_{n-1} + \binom{n}{2} A_{n-2} - \dots (-1)^n \binom{n}{n} A_0 ,$$

d'où pour tout $n \in \mathbb{N}$:

$$q_n - t_n = \sum_{p=0}^{n} \frac{(-1)^p}{p!} A_{n-p} .$$

On reconnaît les coefficients de la série formelle $\Phi_2(X)\exp(-X)$; on voit alors que :

$$\begin{aligned}\Psi_2(X) &= \sum_{n\in\mathbb{N}} \frac{(q_n + t_n) - (q_n - t_n)}{2} X^n = \frac{1}{4}\frac{X^2}{1-X} - \frac{1}{2}\Phi_2(X)\exp(-X) = \\ &= \frac{1}{4}\frac{X^2}{1-X}(1 - \exp(-2X)) = \\ &= \frac{1}{4}\left(\frac{1}{1-X} - (1+X)\right)(1 - \exp(-2X)) .\end{aligned}$$

Déterminons enfin la valeur des coefficients S_n et T_n. On voit que :

$$\begin{aligned}(1+X)\exp(-2X) &= (1+X)\sum_{n\in\mathbb{N}} \frac{(-1)^n 2^n}{n!} X^n = \\ &= 1 + \sum_{n\geq 1} (-1)^{n-1} 2^{n-1} \frac{n-2}{n!} X^n .\end{aligned}$$

Nous obtenons aussi :

$$\frac{\exp(-2X)}{1-X} = \left(\sum_{p\geqslant 0} X^p\right)\left(\sum_{q\geqslant 0}(-1)^q\frac{2^q}{q!}X^q\right) = \sum_{n\geqslant 0}\left(\sum_{q=0}^{n}(-1)^q\frac{2^q}{q!}\right)X^n \ .$$

On en déduit que :

$$4\Psi_1(X) = 4\sum_{n\geqslant 0}\frac{S_n}{n!}X^n =$$
$$= (1+X) + \frac{1}{1-X} + (1+X)\exp(-2X) + \frac{1}{1-X}\exp(-2X) \ ,$$

d'où, pour tout $n \geqslant 2$ ($S_0 = 1, S_1 = 0$) :

$$S_n = \frac{1}{4}\left(n! + (-1)^{n-1}2^{n-1}(n-2) + n!\sum_{q=0}^{n}(-1)^q\frac{2^q}{q!}\right) \ .$$

De manière analogue nous obtenons :

$$4\Psi_2(X) = 4\sum_{n\geqslant 0}\frac{T_n}{n!}X^n =$$
$$= \frac{1}{1-X} - (1+X) + (1+X)\exp(-2X) - \frac{1}{1-X}\exp(-2X) \ ,$$

d'où, pour tout $n \geqslant 2$ ($T_0 = T_1 = 0$) :

$$T_n = \frac{1}{4}\left(n! + (-1)^{n-1}2^{n-1}(n-2) - n!\sum_{q=0}^{n}(-1)^q\frac{2^q}{q!}\right) \ .$$

Chapitre IX

ESPACES VECTORIELS ; DIMENSION DES ESPACES VECTORIELS

§ IX.1 *SOUS-ESPACES SUPPLÉMENTAIRES, PROJECTEURS*

Exercice 2 :

(On admet que dans tout K-ev, tout sous-K-ev a au moins un supplémentaire).

a) Soit E un K-ev, et $u \in \mathrm{Hom}_K(E)$. Montrer qu'il existe un projecteur p de E et un automorphisme α de E tels que $u = \alpha \circ p$.

b) Prouver de même qu'il existe un projecteur q de E et un automorphisme β de E tels que $u = q \circ \beta$. ■

a) Remarquons que u et p ont nécessairement même noyau. En particulier, si u est injectif, alors p est injectif, donc $p = \mathrm{Id}_E$, et $u = \alpha$ est bijectif. La propriété est donc fausse si E n'est pas un espace de dimension finie. Nous supposerons dans la suite que E est de dimension finie.

Soient S et J deux sous-K-ev de E tels que $E = \mathrm{Ker}(u) \oplus S$ et $E = J \oplus \mathrm{Im}(u)$. Soit p le projecteur de noyau $\mathrm{Ker}(u)$ et d'image S, et v la restriction de u à S pour le départ et $\mathrm{Im}(u)$ pour l'arrivée. Montrons que v est une bijection linéaire.
Son noyau est $\mathrm{Ker}(u) \cap S = \{0_E\}$; elle est donc injective. Si $y \in \mathrm{Im}(u)$, il existe $x \in E$ tel que $u(x) = y$; écrivons $x = x_1 + x_2$, où $x_1 \in \mathrm{Ker}(u)$ et $x_2 \in S$, on voit que $y = u(x_1 + x_2) = u(x_2)$, donc y est dans l'image de v. L'application linéaire v est donc surjective. Les espaces S et $\mathrm{Im}(u)$ étant isomorphes, ils ont même dimension, et leurs supplémentaires $\mathrm{Ker}(u)$ et J ont même dimension et sont donc isomorphes (c'est ici qu'intervient l'hypothèse que E est de dimensic

σ un isomorphisme $\mathrm{Ker}\,(u) \to J$. On voit qu'on définit un isomorphisme linéaire $\alpha : E \to E$ en posant :

$$\alpha(x) = \sigma(x_1) + v(x_2) \quad \text{si} \quad x = x_1 + x_2, \quad x_1 \in \mathrm{Ker}\,(u),\ x_2 \in S\ .$$

Montrons que $\alpha \circ p = u$. Si $x \in S$, alors $\alpha \circ p(x) = \alpha(x) = v(x) = u(x)$, si $x \in \mathrm{Ker}\,(u)$, alors $\alpha \circ p(x) = \alpha(0_E) = 0_E = u(x)$. Les deux endomorphismes $\alpha \circ p$ et u coïncident donc sur deux espaces supplémentaires et sont par conséquent égaux ; ce qu'il fallait démontrer.

b) On peut remarquer que nécessairement $\mathrm{Im}\,(u) = \mathrm{Im}\,(q)$. En particulier, si u est surjectif, q est surjectif, donc $q = \mathrm{Id}_E$, et $u = \beta$ est bijective. La propriété est donc fausse si E n'est pas de dimension finie. Nous supposerons dans la suite que E est de dimension finie.

Nous gardons les mêmes notations que dans le *a*). Montrons que le projecteur q d'image $\mathrm{Im}\,(u)$ et de noyau J convient (en gardant le même automorphisme), c'est-à-dire $u = q \circ \alpha$. Si $x \in S$, alors $\alpha(x) = u(x) \in \mathrm{Im}\,(u)$, donc $q \circ \alpha(x) = u(x)$. Si $x \in \mathrm{Ker}\,(u)$, alors $\alpha(x) \in J$, donc $q \circ \alpha(x) = 0_E = u(x)$. Les endomorphismes $q \circ \alpha$ et u coïncident sur les sous-espaces supplémentaires S et $\mathrm{Ker}\,(u)$, et sont par conséquent égaux ; ce qu'il fallait démontrer.

Exercice 3 :

> Soit E un K-ev. Chercher tous les couples (p, q) de projecteurs de E tels que $p \circ q = q \circ p$. ■

Montrons que si p et q sont des projecteurs qui commutent, alors le noyau (resp. l'image) de l'un est stable par l'autre. Si $x \in E$ et $p(x) = 0_E$, alors $q(p(x)) = 0_E = p(q(x))$; on voit donc que $\mathrm{Ker}\,(p)$ est stable par q. Si $y = p(x)$, où $x \in E$, $q(y) = q(p(x)) = p(q(x)) \in \mathrm{Im}\,(p)$; on voit donc que $\mathrm{Im}\,(p)$ est stable par q. On peut donc considérer l'endomorphisme de $\mathrm{Ker}\,(p)$ induit par q sur $\mathrm{Ker}\,(p)$; c'est un projecteur de ce K-ev, notons le q_1. On peut de même considérer l'endomorphisme de l'espace $\mathrm{Im}\,(p)$ induit par q sur $\mathrm{Im}\,(p)$; c'est un projecteur, notons le q_2. On peut écrire :

$$\mathrm{Ker}\,(p) = \mathrm{Ker}\,(q_1) \oplus \mathrm{Im}\,(q_1) \quad \text{et} \quad \mathrm{Im}\,(p) = \mathrm{Ker}\,(q_2) \oplus \mathrm{Im}\,(q_2)\ ,$$

d'où :

$$E = \mathrm{Ker}\,(q_1) \oplus \mathrm{Im}\,(q_1) \oplus \mathrm{Ker}\,(q_2) \oplus \mathrm{Im}\,(q_2)\ .$$

Nous obtenons donc quatre sous-espaces en somme directe : $E_1 = \mathrm{Ker}\,(q_1)$, $E_2 = \mathrm{Im}\,(q_1)$, $E_3 = \mathrm{Ker}\,(q_2)$, $E_4 = \mathrm{Im}\,(q_2)$, auxquels sont associés quatre projecteurs, p_1, p_2, p_3, p_4. On vérifie que si un élément $x \in E$ s'écrit $x = x_1 + x_2 + x_3 + x_4$, où $x_i \in E_i$ pour tout $i \in [\![1, 4]\!]$, alors :

$$p(x) = x_3 + x_4 \quad \text{et} \quad q(x) = q_1(x_1 + x_2) + q_2(x_3 + x_4) = x$$

d'où :

$$p = p_3 + p_4 \quad \text{et} \quad q = p_2 + p_4 \ .$$

Inversement, si $E = E_1 \oplus E_2 \oplus E_3 \oplus E_4$, et que p_1, p_2, p_3, p_4 sont les projecteurs dans cette somme directe sur les espaces E_1, E_2, E_3, E_4 respectivement, les endomorphismes :

$$p = p_3 + p_4 \quad \text{et} \quad q = p_2 + p_4 \ ,$$

sont des projecteurs qui commutent. En effet p est le projecteur sur $E_3 \oplus E_4$ parallèlement à $E_1 \oplus E_2$, et q est le projecteur sur $E_2 \oplus E_4$ parallèlement à $E_1 \oplus E_3$, et si $x = x_1 + x_2 + x_3 + x_4$, où $x_i \in E_i$ pour tout $i \in [\![1, 4]\!]$, alors :

$$p \circ q(x) = p(x_2 + x_4) = x_4 \quad \text{et} \quad q \circ p(x) = q(x_3 + x_4) = x_4 \ .$$

On peut remarquer que, puisque avec ces notations $p(x) = x_3 + x_4$ et $q(x) = x_2 + x_4$, $E_1 = \mathrm{Ker}\,(p) \cap \mathrm{Ker}\,(q)$, $E_2 = \mathrm{Ker}\,(p) \cap \mathrm{Im}\,(q)$, $E_3 = \mathrm{Ker}\,(q) \cap \mathrm{Im}\,(p)$, et $E_4 = \mathrm{Im}\,(p) \cap \mathrm{Im}\,(q)$. On voit aussi que $p \circ q = q \circ p = p_4$; c'est le projecteur sur $E_4 = \mathrm{Im}\,(p) \cap \mathrm{Im}\,(q)$ parallèlement à $E_1 \oplus E_2 \oplus E_3 = \mathrm{Ker}\,(p) + \mathrm{Ker}\,(q)$. De manière analogue, $p + q - p \circ q = p_2 + p_3 + p_4$, est le projecteur sur $E_2 \oplus E_3 \oplus E_4 = \mathrm{Im}\,(p) + \mathrm{Im}\,(q)$ parallèlement à $E_1 = \mathrm{Ker}\,(p) \cap \mathrm{Ker}\,(q)$.

On peut considérer qu'il s'agit là d'une caractérisation des couples de projecteurs qui commutent.

Exercice 6 :

> A quelle condition la somme de deux projecteurs p et q est-elle un projecteur ? Si c'est le cas, montrer que $\mathrm{Im}\,(p) \cap \mathrm{Im}\,(q) = \{0\}$ et $\mathrm{Ker}\,(p) \cap \mathrm{Ker}\,(q) = \mathrm{Ker}\,(p + q)$. ■

L'endomorphisme $p+q$ est un projecteur si, et seulement si, $(p+q)^2 = p+q$, soit en développant $p \circ q + q \circ p = 0$. Si la caractéristique du corps est 2, cela équivaut à dire que les projecteurs p et q commutent ; nous sommes ramenés à l'exercice précédent. Nous supposerons dans ce qui suit que la caractéristique du corps n'est pas 2.
Supposons que $p \circ q + q \circ p = 0$. Si $x \in \mathrm{Im}\,(q)$, alors $q(x) = x$, donc $p(q(x)) = p(x) = -q(p(x))$; donc $q^2(p(x)) = q(p(x)) = -p(x) = p(x)$; comme la caractéristique du corps n'est pas 2, nous en déduisons $p(x) = 0$ (on pourrait dire que -1 n'est pas valeur propre de q). Cela signifie que $\mathrm{Im}\,(q) \subset \mathrm{Ker}\,(p)$, soit $p \circ q = 0$; et bien sûr $q \circ p = 0$.
Inversement si p et q sont des projecteurs tels que $p \circ q = q \circ p = 0$, on voit que $(p + q)^2 = p^2 + q^2 = p + q$, et que par conséquent $p + q$ est un projecteur.

Supposons ces conditions réalisées.
Si $x \in \mathrm{Im}\,(p) \cap \mathrm{Im}\,(q)$, alors $0 = p(q(x)) = p(x) = x$, donc $\mathrm{Im}\,(p) \cap \mathrm{Im}\,(q) = \{0_E\}$.
L'inclusion $\mathrm{Ker}\,(p) \cap \mathrm{Ker}\,(q) \subset \mathrm{Ker}\,(p+q)$ étant évidente, démontrons l'inclusion opposée. Si $x \in \mathrm{Ker}\,(p+q)$, alors $p \circ (p+q)(x) = p^2(x) = p(x) = 0_E$, et de même $q(x) = 0_E$; donc $x \in \mathrm{Ker}\,(p) \cap \mathrm{Ker}\,(q)$. Nous en déduisons $\mathrm{Ker}\,(p+q) = \mathrm{Ker}\,(p) \cap \mathrm{Ker}\,(q)$.

En reprenant les notations de l'exercice précédent, nous voyons que l'espace $E_4 = \mathrm{Im}\,(p) \cap \mathrm{Im}\,(q)$ est ici nul. Il existe donc trois espaces E_1, E_2, E_3, tels que $E = E_1 \oplus E_2 \oplus E_3$, tels que si p_1, p_2, p_3 sont les projecteurs dans cette somme directe :

$$p = p_3 \quad \text{et} \quad q = p_2 \,.$$

Exercice 8 :

> Montrer que pour que deux endomorphismes u et v du K-ev E vérifient : $u \circ v = u$ et $v \circ u = v$, il faut et il suffit que ce soient deux projecteurs de même noyau. ■

Supposons que u et v soient des projecteurs de même noyau.
Alors $\mathrm{Im}\,(\mathrm{Id}_E - u) = \mathrm{Ker}\,(u) = \mathrm{Ker}\,(v)$, donc $v \circ (\mathrm{Id}_E - u) = 0$, soit encore $v = v \circ u$; de même $u = u \circ v$.

Supposons que u et v soient des endomorphismes de E tels que $u \circ v = u$ et $v \circ u = v$. Il est clair que $\mathrm{Ker}\,(u) \subset \mathrm{Ker}\,(v)$ et $\mathrm{Ker}\,(v) \subset \mathrm{Ker}\,(u)$, d'où $\mathrm{Ker}\,(u) = \mathrm{Ker}\,(v)$. Comme $u \circ (\mathrm{Id}_E - v) = 0$, $\mathrm{Im}\,(\mathrm{Id}_E - v) \subset \mathrm{Ker}\,(u) = \mathrm{Ker}\,(v)$, d'où $v \circ (\mathrm{Id}_E - v) = 0$, soit encore $v = v^2$. L'endomorphisme v est donc un projecteur. On montrerait de même que u est un projecteur. Les endomorphismes u et v sont donc bien des projecteurs de même noyau.

§ IX.2 *PRODUITS ET SOMMES D'ESPACES VECTORIELS*

Exercice 2 :

> Soit $E_1, E_2, \ldots, E_n$ des sous-K-ev de E. Pour que les E_i soient indépendants, il faut et il suffit que
>
> $$\forall i \in [\![2, n]\!] \,, \quad E_i \cap \left(\sum_{j=1}^{i-1} E_j \right) = \{0\} \,. \blacksquare$$

Montrons que la condition est nécessaire. Soit $i \in [\![2, n]\!]$, et soit

$$x_i = x_1 + \ldots + x_{i-1} \,,$$

un élément commun aux sous-K-ev E_i et $\sum_{j=1}^{i-1} E_j$. On peut écrire :

$$x_1 + \ldots + x_{i-1} - x_i = 0 \ ,$$

donc, par unicité, $x_i = x_1 = \ldots = x_{i-1} = 0$.

Montrons que la condition est suffisante. Supposons que le critère soit réalisé, et que :

$$x_1 + x_2 + \ldots + x_n = 0 \ ,$$

où pour tout $j \in [\![1, n]\!]$, $x_j \in E_j$. Si le n-uplet $(x_1, x_2, \ldots, x_n)$ n'était pas nul, on pourrait considérer le plus grand entier $i \in [\![1, n]\!]$ tel que $x_i \neq 0$ (donc $i \geqslant 2$). On aurait alors :

$$x_1 + \ldots + x_{i-1} = -x_i \ \in E_i \cap \left(\sum_{j=1}^{i-1} E_j \right) = \{0\} \ ,$$

ce qui est contradictoire. Donc pour tout $j \in [\![1, n]\!]$, $x_i = 0$. Les espaces $E_1, E_2, \ldots, E_n$ sont donc indépendants.

Exercice 4 :

Soit E, F, G trois sous-K-ev d'un K-ev E. On suppose $F \subset G$, $E \cap F = E \cap G$ et $E + F = E + G$. Montrer que $F = G$. ■

Il suffit évidemment de montrer $G \subset F$. Soit $x \in G$, comme $x \in E + G = E + F$, on peut trouver $u \in E$ et $v \in F$ tels que $x = u + v$. Comme $F \subset G$, nous pouvons écrire $u = x - v \in G$, donc $u \in E \cap G = E \cap F$, d'où $u \in F$. Nous en déduisons que $x = u + v$ est aussi élément de F. Cela démontre l'inclusion $G \subset F$, et finalement l'égalité $F = G$.

Exercice 6 :

Soit E, F, G trois sous-K-ev d'un K-ev. Montrer que
$$E \cap \big(F + (E \cap G)\big) = (E \cap F) + (E \cap G) \ . \ ■$$

Il est clair que les sous-K-ev $E \cap F$ et $E \cap G$ sont tous les deux inclus dans le sous-K-ev $E \cap \big(F + (E \cap G)\big)$. D'où l'inclusion :

$$(E \cap F) + (E \cap G) \subset E \cap \big(F + (E \cap G)\big) \ .$$

Si $x \in E \cap \big(F + (E \cap G)\big)$, alors on peut trouver $u \in F$ et $v \in E \cap G$ tels que $x = u + v$. Comme $u = x - v$, et que x et v sont

E, nous en déduisons $u \in E$, et par conséquent $u \in E \cap F$. On voit donc que $x = u + v$ est dans le sous-K-ev $(E \cap F) + (E \cap G)$. Nous avons donc démontré l'inclusion opposée :

$$E \cap \big(F + (E \cap G)\big) \subset (E \cap F) + (E \cap G) \ ;$$

d'où l'égalité de ces deux sous-K-ev.

Exercice 7 :

Soit E un K-ev et $p_1, p_2, \ldots, p_n$ des *projecteurs deux à deux permutables* tels que $p_1 + p_2 + \ldots + p_n = \mathrm{Id}_E$. On pose $E_i = \mathrm{Im}\,(p_i)$. Montrer que $E = \bigoplus_{i=1}^{n} E_i$ et que les p_i sont les projecteurs associés à cette décomposition de E. ■

Rappelons que si p et q sont des projecteurs qui commutent, alors le noyau (resp. l'image) de l'un est stable par l'autre. L'endomorphisme induit sur $\mathrm{Im}\,(p)$ (resp. sur $\mathrm{Ker}\,(p)$) par q, est un projecteur de ce sous-K-ev (cf. §IX.1 exercice 3).

Remarquons que la propriété à démontrer est fausse si le corps est de caractéristique finie k, car $(k+1)\mathrm{Id}_E = \mathrm{Id}_E$. Nous supposerons dans la suite que le corps K est de caractéristique nulle.

Montrons d'abord par récurrence sur l'entier n, que si $p_1, p_2, \ldots, p_n$ sont n projecteurs dans un K-ev E *non nul*, qui commutent et tels que $p_1 + \ldots + p_n = \lambda \mathrm{Id}_E$, où $\lambda \in K$, alors $\lambda \in [\![0, n]\!]$.
C'est vrai pour $n = 0$, car $E \neq \{0\}$. Supposons le résultat vrai pour $n-1$, ($n > 0$). Soient dans un espace non nul E, n projecteurs $p_1, p_2, \ldots, p_n$ qui commutent et tels que $p_1 + \ldots + p_n = \lambda \mathrm{Id}_E$, où $\lambda \in K$. Si ces projecteurs sont tous nuls, alors $\lambda = 0$ (car $E \neq \{0\}$). Si ces projecteurs ne sont pas tous nuls, on peut supposer par exemple $p_n \neq 0$. L'espace $F = \mathrm{Im}\,(p_n)$ n'est pas nul, il est stable par les autres projecteurs, et les endomorphismes induits sur F par ces projecteurs sont $n-1$ projecteurs du K-ev F deux à deux permutables. Notons $p'_1, \ldots, p'_{n-1}$ ces projecteurs. On voit que :

$$p'_1 + \ldots + p'_{n-1} + \mathrm{Id}_F = \lambda \mathrm{Id}_F \ ,$$

d'où :

$$p'_1 + \ldots + p'_{n-1} = (\lambda - 1)\mathrm{Id}_F \ .$$

Nous en déduisons $(\lambda - 1) \in [\![0, n-1]\!]$ (hypothèse de récurrence), soit $\lambda \in [\![1, n]\!]$. Dans tous les cas $\lambda \in [\![0, n]\!]$. La propriété est donc démontrée par récurrence.

Montrons maintenant que pour tout entier $n \geqslant 1$, si n projecteurs p_1, ..., p_n, deux à deux permutables d'un K-ev E, ont une somme nulle, ils sont tous nuls. Supposons qu'ils ne soient pas tous nuls, ce qui implique $E \neq \{0\}$. On peut supposer par exemple $p_n \neq 0$. L'espace $F = \mathrm{Im}\,(p_n)$ est non nul, et si on note $p'_1, \ldots, p'_{n-1}$, les endomorphismes de F induits par les autres projecteurs, on voit que ce sont des projecteurs de F qui commutent deux à deux, et vérifient :

$$p'_1 + \ldots + p'_{n-1} + \mathrm{Id}_F = 0 \quad \text{soit} \quad p'_1 + \ldots + p'_{n-1} = -\mathrm{Id}_F \ ,$$

ce qui est impossible d'après ce qui précède. Nous en déduisons que les projecteurs $p_1, \ldots, p_n$ sont tous nuls.

Supposons enfin que $p_1, \ldots, p_n$ soient n projecteurs permutables tels que :

$$p_1 + \ldots + p_n = \mathrm{Id}_E \ .$$

Notons $F = \mathrm{Im}\,(p_n)$, c'est un sous-K-ev de E stable par les projecteurs $p_1, \ldots, p_{n-1}$. Notons $p'_1, \ldots, p'_{n-1}$ les projecteurs induits sur F par les projecteurs $p_1, \ldots, p_{n-1}$; on voit que :

$$p'_1 + \ldots + p'_{n-1} + \mathrm{Id}_F = \mathrm{Id}_F \quad \text{soit} \quad p'_1 + \ldots + p'_{n-1} = 0 \ .$$

D'après ce qui précède, nous pouvons en déduire que $p'_1 = \ldots = p'_{n-1} = 0$. Cela signifie que pour tout $i \in [\![1, n-1]\!]$, $p_i \circ p_n = 0$. De manière générale, en changeant la numérotation des projecteurs, on voit que pour tous i et j dans $[\![1, n]\!]$ tels que $i \neq j$, $p_i \circ p_j = 0$.

Montrons enfin que $E = \bigoplus_{i=1}^{n} E_i$ et que les p_i sont les projecteurs associés à cette décomposition de E. Comme pour tout $x \in E$, $x = \sum_{i=1}^{n} p_i(x)$, il est clair que $E = E_1 + \ldots + E_n$. Supposons que $x = x_1 + \ldots + x_n$, où pour tout $i \in [\![1, n]\!]$, $x_i \in E_i$. On peut écrire :

$$x = \sum_{i=1}^{n} x_i = \sum_{i=1}^{n} p_i(x_i) \ ,$$

d'où, pour tout $j \in [\![1, n]\!]$:

$$p_j(x) = \sum_{i=1}^{n} p_j(p_i(x_i)) = p_j^2(x_j) = x_j \ .$$

Cela prouve que la décomposition est unique, donc que la somme est directe, et que les projecteurs p_j, où $j \in [\![1, n]\!]$, sont les projecteurs associés à cette somme directe.

Exercice 10 :

Soit E un K-ev et deux projecteurs p et q tels que $p \circ q = 0$. Montrer que $r = p+q-q\circ p$ est un projecteur tel que $\mathrm{Ker}\,(r) = \mathrm{Ker}\,(p) \cap \mathrm{Ker}\,(q)$ et $\mathrm{Im}\,(r) = \mathrm{Im}\,(p) \oplus \mathrm{Im}\,(q)$. ■

On peut écrire l'hypothèse sous la forme $\mathrm{Im}\,(q) \subset \mathrm{Ker}\,(p)$, donc :

$$\mathrm{Im}\,(q) \cap \mathrm{Im}\,(p) \subset \mathrm{Ker}\,(p) \cap \mathrm{Im}\,(p) = \{0\} \ .$$

Notons $S = \mathrm{Im}\,(p) \oplus \mathrm{Im}\,(q)$.

Montrons $\mathrm{Ker}\,(r) = \mathrm{Ker}\,(p) \cap \mathrm{Ker}\,(q)$. Si $x \in E$, $r(x) = 0$ si, et seulement si, $p(x) + q(x - p(x)) = 0$. Comme les sous-K-ev $\mathrm{Im}\,(p)$ et $\mathrm{Im}\,(q)$ sont indépendants, on voit que $x \in \mathrm{Ker}\,(r)$ si, et seulement si, $p(x) = 0$ et $q(x - p(x)) = 0$, soit si, et seulement si, $p(x) = 0$ et $q(x) = 0$. Nous en déduisons $\mathrm{Ker}\,(r) = \mathrm{Ker}\,(p) \cap \mathrm{Ker}\,(q)$.

Pour tout $x \in E$, $r(x) = p(x) + q(x - p(x))$, on voit donc que :

$$\mathrm{Im}\,(r) \subset \mathrm{Im}\,(p) \oplus \mathrm{Im}\,(q) = S \ .$$

Pour prouver que r est un projecteur d'image S, il suffit de prouver que pour tout $x \in S$, $r(x) = x$. Soit $x = p(u) + q(v)$, où $(u, v) \in E^2$, un élément de S, on voit que :

$$r(x) = p^2(u) + q(p(u)) - q(p^2(u)) + p(q(v)) + q^2(v) - q(p(q(v))) \ ,$$

d'où, en tenant compte de l'hypothèse $p \circ q = 0$:

$$r(x) = p(u) + q(p(u)) - q(p(u)) + q(v) = p(u) + q(v) = x \ .$$

L'endomorphisme r est donc bien le projecteur de noyau $\mathrm{Ker}\,(p) \cap \mathrm{Ker}\,(q)$ et d'image $\mathrm{Im}\,(p) \oplus \mathrm{Im}\,(q)$.

§ IX.3 *ESPACES DE DIMENSION FINIE*

Exercice 3 :

a) Soit E un K-ev de dimension finie $d \geqslant 1$. On suppose le corps K fini, de cardinal q. Montrer que : $\mathrm{card}\,(E) = q^d$.

b) Soit K un corps fini, de caractéristique p. Montrer que $\mathrm{card}\,(K) = p^n$ pour un certain $n \in \mathbb{N}^*$.

c) Montrer que, pour chaque entier $k \in [\![1, d]\!]$, le nombre de suites libres $(x_1, \ldots, x_k)$ à k termes dans E est :

$$(q^d-1)(q^d-q)\dots(q^d-q^{k-1})\,.$$

En particulier quel est le nombre de bases de E, le nombre d'automorphismes du K-ev E ? ■

a) Comme E est en tant que K-ev isomorphe au K-ev K^d, il est en bijection avec cet ensemble. Il est donc fini de cardinal q^d.

b) Comme le corps K est de caractéristique p, il contient un sous-corps A de cardinal p (son sous-corps premier, cf. §IV.4). On peut munir le corps K d'une structure de A-ev, et comme K est un ensemble fini, il est évidemment un A-ev de dimension finie. Si n est la dimension de ce A-ev ($n \geqslant 1$ car $A \subset K$), le cardinal de K est p^n (cf. *a*)).

c) Montrons par récurrence sur $k \in \mathbb{N}^*$ que le nombre de suites $(x_1,\dots,x_k)$ libres dans un K-ev de dimension $d \geqslant k$ est :

$$\prod_{i=0}^{k-1}(q^d-q^i)\,.$$

C'est vrai pour $k=1$. Supposons que ce soit vrai pour $k \geqslant 1$. Si E est un K-ev de dimension $d \geqslant k+1$, une suite $(x_1,\dots,x_k,x_{k+1})$ est libre dans E si, et seulement si, la suite $(x_1,\dots,x_k)$ est libre et x_{k+1} n'est pas dans le sous-espace engendré par la suite $(x_1,\dots,x_k)$. Pour une suite $(x_1,\dots,x_k)$ libre donnée, il y a donc q^d-q^k éléments x_{k+1} de E tels que la suite $(x_1,\dots,x_k,x_{k+1})$ soit libre. Le nombre de suites $(x_1,\dots,x_k,x_{k+1})$ libres est donc, en utilisant l'hypothèse de récurrence :

$$(q^d-q^k)\prod_{i=0}^{k-1}(q^d-q^i)=\prod_{i=0}^{k}(q^d-q^i)\,.$$

La proposition est donc démontrée par récurrence.

Le nombre de bases de E indexées par $[\![1,d]\!]$, est le nombre de suites $(x_1,\dots,x_d)$ libres, soit :

$$\prod_{i=0}^{d-1}(q^d-q^i)\,.$$

Une base $(e_1,\dots,e_d)$ de E étant fixée, l'application $f \mapsto (f(e_1),\dots,f(e_d))$ est une bijection entre l'ensemble des automorphismes de E et l'ensemble des bases de E indexées par $[\![1,d]\!]$. Le nombre des automorphismes de E est donc égal au nombre de bases $(x_1,\dots,x_d)$ de E.

Exercice 6 :

> Soit u un endomorphisme d'un K-ev de dimension finie. Montrer que pour que $\mathrm{Ker}\,(u)$ et $\mathrm{Im}\,(u)$ soient supplémentaires, il faut et il suffit que $\mathrm{Im}\,(u^2) = \mathrm{Im}\,(u)$. ■

Le K-ev sera noté E .
Comme $\dim \mathrm{Ker}\,(u) + \dim \mathrm{Im}\,(u) = \dim E$, les sous-K-ev $\mathrm{Ker}\,(u)$ et $\mathrm{Im}\,(u)$ sont supplémentaires si, et seulement si, $\mathrm{Ker}\,(u) \cap \mathrm{Im}\,(u) = \{0\}$. Considérons l'endomorphisme v induit par u sur le sous-K-ev u-stable $\mathrm{Im}\,(u)$; son noyau est $\mathrm{Ker}\,(u) \cap \mathrm{Im}\,(u)$, et ce sous-K-ev est nul si, et seulement si, v est injectif. Comme $\mathrm{Im}\,(u)$ est un K-ev de dimension finie, l'endomorphisme v est injectif si, et seulement si, il est surjectif ; or il est clair que $\mathrm{Im}\,(v) = \mathrm{Im}\,(u^2)$. On voit donc que les sous-K-ev $\mathrm{Ker}\,(u)$ et $\mathrm{Im}\,(u)$ sont supplémentaires si, et seulement si, $\mathrm{Im}\,(u^2) = \mathrm{Im}\,(u)$.

Exercice 9 :

> Soit E un K-ev de dimension finie $n \geqslant 2$. Montrer que le K-ev $\mathrm{Hom}_K(E)$ est engendré par $\mathrm{Hom}_K(E) \setminus \mathrm{GL}_K(E)$ et qu'il est aussi engendré par $\mathrm{GL}_K(E)$. ■

Soit $(e_1, \ldots, e_n)$ une base de E . Pour tout $(i,j) \in [\![1,n]\!]^2$, notons $\varphi_{i,j}$ l'application linéaire telle que pour tout $k \in [\![1,n]\!]$, $\varphi_{i,j}(e_k) = \delta_{j,k}\, e_i$, où $\delta_{j,k} = 0$ si $j \neq k$, et $\delta j,k = 1$ si $j = k$. On sait qu'il s'agit d'une base du K-ev $\mathrm{Hom}_K(E)$. On voit que pour tout $(i,j) \in [\![1,n]\!]^2$, $\mathrm{Im}\,(\varphi_{i,j}) = K\, e_i$; comme $\dim E = n \geqslant 2$, ces endomorphismes ne sont pas surjectifs, donc pas bijectifs : ce sont des éléments de $\mathrm{Hom}_K(E) \setminus \mathrm{GL}_K(E)$.

Nous avons démontré dans la résolution de l'exercice 2 du §IX.2, que tout endomorphisme $u \in \mathrm{Hom}_K(E)$ peut s'écrire $\alpha \circ p$, où p est un projecteur, et α un automorphisme de E . Il suffit donc, pour montrer que le K-ev $\mathrm{Hom}_K(E)$ peut être engendré par $\mathrm{GL}_K(E)$, de démontrer que tout projecteur de E peut s'écrire comme combinaison linéaire d'automorphismes de E .
Supposons que le corps K ait au moins trois éléments ; il a donc un élément λ , $\lambda \neq 0$ et $\lambda \neq 1$. Il est clair que si p et q sont deux projecteurs tels que $p + q = \mathrm{Id}_E$, $\lambda \cdot p + q$ est un automorphisme de E . On voit alors que :

$$p = \frac{1}{\lambda - 1}\left((\lambda \cdot p + q) - (p + q)\right) .$$

Le projecteur p est bien dans le sous-K-ev engendré par $\mathrm{GL}_K(E)$.

On peut aussi utiliser la démonstration suivante, qui ne nécessite pas cette hypothèse. On peut d'abord supposer, éventuellement en remp

$\mathrm{Id}_E - p$ que $2\,\mathrm{rg}(p) \leqslant \dim E$. Posons $A = \mathrm{Im}\,(p)$, on peut trouver un sous-K-ev B de même dimension que A, et un sous-K-ev C tels que :

$$\mathrm{Ker}\,(p) = B \oplus C \quad \text{d'où} \quad E = A \oplus B \oplus C\,.$$

Notons q et r les projecteurs sur les K-ev B et C dans cette somme directe, et $\sigma : A \to B$ un isomorphisme de K-ev. L'endomorphisme de E :

$$\varphi = \sigma^{-1} \circ q + \sigma \circ p + r\,,$$

est injectif ; en effet, si $x = x_A + x_B + x_C$, où $x_A \in A$, $x_B \in B$, $x_C \in C$, est tel que $\varphi(x) = \sigma^{-1}(x_B) + \sigma(x_A) + x_C = 0$, comme $\sigma^{-1}(x_B) \in A$, $\sigma(x_A) \in B$ et $x_C \in C$, on voit que $\sigma^{-1}(x_B) = 0$, $\sigma(x_A) = 0$ et $x_C = 0$, d'où $x = 0$. L'endomorphisme φ est donc un automorphisme.
L'endomorphisme $\psi = p + \varphi$ est aussi injectif. En effet, avec les mêmes notations que ci-dessus, si $\psi(x) = x_A + \sigma^{-1}(x_B) + \sigma(x_A) + x_C = 0$, alors, comme $x_A + \sigma^{-1}(x_B) \in A$, $\sigma(x_A) \in B$ et $x_C \in C$, on voit que $x_A + \sigma^{-1}(x_B) = 0$, $\sigma(x_A) = 0$ et $x_C = 0$, d'où $x_A = 0$, puis $x_B = 0$ et $x_C = 0$, soit $x = 0$. L'endomorphisme ψ est donc un automorphisme du K-ev E.
Le projecteur $p = \psi - \varphi$, est donc bien dans le sous-K-ev engendré par $\mathrm{GL}_K(E)$, ce qu'il fallait démontrer.

§ IX.4 *PROPRIÉTÉS DES ESPACES DE DIMENSION FINIE*

Exercice 1 :

Soit E et F deux K-ev de dimensions finies respectives $n \geqslant 1$ et $p \geqslant 1$, et soit G un sous-K-ev de E. On pose $\mathscr{L}_G = \{u \in \mathrm{Hom}_K(E,F) \mid G \subset \mathrm{Ker}\,(u)\}$, et $r = \dim(G)$.

a) Montrer que $\mathscr{L}_G$ est un sous-K-ev de $\mathrm{Hom}_K(E,F)$.

b) Calculer $\dim_K(\mathscr{L}_G)$ en fonction de n, p et r. ■

a) Soit i_G l'application K-linéaire $x \mapsto x$, $G \to E$. Les éléments de $\mathscr{L}_G$ sont les applications K-linéaires $u : E \to F$, telles que $u \circ i_G = 0$. Nous en déduisons que $\mathscr{L}_G$ est le noyau de l'application K-linéaire $u \mapsto u \circ i_G$, $\mathrm{Hom}_K(E,F) \to \mathrm{Hom}_K(G,F)$; c'est donc bien un sous-K-ev de $\mathrm{Hom}_K(E,F)$.

b) Soit S un supplémentaire du sous-K-ev G ; l'application $u \mapsto u_{|S} = u \circ i_S$, $\mathscr{L}_G \to \mathrm{Hom}_K(S,F)$ est K-linéaire bijective ; en effet, s

est une application linéaire, on sait qu'il existe une et une seule application linéaire $u : E \to F$, telle que $u_{|G} = 0$ et $u_{|S} = v$.
Nous en déduisons :

$$\dim_K \mathcal{L}_G = \dim_K \mathrm{Hom}_K(S, F) = \dim_K S \times \dim_K F = (n-r)p \ .$$

Exercice 2 :

Soit A, B, C, D des K-ev de dimension finie. On considère des applications K-linéaires α, β, γ : $A \xrightarrow{\alpha} B \xrightarrow{\beta} C \xrightarrow{\gamma} D$. Montrer : $\mathrm{rg}(\beta \circ \alpha) + \mathrm{rg}(\gamma \circ \beta) \leqslant \mathrm{rg}(\beta) + \mathrm{rg}(\gamma \circ \beta \circ \alpha)$. ■

Nous pouvons écrire l'inégalité de l'énoncé sous la forme :

$$\mathrm{rg}(\beta \circ \alpha) - \mathrm{rg}(\gamma \circ \beta \circ \alpha) \leqslant \mathrm{rg}(\beta) - \mathrm{rg}(\gamma \circ \beta) \ .$$

Notons $C_1 = \mathrm{Im}\,(\beta)$, et γ_1 la restriction de γ à C_1, $\gamma_1 : C_1 \to D$. On voit que :

$$\mathrm{rg}(\beta) - \mathrm{rg}(\gamma \circ \beta) = \dim C_1 - \mathrm{rg}(\gamma_1) = \dim \mathrm{Ker}\,(\gamma_1) \ .$$

Nous obtenons donc finalement :

$$\mathrm{rg}(\beta) - \mathrm{rg}(\gamma \circ \beta) = \dim(\mathrm{Ker}\,(\gamma) \cap \mathrm{Im}\,(\beta)) \ .$$

Nous obtiendrions de manière analogue l'égalité :

$$\mathrm{rg}(\beta \circ \alpha) - \mathrm{rg}(\gamma \circ \beta \circ \alpha) = \dim\big(\mathrm{Ker}\,(\gamma) \cap \mathrm{Im}\,(\beta \circ \alpha)\big) \ .$$

Comme $\mathrm{Im}\,(\beta \circ \alpha) \subset \mathrm{Im}\,(\beta)$, nous en déduisons :

$$\mathrm{rg}(\beta \circ \alpha) - \mathrm{rg}(\gamma \circ \beta \circ \alpha) \leqslant \mathrm{rg}(\beta) - \mathrm{rg}(\gamma \circ \beta) \ ,$$

ce qu'il fallait démontrer.

Exercice 4 :

Soit $x_1, x_2, \ldots, x_n$ dans $\mathbb{R}$ avec $x_1 < x_2 < \ldots < x_n$. On note E le $\mathbb{R}$-ev des fonctions *de classe* C^1 : $f : \mathbb{R} \to \mathbb{R}$ telles que :

$$f_{|]-\infty, x_1]}, f_{|[x_n, +\infty[} \text{ et } f_{|[x_i, x_{i+1}]} \quad (1 \leqslant i \leqslant n-1)$$

soient des fonctions polynomiales de degré $\leqslant 2$. Montrer que E est de dimension finie ; préciser cette dimension ; trouver une base de E. ■

Soit A l'ensemble des applications polynomiales : $\mathbb{R} \to \mathbb{R}$ de degré $\leqslant 2$. C'est un sous-$\mathbb{R}$-ev de dimension 3 de E. Soit B le sous-$\mathbb{R}$-ev des éléments de E dont la restriction à l'intervalle $]-\infty, x_1]$ est nulle ; montrons que $E = A \oplus B$.
Soit $f \in E$, si $f = P + g$, où $P \in A$ et $g \in B$, on voit que P ne peut être que l'application polynomiale de degré $\leqslant 2$ qui coïncide sur l'intervalle $]-\infty, x_1]$ avec f. Il y a donc unicité de la décomposition. Inversement, si $f \in E$, soit P l'application polynomiale de degré $\leqslant 2$, $P : \mathbb{R} \to \mathbb{R}$, qui coïncide avec f sur l'intervalle $]-\infty, x_1]$. Comme $P \in E$, on en déduit $g = f - P \in E$, et puisque $g = f - P$ est nulle sur l'intervalle $]-\infty, x_1]$, on voit que $g \in B$. Finalement $f = P + g$, où $P \in A$ et $g \in B$.
Nous avons bien démontré $E = A \oplus B$.

Montrons maintenant que l'application linéaire qui à $f \in B$ fait correspondre le n-uplet des valeurs de la dérivée seconde de f sur les n intervalles $]x_i, x_{i+1}[$, où $i \in [\![1, n-1]\!]$ et $]x_n, +\infty[$, est injective. Si f'' est nulle sur ces intervalles, f' est constante sur les intervalles fermés correspondants (f' est continue), et comme $f'(x_1) = 0$ (puisque f est nulle sur l'intervalle $]-\infty, x_1]$), on voit que $f' = 0$. L'application f est donc constante sur $\mathbb{R}$, donc nulle. Le $\mathbb{R}$-espace B est donc de dimension finie $\leqslant n$.

Exhibons maintenant une base de B. Considérons, pour $a \in \mathbb{R}$, l'application $f_a : \mathbb{R} \to \mathbb{R}$, définie pour tout $x \in \mathbb{R}$ par : $f_a(x) = 0$ si $x \leqslant a$, et $f_a(x) = (x-a)^2$ si $x \geqslant a$. Il est clair que pour tout $i \in [\![1, n]\!]$, $f_{x_i} \in B$. Montrons que la famille $(f_{x_i})_{i \in [\![1,n]\!]}$ est libre. Supposons que $(\lambda_i)_{i \in [\![1,n]\!]}$ soit une famille non nulle de scalaires telle que :

$$\sum_{i \in [\![1,n]\!]} \lambda_i \cdot f_{x_i} = 0 .$$

Soit i_0 le plus petit indice tel que $\lambda_i \neq 0$ (donc $i_0 < n$). Comme pour tout $i > i_0$, f_i est nulle sur l'intervalle $[x_{i_0}, x_{i_0+1}]$, on voit que $\lambda_{i_0} \cdot f_{x_{i_0}}$ devrait aussi être nulle sur cet intervalle, ce qui est évidemment contradictoire.
La famille $(f_{x_i})_{i \in [\![1,n]\!]}$ est donc bien libre dans le $\mathbb{R}$-ev B, et comme cet espace est de dimension $\leqslant n$, on voit que cette famille est une base de B et que $\dim B = n$.

L'espace $E = A \oplus B$ est donc de dimension $n+3$, et on obtient une base de E en adjoignant à la famille $(f_{x_i})_{i \in [\![1,n]\!]}$ une base de l'espace des fonctions polynomiales de $\mathbb{R}$ dans $\mathbb{R}$ de degré $\leqslant 2$.

Exercice 8 :

‖ Soit u et v deux éléments de $\mathrm{Hom}_K(E, F)$, avec .

de dimension finie. Montrer :

$$(*) \quad |\mathrm{rg}(u) - \mathrm{rg}(v)| \leqslant \mathrm{rg}(u+v) \leqslant \\ \leqslant \mathrm{Min}\,(\dim(E), \dim(F), \mathrm{rg}(u) + \mathrm{rg}(v)) \ .$$

Montrer que, pour $\mathrm{rg}(u)$ et $\mathrm{rg}(v)$ donnés, $\mathrm{rg}(u+v)$ peut prendre toutes les valeurs possibles autorisées par $(*)$. ■

Il est clair que $\mathrm{Im}\,(u+v) \subset \mathrm{Im}\,(u) + \mathrm{Im}\,(v)$ (attention : il n'y a pas en général égalité). Nous en déduisons que pour tous éléments u et v de $\mathrm{Hom}_K(E,F)$:

$$\mathrm{rg}(u+v) = \dim \mathrm{Im}\,(u+v) \leqslant \dim\,(\mathrm{Im}\,(u) + \mathrm{Im}\,(v)) \leqslant \\ \leqslant \dim \mathrm{Im}\,(u) + \dim \mathrm{Im}\,(v) = \mathrm{rg}(u) + \mathrm{rg}(v) \ .$$

Comme le rang d'une application linéaire est toujours inférieur à la dimension de l'espace de départ et à la dimension de l'espace d'arrivée, nous en déduisons :

$$\mathrm{rg}(u+v) \leqslant \mathrm{Min}\,(\dim(E), \dim(F), \mathrm{rg}(u) + \mathrm{rg}(v)) \ .$$

On voit aussi que pour tous éléments u et v de $\mathrm{Hom}_K(E,F)$:

$$\mathrm{rg}(u) = \mathrm{rg}(-v + (u+v)) \leqslant \mathrm{rg}(-v) + \mathrm{rg}(u+v) = \mathrm{rg}(v) + \mathrm{rg}(u+v) \ ,$$

d'où :

$$\mathrm{rg}(u) - \mathrm{rg}(v) \leqslant \mathrm{rg}(u+v) \ .$$

Comme de même $\mathrm{rg}(v) - \mathrm{rg}(u) \leqslant \mathrm{rg}(u+v)$, nous en déduisons finalement :

$$|\mathrm{rg}(u) - \mathrm{rg}(v)| \leqslant \mathrm{rg}(u+v) \ .$$

Démontrons maintenant que, E et F étant des K-ev de dimension finie et p et q des entiers tous les deux $\leqslant \mathrm{Min}\,(\dim E, \dim F)$, pour tout entier r tel que $|q-p| \leqslant r \leqslant \mathrm{Min}\,(\dim E, \dim F, p+q)$, il existe deux éléments u et v de $\mathrm{Hom}_K(E,F)$, tels que $p = \mathrm{rg}(u)$, $q = \mathrm{rg}(v)$ et $r = \mathrm{rg}(u+v)$. Nous supposerons que le corps de base a au moins 3 éléments. En effet si $K = \mathbb{Z}/2\mathbb{Z}$, et que u et v sont des homomorphismes de rang 1, leur somme est soit de rang 2 si leurs images sont indépendantes, soit nulle si leurs images sont identiques, leur somme n'est donc jamais de rang 1. Nous utiliserons le lemme suivant :

Lemme :

Soient F_1 un K-ev de dimension finie r, deux entiers p et q tels que $p \leqslant r$, $q \leqslant r$ et $r \leqslant p+q$; il existe deux endomorphismes u_1 et v_1 du K-ev F_1 tels que $\mathrm{rg}(u_1) = p$, $\mathrm{rg}(v_1) = q$, et $\mathrm{rg}(u_1 + v_1) = r$ (donc $u_1 + v_1$ automorphisme). ■

Soit λ un scalaire tel que $\lambda \neq 0$ et $\lambda \neq 1$. Il existe trois sous-K-ev A, B, C de F_1, A de dimension $r-p$, B de dimension $p+q-r$ et C de dimension $r-q$ tels que $F_1 = A \oplus B \oplus C$. En notant p_A, p_B, p_C les projecteurs dans cette somme directe, on voit facilement que $v_1 = p_A + \lambda p_B$ est de rang $r-p+p+q-r = q$, que $u_1 = -p_B + p_C$ est de rang $p+q-r+r-q = p$, et que $u_1 + v_1 = p_A + (\lambda - 1)p_B + p_C$ est de rang $r-p+p+q-r+r-q = r$. Fin du lemme

Nous reprenons les notations précédentes.
Supposons d'abord $\text{Max}(p,q) \leqslant r$. Comme $r \leqslant \dim F$, il existe un sous-K-ev F_1 de dimension r, du K-ev F ; comme $r \leqslant \dim E$, il existe une surjection linéaire $\varphi : E \to F_1$. D'après le lemme, il existe deux endomorphismes u_1 et v_1 du K-ev F_1 tels que $\text{rg}(u_1) = p$, $\text{rg}(v_1) = q$ et $\text{rg}(u_1+v_1) = r$. Notons i_{F_1}, l'application linéaire $x \mapsto x$, $F_1 \to F$. On voit que $u = i_{F_1} \circ u_1 \circ \varphi$ et $v = i_{F_1} \circ v_1 \circ \varphi$ sont des éléments de $\text{Hom}_K(E,F)$, tels que $\text{rg}(u) = p$, $\text{rg}(v) = q$, et puisque $u + v = i_{F_1} \circ (u_1 + v_1) \circ \varphi$, $\text{rg}(u+v) = r$.

Supposons maintenant $|q-p| \leqslant r < \text{Max}(p,q)$. On peut supposer $p \leqslant q$; la condition sur r devient alors : $q-p \leqslant r < q$. Comme $q \leqslant \dim F$, il existe un sous-K-ev F_1 de dimension q, du K-ev F ; comme $q \leqslant \dim E$, il existe une surjection linéaire φ, $E \to F_1$. Posons $r_1 = q$, $p_1 = p$, et $q_1 = r$. On vérifie les hypothèses du lemme : $p_1 \leqslant r_1$ (puisque $p \leqslant q$), $q_1 \leqslant r_1$ (puisque $r \leqslant q$), et $r_1 \leqslant p_1 + q_1$ (puisque $q \leqslant p + r$). Il existe donc deux endomorphismes u_1 et v_1 du K-ev F_1, tels que $\text{rg}(u_1) = p_1 = p$, $\text{rg}(v_1) = q_1 = r$, et $\text{rg}(u_1 + v_1) = r_1 = q$. On voit que les applications $v = i_{F_1} \circ (u_1 + v_1) \circ \varphi$, et $u = -i_{F_1} \circ u_1 \circ \varphi$ sont des éléments de $\text{Hom}_K(E,F)$, tels que $\text{rg}(u) = p$, $\text{rg}(v) = q$, et puisque $u+v = i_{F_1} \circ v_1 \circ \varphi$, $\text{rg}(u+v) = r$.

La proposition est donc démontrée dans tous les cas.

Exercice 13 :

Soit $\mathcal{P}$ l'ensemble des projecteurs d'un K-ev E. Si $p \in \mathcal{P}$ et $q \in \mathcal{P}$ on note $p \preceq q$ ssi $pq = qp = p$.

a) Montrer que $(\mathcal{P}, \preceq)$ est un ensemble ordonné.

b) Soit p et q dans $\mathcal{P}$ avec $pq = qp$. On pose $p \wedge q = pq$ et $p \vee q = p + q - pq$.
Montrer : $p \wedge q \in \mathcal{P}$, et $p \wedge q$ est la borne inférieure de $\{p, q\}$ dans $\mathcal{P}$, et $\text{Im}(p \wedge q) = \text{Im}(p) \cap \text{Im}(q)$.
Montrer : $p \vee q \in \mathcal{P}$, $p \vee q$ est la borne supérieure de $\{p, q\}$ dans $\mathcal{P}$, et $\text{Im}(p \vee q) = \text{Im}(p) + \text{Im}(q)$. ■

Si $p \in \mathcal{P}$, nous dirons que $\text{Id}_E - p$ est le projecteur conjugu

sait que si p et p' sont des projecteurs conjugués, le noyau de l'un est égal à l'image de l'autre.

a) Les conditions $pq = qp = p$ s'écrivent aussi $p(\mathrm{Id}_E - q) = (\mathrm{Id}_E - q)p = 0$, soit encore $\mathrm{Im}\,(\mathrm{Id}_E - q) \subset \mathrm{Ker}\,(p)$ et $\mathrm{Im}\,(p) \subset \mathrm{Ker}\,(\mathrm{Id}_E - q)$. D'après la remarque initiale, on voit que $p \preceq q$ si, et seulement si, $\mathrm{Ker}\,(q) \subset \mathrm{Ker}\,(p)$ et $\mathrm{Im}\,(p) \subset \mathrm{Im}\,(q)$. Il est alors clair que la relation $\preceq$ est réflexive et transitive ; elle est antisymétrique car deux projecteurs de même noyau et de même image sont identiques.

b) Comme les projecteurs p et q commutent, $(pq)^2 = p^2q^2 = pq$; pq est donc un projecteur. Comme $p \wedge q = pq$, on voit que $\mathrm{Im}\,(p \wedge q) \subset \mathrm{Im}\,(p)$ et comme $p \wedge q = qp$, on voit que $\mathrm{Im}\,(p \wedge q) \subset \mathrm{Im}\,(q)$; nous en déduisons $\mathrm{Im}\,(p \wedge q) \subset \mathrm{Im}\,(p) \cap \mathrm{Im}\,(q)$. Pour tout $x \in \mathrm{Im}\,(p) \cap \mathrm{Im}\,(q)$, x est invariant par p et par q, donc invariant par $p \wedge q = qp$; nous en déduisons que $\mathrm{Im}\,(p) \cap \mathrm{Im}\,(q) \subset \mathrm{Im}\,(p \wedge q)$, d'où finalement $\mathrm{Im}\,(p) \cap \mathrm{Im}\,(q) = \mathrm{Im}\,(p \wedge q)$.

Montrons que $\mathrm{Ker}\,(p \wedge q) = \mathrm{Ker}\,(p) + \mathrm{Ker}\,(q)$. Il est clair que $\mathrm{Ker}\,(p) \subset \mathrm{Ker}\,(qp)$ et $\mathrm{Ker}\,(q) \subset \mathrm{Ker}\,(pq)$, donc $\mathrm{Ker}\,(p) + \mathrm{Ker}\,(q) \subset \mathrm{Ker}\,(p \wedge q)$. Inversement, supposons $x \in \mathrm{Ker}\,(qp)$; écrivons $x = p(x) + x - p(x)$, on voit que $p(x) \in \mathrm{Ker}\,(q)$ et $x - p(x) \in \mathrm{Ker}\,(p)$. Nous en déduisons $\mathrm{Ker}\,(qp) \subset \mathrm{Ker}\,(p) + \mathrm{Ker}\,(q)$ et finalement $\mathrm{Ker}\,(qp) = \mathrm{Ker}\,(p) + \mathrm{Ker}\,(q)$.

Un projecteur r minore p et q si, et seulement si, $\mathrm{Im}\,(r) \subset \mathrm{Im}\,(p)$, $\mathrm{Im}\,(r) \subset \mathrm{Im}\,(q)$, $\mathrm{Ker}\,(p) \subset \mathrm{Ker}\,(r)$ et $\mathrm{Ker}\,(q) \subset \mathrm{Ker}\,(r)$. On voit donc que le projecteur r minore p et q si, et seulement si $\mathrm{Im}\,(r) \subset \mathrm{Im}\,(p) \cap \mathrm{Im}\,(q) = \mathrm{Im}\,(p \wedge q)$ et $\mathrm{Ker}\,(r) \supset \mathrm{Ker}\,(p) + \mathrm{Ker}\,(q) = \mathrm{Ker}\,(p \wedge q)$. Nous en déduisons que r minore la paire $\{p, q\}$ si, et seulement si, r minore $p \wedge q$. On voit donc que $p \wedge q$ est la borne inférieure de la paire $\{p, q\}$.

Introduisons l'application $c : p \mapsto \mathrm{Id}_E - p$, $\mathscr{P} \to \mathscr{P}$ (c'est une involution). On a déjà remarqué que pour tout $p \in \mathscr{P}$, $\mathrm{Im}\,(p) = \mathrm{Ker}\,(c(p))$ et $\mathrm{Ker}\,(p) = \mathrm{Im}\,(c(p))$. On voit donc que c est une involution strictement décroissante pour l'ordre $\preceq$. De plus, pour tous projecteurs p et q qui commutent, $p + q - pq = \mathrm{Id}_E - (\mathrm{Id}_E - p)(\mathrm{Id}_E - q)$, soit $c(p \vee q) = c(p) \wedge c(q)$. On voit donc que $c(p \vee q)$ est le projecteur de noyau $\mathrm{Ker}\,(c(p)) + \mathrm{Ker}\,(c(q)) = \mathrm{Im}\,(p) + \mathrm{Im}\,(q)$, et d'image $\mathrm{Im}\,(c(p)) \cap \mathrm{Im}\,(c(q)) = \mathrm{Ker}\,(p) \cap \mathrm{Ker}\,(q)$. Par conséquent $p \vee q$ est le projecteur de noyau $\mathrm{Ker}\,(p) \cap \mathrm{Ker}\,(q)$ et d'image $\mathrm{Im}\,(p) + \mathrm{Im}\,(q)$. On prouve facilement que $p \vee q$ est la borne supérieure de la paire $\{p, q\}$, en utilisant le fait que c est strictement décroissante.

Exercice 14 :

‖ Soit E et F deux K-ev de dimension finie, $f \in$ E

$g \in \mathrm{Hom}_K(F,E)$. On fait les hypothèses $g \circ f \circ g = g$ et $f \circ g \circ f = f$.

a) Montrer que : $E = \mathrm{Im}\,(g) \oplus \mathrm{Ker}\,(f)$.

b) Comparer les rangs de f et de g. ■

On sait que le rang de la composée de deux applications linéaires est inférieur ou égal au rang de chacune de ces applications linéaires. Nous en déduisons $\mathrm{rg}(g) = \mathrm{rg}(g \circ f \circ g) \leqslant \mathrm{rg}(f)$ et $\mathrm{rg}(f) = \mathrm{rg}(f \circ g \circ f) \leqslant \mathrm{rg}(g)$; donc $\mathrm{rg}(f) = \mathrm{rg}(g)$.

Montrons que les sous-K-ev $\mathrm{Im}\,(g)$ et $\mathrm{Ker}\,(f)$ sont indépendants.
Si $z \in \mathrm{Im}\,(g) \cap \mathrm{Ker}\,(f)$, il existe $y \in E$ tel que $z = g(y)$, et $f(g(y)) = 0$; donc $g(f(g(y)) = g(y) = z = 0$. Les sous-K-ev $\mathrm{Im}\,(g)$ et $\mathrm{Ker}\,(f)$ sont donc bien indépendants.

Comme $\mathrm{rg}(f) = \mathrm{rg}(g)$, on voit que :

$$\dim(\mathrm{Im}\,(g) \oplus \mathrm{Ker}\,(f)) = \dim \mathrm{Im}\,(g) + \dim \mathrm{Ker}\,(f) =$$
$$= \dim \mathrm{Im}\,(f) + \dim \mathrm{Ker}\,(f) = \dim E\ .$$

Nous en déduisons :

$$\mathrm{Im}\,(g) \oplus \mathrm{Ker}\,(f) = E\ ,$$

ce qu'il fallait démontrer.

§ IX.5 *HYPERPLANS*

Exercice 3 :

Soit E un $\mathbb{Q}$-ev admettant une base *dénombrable* $(e_i)_{i \in I}$ (I équipotent à $\mathbb{N}$). Montrer que l'ensemble E est dénombrable.

On considère alors $\mathbb{R}$ comme $\mathbb{Q}$-ev ; on admet l'existence d'une base $(x_i)_{i \in I}$ de ce $\mathbb{Q}$-ev (une telle base est dite *de Hamel*, mais on ne cherchera pas à en exhiber une !). Démontrer que I est équipotent à $\mathbb{R}$. Soit $i_0 \in I$ fixé, et soit φ la $\mathbb{Q}$-forme linéaire sur $\mathbb{R}$ associant, à tout $\xi \in \mathbb{R}$, *sa coordonnée sur* (x_{i_0}) *dans la base* (x_i). Démontrer que φ n'est pas continue sur $\mathbb{R}$, que $\mathrm{Ker}\,(\varphi)$ est partout dense dans $\mathbb{R}$, et que pour *tout* intervalle ouvert non vide U de $\mathbb{R}$, l'ensemble $\varphi(U)$ est partout dense dans $\mathbb{R}$. ■

Si le $\mathbb{Q}$-ev E admet une base dénombrable, on peut supposer que cette base est indexée par $\mathbb{N}$. Soit $(e_i)_{i \in \mathbb{N}}$ une telle base. Pour tout $n \in$

E_n le sous-$\mathbb{Q}$-ev de E engendré par la famille $(e_i)_{i\in[\![0,n-1]\!]}$. On voit que E_n est un $\mathbb{Q}$-ev de dimension n ; il est donc dénombrable puisqu'en bijection avec l'ensemble dénombrable $\mathbb{Q}^n$. Comme $E = \bigcup_{n\in\mathbb{N}^*} E_n$, on voit que E est dénombrable.

Nous supposerons connu que si un ensemble I est infini, $I\times I$ est équipotent à I (§II.3 exercice 10). Nous en déduisons que si I est infini, $\mathbb{N}\times I$ est équipotent à I. En effet, il existe une injection de I dans $\mathbb{N}\times I$ et puisqu'il existe une injection de $\mathbb{N}$ dans I (Théorème II.3.8), il existe une injection de $\mathbb{N}\times I$ dans $I\times I$, donc dans I ; d'après le théorème de Bernstein (II.3.10), les ensembles $\mathbb{N}\times I$ et I sont équipotents. On voit alors facilement par récurrence que pour tout entier $n\in\mathbb{N}^*$, les ensembles $\mathbb{Q}^n\times I^n$ et I sont équipotents.

Soit $(e_i)_{i\in I}$ une base du $\mathbb{Q}$-ev $\mathbb{R}$. Comme $\mathbb{R}$ n'est pas dénombrable, on voit d'après ce qui précède que I est nécessairement infini non dénombrable, et comme il existe une injection de I dans $\mathbb{R}$ ($i\mapsto e_i$), le "cardinal" de I est strictement plus grand que celui de $\mathbb{N}$ et inférieur ou égal à celui de $\mathbb{R}$. Si on admet l'hypothèse du continu (cf. §II.3), on peut affirmer que I est équipotent à $\mathbb{R}$, mais ce n'est pas nécessaire. Pour tout $n\in\mathbb{N}^*$, notons $\mathbb{R}_n$ l'ensemble des éléments de $\mathbb{R}$ qui ont un nombre $\leqslant n$ de coordonnées non nulles dans la base $(e_i)_{i\in I}$. L'ensemble $\mathbb{R}_n$ est l'image de l'application :

$$\varphi_n : \mathbb{Q}^n\times I^n\to\mathbb{R}\quad \big((r_1,r_2,\dots,r_n),(i_1,i_2,\dots,i_n)\big)\mapsto r_1\,e_{i_1}+\dots r_n\,e_{i_n}\ .$$

Il existe donc pour tout $n\in\mathbb{N}^*$ une surjection $\psi_n : I\to\mathbb{R}_n$. Il existe par conséquent une surjection $\psi : \mathbb{N}\times I\to\bigcup_{n\in\mathbb{N}^*}\mathbb{R}_n=\mathbb{R}$. Enfin, comme $\mathbb{N}\times I$ est équipotent à I, on voit qu'il existe une surjection de I dans $\mathbb{R}$, donc (axiome du choix) une injection de $\mathbb{R}$ dans I. Puisqu'il existe aussi une injection de I dans $\mathbb{R}$, on peut conclure en utilisant le théorème de Bernstein, que les ensembles I et $\mathbb{R}$ sont équipotents.

Soit φ une $\mathbb{Q}$-forme linéaire non nulle $\mathbb{R}\to\mathbb{Q}$. Son image est un sous-$\mathbb{Q}$-ev non nul de $\mathbb{Q}$, c'est donc $\mathbb{Q}$. Comme φ n'est pas injective il existe un réel non nul x tel que $x\in\mathrm{Ker}\,(\varphi)$. On voit que $\mathbb{Q}\cdot x\subset\mathrm{Ker}\,(\varphi)$; puisque $\mathbb{Q}\cdot x$ est, comme $\mathbb{Q}$, partout dense dans $\mathbb{R}$, il est clair que $\mathrm{Ker}\,(\varphi)$ est partout dense dans $\mathbb{R}$. Si φ était continue, son noyau serait un fermé de $\mathbb{R}$, donc égal à $\mathbb{R}$; l'application $\mathbb{Q}$-linéaire φ serait identiquement nulle, ce qui est faux.

Soit $U\subset\mathbb{R}$ un intervalle ouvert non vide. Montrons que $\varphi(U)=\mathbb{Q}$ (c'est a priori une partie de $\mathbb{Q}$), et que par conséquent $\varphi(U)$ est partout dense. On peut trouver deux rationnels q et r, $r>0$, tels que $[q-r,q+r]\subset U$. On voit que $\varphi(U)\supset\varphi([q-r,q+r])\ =\varphi(q)+\varphi([-r,+r])$. Il suffit donc de démontrer l'égalité : $\varphi([-r,+r])=\mathbb{Q}$.

L'ensemble $\varphi([-r,+r])$ est une partie de $\mathbb{Q}$ symétrique par rapport à 0. Montrons que c'est une partie non bornée (donc ni majorée, ni minorée). Supposons qu'il existe un rationnel $M > 0$ tel que pour tout $x \in [-r,r]$, $|\varphi(x)| \leqslant M$. Pour tout réel $x \neq 0$, on peut trouver un rationnel $q > 0$ tel que :

$$\frac{r}{2\,|x|} \leqslant q \leqslant \frac{r}{|x|} \quad \text{d'où} \quad \frac{r}{2} \leqslant |q\,x| \leqslant r\ .$$

Nous en déduisons :

$$|\varphi(q\,x)| \leqslant M \quad \text{d'où} \quad |\varphi(x)| \leqslant \frac{M}{q} \leqslant \frac{2\,M}{r}\,|x|\ .$$

Cette inégalité est aussi vérifiée si $x = 0$. On voit donc que pour tout $(x,x') \in \mathbb{R}^2$:

$$|\varphi(x') - \varphi(x)| = |\varphi(x'-x)| \leqslant \frac{2\,M}{r}\,|x'-x|\ .$$

L'application φ serait continue sur $\mathbb{R}$, ce qui est faux.
Nous avons donc démontré que $\varphi([-r,+r])$ n'est ni majorée, ni minorée.
Soient x_1 et x_2 des réels éléments de $[-r,+r]$. Pour tout rationnel $\lambda \in [0,1]$, $\lambda\,x_1 + (1-\lambda)\,x_2 \in [-r,+r]$, donc

$$\varphi(\lambda\,x_1 + (1-\lambda)\,x_2) = \lambda\,\varphi(x_1) + (1-\lambda)\,\varphi(x_2) \in \varphi([-r,+r])\ .$$

On voit donc que si les rationnels y_1 et y_2 sont dans $\varphi([-r,+r])$, tous les rationnels compris entre y_1 et y_2 sont aussi dans $\varphi([-r,+r])$. Comme $\varphi([-r,+r])$ n'est ni majorée ni minorée, il est clair que $\varphi([-r,+r]) = \mathbb{Q}$; ce qu'il fallait démontrer.

§ IX.6 *ENDOMORPHISMES. GROUPE LINÉAIRE*

Exercice 1 :

> Le corps de base K est fini, de cardinal q ; E est un K-ev de dimension $n \geqslant 1$.
> *a*) Quel est le cardinal de $\mathrm{GL}_K(E)$?
> *b*) Soit $p \in [\![0,n]\!]$ et $\mathcal{G}_p(E)$ l'ensemble des sous-K-ev de dimension p de E. En considérant l'opération à gauche de $\mathrm{GL}_K(E)$ sur l'ensemble $\mathcal{G}_p(E)$, trouver $\mathrm{card}\,(\mathcal{G}_p(E))$. ■

a) Nous avons démontré dans l'exercice 3 du §IX.3, que pour tout entier $p \leqslant n$, le nombre de suites $(x_1,\ldots,x_p)$ libres dans un K-ev de dimension n est :

$$\prod_{i=0}^{p-1}(q^n - q^i)\ .$$

Nous avons aussi démontré que le nombre d'automorphismes de l'espace E est le nombre de bases indexées par $[\![1,n]\!]$, c'est-à-dire :

$$\prod_{i=0}^{n-1}(q^n - q^i) .$$

b) Considérons l'application qui à un p-uplet libre dans le K-ev E fait correspondre le sous-K-ev de dimension p engendré. Un sous-K-ev F de dimension p étant donné, il est l'image par cette application des p-uplets libres dans ce K-ev F ; le nombre de ces p-uplets est donc :

$$\prod_{i=0}^{p-1}(q^p - q^i) .$$

Le nombre des sous-K-ev de dimension p est donc :

$$\frac{\prod_{i=0}^{p-1}(q^n - q^i)}{\prod_{i=0}^{p-1}(q^p - q^i)} .$$

Exercice 2 :

> Soit E un K-ev et $u \in \mathrm{Hom}_K(E)$. On note Φ_u (resp. Ψ_u) l'élément de $\mathrm{Hom}_K(\mathrm{Hom}_K(E))$ défini par $\Phi_u(v) = u \circ v$ (resp. $\Psi_u(v) = v \circ u$) pour $v \in \mathrm{Hom}_K(E)$. Si E est de dimension finie $n \geqslant 1$, et si $\mathrm{rg}(u) = r$, calculer $\mathrm{rg}(\Phi_u)$ et $\mathrm{rg}(\Psi_u)$ en fonction de n et r. ■

Pour u et v endomorphismes du K-ev E, $u \circ v = 0$ si, et seulement si, $\mathrm{Im}\,(v) \subset \mathrm{Ker}\,(u)$. Le noyau de l'application linéaire Φ_u est donc isomorphe au K-ev des applications linéaires $E \to \mathrm{Ker}\,(u)$. Il est donc de dimension :

$$\dim(\mathrm{Hom}_K(E, \mathrm{Ker}\,(u)) = \dim(E) \times \dim \mathrm{Ker}\,(u) = n\,(n-r) .$$

Le rang de Φ_u est donc :

$$\dim \mathrm{Hom}_K(E) - \dim \mathrm{Ker}\,(\Phi_u) = n^2 - n\,(n-r) = n\,r .$$

Le noyau N de l'application linéaire Ψ_u est l'ensemble des endomorphismes du K-ev E dont la restriction au sous-K-ev $\mathrm{Im}\,(u)$ est nulle

supplémentaire de $\mathrm{Im}\,(u)$. Considérons l'application qui à $v \in N$ fait correspondre sa restriction à S, c'est-à-dire $v \circ i_S$, où i_S est l'injection canonique $S \to E$. Cette application est K-linéaire. Elle est bijective, car comme $E = S \oplus \mathrm{Im}\,(u)$, pour toute application K-linéaire $g : S \to E$, il existe une et une seule application K-linéaire $E \to E$ dont la restriction à S est g et dont la restriction à $\mathrm{Im}\,(u)$ est nulle. Le noyau de Ψ_u est donc un K-ev isomorphe au K-ev $\mathrm{Hom}_K(S, E)$. Sa dimension est donc :

$$\dim \mathrm{Ker}\,(\Psi_u) = \dim S \times \dim E = (n - r)\, n\ .$$

Le rang de l'application K-linéaire Ψ_u est donc :

$$\dim \mathrm{Hom}_K(E) - \dim \mathrm{Ker}\,(\Psi_u) = n^2 - n\,(n - r) = n\,r\ .$$

Exercice 3 :

> Soit E un K-ev de dimension finie $n \geqslant 1$. Trouver les parties G de $\mathrm{Hom}_K(E) \setminus \mathrm{GL}_K(E)$ qui sont des groupes pour la loi $(u, v) \mapsto u \circ v$. ■

Soit e l'élément neutre d'un tel groupe. Comme $e \circ e = e$, l'endomorphisme e est un projecteur. Comme pour tout élément $f \in G$, $e \circ f = f$, on voit que pour tout $f \in G$, $\mathrm{Im}\,(f) \subset \mathrm{Im}\,(e)$. Comme pour tout $f \in G$, $f \circ e = f$, on voit que $\mathrm{Ker}\,(e) \subset \mathrm{Ker}\,(f)$. Pour tout $f \in G$, il existe un élément $g \in G$ tel que $f \circ g = e$, et $g \circ f = e$; donc $\mathrm{Im}\,(e) \subset \mathrm{Im}\,(f)$ et $\mathrm{Ker}\,(f) \subset \mathrm{Ker}\,(e)$. On voit donc que pour tout $f \in G$, $\mathrm{Im}\,(e) = \mathrm{Im}\,(f)$ et $\mathrm{Ker}\,(e) = \mathrm{Ker}\,(f)$. Nous en déduisons que si $(G, \circ)$ est un groupe qui coupe $\mathrm{GL}_K(E)$, alors son élément neutre est un projecteur de rang n ; c'est Id_E et $(G, \circ)$ est un sous-groupe de $\mathrm{GL}_K(E)$.

Soit e un projecteur du K-ev E. Notons G_e l'ensemble des endomorphismes f du K-ev E tels que $\mathrm{Im}\,(f) = \mathrm{Im}\,(e) = A$ et $\mathrm{Ker}\,(f) = \mathrm{Ker}\,(e) = B$. Considérons l'application $\Phi_e : G_e \to \mathrm{Hom}_K(A)$, qui à un élément de G_e fait correspondre l'endomorphisme du K-ev A qu'il induit sur $A = \mathrm{Im}\,(e)$; cet endomorphisme est injectif, car $\mathrm{Ker}\,(f) \cap \mathrm{Ker}\,(e) = \mathrm{Im}\,(e) \cap \mathrm{Ker}\,(e) = \{0\}$; c'est donc un automorphisme du K-ev A. L'application Φ_e est donc une application de G_e dans $\mathrm{GL}_K(A)$. Considérons inversement l'application Ψ_e qui à un élément $g \in \mathrm{GL}_K(A)$ fait correspondre $i_A \circ g \circ e$, élément de $\mathrm{Hom}_K E$. L'endomorphisme induit par $i_A \circ g \circ e$ sur le K-ev A est évidemment g ; et si $f \in G_e$, $i_A \circ \left(f|^A_A\right) \circ e = f$, car cet endomorphisme du K-ev E coïncide avec f sur les espaces A et $B = \mathrm{Ker}\,(f) = \mathrm{Ker}\,(e)$. Les applications Φ_e et Ψ_e sont donc bijectives réciproques l'une de l'autre. Comme Ψ_e est un homomorphisme pour la composition des applications linéaires, et que $(\mathrm{GL}_K(A), \circ)$ est un groupe, on voit que $(G_e, \circ)$ est aussi un groupe, isomorphe au groupe $(\mathrm{GL}_K(A), \circ)$.

Dans la première partie de cette résolution, nous avons remarqué que si $(G, \circ)$ était un groupe, alors il était inclus dans le groupe $(G_e, \circ)$, où e est son élément neutre (c'est un projecteur). Les parties G de $\mathrm{Hom}_K E \setminus \mathrm{GL}_K(E)$ telles que $(G, \circ)$ soit un groupe, sont donc les sous-groupes des groupes $(G_e, \circ)$, où e est un projecteur $\neq \mathrm{Id}_E$, du K-ev E.

Exercice 6 :

Soit E un K-ev de dimension finie $n \geqslant 2$. On donne des entiers $d_1, d_2, \ldots, d_p \geqslant 1$ tels que $d_1 + d_2 + \ldots + d_p = n$. Soit $\mathcal{S}(d_1, \ldots, d_p)$ l'ensemble des suites $(V_1, \ldots, V_p)$ de sous-K-ev de E tels que $\bigoplus_{i=1}^{p} V_i = E$, et $(\forall i \in [\![1, p]\!])\ \dim V_i = d_i$. Etudier l'action à gauche naturelle du groupe $\mathrm{GL}_K(E)$ sur $\mathcal{S}(d_1, \ldots, d_p)$. Si de plus K est fini, de cardinal q, trouver le cardinal d'une orbite et d'un stabilisateur. ■

Montrons que l'action du groupe $\mathrm{GL}_K(E)$ sur $\mathcal{S}(d_1, \ldots, d_p)$ est transitive. Si $(V_1, \ldots, V_p)$ et $(V'_1, \ldots, V'_p)$ sont des éléments de $\mathcal{S}(d_1, \ldots, d_p)$, comme pour tout $i \in [\![1, p]\!]$, $\dim V_i = \dim V'_i = d_i$, il existe une application K-linéaire injective $u_i : V_i \to E$ dont l'image est V'_i. Notons $q_1, \ldots, q_p$ les projecteurs dans la somme directe $E = \bigoplus_{i=1}^{p} V_i$, et considérons l'endomorphisme $u = \sum_{i=1}^{p} u_i \circ q_i$. Pour tout $x \in E$, si $x = x_1 + \ldots + x_p$, où pour tout $i \in [\![1, p]\!]$, $x_i \in V_i$, $u(x) = \sum_{i=1}^{p} u_i(x_i)$. Comme $E = \bigoplus_{i=1}^{p} V'_i$, et que pour tout $i \in [\![1, p]\!]$ u_i est injective d'image V'_i, on voit que u est un automorphisme du K-ev E. Il est clair que pour tout $i \in [\![1, p]\!]$, $u(V_i) = V'_i$; on a donc, pour l'opération à gauche du groupe $\mathrm{GL}_K(E)$ sur $\mathcal{S}(d_1, \ldots, d_p)$, $u \cdot (V_1, \ldots, V_p) = (V'_1, \ldots, V'_p)$. L'action du groupe $\mathrm{GL}_K(E)$ sur $\mathcal{S}(d_1, \ldots, d_p)$ est donc bien transitive.

Déterminons le stabilisateur S d'un élément $(V_1, \ldots, V_p)$ de $\mathcal{S}(d_1, \ldots, d_p)$. Les éléments de S sont les automorphismes u du K-ev E tels que pour tout $i \in [\![1, p]\!]$, $u(V_i) = V_i$. On voit donc le groupe S est isomorphe au groupe $\prod_{i=1}^{p} \mathrm{GL}_K(V_i)$.

Si K est fini de cardinal q, on sait que (cf. exercice 1) pour chaque $i \in [\![1, p]\!]$:

$$\mathrm{card}\,(\mathrm{GL}_K(V_i)) = \prod_{k=0}^{d_i - 1} (q^{d_i} - q^k)\ .$$

Le cardinal du stabilisateur d'un élément de $\mathcal{S}(d_1, \ldots, d_p)$ est, d'après ce qui précède :

$$\operatorname{card}(S) = \prod_{i=1}^{p} \prod_{k=0}^{d_i - 1} (q^{d_i} - q^k) \ .$$

Le cardinal de $\mathrm{GL}_K(E)$ est :

$$\operatorname{card}(\mathrm{GL}_K(E)) = \prod_{k=0}^{n-1} (q^n - q^k) \ .$$

Le cardinal de $\mathcal{S}(d_1, \ldots, d_p)$, qui est la seule orbite puisque l'opération est transitive, est donc :

$$\operatorname{card}(\mathcal{S}(d_1, \ldots, d_p)) = \frac{\displaystyle\prod_{k=0}^{n-1} (q^n - q^k)}{\displaystyle\prod_{i=1}^{p} \prod_{k=0}^{d_i - 1} (q^{d_i} - q^k)} \ .$$

Exercice 10 :

> Soit E un K-ev de dimension finie $n \geqslant 1$ et u et v deux endomorphismes de E ayant exactement le même noyau H et la même *image* G *de dimension 1*. Cela entraîne-t-il qu'il existe $\alpha \in K^*$ tel que $u = \alpha v$? ■

Comme u et v sont de rang 1, leur noyau commun H est de codimension 1, c'est un hyperplan du K-ev E. Soit a un élément de E qui n'est pas dans H, on sait que $E = Ka \oplus H$. Puisque $u(a)$ et $v(a)$ sont des éléments non nuls de la même droite G, il existe un scalaire $\alpha \in K^*$, tel que $u(a) = \alpha v(a)$. L'égalité $u(x) = \alpha v(x)$ est évidemment vraie pour $x \in Ka$ et pour $x \in H$, noyau commun de u et de v ; elle est donc vraie pour tout $x \in E$. Nous en déduisons $u = \alpha v$.

§ IX.7 *ÉLÉMENTS ALGÉBRIQUES D'UNE EXTENSION D'UN CORPS*

Exercice 6 :

> Soit $\theta = \sqrt[3]{2} + \sqrt{3}$: θ est un nombre algébrique.
>
> *a*) Trouver le polynôme minimal de θ sur $\mathbb{Q}$.
>
> *b*) Démontrer que $\mathbb{Q}[\theta] = \mathbb{Q}[\sqrt[3]{2}, \sqrt{3}]$.

c) Trouver tous les $\mathbb{Q}$-automorphismes (automorphismes de $\mathbb{Q}$-algèbre) du corps $\mathbb{Q}[\theta]$.

d) Trouver tous les sous-corps de $\mathbb{Q}[\theta]$. ■

a) *b*) Comme $(\theta - \sqrt{3})^3 = 2$, on voit que :

$$\theta^3 - 3\sqrt{3}\,\theta^2 + 9\theta - 3\sqrt{3} = 2 \quad \text{d'où} \quad \sqrt{3} = \frac{\theta^3 + 9\theta - 2}{3(\theta^2 + 1)} .$$

Nous en déduisons $\sqrt{3} \in \mathbb{Q}[\theta]$, et aussi $\sqrt[3]{2} = \theta - \sqrt{3} \in \mathbb{Q}[\theta]$. On voit donc que $\mathbb{Q}[\sqrt[3]{2}, \sqrt{3}] \subset \mathbb{Q}[\theta]$, et donc finalement que $\mathbb{Q}[\sqrt[3]{2}, \sqrt{3}] = \mathbb{Q}[\theta]$.

D'après ce qui précède :

$$27(\theta^2 + 1)^2 = (\theta^3 + 9\theta - 2)^2 .$$

Le réel θ est donc algébrique de degré $\leqslant 6$. On peut écrire les tours d'extensions :

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\theta) \quad \text{et} \quad \mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\theta) .$$

Le degré de θ sur $\mathbb{Q}$ est donc un multiple commun des degrés de $\sqrt{3}$ et de $\sqrt[3]{2}$; ce degré est donc 6. Le polynôme minimal de θ sur $\mathbb{Q}$ est donc le polynôme :

$$(X^3 + 9X - 2)^2 - 27(X^2 + 1)^2 = X^6 - 9X^4 - 4X^3 + 27X^2 - 36X - 23 .$$

c) Soit φ un automorphisme du corps $\mathbb{Q}(\theta)$ $(\subset \mathbb{R})$, $\varphi(\sqrt[3]{2})$ est un zéro réel du polynôme $X^3 - 2$, ce ne peut être que $\sqrt[3]{2}$; $\varphi(\sqrt{3})$ est un zéro réel du polynôme $X^2 - 3$, c'est donc $\sqrt{3}$ ou $-\sqrt{3}$. Il n'y a donc pour $\varphi(\theta)$ que deux possibilités, θ, et alors φ est l'identité, et $\theta' = \sqrt[3]{2} - \sqrt{3}$. Considérons de nouveau la tour d'extension :

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2})(\sqrt{3}) = \mathbb{Q}[\sqrt[3]{2}, \sqrt{3}] = \mathbb{Q}(\theta) .$$

Il est clair que l'application $\varphi : \mathbb{Q}(\sqrt[3]{2})(\sqrt{3}) \to \mathbb{Q}(\sqrt[3]{2})(\sqrt{3})$, telle que pour tout $(x, y) \in \left(\mathbb{Q}(\sqrt[3]{2})\right)^2$, $\varphi(x + y\sqrt{3}) = x - y\sqrt{3}$, est un automorphisme du corps $\mathbb{Q}(\sqrt[3]{2})(\sqrt{3}) = \mathbb{Q}(\theta)$, qui laisse le corps $\mathbb{Q}(\sqrt[3]{2})$ invariant. Comme $\varphi(\sqrt{3}) = -\sqrt{3}$, c'est le seul automorphisme du corps $\mathbb{Q}(\theta)$ différent de l'identité. Le corps $\mathbb{Q}(\theta)$ a donc deux automorphismes, qui sont l'identité et φ.

d) Soit K un corps tel que $\mathbb{Q} \subset K \subset \mathbb{Q}(\theta)$. A part si $K = \mathbb{Q}$ ou $K = \mathbb{Q}(\theta)$, comme :

$$6 = \dim_{\mathbb{Q}} \mathbb{Q}(\theta) = \dim_{\mathbb{Q}} K \times \dim_K \mathbb{Q}(\theta) ,$$

on voit que $\dim_{\mathbb{Q}} K = 2$ ou $\dim_{\mathbb{Q}} K = 3$.

Sous-corps de dimension 2 sur $\mathbb{Q}$.
Tout élément β irrationnel d'un tel corps K est de degré 2 sur $\mathbb{Q}$. On peut écrire :

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{3})(\beta) \subset \mathbb{Q}(\theta) .$$

Si l'extension $\mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{3})(\beta)$ était de degré 2, le degré de l'extension $\mathbb{Q} \subset \mathbb{Q}(\theta)$ serait divisible par 4, ce qui est faux. Le degré de l'extension $\mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{3})(\beta)$ est donc 1, c'est-à-dire $\beta \in \mathbb{Q}(\sqrt{3})$. Tout sous-corps K de $\mathbb{Q}(\theta)$, de dimension 2 sur $\mathbb{Q}$, est donc inclus dans $\mathbb{Q}(\sqrt{3})$, donc égal à $\mathbb{Q}(\sqrt{3})$. Le sous-corps $\mathbb{Q}(\sqrt{3})$ est donc le seul sous-corps de $\mathbb{Q}(\theta)$ de dimension 2 sur $\mathbb{Q}$.

Sous-corps de dimension 3 sur $\mathbb{Q}$.
Soit K un sous-corps de $\mathbb{Q}(\theta)$ de dimension 3 sur $\mathbb{Q}$, et γ un élément irrationnel de K. On peut écrire :

$$\mathbb{Q} \subset \mathbb{Q}(\gamma) \subset K .$$

Le degré de γ sur $\mathbb{Q}$ divise donc 3, et comme ce n'est pas 1, c'est 3 ; et par conséquent $\mathbb{Q}(\gamma) = K$. D'autre part :

$$\mathbb{Q} \subset K = \mathbb{Q}(\gamma) \subset \mathbb{Q}(\gamma)(\sqrt[3]{2}) \subset \mathbb{Q}(\theta) .$$

Soit d le degré de l'extension $K = \mathbb{Q}(\gamma) \subset \mathbb{Q}(\gamma)(\sqrt[3]{2})$. On voit que le degré de l'extension $\mathbb{Q} \subset \mathbb{Q}(\gamma)(\sqrt[3]{2})$ est $3d$, et qu'il divise 6. Nous en déduisons que d divise 2. Le polynôme minimal de $\sqrt[3]{2}$ sur le corps K est donc de degré 1 ou 2, et il divise dans $K[X]$ le polynôme $X^3 - 2$. Si le polynôme minimal P de $\sqrt[3]{2}$ sur le corps K était de degré 2, le quotient exact dans $K[X]$ de $X^3 - 2$ par P serait de degré 1, et le polynôme $X^3 - 2$ aurait un zéro dans K ($K \subset \mathbb{R}$), donc dans ce cas $\sqrt[3]{2} \in K$, ce qui est contradictoire. Nous en déduisons $d = 1$, $\sqrt[3]{2} \in K$, et finalement $K = \mathbb{Q}(\sqrt[3]{2})$.

Le corps $\mathbb{Q}(\theta)$ a donc 4 sous-corps, $\mathbb{Q}$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt[3]{2})$ et $\mathbb{Q}(\theta)$.

Exercice 7 :

Soit K le corps $\mathbb{Q}[\sqrt[3]{2}, \mathrm{j}]$ (où $\mathrm{j} = \exp(2\,\mathrm{i}\,\pi/3)$).
a) Si $\theta = \sqrt[3]{2} + \mathrm{j}\sqrt[3]{4}$, montrer que $K = \mathbb{Q}(\theta)$

polynôme minimal de θ sur $\mathbb{Q}$.

b) Prouver que le groupe des $\mathbb{Q}$-automorphismes de K est isomorphe à $\mathfrak{S}_3$.

c) Trouver tous les sous-corps de K. ■

a) Posons $\alpha = \sqrt[3]{2}$. On voit que $\theta = \alpha + \mathrm{j}\alpha^2$, que $\alpha^3 = 2$, et que $\theta \neq 0$ car $\mathrm{j} \notin \mathbb{R}$. On obtient :

$$\theta^3 = 2 + 4 + 6\theta\mathrm{j} \quad \text{d'où} \quad \mathrm{j} = \frac{\theta^3 - 6}{6\theta} .$$

Nous en déduisons $\mathrm{j} \in \mathbb{Q}(\theta)$. D'autre part :

$$\alpha\theta = \alpha^2 + 2\mathrm{j} \quad \text{soit} \quad \alpha^2 = \alpha\theta - 2\mathrm{j} ,$$

d'où :

$$\theta = \alpha + \mathrm{j}\alpha^2 = \alpha + \mathrm{j}\,(\alpha\theta - 2\mathrm{j}) \quad \text{soit} \quad \alpha(1 + \mathrm{j}\theta) = \theta + 2\mathrm{j}^2 .$$

Comme $1 + \mathrm{j}\theta$ et $\theta + 2\mathrm{j}^2$ ne sont pas tous les deux nuls, nous en déduisons :

$$\sqrt[3]{2} = \alpha = \frac{\theta + 2\mathrm{j}^2}{1 + \mathrm{j}\theta} \in \mathbb{Q}(\theta) .$$

Nous obtenons donc $\mathbb{Q}(\theta) = \mathbb{Q}[\sqrt[3]{2}, \mathrm{j}] = K$.

Comme :

$$\mathrm{j} = \frac{\theta^3 - 6}{6\theta} ,$$

nous en déduisons :

$$1 + \frac{\theta^3 - 6}{6\theta} + \frac{(\theta^3 - 6)^2}{36\theta^2} = 0 \quad \text{soit} \quad 36\theta^2 + 6\theta(\theta^3 - 6) + (\theta^3 - 6)^2 = 0 .$$

Nous en déduisons que le degré de θ est $\leqslant 6$. Comme :

$$\mathbb{Q} \subset \mathbb{Q}(\mathrm{j}) \subset \mathbb{Q}(\theta) \quad \text{et} \quad \mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\theta) ,$$

on voit que le degré de θ sur $\mathbb{Q}$ est un multiple de 3 et de 2 ; c'est donc 6, et le polynôme trouvé ci-dessus :

$$36X^2 + 6X(X^3 - 6) + (X^3 - 6)^2 = X^6 + 6X^4 - 12X^3 + 36X^2 - 36X + 36 ,$$

est son polynôme minimal sur $\mathbb{Q}$.

b) Les zéros dans $\mathbb{C}$ du polynôme $X^3 - 2$ sont $\alpha, \mathrm{j}\,\alpha$ et $\mathrm{j}^2\alpha$, ce sont tous des éléments de $\mathbb{Q}(\theta)$. Notons Z l'ensemble de ces zéros. Soit φ un automorphisme du corps $\mathbb{Q}(\theta)$, l'ensemble Z de cardinal 3 est stable par φ, et φ induit sur Z une permutation $\sigma_\varphi = \varphi|_Z^Z$. L'application $\varphi \mapsto \sigma_\varphi$, est visiblement un homomorphisme du groupe des automorphismes du corps $\mathbb{Q}(\theta)$ dans le groupe $\mathfrak{S}_Z$. C'est un homomorphisme injectif, car si $\varphi(\alpha) = \alpha$ et $\varphi(\mathrm{j}\,\alpha) = \mathrm{j}\,\alpha$, alors $\varphi(\mathrm{j}) = \mathrm{j}$, d'où $\varphi(\theta) = \theta$; donc pour tout polynôme $P \in \mathbb{Q}[X]$, $\varphi(P(\theta)) = P(\varphi(\theta)) = P(\theta)$, donc $\varphi = \mathrm{Id}_{\mathbb{Q}(\theta)}$.

Montrons que cet homomorphisme de groupes est surjectif.
Le corps $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt[3]{2})(\mathrm{j})$ est stable par la conjugaison, car $\bar{\mathrm{j}} = -1 - \mathrm{j}$. La conjugaison de $\mathbb{C}$ induit donc un automorphisme involutif ψ de $\mathbb{Q}(\theta)$ qui échange $\mathrm{j}\,\alpha$ et $\mathrm{j}^2\alpha$. Par conséquent σ_ψ est la transposition $\tau_{\mathrm{j}\,\alpha, \mathrm{j}^2\alpha}$.
Notons $L = \mathbb{Q}(\mathrm{j})$, de telle sorte que $\mathbb{Q}(\theta) = L(\alpha)$. On a

$$\dim_{\mathbb{Q}}(\mathbb{Q}(\theta)) = 6 = \dim_{\mathbb{Q}}(L)\,\dim_L(L(\alpha)) = 2\,\dim_L(L(\alpha))\ .$$

Nous en déduisons que $\dim_L(L(\alpha)) = 3$ et que le polynôme minimal de α sur L est le polynôme $X^3 - 2$ (et $L \cap Z = \emptyset$). On voit aussi que $\mathbb{Q}(\theta) = L(\mathrm{j}\,\alpha)$.
Considérons alors les homomorphismes surjectifs d'anneaux $L[X] \to \mathbb{Q}(\theta)$, $f : P \mapsto P(\alpha)$ et $g : P \mapsto P(\mathrm{j}\,\alpha)$. Ces homomorphismes d'anneaux ont pour noyau l'idéal engendré par le polynôme $X^3 - 2$, irréductible dans $L[X]$. On obtient donc des homomorphismes factorisés :

$$\bar{f} : L[X]/_{(X^3 - 2)\,L[X]} \to \mathbb{Q}(\theta) \quad \text{et} \quad \bar{g} : L[X]/_{(X^3 - 2)\,L[X]} \to \mathbb{Q}(\theta)\ ,$$

qui sont des isomorphismes d'anneaux, donc de corps. L'application $\varphi = \bar{g} \circ \bar{f}^{-1}$ est un automorphisme du corps $\mathbb{Q}(\theta)$, qui laisse invariant le sous-corps $L = \mathbb{Q}(\mathrm{j})$, et on vérifie que $\varphi(\alpha) = \mathrm{j}\,\alpha$. On obtient $\varphi(\mathrm{j}\,\alpha) = \mathrm{j}\,\varphi(\alpha) = \mathrm{j}^2\alpha$, et $\varphi(\mathrm{j}^2\alpha) = \mathrm{j}^3\alpha = \alpha$. On voit donc que σ_φ est le 3-cycle $\langle \alpha, \mathrm{j}\,\alpha, \mathrm{j}^2\alpha \rangle$.
Nous avons démontré que le sous-groupe des permutations de Z induites sur Z par les automorphismes du corps $\mathbb{Q}(\theta)$ contient une transposition et un cycle d'ordre 3, c'est donc le groupe $\mathfrak{S}_Z$. Le groupe des automorphismes du corps $\mathbb{Q}(\theta)$ est donc isomorphe à $\mathfrak{S}_3$.

c) Nous reprenons ici la méthode utilisée dans l'exercice précédent. Soit L un corps tel que $\mathbb{Q} \subset L \subset \mathbb{Q}(\theta)$. A part si $L = \mathbb{Q}$ ou $L = \mathbb{Q}(\theta)$, comme :

$$6 = \dim_{\mathbb{Q}} \mathbb{Q}(\theta) = \dim_{\mathbb{Q}} L \times \dim_L \mathbb{Q}(\theta)\ ,$$

on voit que $\dim_{\mathbb{Q}} L = 2$ ou $\dim_{\mathbb{Q}} L = 3$.

Sous-corps de dimension 2 sur $\mathbb{Q}$.
Tout élément β irrationnel d'un tel corps L est de degré 2 sur $\mathbb{Q}$. On peut écrire :

$$\mathbb{Q} \subset \mathbb{Q}(\mathrm{j}) \subset \mathbb{Q}(\mathrm{j})(\beta) \subset \mathbb{Q}(\theta)\ .$$

Si l'extension $\mathbb{Q}(\mathrm{j}) \subset \mathbb{Q}(\mathrm{j})(\beta)$ était de degré 2, le degré de l'extension $\mathbb{Q} \subset \mathbb{Q}(\theta)$ serait divisible par 4, ce qui est faux. Le degré de l'extension $\mathbb{Q}(\mathrm{j}) \subset \mathbb{Q}(\mathrm{j})(\beta)$ est donc 1, c'est-à-dire $\beta \in \mathbb{Q}(\mathrm{j})$. Tout sous-corps L de $\mathbb{Q}(\theta)$, de dimension 2 sur $\mathbb{Q}$, est donc inclus dans $\mathbb{Q}(\mathrm{j})$, donc égal à $\mathbb{Q}(\mathrm{j})$. Le sous-corps $\mathbb{Q}(\mathrm{j})$ est donc le seul sous-corps de $\mathbb{Q}(\theta)$ de dimension 2 sur $\mathbb{Q}$.

Sous-corps de dimension 3 sur $\mathbb{Q}$.
Soit L un sous-corps de $\mathbb{Q}(\theta)$ de dimension 3 sur $\mathbb{Q}$, et γ un élément irrationnel de L. On peut écrire :

$$\mathbb{Q} \subset \mathbb{Q}(\gamma) \subset L\ .$$

Le degré de γ sur $\mathbb{Q}$ divise donc 3, et comme ce n'est pas 1, c'est 3 ; et par conséquent $\mathbb{Q}(\gamma) = L$. D'autre part :

$$\mathbb{Q} \subset L = \mathbb{Q}(\gamma) \subset \mathbb{Q}(\gamma)(\sqrt[3]{2}) \subset \mathbb{Q}(\theta)\ .$$

Soit d le degré de l'extension $L = \mathbb{Q}(\gamma) \subset \mathbb{Q}(\gamma)(\sqrt[3]{2})$. On voit que le degré de l'extension $\mathbb{Q} \subset \mathbb{Q}(\gamma)(\sqrt[3]{2})$ est $3d$, et qu'il divise 6. Nous en déduisons que d divise 2. Le polynôme minimal P de $\sqrt[3]{2}$ sur le corps L est donc de degré 1 ou 2, et il divise dans $L[X]$ le polynôme $X^3 - 2$. Si P est de degré 1, alors $\sqrt[3]{2} \in L$. Si P est de degré 2, le quotient exact dans $L[X]$ de $X^3 - 2$ par P est de degré 1, et le polynôme $X^3 - 2$ a un zéro dans L, donc dans ce cas, comme $\alpha = \sqrt[3]{2} \notin L$, on voit que $\mathrm{j}\alpha \in L$ ou $\mathrm{j}^2\alpha \in L$. On voit donc que dans tous les cas, le corps L contient l'un des zéros du polynôme $X^3 - 2$. Comme ces zéros sont tous de degré 3 sur $\mathbb{Q}$, le corps L est nécessairement l'un des corps $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\mathrm{j}\alpha)$ ou $\mathbb{Q}(\mathrm{j}^2\alpha)$. Le sous-corps $\mathbb{Q}(\alpha)$, qui est inclus dans $\mathbb{R}$, est bien distinct des deux autres. Ces trois corps sont $\mathbb{Q}(\alpha)$, $\varphi(\mathbb{Q}(\alpha)), \varphi^2(\mathbb{Q}(\alpha))$, où φ est l'automorphisme d'ordre 3 que nous avons mis en évidence dans la question précédente. Comme $\mathbb{Q}(\alpha) \neq \varphi(\mathbb{Q}(\alpha))$, nous en déduisons $\varphi(\mathbb{Q}(\alpha)) \neq \varphi^2(\mathbb{Q}(\alpha))$. Ces trois sous-corps sont donc bien distincts.

Le corps $\mathbb{Q}(\theta)$ a donc 6 sous-corps, $\mathbb{Q}$, $\mathbb{Q}(\mathrm{j})$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\mathrm{j}\sqrt[3]{2})$, $\mathbb{Q}(\mathrm{j}^2\sqrt[3]{2})$ et $\mathbb{Q}(\theta)$.

Exercice 13 (discriminant du polynôme cyclotomique) **:**

On fixe $n \in \mathbb{N}^*$, $n > 2$. On note $\mathcal{P}_n$ l'ensemble des racines primitives n-ièmes de 1 dans $\mathbb{C}$ et par S_n le *support premier* de l'entier n. On se propose de calculer $\Delta_n = \prod_{1 \leqslant i < j \leqslant \varphi(n)} (t_i - t_j)^2$, où $(t_k)_{1 \leqslant k \leqslant \varphi(n)}$ est un numérotage de $\mathcal{P}_n$. On note $\Phi_n(X)$ le polynôme cyclotomique $\prod_{1 \leqslant k \leqslant \varphi(n)} (X - t_k)$.

a) Soit $D_n = \prod_{\zeta \in \mathcal{P}_n} \Phi'_n(\zeta)$. Calculer Δ_n en fonction de D_n.

b) Pour $I \subset S_n$, soit $P_I = \prod_{p \in I} p$, $N_I = \dfrac{n}{P_I}$ et $[I] = \text{card}\,(I)$.

Exprimer $\Phi'_n(X)$ à l'aide des $[I]$, des N_I et des P_I (cf. exercice 12 *b*)). Montrer, si $\zeta \in \mathcal{P}_n$:

$$\Phi'_n(\zeta) = n\,\zeta^{n-1} \prod_{J \subset S_n,\, J \neq \emptyset} \left(\zeta^{N_J} - 1\right)^{\left((-1)^{[J]}\right)} .$$

Montrer :

$$D_n = s_n\, n^{\varphi(n)} \prod_{J \subset S_n,\, J \neq \emptyset} \left\{ \prod_{\zeta \in \mathcal{P}_n} \left(\zeta^{N_J} - 1\right) \right\}^{\left((-1)^{[J]}\right)} ,$$

avec $s_n = \prod_{\zeta \in \mathcal{P}_n} \zeta$.

c) Montrer : $\varphi(n) = \sum_{d \mid n} \mu(d) \dfrac{n}{d}$, où μ est la fonction de Möbius (cf. exercice 12). Calculer $\prod_{d \mid n} s_d$ et en déduire $s_n = (-1)^{\varphi(n)}$.

d) Soit $J \subset S_n$, $J \neq \emptyset$. On pose $H_J = \prod_{\zeta \in \mathcal{P}_n} \left(\zeta^{N_J} - 1\right)$ et $E_J = \dfrac{\varphi(n)}{\varphi(P_J)}$.

d_1) Montrer $H_J = [\Phi_{P_J}(1)]^{E_J} \times (-1)^{\varphi(n)}$ (observer que ζ^{N_J} est une racine primitive P_J-ième de 1 et calculer combien de fois on trouve ainsi ces racines).

d_2) On pose pour tout entier $m > 1$, $g(m) = \Phi_m(1)$, et $g(1) = 1$. Montrer que pour tout $m \geqslant 1$:

$$g(m) = \prod_{d \mid m} \left(\frac{m}{d}\right)^{\mu(d)} ,$$

(cf. exercice 12). En déduire que pour tout $d \geqslant 1$:

$$g(d) = \begin{cases} p \text{ si } d \text{ est de la forme } p^\alpha,\ p \text{ premier},\ \alpha \in \mathbb{N}^* ; \\ 1 \text{ sinon.} \end{cases}$$

e) Montrer, si $J \subset S_n$, $J \neq \emptyset$:

$$H_J = (-1)^{\varphi(n)} \text{ si } [J] \geqslant 2 ,$$

et

$$H_J = p^{\varphi(n)/(p-1)} \times (-1)^{\varphi(n)} \text{ si } J = \{p\} \ .$$

f) Etablir l'égalité :

$$\Delta_n = (-1)^{\frac{1}{2}\varphi(n)} \times \frac{n^{\varphi(n)}}{\prod\limits_{p \in S_n} p^{\frac{\varphi(n)}{p-1}}} \ .$$

dite "formule du discriminant". ■

a) Nous utiliserons le lemme suivant :

Lemme :

Soit K un corps, $n \in \mathbb{N}$, $n \geqslant 1$, et $(x_1, \ldots, x_n)$, une famille d'éléments de K. Le *discriminant* du polynôme

$$P = (X - x_1) \ldots (X - x_n) \ ,$$

est $\Delta(P) = \prod\limits_{(i,j) \in [\![1,n]\!]^2,\ i \neq j} (x_i - x_j)^2 \ .$

On a l'égalité :

$$\Delta(P) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \in [\![1,n]\!]} P'(x_i) \ . \blacksquare$$

Pour tout $i \in [\![1, n]\!]$, posons $P = (X - x_i) P_i$. En dérivant nous obtenons $P' = (X - x_i) P_i' + P_i$, d'où en prenant la valeur en x_i,

$$P'(x_i) = P_i(x_i) = \prod_{j \in [\![1,n]\!],\ j \neq i} (x_i - x_j) \ .$$

Nous obtenons enfin :

$$\prod_{i=1}^{n} P'(x_i) = \prod_{(i,j) \in [\![1,n]\!]^2,\ i \neq j} (x_i - x_j) \ .$$

On voit bien que ce produit est au signe près le discriminant. On peut écrire (les couples (i, j) variant toujours dans $[\![1, n]\!]^2$) :

$$\prod_{i \neq j} (x_i - x_j) = \prod_{i<j} (x_i - x_j) \times \prod_{j<i} (x_i - x_j) = \prod_{i<j} (x_i - x_j) \times \prod_{i<j} (x_j - x_i) \ .$$

Chacun de ces produits est formé de $\frac{n(n-1)}{2}$ facteurs, donc :

$$\prod_{i \neq j} (x_i - x_j) = \prod_{i<j} (x_i - x_j) \times (-1)^{\frac{n(n-1)}{2}} \prod_{i<j} (x_i - x_j) = (-1)^{\frac{n(n-1)}{2}} \prod (x_i - x_i)^2 \ .$$

Nous en déduisons finalement l'égalité :

$$\Delta(P) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \in [\![1,n]\!]} P'(x_i) \ .$$

Fin du lemme.

Nous appliquerons ce lemme au polynôme Φ_n, qui est de degré $\varphi(n)$. Remarquons que puisque $n > 2$, soit n a au moins un facteur premier impair p, et $\varphi(n)$ est un nombre pair puisqu'il est divisible par $p-1$, soit $n = 2^k$, où $k > 1$, et $\varphi(n) = 2^{k-1}$ est aussi un nombre pair. On voit donc que :

$$(-1)^{\frac{\varphi(n)(\varphi(n)-1)}{2}} = (-1)^{\frac{\varphi(n)}{2}(\varphi(n)-1)} = (-1)^{\frac{\varphi(n)}{2}} \ .$$

En appliquant le lemme nous trouvons donc :

$$\Delta_n = (-1)^{\frac{\varphi(n)}{2}} D_n \ .$$

b) D'après le *c*) de l'exercice 12, on a :

$$\Phi_n = \prod_{d \mid n} \left(X^{\frac{n}{d}} - 1\right)^{\mu(d)} \ .$$

Comme $\mu(d) = 0$ si d n'est pas l'un des entiers P_I, où $I \subset S_n$, on peut ne garder que ces facteurs. Si $d = P_I$, alors $\dfrac{n}{d} = N_I$, et $\mu(d) = (-1)^{[I]}$. Nous obtenons la formule :

$$\Phi_n = \prod_{I \subset S_n,\, I \neq \emptyset} \left(X^{N_I} - 1\right)^{\left((-1)^{[I]}\right)} \times (X^n - 1) = \Psi_n(X)\,(X^n - 1) \ ,$$

où $\Psi_n(X)$ est une fraction rationnelle. En dérivant nous obtenons :

$$\Phi'_n = n\,X^{n-1}\,\Psi_n(X) + (X^n - 1)\,\Psi'_n(X) \ .$$

Pour tout $\zeta \in \mathcal{P}_n$, $\zeta^n - 1 = 0$; au contraire, comme ζ est une racine primitive d'ordre n, les nombres $\zeta^{N_I} - 1$, où $I \subset S_n$, $I \neq \emptyset$, sont tous non nuls car N_I est un diviseur strict de n. Donc :

$$\Phi'_n(\zeta) = n\,\zeta^{n-1}\,\Psi_n(\zeta) = n\,\zeta^{-1} \prod_{I \subset S_n,\, I \neq \emptyset} \left(\zeta^{N_I} - 1\right)^{\left((-1)^{[I]}\right)} \ .$$

Le nombre complexe D_n est le produit de ces nombres pour $\zeta \in \mathcal{P}_n$. On en déduit donc facilement l'égalité :

$$D_n = s_n\, n^{\varphi(n)} \prod_{J \subset S_n,\, J \neq \emptyset} \left\{ \prod_{\zeta \in \mathcal{P}_n} (\zeta^{N_J} - 1) \right\}^{\left((-1)^{[J]}\right)} ,$$

avec

$$s_n = \prod_{\zeta \in \mathcal{P}_n} \zeta^{-1} = \prod_{\zeta \in \mathcal{P}_n} \zeta \, .$$

c) On sait que pour tout $n \in \mathbb{N}^*$:

$$n = \sum_{d \mid n} \varphi(d) \, .$$

D'après la formule d'inversion donnée dans le *b*) de l'exercice 12, appliquée au groupe abélien $\mathbb{Z}$, pour tout $n \in \mathbb{N}^*$:

$$\varphi(n) = \sum_{d \mid n} \mu(d) \frac{n}{d} \, .$$

Il est clair que $\prod_{d \mid n} s_d$ est le produit de toutes les racines n-ième de l'unité, c'est-à-dire $(-1)^{n-1}$. En utilisant la formule d'inversion dans le groupe multiplicatif des rationnels non nuls, nous obtenons pour tout $n \geqslant 1$:

$$s_n = \prod_{d \mid n} \left((-1)^{\frac{n}{d}-1}\right)^{\mu(d)} \, .$$

Pour tout $n > 1$, comme :

$$\sum_{d \mid n} \mu(d) = 0 \quad \text{et} \quad \varphi(n) = \sum_{d \mid n} \mu(d) \frac{n}{d} \, ,$$

on voit que $s_n = (-1)^{\varphi(n)}$. Remarquons pour conclure que $s_1 = 1$, $s_2 = -1$, et que pour tout $n > 2$, $s_n = 1$, puisque $\varphi(n)$ est alors pair.

Nous aurions pu aussi reprendre la formule donnée dans l'exercice 12 *c*) : pour tout $n > 1$

$$\Phi_n = \prod_{d \mid n} (X^{\frac{n}{d}} - 1)^{\mu(d)} \, .$$

Nous en déduisons :

$$\Phi_n(0) = (-1)^{\varphi(n)} s_n = \prod_{d \mid n} (-1)^{\mu(d)} \, ,$$

et comme $\sum_{d \mid n} \mu(d) = 0$, puisque $n > 1$, on voit que :

$$s_n = (-1)^{\varphi(n)} = 1 .$$

d) 1) Considérons l'application f qui à $\zeta \in \mathcal{P}_n$ fait correspondre ζ^{N_J}. Il est clair que cette application est à valeurs dans $\mathcal{P}_{(N/N_J)} = \mathcal{P}_{P_J}$. Si cette application vérifie les hypothèses du théorème du Berger, alors chaque racine primitive d'ordre P_J est l'image du même nombre de racines primitives d'ordre n, ce nombre ne pouvant être qu'égal à $\varphi(n)/\varphi(P_J)$. Il suffit donc de démontrer que f vérifie les hypothèses du théorème du Berger.

Soient α et β deux éléments de $\mathcal{P}_{P_J}$. Il existe un entier k_0, premier avec P_J tel que $\beta = \alpha^{k_0}$. Il y a d'autres solutions : tous les entiers de la forme $k = k_0 + m\,P_J$. Si k est un tel entier, et que $\zeta^{N_I} = \alpha$, alors $\left(\zeta^k\right)^{N_I} = \alpha^k = \beta$. S'il existe un tel entier k premier avec n, alors l'application $\zeta \mapsto \zeta^k$ établira une bijection entre l'ensemble des solutions dans $\mathcal{P}_n$ de l'équation $\zeta^{N_I} = \alpha$, et l'ensemble des solutions dans $\mathcal{P}_n$ de l'équation $\zeta^{N_I} = \beta$; les deux ensembles auront même cardinal, ce qu'il faut démontrer.

Montrons que si k_0 est un entier premier avec P_J, il existe des entiers k premiers avec n de la forme $k_0 + m\,P_J$. Ces entiers sont évidemment tous premiers avec tous les nombres premiers éléments de J. Pour que $k = k_0 + m\,P_J$ soit premier avec n, il faut et il suffit qu'il ne soit divisible par aucun nombre premier $p \in S_n \setminus J$. Nous obtenons les conditions :

$$(\forall\, p \in S_n \setminus J) \quad k_0 + m\,P_J \not\equiv 0 \bmod (p) .$$

Comme dans la condition ci-dessus, P_J est premier avec p, il existe pour tout p fixé une solution pour m, et d'après le théorème Chinois, une solution pour m qui convienne pour tout $p \in S_n \setminus J$.

La fonction f vérifie donc les hypothèses du théorème du Berger. Nous en déduisons comme annoncé que si ζ décrit $\mathcal{P}_n$, ζ^{N_J} décrit $\mathcal{P}_{P_J}$, chaque élément de $\mathcal{P}_J$ étant répété un nombre de fois égal à $E_J = \varphi(n)/\varphi(P_J)$. Nous obtenons par conséquent l'égalité :

$$H_J = (-1)^{\varphi(n)} \prod_{\zeta \in \mathcal{P}_n} \left(1 - \zeta^{N_J}\right) =$$

$$= (-1)^{\varphi(n)} \left(\prod_{\alpha \in \mathcal{P}_{P_J}} (1 - \alpha) \right)^{E_J} = (-1)^{\varphi(n)} \left(\Phi_{P_J}(1)\right)^{E_J} .$$

2) Nous savons que (cf. exercice 12 *c*)), pour tout $m > 1$:

$$\Phi_m(X) = \prod_{d \mid m} \left(\frac{X^{\frac{m}{d}} - 1}{X - 1} \right)^{\mu(d)} .$$

En effectuant la division par $X - 1$ et en substituant 1 à X, nous obtenons pour tout entier $m > 1$ l'égalité :

$$g(m) = \prod_{d \mid m} \left(\frac{m}{d} \right)^{\mu(d)} .$$

Cette formule est aussi vérifiée si $m = 1$, puisque $g(1) = 1$ et $\mu(1) = 1$. Posons pour tout $m \in \mathbb{N}^*$, $h(m) = 1$ sauf si $m = p^\alpha$, où p est premier et $\alpha \in \mathbb{N}^*$, auquel cas $h(m) = p$. On vérifie que pour tout $m \geqslant 1$:

$$m = \prod_{d \mid m} h(d) .$$

En effet, pour p diviseur premier de m donné, le nombre de puissances de p (de la forme p^α, où $\alpha > 0$) qui divisent m est égal à la puissance de p dans le développement en produit de facteurs premiers de l'entier m. Nous en déduisons par la formule d'inversion que pour tout $m \geqslant 1$:

$$h(m) = \prod_{d \mid m} \left(\frac{m}{d} \right)^{\mu(d)} = g(m) ,$$

ce qu'il fallait démontrer.

e) Si J est une partie non vide de S_n, alors $P_J \neq 1$. Nous en déduisons l'égalité :

$$H_J = (-1)^{\varphi(n)} \, (g(P_J))^{E_J} .$$

Pour toute partie J qui n'est pas un singleton, P_J n'est pas une puissance de nombre premier donc $g(P_J) = 1$. On obtient alors :

$$H_J = (-1)^{\varphi(n)} = 1 .$$

Si $J = \{p\}$, alors $g(P_J) = p$, $[J] = 1$ et :

$$E_J = \frac{\varphi(n)}{\varphi(P_J)} = \frac{\varphi(n)}{\varphi(p)} = \frac{\varphi(n)}{p - 1} .$$

Nous obtenons l'égalité :

$$H_J = (-1)^{\varphi(n)} \, p^{\frac{\varphi(n)}{p-1}} = p^{\frac{\varphi(n)}{p-1}} .$$

f) D'après le *b*), nous avons l'égalité :

$$D_n = s_n\, n^{\varphi(n)} \prod_{J \subset S_n,\, J \neq \emptyset} H_J^{\left((-1)^{[J]}\right)} .$$

D'après la question *c*), $s_n = 1$, et en utilisant la question précédente nous obtenons l'égalité :

$$D_n = n^{\varphi(n)} \prod_{p \in S_n} \left(p^{\frac{\varphi(n)}{p-1}}\right)^{\left((-1)^1\right)} = \frac{n^{\varphi(n)}}{\prod\limits_{p \in S_n} p^{\frac{\varphi(n)}{p-1}}} .$$

Enfin, en utilisant le *a*), nous obtenons la valeur du discriminant du polynôme cyclotomique Φ_n :

$$\Delta_n = (-1)^{\frac{1}{2}\varphi(n)} \frac{n^{\varphi(n)}}{\prod\limits_{p \in S_n} p^{\frac{\varphi(n)}{p-1}}} .$$

Chapitre X

FONCTIONS POLYNOMIALES SUR K^n; ÉQUATIONS ALGÉBRIQUES

§ X.1 *POLYNÔMES À n LETTRES*

Exercice 1 :

Le corps de base est $K = \mathbb{R}$ (ou $K = \mathbb{C}$). On donne $n \in \mathbb{N}^*$. Une fonction polynomiale $f : K^n \to K$ est supposée nulle au voisinage d'un point $a \in K^n$. Montrer que $f = 0$; donc, si $f \neq 0$, $\{x \in K^n \mid f(x) \neq 0\}$ est un ouvert dense de K^n. ■

Il existe un réel $\varepsilon > 0$ tel que pour tout x appartenant à une boule de centre 0 et de rayon ε, $f(x) = 0$. On peut prendre sur l'espace K^n une norme telle que pour cette norme, la boule de centre 0 et de rayon ε soit le produit cartésien $E_1 \times E_2 \times \ldots \times E_n$, où pour tout $i \in [\![1, n]\!]$, $E_i = \{t \in K ; |t| < \varepsilon\}$. Chacun de ces ensembles étant infini, on peut appliquer le théorème X.1.2, et conclure $f = 0$.

Exercice 2 :

Le corps de base est $K = \mathbb{R}$ ou $K = \mathbb{C}$ et $n \in \mathbb{N}^*$. Soit une fonction $f : K^n \to K$ telle que tout point $a \in K^n$ possède un voisinage V_a pour lequel $f_{|V_a}$ est polynomiale. Montrer que f est polynomiale. ■

Remarquons que si P et Q sont deux applications polynomiales sur K^n qui coïncident dans un voisinage de $a \in K^n$, alors $P = Q$ (cf. exercice 1). Choisissons pour tout $a \in K^n$ un voisinage ouvert V_a tel que $f_{|V_a}$ soit polynomiale, et considérons l'application φ qui à $a \in K^n$ fait correspondre l'application polynomiale $P_a : K^n \to K$, qui coïncide avec f sur V_a. L'application φ est localement constante : si $b \in V_a$, P_b et P_a coïncident sur l'ouvert non vide $V_a \cap V_b$, donc $P_a = P_b$. Comme K^n est un espace métrique connexe, nous pouvons en déduire que φ e

L'application f coïncide sur K^n avec l'application polynomiale P, qui est la valeur constante de φ. L'application f est donc polynomiale.

Exercice 5 :

> Soit K un corps commutatif. On donne $f : K^2 \to K$ possédant les propriétés suivantes : pour tout $x \in K$, la fonction $f_x : K \to K$, $y \mapsto f(x,y)$ est polynomiale et pour tout $y \in K$, la fonction $f^y : K \to K$, $x \mapsto f(x,y)$ est polynomiale.
>
> *a*) Si $K = \mathbb{R}$ ou $\mathbb{C}$, montrer que f est polynomiale.
>
> *b*) Si $K = \mathbb{Q}$, montrer que f n'est pas nécessairement polynomiale. ■

a) Montrons que si f vérifie les hypothèses de l'énoncé et que le corps de base n'est pas dénombrable, alors f est polynomiale.

Pour tout $n \in \mathbb{N}$, posons $U_n = \{x \mid f_x \in K_n[X]\}$. La suite $(U_n)_{n\in\mathbb{N}}$ est une suite croissante de parties de K et, d'après l'hypothèse, $\bigcup_{n\in\mathbb{N}} U_n = K$. Si l'ensemble U_n était fini pour tout $n \in \mathbb{N}$, l'ensemble K serait dénombrable, ce qui est contraire à l'hypothèse. Nous en déduisons qu'il existe un entier n tel que U_n est infini. Prenons alors $n+1$ éléments distincts dans K, $y_0, y_1, \ldots, y_n$, et notons P_j, pour tout $j \in [\![0,n]\!]$, le polynôme dont la fonction polynomiale est f^{y_j} (donc $f(x,y_j) = P_j(x)$ pour tout $x \in K$). Pour tout x fixé dans U_n, l'application $y \mapsto f(x,y)$ est une application polynomiale de degré $\leqslant n$, qui prend en les $n+1$ éléments $y_0, \ldots, y_n$ les valeurs $P_0(x), \ldots, P_n(x)$. C'est donc la fonction polynomiale donnée par la formule d'interpolation de Lagrange :

$$(1) \qquad \sum_{j=0}^{n} P_j(x) \frac{\prod_{i\neq j}(y - y_i)}{\prod_{i\neq j}(y_j - y_i)} = Q(x,y) \ .$$

Pour tout $x \in U_n$ et pour tout $y \in K$, on a l'égalité $f(x,y) = Q(x,y)$. Comme U_n est infini, nous en déduisons $f = Q$, et par conséquent que l'application f est polynomiale.

b) Montrons maintenant que si le corps K est dénombrable (ce qui est le cas pour le corps $\mathbb{Q}$), il existe des applications f qui vérifient les conditions de l'énoncé, et qui ne sont pas polynomiales.

Soit $(r_n)_{n\in\mathbb{N}}$ une suite qui établit une bijection $\mathbb{N}\to K$. Posons pour tout $(x,y)\in K^2$:

$$f(x,y)=\sum_{n\in\mathbb{N}}\prod_{i=0}^{n}(x-r_i)(y-r_i)\ .$$

Cette formule a bien un sens, car si $(x,y)\in K^2$, il existe $j\in\mathbb{N}$ tel que $x=r_j$, et pour tout $n\geqslant j$, $\prod_{i=0}^{n}(x-r_i)(y-r_i)=0$.

Pour tout $x\in K$ fixé, si $x=r_j$, d'après ce qui précède, pour tout $y\in K$, on a l'égalité :

$$f(x,y)=\sum_{n=0}^{j-1}\prod_{i=0}^{n}(r_j-r_i)(y-r_i)\ .$$

L'application $f_x : y\mapsto f(x,y)$ est donc polynomiale. On voit de même que pour tout $y\in K$ fixé, l'application f^y est polynomiale.

Montrons que f n'est pas polynomiale. Soit $p\in\mathbb{N}$, pour tout $y\in K$ on a l'égalité ;

$$f(r_{p+1},y)=\sum_{n=0}^{p}\prod_{i=0}^{n}(r_{p+1}-r_i)\,(y-r_i)\ .$$

On voit que puisque la suite $(r_n)_{n\in\mathbb{N}}$ est injective, $f_{r_{p+1}}$ est polynomiale de degré $p+1$, de coefficient dominant $\prod_{i=0}^{p}(r_{p+1}-r_i)$. Si f était polynomiale, ses fonctions partielles seraient polynomiales, mais de degré majoré par le degré de f. Nous en déduisons que l'application f n'est pas polynomiale.

Exercice 12 :

> Soit une K-algèbre de polynômes à n lettres $K[X_1,\dots,X_n]=\mathcal{P}$ ($n\geqslant 1$, K infini). On considère $L_1,L_2,\dots,L_n$ et $G_1,G_2,\dots,G_n$ dans $\mathcal{P}$ tels que : pour chaque $i\in[\![1,n]\!]$, $\mathrm{val}\,(G_i)\geqslant 2$; $L_1,L_2,\dots,L_n$ sont homogènes de degré 1 et linéairement indépendants. Soit $Y_i=L_i+G_i$ ($1\leqslant i\leqslant n$). Montrer que la famille $(Y_1,Y_2,\dots,Y_n)$ est algébriquement libre sur K. ■

Montrons que les polynômes $L_1,\dots,L_n$ sont algébriquement indépendants. Considérons les formes linéaires $\varphi_1,\varphi_2,\dots,\varphi_n$ qui sont les applications polynomiales associées au polynômes $L_1,L_2,\dots,L_n$, homogènes de degré 1. Ces formes linéaires sont évidemment linéairement indépendantes. Considérons l'application K-linéaire :

$$\Phi : x\mapsto(\varphi_1(x),\dots,\varphi_n(x))\ ,$$

de K^n dans K^n. Son noyau est $\bigcap_{i=1}^{n} \operatorname{Ker}\varphi_i$; ce noyau est nul puisque les formes linéaires $(\varphi_1, \ldots, \varphi_n)$ sont linéairement indépendantes. L'application Φ est donc un automorphisme du K-ev K^n. Notons Ψ l'inverse de Φ ; nous poserons pour tout $x \in K^n$:

$$\Psi(x) = (\psi_1(x), \ldots, \psi_n(x)) .$$

Les applications $\psi_1, \ldots, \psi_n$, sont n formes linéaires linéairement indépendantes, qui sont les applications polynomiales associées à n polynômes homogènes de degré 1 : $M_1, M_2, \ldots, M_n$, linéairement indépendants. Par définition de l'application Ψ, pour tout $i \in [\![1, n]\!]$, et pour tout $(x_1, \ldots, x_n) \in K^n$, on a :

$$x_i = \varphi_i\big(\psi_1(x_1, \ldots, x_n), \ldots, \psi_n(x_1, \ldots, x_n)\big) .$$

Nous pouvons en déduire pour tout $i \in [\![1, n]\!]$, l'égalité entre polynômes :

$$X_i = L_i(M_1, \ldots, M_n) .$$

Supposons que $P \in K[X_1, \ldots, X_n]$ soit tel que $P(L_1, \ldots, L_n) = 0$; par substitution nous en déduisons $P\big(L_1(M_1, \ldots, M_n), \ldots, L_n(M_1, \ldots, M_n)\big) = 0$, soit $P(X_1, \ldots, X_n) = 0$. Les polynômes $L_1, L_2, \ldots, L_n$ sont donc algébriquement indépendants. Si $P \in K[X_1, \ldots, X_n]$, le polynôme $P(L_1, \ldots, L_n)$ sera noté $T(P)$. D'après le théorème de substitution, l'application T est un endomorphisme de l'algèbre $K[X_1, \ldots, X_n]$; il est, d'après ce qui précède, injectif.

Montrons que pour tout $k \in \mathbb{N}$, le sous-espace H_k de $K[X_1, \ldots, X_n]$ formé par les polynômes homogènes de degré k (et 0) est stable par T. Soit $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ un multi-indice tel que $\alpha_1 + \ldots + \alpha_n = k$, et M_α le monôme homogène de degré k associé. Comme les polynômes $L_1, \ldots, L_n$ sont tous homogènes de degré 1, on voit que le polynôme $L_1^{\alpha_1} \ldots L_n^{\alpha_n} = T(M_\alpha)$ est homogène de degré k. Il est donc clair que si P est homogène de degré k, alors $T(P)$ est aussi homogène de degré k. Rappelons que si $P \neq 0$, alors $T(P) \neq 0$. Nous déduisons de ce qui précède que pour tout polynôme $P \in K[X_1, \ldots, X_n]$, $\operatorname{val}(T(P)) = \operatorname{val}(P)$.

Pour $P \in K[X_1, \ldots, X_n]$, le polynôme $P(L_1 + G_1, \ldots, L_n + G_n)$ sera noté $R(P)$. L'application R est aussi, d'après le théorème de substitution, un endomorphisme de l'algèbre $K[X_1, \ldots, X_n]$.
Considérons l'ensemble $\mathcal{A} \subset K[X_1, \ldots, X_n]$, dont les éléments sont les polynômes P tels que $R(P) - T(P)$ soit nul ou de valuation $> \operatorname{val}(P)$. Si $P \in \mathcal{A}$, on voit que $\operatorname{val}(R(P)) = \operatorname{val}(T(P)) = \operatorname{val}(P)$. L'ensemble $\mathcal{A}$ contient les polynômes constants, et les polynômes $X_1, X_2, \ldots, X_n$, par hypothèse. Montrons que $\mathcal{A}$ est stable par la multiplication.
Pour tous polynômes P et Q :

$$R(P \times Q) - T(P \times Q) = R(P) \times R(Q) - T(P) \times T(Q) =$$
$$(R(P) - T(P)) \times R(Q) + T(P) \times (R(Q$$

Comme $R(P)-T(P)$ est nul ou de valuation $>\text{val}(P)$ et que $R(Q)-T(Q)$ est nul ou de valuation $>\text{val}(Q)$, alors $R(P\times Q)-T(P\times Q)$ est nul ou de valuation $>\text{val}(P)+\text{val}(Q)=\text{val}(PQ)$. L'ensemble $\mathcal{A}$ contient donc les monômes M_α, où $\alpha=(\alpha_1,\ldots,\alpha_n)$ est un multi-indice élément de $\mathbb{N}^n$. Soit P un polynôme de valuation k, on peut écrire :

$$P=\sum_{\alpha_1+\ldots+\alpha_n\geqslant k} a_\alpha M_\alpha\ ,$$

donc :

$$R(P)-T(P)=\sum_{\alpha_1+\ldots+\alpha_n\geqslant k} a_\alpha\,(R(M_\alpha)-T(M_\alpha))\ .$$

Dans cette somme tous les termes sont de valuation $>k$; le polynôme $R(P)-T(P)$ est donc nul ou de valuation $>\text{val}(P)$. Nous en déduisons enfin que si $P\neq 0$, $R(P)$ n'est pas nul et est de même valuation que $T(P)$ et que P.

Nous avons démontré que si $P(L_1+G_1,\ldots,L_n+G_n)=0$, alors $P=0$. Cela signifie que les polynômes $L_1+G_1,\ldots,L_n+G_n$ sont algébriquement indépendants.

§ X.3 *FONCTIONS SYMÉTRIQUES*

Exercice 7(calcul exact des A_ν du lemme 3 du § X.3) **:**

Dans tout ce qui suit le nombre de variables est $n\geqslant 2$. Pour $d\in\mathbb{N}^*$, et $\omega_0,\omega_1,\ldots,\omega_d$ une suite d'entiers telle que $\omega_0+\ldots+\omega_d=n$, nous noterons S_ω la fonction monomiale G_λ, où λ est la suite décroissante de n entiers comportant ω_d fois le nombre d, ω_{d-1} fois le nombre $d-1$, etc., ω_0 fois le nombre 0. Les entiers ω_i peuvent être nuls, y compris ω_d. Nous utiliserons la notation :

$$G_\lambda=S_\omega=\left\{\begin{matrix} d & d-1 & \ldots & 1 & 0\\ \omega_d & \omega_{d-1} & \ldots & \omega_1 & \omega_0\end{matrix}\right\}\ .$$

Avec les notations précédentes, montrer que si $m\in[\![1,d]\!]$ on a l'égalité :

$$\sigma_m S_\omega=\sum_{k\in E_{m,\omega}} U_k\,\Sigma(k,\omega)\ ,$$

où

- $E_{m,\omega}$ désigne l'ensemble des suites $(k_0,k_1,\ldots,k_d)$ d'entiers tels que pour tout $i\in[\![0,d]\!]$, $k_i\leqslant\omega_i$, et $\sum_{i=0}^{d} k_i=$

- U_k est le produit :

$$U_k = \prod_{j=1}^{d} \binom{\alpha_j}{k_{j-1}} ,$$

où $\alpha_j = \omega_j - k_j + k_{j-1}$;

- $\Sigma(k,\omega)$ est la fonction monomiale :

$$\Sigma(k,\omega) = \begin{Bmatrix} d+1 & d & \dots & 1 & 0 \\ k_d & \alpha_d & \dots & \alpha_1 & \omega_0 - k_0 \end{Bmatrix} . \blacksquare$$

Soit $\omega = (\omega_0, \dots, \omega_d)$ une suite d'entiers tels que $\omega_0 + \dots + \omega_d = n$, nous noterons $\mathcal{E}_\omega$, l'ensemble des suites $(P_0, P_1, \dots, P_d)$ de parties de $[\![1,n]\!]$, qui sont des partages de $[\![1,n]\!]$ et qui sont telles que pour tout $i \in [\![0,d]\!]$, $\text{card}\,(P_i) = \omega_i$.

A la suite $\omega = (\omega_0, \dots, \omega_d)$, on peut faire correspondre l'ensemble des suites $\alpha = (\alpha_1, \dots, \alpha_n)$ d'entiers qui prennent ω_i fois la valeur i pour tout $i \in [\![0,d]\!]$ (et pas d'autres valeurs). Cet ensemble de suites est une orbite de $\mathbb{N}^n$ pour l'action naturelle de $\mathfrak{S}_n$. La fonction monomiale associée à cette orbite $\mathcal{O}$, est $G = \sum_{\alpha \in \mathcal{O}} \mathcal{M}_\alpha(X)$, elle s'écrit aussi G_λ, où $\lambda = (\lambda_1, \dots, \lambda_n)$ est la seule suite décroissante qui soit dans $\mathcal{O}$ (lemme 1 du § X.3). Par définition :

$$S_\omega = G_\lambda = \sum_{\alpha \in \mathcal{O}} \mathcal{M}_\alpha(X) .$$

Soit $\alpha = (\alpha_1, \dots, \alpha_n)$ un élément de l'orbite $\mathcal{O}$ associée à ω ; on peut faire correspondre à α la suite de parties de $[\![1,n]\!]$ notée $E_0, E_1, \dots, E_d$, où pour tout $i \in [\![0,d]\!]$, $E_i = \{j \in [\![1,n]\!] \mid \alpha_j = i\}$. Cette suite est un partage de $[\![1,n]\!]$. Il est clair qu'on définit ainsi une bijection entre l'orbite $\mathcal{O}$ et l'ensemble $\mathcal{E}_\omega$.

Si $\alpha \in \mathcal{O}$ est associé au partage $(E_0, E_1, \dots, E_d)$ de $[\![1,n]\!]$, le monôme $\mathcal{M}_\alpha$ peut s'écrire :

$$\mathcal{M}_\alpha = \prod_{j=1}^{n} X_j^{\alpha_j} = \prod_{i=0}^{d} \prod_{j \in E_i} X_j^{\alpha_j} = \prod_{i=0}^{d} \prod_{j \in E_i} X_j^i = \prod_{i=1}^{d} \Big(\prod_{j \in E_i} X_j \Big)^i .$$

On obtient donc l'égalité :

$$G_\lambda = S_\omega = \sum_{(E_0,\dots,E_d) \in \mathcal{E}_\omega} \prod_{i=1}^{d} \Big(\prod_{j \in E_i} X_j \Big)^i .$$

Pour $E \subset [\![1,n]\!]$, nous utiliserons la notation :

$$\Pi_E = \prod_{i \in E} X_i \ ,$$

de telle sorte que l'égalité ci-dessus devient :

$$G_\lambda = S_\omega = \sum_{(E_0,\ldots,E_d) \in \mathscr{E}_\omega} \prod_{i=1}^{d} \Pi^i_{E_i} \ .$$

Nous désignerons par $\mathscr{P}_k(E)$ l'ensemble des parties de cardinal k de l'ensemble E. Si E est l'ensemble $[\![1,n]\!]$, nous écrirons, par abréviation, $\mathscr{P}_k$. On voit que pour tout $m \in [\![1,n]\!]$:

$$\sigma_m = \sum_{Q \in \mathscr{P}_m} \Pi_Q \ .$$

En utilisant ces différentes notations, nous obtenons :

$$\sigma_m \times S_\omega = \sum_{Q \in \mathscr{P}_m,\ (P_0,\ldots,P_d) \in \mathscr{E}_\omega} \Pi_Q \prod_{i=0}^{d} \Pi^i_{P_i} \ .$$

En utilisant les propriétés évidentes de la notation Π, nous obtenons pour chaque terme de cette somme :

$$\Pi_Q \prod_{i=0}^{d} \Pi^i_{P_i} = \prod_{i=0}^{d} \Pi_{P_i \cap Q} \prod_{i=0}^{d} \Pi^i_{P_i} = \prod_{i=0}^{d} \Pi^{i+1}_{P_i \cap Q} \ \Pi^i_{P_i \setminus Q} \ ,$$

soit encore en développant :

$$\Pi^0_{P_0 \setminus Q} \, \Pi^1_{P_0 \cap Q} \, \Pi^1_{P_1 \setminus Q} \ldots \Pi^d_{P_{d-1} \cap Q} \, \Pi^d_{P_d \setminus Q} \, \Pi^{d+1}_{P_d \cap Q} \ .$$

D'où, en regroupant les facteurs affectés de la même puissance :

$$\Pi^0_{P_0 \setminus Q} \, \Pi^1_{(P_0 \cap Q) \cup (P_1 \setminus Q)} \ldots \Pi^d_{(P_{d-1} \cap Q) \cup (P_d \setminus Q)} \, \Pi^{d+1}_{P_d \cap Q} \ .$$

Faisons maintenant un partage de l'ensemble des couples $\big(Q, (P_0, \ldots, P_d)\big) \in \mathscr{P}_m \times \mathscr{E}_\omega$ suivant la valeur de la famille $(k_0, k_1, \ldots, k_d)$ où pour tout $i \in [\![0,d]\!]$, $k_i = \operatorname{card}(Q \cap P_i)$; on voit que pour tout $i \in [\![0,d]\!]$, $k_i \leqslant \omega_i$, et que $\sum_{i=0}^{d} k_i = m$. Pour une telle famille d'entiers, $k = (k_0, k_1, \ldots, k_d)$, nous noterons $\mathscr{F}_{\omega,k}$ l'ensemble des couples $\big(Q, (P_0, \ldots, P_d)\big) \in \mathscr{P}_m \times \mathscr{E}_\omega$, tels que pour tout $i \in [\![0,d]\!]$, $\operatorname{card}(Q \cap P_i) = k_i$. Rappelons enfi

$E_{m,\omega}$ qui désigne l'ensemble des suites $(k_0, k_1, \ldots, k_d)$ vérifiant les conditions énoncées ci-dessus. Avec ces notations nous obtenons l'égalité :

$$\sigma_m \times S_\omega = \sum_{k \in E_{m,\omega}} \sum_{\left(Q,(P_0,\ldots,P_d)\right) \in \mathcal{F}_{k,\omega}} \Pi^0_{P_0 \setminus Q}\, \Pi^1_{(P_0 \cap Q) \cup (P_1 \setminus Q)} \cdots \Pi^d_{(P_{d-1} \cap Q) \cup (P_d \setminus Q)}\, \Pi^{d+1}_{P_d \cap Q} \,.$$

Le couple $C = \left(Q, (P_0, \ldots, P_d)\right)$ étant un élément fixé de $\mathcal{F}_{k,\omega}$, la suite

(1) $\Phi(C) = \left(P_0 \setminus Q,\ (P_0 \cap Q) \cup (P_1 \setminus Q),\ \ldots,\ (P_{d-1} \cap Q) \cup (P_d \setminus Q),\ P_d \cap Q\right)$,

est un partage de $[\![1, n]\!]$ en des parties de cardinaux :

$$\omega_0 - k_0,\ \omega_1 - k_1 + k_0,\ \ldots,\ \omega_d - k_d + k_{d-1},\ k_d \,.$$

Notons α cette suite d'entiers. L'application Φ est donc une application de $\mathcal{F}_{k,\omega}$ à valeurs dans l'ensemble $\mathcal{C}_\alpha$. Montrons qu'elle vérifie les hypothèses du théorème du Berger.

Soit $R = (R_0, R_1, \ldots, R_d, R_{d+1})$ un élément de $\mathcal{C}_\alpha$; montrons qu'un couple $C = \left(Q, (P_0, \ldots, P_d)\right)$ tel que $\Phi(C) = R$ est déterminé par les parties $A_i = P_{i-1} \cap Q$, où i varie de 1 à d. Pour tout $i \in [\![1, d]\!]$, A_i est nécessairement une partie de R_i, et son cardinal est par hypothèse k_{i-1}. Inversement, si pour tout $i \in [\![1, d]\!]$, $A_i \in \mathcal{P}_{k_{i-1}}(R_i)$, il y a une seule valeur possible pour le couple $C = \left(Q, (P_0, \ldots, P_d)\right)$, puisque :
- $P_0 = (P_0 \setminus Q) \cup (P_0 \cap Q) = R_0 \cup A_1$;
- $P_1 = (P_1 \setminus Q) \cup (P_1 \cap Q) = (R_1 \setminus A_1) \cup A_2$;
etc. ;
- $P_{d-1} = (P_{d-1} \setminus Q) \cup (P_{d-1} \cap Q) = (R_{d-1} \setminus A_{d-1}) \cup A_d$;
- $P_d = (P_d \setminus Q) \cup (P_d \cap Q) = (R_d \setminus A_d) \cup R_{d+1}$;
enfin $Q = (Q \cap P_0) \cup \ldots \cup (Q \cap P_d) = A_1 \cup \ldots \cup A_d \cup R_{d+1}$.

Inversement pour toute suite $(A_1, \ldots, A_d)$ telle que pour tout $i \in [\![1, d]\!]$, $A_i \in \mathcal{P}_{k_{i-1}}(R_i)$, on vérifie sans difficulté que les formules ci-dessus donnent un couple $C = \left(Q, (P_0, \ldots, P_d)\right)$, élément de $\mathcal{F}_{k,\omega}$, tel que $\Phi(C) = R$, et tel que pour tout $i \in [\![1, d]\!]$, $P_{i-1} \cap Q = A_i$.

Le nombre de couples $\left(Q, (P_0, \ldots, P_d)\right) \in \mathcal{F}_{k,\omega}$ qui ont pour image un partage $(R_0, R_1, \ldots, R_d, R_{d+1})$, élément de $\mathcal{C}_\alpha$ donné, est donc :

$$U_k = \binom{\omega_1 - k_1 + k_0}{k_0} \times \ldots \times \binom{\omega_d - k_d + k_{d-1}}{k_{d-1}} \,.$$

La somme :

$$\sum_{\left(Q,(P_0,\ldots,P_d)\right) \in \mathcal{F}_{k,\omega}} \Pi^0_{P_0 \setminus Q}\, \Pi^1_{(P_0 \cap Q) \cup (P_1 \setminus Q)} \cdots \Pi^d_{(P_{d-1} \cap Q) \cup (P_d \setminus Q)}\, \Pi^{d+1}_{P_d \cap Q}$$

est donc égale, avec les notations introduites ci-dessus, à :

$$U_k \sum_{(R_0,R_1,\ldots,R_d,R_{d+1})\in\mathcal{C}_\alpha} \Pi^0_{R_0}\Pi^1_{R_1}\ldots\Pi^{d+1}_{R_{d+1}} = U_k\ S_\alpha\ ,$$

où α est la suite :

$$\omega_0 - k_0,\ \omega_1 - k_1 + k_0,\ \ldots,\ \omega_d - k_d + k_{d-1},\ k_d\ .$$

Nous en déduisons finalement l'égalité :

$$\sigma_m\, S_\omega = \sum_{k\in E_{m,\omega}} U_k\, \Sigma(k,\omega)\ ,$$

où

- $E_{m,\omega}$ désigne l'ensemble des suites $(k_0,k_1,\ldots,k_d)$ d'entiers tels que pour tout $i\in[\![0,d]\!]$, $k_i \leqslant \omega_i$, et $\sum_{i=0}^{d} k_i = m$;
- U_k est le produit :

$$U_k = \prod_{j=1}^{d} \binom{\alpha_j}{k_{j-1}}\ ,$$

où $\alpha_j = \omega_j - k_j + k_{j-1}$;

- $\Sigma(k,\omega)$ est la fonction monomiale :

$$\Sigma(k,\omega) = \left\{ \begin{matrix} d+1 & d & \ldots & 1 & 0 \\ k_d & \alpha_d & \ldots & \alpha_1 & \omega_0 - k_0 \end{matrix} \right\}.$$

Exercice 1 :

Calculer en fonction des σ_k les fonctions monomiales suivantes :

a) $F = \left\{ \begin{matrix} 3 & 2 & 1 & 0 \\ 1 & 2 & 0 & n-3 \end{matrix} \right\}$ $(n \geqslant 7)$;

b) $F = \left\{ \begin{matrix} 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & n-4 \end{matrix} \right\}$ $(n \geqslant 6)$;

c) $F = \left\{ \begin{matrix} 3 & 2 & 1 & 0 \\ 2 & 0 & 0 & n-2 \end{matrix} \right\}$ $(n \geqslant 6)$;

d) $F = \left\{ \begin{matrix} 4 & 3 & 2 & 1 & 0 \\ 1 & 0 & 0 & 2 & n-3 \end{matrix} \right\}$ $(n \geqslant 6)$. ■

Nous utiliserons l'exercice 7, qui donne les valeurs des coefficients nécessaires à la mise en œuvre de l'algorithme de décomposition utilisé dans la démonstration du théorème X.3.2. Précisons d'abord l'algorithme utili

Soit à décomposer la fonction monomiale :

$$S_\beta = \begin{Bmatrix} d+1 & d & \dots & 1 & 0 \\ \beta_{d+1} & \beta_d & \dots & \beta_1 & \beta_0 \end{Bmatrix} .$$

Calculons en utilisant la formule donnée dans l'exercice 7 le produit :

$$\sigma_{\beta_{d+1}} \times \begin{Bmatrix} d & d-1 & \dots & 1 & 0 \\ \beta_{d+1}+\beta_d & \beta_{d-1} & \dots & \beta_1 & \beta_0 \end{Bmatrix} .$$

On trouve une combinaison à coefficients entiers de fonctions monomiales :

$$\sum_{(k_0,k_1,\dots,k_d)} U_k \begin{Bmatrix} d+1 & d & d-1 & \dots & 1 & 0 \\ k_d & \alpha_d & \alpha_{d-1} & \dots & \alpha_1 & \beta_0-k_0 \end{Bmatrix} ;$$

où $\alpha_d = \beta_{d+1}+\beta_d-k_d+k_{d-1}$, $\alpha_{d-1} = \beta_{d-1}-k_{d-1}+k_{d-2}$, etc., $\alpha_1 = \beta_1-k_1+k_0$; la suite $k = (k_0,\dots,k_d)$ est une suite d'entiers telle que $\sum_{i=0}^{d} k_i = \beta_{d+1}$, et pour tout $i \in [\![0, d-1]\!]$, $k_i \leqslant \beta_i$ (la condition $k_d \leqslant \beta_{d+1}+\beta_d$ est respectée).

Parmi ces fonctions monomiales, figure celle qui correspond à la suite $k_d = \beta_{d+1}$, tous les autres termes étant nuls ; cette fonction monomiale est :

$$\begin{Bmatrix} d+1 & d & \dots & 1 & 0 \\ \beta_{d+1} & \beta_d & \dots & \beta_1 & \beta_0 \end{Bmatrix} ,$$

c'est-à-dire la fonction monomiale qu'on voulait décomposer ; elle est affectée du coefficient U_k , qui est, d'après l'exercice 7 :

$$U_k = \binom{\alpha_1}{k_0} \times \dots \times \binom{\alpha_d}{k_{d-1}} = 1 ,$$

puisque $k_0 = \dots = k_{d-1} = 0$. Toutes les autres fonctions monomiales qui apparaissent dans le calcul, y compris celle par laquelle on multiplie $\sigma_{\beta_{d+1}}$, sont en un certain sens plus "petites" que celle-ci (cf. démonstration du théorème X.3.2).

Pour effectuer pratiquement le calcul, on établira d'abord la liste des suites k possibles ; pour chacune des valeurs trouvées, on calculera $(\alpha_1,\dots,\alpha_d)$, $\beta_0 - k_0$, et le coefficient U_k .

Etablissons d'abord des formules générales donnant les fonctions monomiales $\mu_{a,b} = S_{(a,b,n-(a+b))}$ portant sur n indéterminées, pour toutes valeurs de a et b entiers, $a+b \leqslant n$.
Calculons le produit $\sigma_a \, \sigma_{a+b} = \sigma_a \, S_{(a+b,n-(a+b))}$. Les suites

sont les suites telles que $k_0 \leqslant n-(a+b)$, et $k_0+k_1=a$; ce sont donc les suites $(i, a-i)$, pour i variant de 0 à $\mathrm{Min}\,(a, n-(a+b))$; pour i donné, on a $\alpha_1 = a+b-(a-i)+i = b+2i$, et le coefficient U_k est $\binom{b+2i}{i}$. Nous obtenons donc l'égalité :

$$\sigma_a\,\sigma_{a+b} = \sum_{i=0}^{\mathrm{Min}(a,n-(a+b))} \binom{b+2i}{i} \begin{Bmatrix} 2 & 1 & 0 \\ a-i & b+2i & n-(a+b)-i \end{Bmatrix} .$$

Pour $i=0$ on retrouve comme prévu le terme cherché : $\mu_{a,b}$. En définitive nous obtenons donc :

$$\mu_{a,b} = \sigma_a\,\sigma_{a+b} - \sum_{i=1}^{\mathrm{Min}(a,n-(a+b))} \binom{b+2i}{i} \mu_{a-i,b+2i} ,$$

formule qui permet de calculer récursivement les valeurs de $\mu_{a,b}$.

Explicitons en particulier le résultat pour $a=1$, et b entier tel que $b+1 \leqslant n$. Si $n=b+1$, nous obtenons évidemment $\mu_{1,b} = \sigma_1\,\sigma_{1+b}$, et sinon la sommation ne comporte qu'un seul terme. On obtient :

$$\mu_{1,b} = \sigma_1\sigma_{b+1} - (b+2)\,\sigma_{b+2} .$$

Pour $a=2$, nous supposerons pour simplifier $a \leqslant n-(a+b)$, i.e. $n \geqslant 4+b$. La sommation comporte alors 2 termes :

$$\mu_{2,b} = \sigma_2\,\sigma_{b+2} - \binom{b+2}{1}\mu_{1,b+2} - \binom{b+4}{2}\sigma_{b+4} .$$

En utilisant le résultat précédent, on trouve sans difficulté l'égalité :

$$\mu_{2,b} = \sigma_2\,\sigma_{b+2} - (b+2)\sigma_1\,\sigma_{b+3} + \frac{(b+4)(b+1)}{2}\sigma_{b+4} .$$

Pour $a=3$, en supposant $n \geqslant 6+b$, on obtient d'abord l'égalité :

$$\mu_{3,b} = \sigma_3\,\sigma_{b+3} - \binom{b+2}{1}\mu_{2,b+2} - \binom{b+4}{2}\mu_{1,b+4} - \binom{b+6}{3}\sigma_{b+6} ,$$

puis en utilisant les formules précédentes, après calcul :

$$\mu_{3,b} = \sigma_3\,\sigma_{b+3} - (b+2)\,\sigma_2\,\sigma_{b+4} + \\ + \frac{1}{2}(b+4)(b+1)\,\sigma_1\,\sigma_{b+5} - \frac{1}{6}(b+6)\,(b+1)\,(b\cdot$$

Etablissons maintenant une formule générale donnant les fonctions monomiales $\mu_{1,a,b} = S_{(1,a,b,n-(a+b+1))}$ portant sur n indéterminées, pour toutes valeurs de a et b entiers, $a+b+1 \leqslant n$.
Calculons le produit $\sigma_1 S_{(a+1,b,n-(a+b+1))}$. Les suites $k = (k_0, k_1, k_2)$, sont les suites telles que $k_0 \leqslant n-(a+b+1)$, $k_1 \leqslant b$, et $k_0 + k_1 + k_2 = 1$; ce sont donc les suites :

$(k_0, k_1, k_2) = (0,0,1)$, et alors
$(\alpha_1, \alpha_2) = (b, a)$, $\beta_0 - k_0 = n-a-b-1$, $U_k = \binom{b}{0}\binom{a}{0} = 1$;

$(k_0, k_1, k_2) = (1,0,0)$, et alors
$(\alpha_1, \alpha_2) = (b+1, a+1)$, $\beta_0 - k_0 = n-a-b-2$, $U_k = \binom{b+1}{1}\binom{a+1}{0} = b+1$;

et, si $b > 0$, $(k_0, k_1, k_2) = (0,1,0)$, et alors
$(\alpha_1, \alpha_2) = (b-1, a+2)$, $\beta_0 - k_0 = n-a-b-1$, $U_k = \binom{b-1}{0}\binom{a+2}{1} = a+2$.

Nous obtenons donc l'égalité :

$$\sigma_a \mu_{a+1,b} = \mu(1,a,b) + (b+1)\mu(a+1,b+1) + (a+2)\mu(a+2,b-1) ,$$

en supprimant le dernier terme si $b = 0$.

Déterminons maintenant les expressions des fonctions monomiales proposées.

a) Nous avons noté cette fonction monomiale $\mu(1,2,0)$. En appliquant la formule trouvée on obtient :

$$\mu(1,2,0) = \sigma_1 \mu(3,0) - \mu(3,1) .$$

Comme $n \geqslant 7$, on peut appliquer les formules donnant $\mu(a,b)$ pour trouver :

$$\mu(3,0) = \sigma_3^2 - 2\sigma_2\sigma_4 + 2\sigma_1\sigma_5 - 2\sigma_6 ,$$

et :

$$\mu(3,1) = \sigma_3\sigma_4 - 3\sigma_2\sigma_5 + 5\sigma_1\sigma_6 - 7\sigma_7 .$$

On obtient après calcul :

$$F = 2\sigma_1^2\sigma_5 - 2\sigma_1\sigma_2\sigma_4 + \sigma_1\sigma_3^2 - 7\sigma_1\sigma_6 + 3\sigma_2\sigma_5 - \sigma_3\sigma_4 + 7\sigma_7 .$$

b) La fonction monomiale est ici ce que nous avons noté $\mu(1,0,3)$. On obtient d'abord :

$$\mu(1,0,3) = \sigma_1\mu(1,3) - 2\mu(2,2) - 4\mu(1,4) .$$

Comme $n \geqslant 6$, on peut appliquer les formules donnant $\mu(a,b)$ pour trouver :

$$\mu(1,3) = \sigma_1\,\sigma_4 - 5\,\sigma_5 \ ,$$

$$\mu(2,2) = \sigma_2\,\sigma_4 - 4\,\sigma_1\,\sigma_5 + 9\,\sigma_6 \ ,$$

$$\mu(1,4) = \sigma_1\,\sigma_5 - 6\,\sigma_6 \ .$$

On obtient après calcul :

$$F = \sigma_1^2\,\sigma_4 - \sigma_1\,\sigma_5 - 2\,\sigma_2\,\sigma_4 + 6\,\sigma_6 \ .$$

c)

$$F = \begin{Bmatrix} 3 & 2 & 1 & 0 \\ 2 & 0 & 0 & n-2 \end{Bmatrix} \quad (n \geqslant 6) \ .$$

Nous allons, en suivant l'algorithme expliqué ci-dessus, calculer le produit :

$$\sigma_2 \begin{Bmatrix} 2 & 1 & 0 \\ 2 & 0 & n-2 \end{Bmatrix} \ .$$

Les suites k doivent vérifier les conditions $k_0 \leqslant n-2$, $k_1 \leqslant 0$, et $k_0 + k_1 + k_2 = 2$. Les solutions sont :
- $k = (0,0,2)$ alors $(\alpha_1,\alpha_2) = (0,0)$, $\beta_0 - k_0 = n-2$, $U_k = 1$;
- $k = (1,0,1)$, $(\alpha_1,\alpha_2) = (1,1)$, $\beta_0 - k_0 = n-3$, $U_k = \binom{1}{1}\binom{1}{0} = 1$;
- $k = (2,0,0)$, $(\alpha_1,\alpha_2) = (2,2)$, $\beta_0 - k_0 = n-4$, $U_k = \binom{2}{2}\binom{2}{0} = 1$.

Nous obtenons donc l'égalité :

$$\sigma_2 \begin{Bmatrix} 2 & 1 & 0 \\ 2 & 0 & n-2 \end{Bmatrix} = \begin{Bmatrix} 3 & 2 & 1 & 0 \\ 2 & 0 & 0 & n-2 \end{Bmatrix} + \begin{Bmatrix} 3 & 2 & 1 & 0 \\ 1 & 1 & 1 & n-3 \end{Bmatrix} + \begin{Bmatrix} 3 & 2 & 1 & 0 \\ 0 & 2 & 2 & n-4 \end{Bmatrix} \ .$$

Le deuxième terme de cette somme est :

$$\mu(1,1,1) = \sigma_1\,\mu(2,1) - 3\,\mu(3,0) - 2\mu(2,2) \ .$$

Nous obtenons :

$$F = \sigma_2\,\mu_{2,0} - \sigma_1\,\mu_{2,1} + \mu_{2,2} + 3\mu_{3,0} \ .$$

En utilisant les formules précédemment démontrées, nous obtenons :
- $\mu_{2,0} = \sigma_2^2 - 2\,\sigma_1\,\sigma_3 + 2\,\sigma_4$,
- $\mu_{2,1} = \sigma_2\,\sigma_3 - 3\,\sigma_1\,\sigma_4 + 5\,\sigma_5$,
- $\mu_{2,2} = \sigma_2\,\sigma_4 - 4\,\sigma_1\,\sigma_5 + 9\,\sigma_6$,

- $\mu_{3,0} = \sigma_3^2 - 2\sigma_2\sigma_4 + 2\sigma_1\sigma_5 + 2\sigma_6$.

D'où après calcul :

$$F = 3\sigma_1^2\sigma_4 - 3\sigma_1\sigma_2\sigma_3 - 3\sigma_1\sigma_5 + \sigma_2^3 - 3\sigma_2\sigma_4 + 3\sigma_3^2 + 15\sigma_6 .$$

d) Reprenons l'algorithme général. Calculons le produit :

$$\sigma_1 \begin{Bmatrix} 3 & 2 & 1 & 0 \\ 1 & 0 & 2 & n-3 \end{Bmatrix} .$$

Les suites k doivent vérifier les conditions $k_0 \leqslant n-3$, $k_1 \leqslant 2$, $k_2 = 0$, et $k_0 + k_1 + k_2 + k_3 = 1$. Les solutions sont :

- $(k_0, k_1, k_2, k_3) = (0,0,0,1)$ alors
$(\alpha_1, \alpha_2, \alpha_3) = (2,0,0)$, $\beta_0 - k_0 = n-3$, $U_k = \binom{2}{0}\binom{0}{0}\binom{0}{0} = 1$;

- $(k_0, k_1, k_2, k_3) = (0,1,0,0)$, alors
$(\alpha_1, \alpha_2, \alpha_3) = (1,1,1)$, $\beta_0 - k_0 = n-3$, $U_k = \binom{1}{0}\binom{1}{1}\binom{1}{0} = 1$;

- $(k_0, k_1, k_2, k_3) = (1,0,0,0)$, alors
$(\alpha_1, \alpha_2, \alpha_3) = (3,0,1)$, $\beta_0 - k_0 = n-4$, $U_k = \binom{3}{1}\binom{0}{0}\binom{1}{0} = 3$.

Nous obtenons donc l'égalité :

$$\sigma_1 \begin{Bmatrix} 3 & 2 & 1 & 0 \\ 1 & 0 & 2 & n-3 \end{Bmatrix} =$$
$$\begin{Bmatrix} 4 & 3 & 2 & 1 & 0 \\ 1 & 0 & 0 & 2 & n-3 \end{Bmatrix} + \begin{Bmatrix} 3 & 2 & 1 & 0 \\ 1 & 1 & 1 & n-3 \end{Bmatrix} + 3 \begin{Bmatrix} 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & n-4 \end{Bmatrix} .$$

Nous en déduisons :

$$F = \sigma_1\,\mu(1,0,2) - \mu(1,1,1) - 3\,\mu(1,0,3) .$$

En utilisant les formules établies nous obtenons :

$$\mu(1,0,2) = \sigma_1\,\mu(1,2) - 2\,\mu(2,1) - 3\,\mu(1,3) ,$$

$$\mu(1,1,1) = \sigma_1\,\mu(2,1) - 3\,\mu(3,0) - 2\mu(2,2) ,$$
$$\mu(1,0,3) = \sigma_1\,\mu(1,3) - 2\,\mu(2,2) - 4\,\mu(1,4) .$$

D'où :

$$F = \sigma_1^2\,\mu(1,2) - 3\sigma_1\,\mu(2,1) - 6\sigma_1\,\mu(1,3) + 3\,\mu(3,0) + 8\,\mu(2,2)$$

Comme $n \geqslant 6$, les formules trouvées pour les $\mu(a,b)$ s'appliquent, ce qui donne :

$$F = \sigma_1^3\,\sigma_3 - \sigma_1^2\,\sigma_4 - 3\,\sigma_1\,\sigma_2\,\sigma_3 + \sigma_1\,\sigma_5 + 2\,\sigma_2\,\sigma_4 + 3\,\sigma_3^2 - 6\,\sigma_6 \ .$$

Exercice 3 :

Pour $n = 3$ calculer en fonction de σ_1, σ_2, σ_3 les polynômes suivants :

a) $F = \begin{Bmatrix} 3 & 2 & 1 & 0 \\ 2 & 1 & 0 & 0 \end{Bmatrix}$; *b)* $F = \begin{Bmatrix} 3 & 2 & 1 & 0 \\ 2 & 0 & 0 & 1 \end{Bmatrix}$;

c) $F = \begin{Bmatrix} 3 & 2 & 1 & 0 \\ 1 & 2 & 0 & 0 \end{Bmatrix}$.

Pour $n = 4$, calculer en fonction de σ_1, σ_2, σ_3, σ_4 les polynômes :

d) $\begin{Bmatrix} 4 & 3 & 2 & 1 & 0 \\ 2 & 2 & 0 & 0 & 0 \end{Bmatrix}$; *e)* $F = \begin{Bmatrix} 2 & 1 & 0 \\ 4 & 0 & 0 \end{Bmatrix}$;

f) $F = (X_1\,X_2 + X_3\,X_4)\,(X_1\,X_3 + X_2\,X_4)\,(X_1\,X_4 + X_2\,X_3)$. ■

Remarquons de manière générale l'égalité suivante entre fonctions monomiales portant sur n indéterminées :

$$\begin{Bmatrix} d & d-1 & \dots & 1 & 0 \\ \omega_d & \omega_{d-1} & \dots & \omega_1 & 0 \end{Bmatrix} = \sigma_n \begin{Bmatrix} d-1 & \dots & 1 & 0 \\ \omega_d & \omega_{d-1} & \dots & \omega_1 \end{Bmatrix} .$$

C'est assez évident dans les cas particuliers. Reprenons la formule utilisée dans la résolution de l'exercice 7, avec les notations introduites alors :

$$S_\omega = \sum_{(P_0,P_1,\dots,P_d)\in\mathscr{E}_\omega} \prod_{i=1}^{d} \Pi_{P_i}^i \ .$$

Pour chaque terme de la somme on a :

$$\prod_{i=1}^{d} \Pi_{P_i}^i = \prod_{i=1}^{d} \Pi_{P_i} \times \prod_{i=1}^{d} \Pi_{P_i}^{i-1} \ ;$$

mais comme $\omega_0 = 0$, $P_0 = \emptyset$, donc :

$$\prod_{i=1}^{d} \Pi_{P_i} = \Pi_{[1,n]} = \sigma_n \ .$$

En changeant d'indice, on obtient :

$$S_\omega = \sigma_n \sum_{(P_1,\dots,P_d)\in\mathcal{C}_{(\omega_1,\dots,\omega_d)}} \prod_{j=0}^{d-1} \Pi_{P_{j+1}}^{j} = \sigma_n \, S_{(\omega_1,\dots,\omega_d)} \ .$$

a) En appliquant la propriété démontrée ci-dessus deux fois, on obtient :

$$F = \sigma_3^2 \begin{Bmatrix} 1 & 0 \\ 2 & 1 \end{Bmatrix} = \sigma_3^2 \, \sigma_2 \ .$$

b) Nous avons exprimé cette fonction monomiale en fonction des polynômes symétriques élémentaires dans l'exercice 1, mais dans le cas où le nombre d'indéterminées était $n \geqslant 6$. Les calculs sont ici similaires, mais des termes disparaissent. On obtient :

$$F = \sigma_2 \begin{Bmatrix} 2 & 1 & 0 \\ 2 & 0 & 1 \end{Bmatrix} - \begin{Bmatrix} 3 & 2 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{Bmatrix} \ ,$$

d'où ici :

$$F = \sigma_2 \, \mu(2,0) - \sigma_3 \, \mu(1,1) \ .$$

En appliquant la formule donnant les $\mu(a,b)$ démontrée dans la résolution de l'exercice 1, on obtient :

$$\mu(1,2) = \sigma_1 \, \sigma_3 \ ;$$

$$\mu(2,0) = \sigma_2^2 - 2\mu(1,2) = \sigma_2^2 - 2\,\sigma_1 \, \sigma_3 \ ;$$

$$\mu(1,1) = \sigma_1 \, \sigma_2 - 3\,\sigma_3 \ .$$

Nous en déduisons :

$$F = \sigma_2 \, (\sigma_2^2 - 2\,\sigma_1 \, \sigma_3) - \sigma_3 \, (\sigma_1 \, \sigma_2 - 3\,\sigma_3) = \sigma_2^3 - 3\,\sigma_1 \, \sigma_2 \, \sigma_3 + 3\,\sigma_3^2 \ .$$

On remarque que c'est la formule obtenue dans l'exercice 1, si on annule les σ_i, où $i \geqslant 4$.

c) D'après la remarque préliminaire nous obtenons ici :

$$F = \sigma_3^2 \begin{Bmatrix} 1 & 0 \\ 1 & 2 \end{Bmatrix} = \sigma_3^2 \, \sigma_1 \ .$$

d) Toujours une utilisant la même propriété, nous obtenons ici :

$$F = \sigma_4^3 \begin{Bmatrix} 1 & 0 \\ 2 & 2 \end{Bmatrix} = \sigma_4^3 \sigma_2 \ .$$

e) Il est évident que :

$$F = \sigma_4^2 \ .$$

f) En développant l'expression on obtient sans difficulté :

$$\begin{aligned} F = & X_1^3 X_2 X_3 X_4 + X_1 X_2^3 X_3 X_4 + X_1 X_2 X_3^3 X_4 + X_1 X_2 X_3 X_4^3 + \\ & + X_2^2 X_3^2 X_4^2 + X_1^2 X_3^2 X_4^2 + X_1^2 X_2^2 X_4^2 + X_1^2 X_2^2 X_3^2 \ , \end{aligned}$$

soit :

$$F = \sigma_4 \sum_{i=1}^{4} X_i^2 + \begin{Bmatrix} 2 & 1 & 0 \\ 3 & 0 & 1 \end{Bmatrix} \ .$$

On obtient facilement :

$$\sum_{i=1}^{4} X_i^2 = \sigma_1^2 - 2\sigma_2 \ ,$$

et en appliquant les formules générales pour $\mu(a,b)$:

$$\begin{Bmatrix} 2 & 1 & 0 \\ 3 & 0 & 1 \end{Bmatrix} = \mu(3,0) = \sigma_3^2 - 2\sigma_2\sigma_4 \ .$$

Nous obtenons finalement :

$$F = \sigma_4 (\sigma_1^2 - 2\sigma_2) + \sigma_3^2 - 2\sigma_2\sigma_4 = \sigma_3^2 - 4\sigma_2\sigma_4 + \sigma_1^2\sigma_4 \ .$$

Exercice 9 :

Soit $z \in \mathbb{C}^*$ tel que $|z| \neq 1$ et soit $n \in \mathbb{N}^*$. On cherche les valeurs $g_1(z), g_2(z), \ldots, g_n(z)$ des polynômes symétriques élémentaires $\sigma_1, \sigma_2, \ldots, \sigma_n$ sur la liste $(1, z, z^2, \ldots, z^{n-1})$. Soit pour cela T une indéterminée sur $\mathbb{C}$ et

$$F(z,T) = (1-T)(1-zT)\ldots(1-z^{n-1}T) \in \mathbb{C}[T] \ .$$

Calculer $F(z, zT)$. En déduire une relation de récurrence simple entre les $g_i(z)$, et enfin donner les valeurs des $g_i(z$

Nous obtenons :

$$F(z, zT) = (1 - zT)(1 - z^2T)\dots(1 - z^nT) .$$

Nous en déduisons l'égalité :

$$(1 - z^nT)\,F(z,T) = (1 - T)\,F(z, zT) .$$

Comme d'autre part :

$$F(z,T) = 1 - g_1(z)\,T + g_2(z)\,T^2 - \dots + (-1)^n\,g_n(z)\,T^n ,$$

nous obtenons en posant $g_0(z) = 1$:

$$(1 - z^nT)\sum_{i=0}^{n}(-1)^i\,g_i(z)\,T^i = (1 - T)\sum_{i=0}^{n}(-1)^i\,g_i(z)\,z^iT^i .$$

Pour tout $k \in [\![1, n]\!]$, en identifiant les coefficients des monômes de degré k, on obtient :

$$(-1)^k(\,g_k(z) + z^n\,g_{k-1}(z)) = (-1)^k(\,g_k(z)\,z^k + g_{k-1}(z)\,z^{k-1}) ,$$

soit encore :

$$(1 - z^k)\,g_k(z) = (z^{k-1} - z^n)\,g_{k-1}(z) .$$

Comme $|z| \neq 1$, $1 - z^k \neq 1$; on obtient par conséquent la relation de récurrence :

$$g_k(z) = z^{k-1}\frac{1 - z^{n-k+1}}{1 - z^k}\,g_{k-1}(z) .$$

Puisque $g_0(z) = 1$, on voit facilement que pour tout $i \in [\![1, n]\!]$:

$$g_i(z) = z\,z^2\dots z^{i-1}\frac{(1 - z^n)\dots(1 - z^{n-i+1})}{(1 - z)\dots(1 - z^i)} =$$

$$= z^{\frac{i(i-1)}{2}}\frac{(1 - z^n)\dots(1 - z^{n-i+1})}{(1 - z)\dots(1 - z^i)} .$$

§ X.4 *FORMULES DE NEWTON*

Exercice 1 :

Soit $n \in \mathbb{N}^*$, $(x_1, \dots, x_n) \in \mathbb{C}^n$ et T une indéterminée sur $\mathbb{C}$. On pose $P = \prod_{j=1}^{n}(1 - x_jT) \in \mathbb{C}[T]$. On note $\tilde{\sigma}_k$ (resp. $\tilde{S}_k$) les valeurs au point $(x_1, \dots, x_n)$ des fonctions σ_k

Développer en série formelle dans $\mathbb{C}[[T]]$ la fraction :

$$\frac{-P'(T)}{P(T)} = \sum_{j=1}^{n} \frac{x_j}{1 - x_j T} .$$

En déduire

$$-P'(T) = P(T) \left(\sum_{k \geqslant 0} \tilde{S}_{k+1} T^k \right) ,$$

et obtenir ainsi une nouvelle démonstration des formules de Newton. ■

Nous obtenons :

$$\frac{-P'(T)}{P(T)} = \sum_{j=1}^{n} x_j \sum_{k \geqslant 0} x_j^k T^k = \sum_{k \geqslant 0} \left(\sum_{j=1}^{n} x_j^{k+1} \right) T^k = \sum_{k \geqslant 0} \tilde{S}_{k+1} T^k .$$

D'autre part, et convenant $\tilde{\sigma}_0 = 1$:

$$P(T) = \sum_{i=0}^{n} (-1)^i \tilde{\sigma}_i T^i \quad \text{et} \quad P'(T) = \sum_{k=1}^{n} (-1)^k k \tilde{\sigma}_k T^{k-1}.$$

Nous obtenons donc l'égalité :

$$S = \sum_{k=1}^{n} (-1)^{k-1} k \tilde{\sigma}_k T^{k-1} = \left(\sum_{i=0}^{n} (-1)^i \tilde{\sigma}_i T^i \right) \left(\sum_{k \geqslant 0} \tilde{S}_{k+1} T^k \right) .$$

En développant le terme de droite on obtient :

$$S = \sum_{j \geqslant 0} \sum_{i=0}^{\mathrm{Min}(j,n)} (-1)^i \tilde{\sigma}_i \tilde{S}_{j-i+1} T^j = \sum_{k \geqslant 1} \sum_{i=0}^{\mathrm{Min}(k-1,n)} (-1)^i \tilde{\sigma}_i \tilde{S}_{k-i} T^{k-1} .$$

En identifiant les coefficients on obtient, pour tout $k \in [\![1, n]\!]$:

$$(-1)^{k-1} k \tilde{\sigma}_k = \sum_{i=0}^{k-1} (-1)^i \tilde{\sigma}_i \tilde{S}_{k-i} ,$$

soit encore, puisque $\tilde{\sigma}_0 = 1$:

$$\tilde{S}_k - \tilde{\sigma}_1 \tilde{S}_{k-1} + \ldots + (-1)^{k-1} \tilde{\sigma}_{k-1} \tilde{S}_1 + (-1)^k k \tilde{\sigma}_k = 0 .$$

On obtient aussi, pour tout $k > n$:

$$0 = \sum_{i=0}^{n} (-1)^i \tilde{\sigma}_i \tilde{S}_{k-i} ,$$

soit

$$\tilde{S}_k - \tilde{\sigma}_1 \tilde{S}_{k-1} + \ldots + (-1)^n \tilde{\sigma}_n \tilde{S}_{k-n} = 0 \ .$$

Ces égalités étant vraies pour tout n-uplet $(x_1, x_2, \ldots, x_n) \in \mathbb{C}^n$, les égalités polynomiales correspondantes, qui sont les formules de Newton, sont vérifiées.

Exercice 4 :

Soit a, b et c dans $\mathbb{Z}^*$ des entiers premiers entre eux deux à deux, non congrus à $0 \mod (17)$, et tels que $a^{17}+b^{17}+c^{17} = 0$.

a) Montrer d'abord l'existence de 3 entiers x, y, z dans $\mathbb{Z}^*$, non congrus à $0 \mod (17)$, tels que $x + y + z = 0$ et $x^{17} + y^{17} + z^{17} = 0 \mod (289)$.

b) Montrer qu'on peut même faire en sorte dans les égalités précédentes que x, y et z soient premiers entre eux deux à deux.

c) On note $\tilde{\sigma}_1$, $\tilde{\sigma}_2$, $\tilde{\sigma}_3$ les valeurs des fonctions σ_1, σ_2, σ_3 au point (x, y, z), et $(\tilde{S}_k)$ les sommes de Newton de x, y, z. Calculer $\tilde{S}_{17}$ à l'aide des $\tilde{\sigma}_i$. En déduire que

$$\tilde{\sigma}_2 \, \tilde{\sigma}_3 \, [\tilde{\sigma}_2^3 + 5\, \tilde{\sigma}_3^2] \, [\tilde{\sigma}_2^3 + 7\, \tilde{\sigma}_3^2] \equiv 0 \mod (17)$$

et en tirer une contradiction avec les hypothèses de départ. On obtient ainsi une démonstration du "premier cas" du grand théorème de Fermat avec $p = 17$ (le "second cas", plus difficile, est celui où l'un des 3 nombres a, b ou c serait multiple de 17). ■

a) Comme a, b et c ne sont pas divisibles par 17, en utilisant le petit théorème de Fermat on trouve :

$$0 \equiv a^{17} + b^{17} + c^{17} \equiv a + b + c \mod (17) \ .$$

Posons $a + b + c = 17\, k$, où $k \in \mathbb{Z}$. En utilisant la formule du binôme de Newton on voit facilement que $(a - 17\, k)^{17} \equiv a^{17} \mod \left(17^2\right)$, donc :

$$(a - 17\, k)^{17} + b^{17} + c^{17} \equiv 0 \mod (289) \ .$$

Les entiers $x = a - 17\, k$, $y = b$ et $z = c$ sont tels que $x + y + z = a + b + c - 17\, k = 0$, et $x^{17} + y^{17} + z^{17} \equiv 0 \mod (289)$. On vérifie aussi que ces entiers ne sont pas divisibles par 17.

b) Les entiers x, y et z ne sont pas nuls puisqu'ils ne sont pas divisibles par 17. Leur pgcd, d, n'est donc pas nul. Posons $x = d$

et $z = d z_1$. Les entiers x_1, y_1, z_1 sont premiers entre eux dans leur ensemble ; ils ne sont pas divisibles par 17 et $x_1 + y_1 + z_1 = 0$. Enfin, comme $17^2 (= 289)$ divise $d^{17} (x_1^{17} + y_1^{17} + z_1^{17})$, et que d est premier avec 17, on voit que $x_1^{17} + y_1^{17} + z_1^{17} \equiv 0 \bmod (289)$.
Les entiers x_1, y_1, z_1 sont aussi premiers entre eux deux à deux. En effet, si un nombre premier p divisait par exemple x_1 et y_1, alors p diviserait aussi $z_1 = -x_1 - y_1$, donc diviserait x_1, y_1 et z_1, ce qui est exclu.
On a donc bien prouvé, si l'hypothèse de départ est vraie, l'existence de trois entiers x, y et z, non divisibles par 17, premiers entre eux deux à deux, tels que $x + y + z = 0$, et tels que $x^{17} + y^{17} + z^{17} \equiv 0 \bmod (289)$.

c) Utilisons les formules de Waring. On obtient ici, en tenant compte du fait qu'il y a 3 indéterminées et que $\tilde{\sigma}_1 = 0$:

$$\tilde{S}_{17} = 17\,(-1)^{17} \sum_{2\alpha_2 + 3\alpha_3 = 17} (-1)^{\alpha_2 + \alpha_3} \frac{(\alpha_2 + \alpha_3 - 1)\,!}{\alpha_2\,!\,\alpha_3} \,\tilde{\sigma}_2^{\alpha_2}\,\tilde{\sigma}_3^{\alpha_3} \ .$$

Si $2\alpha_2 + 3\alpha_3 = 17$, alors $\alpha_2 \equiv 1 \bmod (3)$; on voit alors facilement que les solutions pour le couple (α_2, α_3) sont $(1,5)$, $(4,3)$ et $(7,1)$. On obtient par conséquent l'égalité :

$$\tilde{S}_{17} = 17\,(-1)^{17} \left((-1)^6 \frac{5\,!}{1\,!\,5\,!}\,\tilde{\sigma}_2\,\tilde{\sigma}_3^5 + (-1)^7 \frac{6\,!}{4\,!\,3\,!}\,\tilde{\sigma}_2^4\,\tilde{\sigma}_3^3 + (-1)^8 \frac{7\,!}{7\,!\,1\,!}\,\tilde{\sigma}_2^7\,\tilde{\sigma}_3 \right) ,$$

soit en effectuant les calculs :

$$\tilde{S}_{17} = -17\,\tilde{\sigma}_2\,\tilde{\sigma}_3\,(\tilde{\sigma}_3^4 - 5\,\tilde{\sigma}_2^3\,\tilde{\sigma}_3^2 + \tilde{\sigma}_2^6) \ .$$

Comme $17^2 (= 289)$ divise $\tilde{S}_{17}$, nous en déduisons :

$$\tilde{\sigma}_2\,\tilde{\sigma}_3\,(\tilde{\sigma}_3^4 - 5\,\tilde{\sigma}_2^3\,\tilde{\sigma}_3^2 + \tilde{\sigma}_2^6) \equiv 0 \bmod (17) \ .$$

Donc :

$$\begin{aligned} 0 \equiv \tilde{\sigma}_2\,\tilde{\sigma}_3\,(\tilde{\sigma}_3^4 - 5\,\tilde{\sigma}_2^3\,\tilde{\sigma}_3^2 + \tilde{\sigma}_2^6) &\equiv \tilde{\sigma}_2\,\tilde{\sigma}_3\,(35\,\tilde{\sigma}_3^4 + 12\,\tilde{\sigma}_2^3\,\tilde{\sigma}_3^2 + \tilde{\sigma}_2^6) \\ &\equiv \tilde{\sigma}_2\,\tilde{\sigma}_3\,(7\,\tilde{\sigma}_3^2 + \sigma_2^3)(5\,\tilde{\sigma}_3^2 + \sigma_2^3) \bmod (17) \ . \end{aligned}$$

Remarquons enfin que $\tilde{\sigma}_3 = x\,y\,z$ n'est pas divisible par 17. L'une des congruences suivantes est donc nécessairement vérifiée (modulo 17) :

$$\tilde{\sigma}_2 \equiv 0 \quad \text{ou} \quad \tilde{\sigma}_2^3 \equiv -7\,\tilde{\sigma}_3^2 \quad \text{ou} \quad \tilde{\sigma}_2^3 \equiv -5\,\tilde{\sigma}_3^2 \ .$$

En utilisant les formules de Waring, on obtient facilement l'égalité :

$$\tilde{S}_8 = 2\,\tilde{\sigma}_2^4 - 8\,\tilde{\sigma}_2\,\tilde{\sigma}_3^2 \ .$$

Pour tout $x \in \mathbb{Z}/_{17\mathbb{Z}}$, $x \neq 0$, on a $x^{16} = 1$, donc $x^8 = 1$ ou $x^8 = -1$.
Par conséquent, les valeurs de $\tilde{S}_8$ ne peuvent être que $1+1+1 = 3$, $-1+1+1 = 1$, $-1-1+1 = -1$ et $-1-1-1 = -3$, modulo 17. Les valeurs de $\tilde{S}_8^4$ ne peuvent donc être que 1 ou $9^2 \equiv -4$.
On voit donc immédiatement que $\tilde{\sigma}_2 \equiv 0 \bmod(17)$ est exclu.
Supposons $\tilde{\sigma}_2^3 \equiv -7\,\tilde{\sigma}_3^2$, soit $\sigma_3^2 \equiv -5\,\sigma_2^3$ ($35 \equiv 1$), d'où $\tilde{S}_8 \equiv 42\,\tilde{\sigma}_2^4 \equiv 8\,\tilde{\sigma}_2^4$ et $\tilde{S}_8^4 \equiv 8^4\,\tilde{\sigma}_2^{16} \equiv (64)^2 \equiv (-4)^2 \equiv -1$; ce qui est impossible.
Supposons $\tilde{\sigma}_2^3 \equiv -5\,\tilde{\sigma}_3^2$, soit $\sigma_3^2 \equiv -7\,\sigma_2^3$, d'où $\tilde{S}_8 \equiv 58\,\tilde{\sigma}_2^4 \equiv 7\,\tilde{\sigma}_2^4$ et $\tilde{S}_8^4 \equiv 7^4\,\tilde{\sigma}_2^{16} \equiv (49)^2 \equiv (-2)^2 \equiv 4$; ce qui est impossible.

Il y a contradiction. Il ne peut donc pas exister trois entiers a, b et c non divisibles par 17, tels que $a^{17} + b^{17} + c^{17} = 0$.

Exercice 5 :

En utilisant les formules de Newton, résoudre dans $\mathbb{C}$ les systèmes suivants :
a) $x^2+y^2+z^2 = 2,\ x^3+y^3+z^3 = 2,\ x^4+y^4+z^4 = 2$
b) $x^2+y^2+z^2 = 0,\ x^4+y^4+z^4 = 0,\ x^5+y^5+z^5 = 0$
c) $x+y+z = 1, x^2+y^2+z^2 = 9, \dfrac{1}{x}+\dfrac{1}{y}+\dfrac{1}{z} = 1$. ■

Nous noterons $\sigma_1, \sigma_2, \sigma_3$, les valeurs en x, y, z des polynômes symétriques élémentaires, et par S_1, S_2, S_3 les valeurs en x, y, z des sommes de Newton.

a) En utilisant les formules de Newton, on voit que les complexes x, y, z vérifient ce système d'équations si, et seulement si, :

$$S_2 = 2 = \sigma_1 S_1 - 2\sigma_2$$
$$S_3 = 2 = \sigma_1 S_2 - \sigma_2 S_1 + 3\sigma_3$$
$$S_4 = 2 = \sigma_1 S_3 - \sigma_2 S_2 + \sigma_3 S_1 .$$

Soit si, et seulement si :

$$2 = \sigma_1 S_1 - 2\sigma_2$$
$$2 = 2\sigma_1 - \sigma_2 S_1 + 3\sigma_3$$
$$2 = 2\sigma_1 - 2\sigma_2 + \sigma_3 S_1 .$$

D'où les conditions équivalentes :

$$\sigma_2 = \frac{1}{2}(\sigma_1^2 - 2)$$
$$\sigma_3 = \frac{1}{3}\big(2 - 2\sigma_1 + \frac{1}{2}\sigma_1(\sigma_1^2 - 2)\big) = \frac{1}{6}\sigma_1^3 - \sigma_1 + \frac{2}{3}$$
$$2 = 2\sigma_1 - (\sigma_1^2 - 2) + \frac{1}{6}\sigma_1^4 - \sigma_1^2 + \frac{2}{3}\sigma_1 = \frac{1}{6}\sigma_1^4 - 2\sigma_1^2 + \frac{8}{3}$$

La dernière condition s'écrit :

$$P(\sigma_1) = \sigma_1(\sigma_1^3 - 12\,\sigma_1 + 16) = 0\ .$$

Une solution évidente initialement est $x = y = 1$ et $z = 0$; une solution de cette équation est donc nécessairement 2. On trouve facilement :

$$P(\sigma_1) = \sigma_1\,(\sigma_1 - 2)^2\,(\sigma_1 + 4)\ .$$

On obtient donc trois solutions pour le triplet $\sigma_1, \sigma_2, \sigma_3$.

- $\sigma_1 = 0$, $\sigma_2 = -1$, $\sigma_3 = 2/3$, et (x, y, z) est un système des zéros du polynôme $X^3 - X - 2/3$.

- $\sigma_1 = 2$, $\sigma_2 = 1$, $\sigma_3 = 0$, et (x, y, z) est un système des zéros du polynôme $X^3 - 2\,X^2 + X = X(X-1)^2$. On retrouve ici les solutions évidentes.

- $\sigma_1 = -4$, $\sigma_2 = 7$, $\sigma_3 = -6$, et (x, y, z) est un système des zéros du polynôme $X^3 + 4\,X^2 + 7\,X + 6$. On trouve ici un zéro rationnel qui est -2. On vérifie que $X^3 + 4\,X^2 + 7\,X + 6 = (X+2)(X^2 + 2\,X + 3)$. Le triplet (x, y, z) est donc, à l'ordre près, égal à $(-2, -1 + \mathrm{i}\sqrt{2}, -1 - \mathrm{i}\sqrt{2})$.

b) En utilisant les formules de Newton, on voit que les complexes x, y, z vérifient ce système d'équations si, et seulement si, :

$$\begin{aligned} S_2 = 0 &= \sigma_1\,S_1 - 2\,\sigma_2 \\ S_4 = 0 &= \sigma_1\,S_3 - \sigma_2\,S_2 + \sigma_3\,S_1 \\ S_5 = 0 &= \sigma_1\,S_4 - \sigma_2\,S_3 + \sigma_3\,S_2\ . \end{aligned}$$

Soit si, et seulement si :

$$\begin{aligned} 0 &= \sigma_1\,S_1 - 2\,\sigma_2 \\ 0 &= \sigma_1\,S_3 + \sigma_3\,S_1 \\ 0 &= -\sigma_2\,S_3\ . \end{aligned}$$

Si $\sigma_1 = S_1 = 0$, les conditions deviennent $\sigma_1 = \sigma_2 = 0$. Les triplets (x, y, z) solutions qui vérifient cette condition sont donc les systèmes de zéros des polynômes de la forme $X^3 - \lambda^3$, où $\lambda \in \mathbb{C}$. On obtient les triplets $(\lambda, \lambda\,\mathrm{j}, \lambda\,\mathrm{j}^2)$.

Si $\sigma_1 = S_1 \neq 0$, alors $\sigma_2 \neq 0$ (première équation) ; les conditions s'écrivent $S_2 = \sigma_1^2 - 2\,\sigma_2 = 0$ et $S_3 = -\sigma_3 = 0$. Comme $S_3 = \sigma_1\,S_2 - \sigma_2\,S_1 + 3\,\sigma_3$, on obtient $0 = 0 - \sigma_2\,\sigma_1 + 0$, ce qui est contradictoire. Il n'y a donc pas de solutions pour lesquelles $\sigma_1 \neq 0$.

c) Ces conditions s'écrivent sous la forme :

$$\sigma_1 = 1 \quad \sigma_1^2 - 2\sigma_2 = 9 \quad \frac{\sigma_2}{\sigma_3} = 1 ,$$

soit encore :

$$\sigma_1 = 1 \quad \sigma_2 = -4 \quad \sigma_3 = -4 .$$

Les triplets (x, y, z) solutions sont donc les systèmes de zéros du polynôme $X^3 - X^2 - 4X + 4$. Un zéro évident de ce polynôme est 1. On obtient facilement la factorisation $X^3 - X^2 - 4X + 4 = (X-1)(X+2)(X-2)$. Les solutions sont donc les 6 triplets (x, y, z) tels que $\{x, y, z\} = \{1, -2, 2\}$.

§ X.5 *EQUATIONS ALGÉBRIQUES. EQUATIONS DE DEGRÉ 3*

Exercice 1 :

Calculer le discriminant des polynômes suivants de $\mathbb{C}[X]$:

a) $(X+a)^n + bX + c$ ($n \geqslant 3$, a, b, c dans $\mathbb{C}$). En déduire le discriminant général en degré 3.

b) $(X+a)^n + bX^n + cX^{n-1}$ ($n \geqslant 3$, a, $b \neq -1$, c dans $\mathbb{C}$).

c) $\dfrac{X^n}{n!} + \dfrac{X^{n-1}}{(n-1)!} + \ldots + 1$. ■

Soit un polynôme $P \in \mathbb{C}[X]$, de degré n, tel que $P = a_n \prod_{i=1}^{n} (X - x_i)$; nous conviendrons que son discriminant réduit est :

$$D(P) = \prod_{i<j} (x_i - x_j)^2 .$$

Deux polynômes associés ont donc même discriminant. On voit aussi que pour tout $a \in \mathbb{C}$, $D(P) = D(P(X-a))$. Rappelons que pour un polynôme réduit $P = \prod_{i=1}^{n} (X - x_i)$, on a l'égalité (cf. exercice 13 § IX.7) :

$$D(P) = (-1)^{\frac{n(n-1)}{2}} P'(x_i) .$$

a) Le discriminant du polynôme $P = (X+a)^n + bX + c$ est le même que celui du polynôme $Q = P(X-a) = X^n + b(X-a) + c = X^n + bX + c - ab$. On a l'égalité :

$$D(Q) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (n x_i^{n-1} + b) ,$$

où $Q = \prod_{i=1}^{n} (X - x_i)$. Posons $\delta = c - a\,b$.

Si $\delta = 0$, les zéros de Q sont tels que $x_i^{n-1} = -b$, sauf pour l'un d'eux qui est 0. Dans ce cas, il est clair que :

$$D(Q) = (-1)^{\frac{n(n-1)}{2}}\, b \prod_{i=1}^{n-1} (-b\,n + b) = (-1)^{\frac{n(n-1)}{2}} b^n\,(1-n)^{n-1}\ .$$

Si $\delta \neq 0$, pour tout $i \in [\![1, n]\!]$:

$$x_i^{n-1} = -b - \frac{\delta}{x_i}\ ,$$

donc :

$$D(Q) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} \left(b - n\left(b + \frac{\delta}{x_i}\right)\right) =$$

$$= (-1)^{\frac{n(n-1)}{2}} (n\,\delta)^n \prod_{i=1}^{n} \left(\frac{b(1-n)}{n\,\delta} - \frac{1}{x_i}\right)\ .$$

En utilisant la transformation par $1/X$ on obtient :

$$1 + b\,X^{n-1} + \delta\,X^n = \delta \prod_{i=1}^{n} \left(X - \frac{1}{x_i}\right)\ ,$$

d'où :

$$\prod_{i=1}^{n} \left(\frac{b(1-n)}{n\,\delta} - \frac{1}{x_i}\right) = \frac{1}{\delta} + \frac{b}{\delta}\left(\frac{b(1-n)}{n\,\delta}\right)^{n-1} + \left(\frac{b(1-n)}{n\,\delta}\right)^n\ .$$

Nous obtenons par conséquent :

$$D(Q) = (-1)^{\frac{n(n-1)}{2}} \left(n^n\,\delta^{n-1} + n\,b^n\,(1-n)^{n-1} + b^n\,(1-n)^n\right) =$$

$$= (-1)^{\frac{n(n-1)}{2}} \left(n^n\,\delta^{n-1} + b^n\,(1-n)^{n-1}\right)\ .$$

On voit que cette expression du discriminant convient aussi dans le cas où $\delta = 0$. L'expression générale du discriminant du polynôme P est donc :

$$D(P) = (-1)^{\frac{n(n-1)}{2}} \left(n^n\,(c - a\,b)^{n-1} + b^n\,(1-n)^{n-1}\right)\ .$$

Dans le cas où $n = 3$, on trouve :

$$D(P) = -\left(27\,(c - a\,b)^2 + 4\,b^3\right)\ ,$$

ce qui est bien la formule connue dans le cas où $a = 0$.
Si $P = X^3 + u X^2 + v X + w$, on écrit :

$$P = (X + u/3)^3 + (v - u^2/3) X + w - u^3/27 .$$

On a donc ici :

$$c - a b = w - u^3/27 - (u/3)(v - u^2/3) = w - u v/3 + 2 u^3/27 .$$

Nous en déduisons :

$$D(P) = -\left(27 \left(w - u v/3 + 2 u^3/27\right)^2 + 4 \left(v - u^2/3\right)^3\right) .$$

Tous calculs faits, on obtient :

$$D(P) = -4 u^3 w + u^2 v^2 + 18 u v w - 4 v^3 - 27 w^2 .$$

b) Si $a = 0$, alors le discriminant de ce polynôme est nul. Si $a \neq 0$, $P(0) \neq 0$, nous pouvons donc utiliser la transformation par $1/X$ pour calculer le discriminant. Etablissons une relation entre le discriminant d'un polynôme P de degré n tel que $a_0 = P(0) \neq 0$, et le discriminant du polynôme $T(P) = X^n P(1/X)$. Posons $P = a_n \prod_{i=1}^{n} (X - x_i)$; alors :

$$T(P) = a_n \prod_{i=1}^{n} (-x_i) \prod_{i=1}^{n} \left(X - \frac{1}{x_i}\right) = a_0 \prod_{i=1}^{n} \left(X - \frac{1}{x_i}\right) .$$

D'où :

$$D(T(P)) = \prod_{i<j} \left(\frac{1}{x_i} - \frac{1}{x_j}\right)^2 = \frac{\prod_{i<j} (x_j - x_i)^2}{\prod_{i<j} x_i^2 x_j^2} .$$

En notant σ_n le produit des x_i, le dénominateur de la fraction est :

$$\prod_{i<j} x_i^2 x_j^2 = \prod_{i<j} x_i x_j \times \prod_{j<i} x_j x_i = \prod_{i=1}^{n} \prod_{j \neq i} x_i x_j = \prod_{i=1}^{n} x_i^{n-1} \prod_{j \neq i} x_j =$$
$$= \prod_{i=1}^{n} x_i^{n-2} \sigma_n = \sigma_n^n \sigma_n^{n-2} = \sigma_n^{2n-2} = \left(\frac{a_0}{a_n}\right)^{2n-2} .$$

Nous obtenons donc l'égalité :

$$a_0^{2n-2} D(T(P)) = a_n^{2n-2} D(P) .$$

Dans le cas de l'exercice,

$$P = (X+a)^n + bX^n + cX^{n-1} \quad \text{et} \quad T(P) = (1+aX)^n + cX + b\,.$$

On peut écrire :

$$T(P) = a^n\left((1/a+X)^n + c/a^n\,X + b/a^n\right)\,.$$

En appliquant la formule trouvée dans le *a*), nous obtenons :

$$D(T(P)) = (-1)^{\frac{n(n-1)}{2}}\left(n^n\left(\frac{b}{a^n} - \frac{1}{a}\frac{c}{a^n}\right)^{n-1} + \left(\frac{c}{a^n}\right)^n (1-n)^{n-1}\right)\,.$$

Comme ici $a_0 = a^n$ et $a_n = 1+b$, on voit que :

$$D(P) = \left(\frac{a^n}{1+b}\right)^{2n-2}(-1)^{\frac{n(n-1)}{2}}\left(n^n\left(\frac{ba-c}{a^{n+1}}\right)^{n-1} + \frac{c^n}{a^{(n^2)}}(1-n)^{n-1}\right)\,.$$

On trouve finalement :

$$D(P) = \frac{(-1)^{\frac{n(n-1)}{2}}}{(1+b)^{2n-2}}\left(n^n\,(ba-c)^{n-1}\,a^{(n-1)^2} + c^n a^{(n^2-2n)}\,(1-n)^{n-1}\right)\,.$$

Cette formule est vraie aussi dans le cas où $a = 0$.

c) On voit facilement ici que :

$$P(X) = \frac{X^n}{n!} + P'(X)\,.$$

Pour tout zéro x_i de P, on a donc $P'(x_i) = -\dfrac{x_i^n}{n!}$. Le discriminant réduit de P est celui du polynôme normalisé $n!\,P$, donc :

$$D(P) = (-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^{n} n!\,P'(x_i) = (-1)^{\frac{n(n-1)}{2}}(-1)^n\prod_{i=1}^{n} x_i^n\,.$$

Comme :

$$\prod_{i=1}^{n} x_i = (-1)^n\,n!\,,$$

on obtient l'égalité :

$$D(P) = (-1)^{\frac{n(n-1)}{2}}(-1)^n\left((-1)^n\,n!\right)^n\,.$$

Enfin, puisque $n+n^2$ est toujours pair, on a :

$$D(P) = (-1)^{\frac{n(n-1)}{2}} (n!)^n \ .$$

Exercice 6 :

Résoudre une équation algébrique de degré n sur $\mathbb{C}$, sachant que ses racines forment une progression arithmétique. ■

Cherchons deux complexes a et b tel que les zéros du polynôme soient les nombres $a+k\,b$, où $k \in [\![1,n]\!]$. Remarquons qu'il y a, a priori, au moins deux solutions, puisque les zéros du polynôme peuvent s'écrire $a, a+b, \ldots, a+(n-1)\,b$ ou $a' = a+(n-1)\,b, a'-b, \ldots, a'-(n-1)\,b$; les deux valeurs de b sont opposées.

Les zéros devant être $a, a+b, \ldots, a+(n-1)\,b$, on a nécessairement :

$$\sigma_1 = n\,a + \frac{n(n-1)}{2}\,b = n\left(a + \frac{n-1}{2}\,b\right) \ ,$$

et par exemple :

$$S_2 = n\,a^2 + n(n-1)a\,b + \left(\sum_{i=0}^{n-1} i^2\right) b^2 =$$
$$= n\left(a^2 + (n-1)\,a\,b + \frac{(n-1)\,(2\,n-1)}{6}\,b^2\right) \ .$$

Nous en déduisons que nécessairement :

$$\frac{S_2}{n} = \left(\frac{\sigma_1}{n} - \frac{n-1}{2}\,b\right)^2 + (n-1)\left(\frac{\sigma_1}{n} - \frac{n-1}{2}\,b\right) b + \frac{(n-1)(2\,n-1)}{6}\,b^2 \ .$$

On trouve la condition :

$$\frac{(n-1)^2}{12}\,b^2 = \frac{S_2}{n} - \frac{\sigma_1^2}{n^2} \ .$$

Il y a donc comme prévu deux solutions pour b, opposées l'une de l'autre, qui donnent chacune une solution pour a.

Exercice 8 :

Soit $P = X^4 - 3\,X^2 + 5\,X - 1 \in \mathbb{C}[X]$, $P = \prod_{k=1}^{4} (X$

On pose $f = \sum_{1 \leqslant i < j \leqslant 4} \dfrac{x_i^4\, x_j^4}{x_i^4\, x_j^4 - x_i^4 - x_j^4 + 1}$.

Montrer que $f = \dfrac{303}{136}$. ■

On voit que :

$$f = \sum_{1 \leqslant i < j \leqslant 4} \frac{x_i^4\, x_j^4}{(x_i^4 - 1)\,(x_j^4 - 1)} = \sum_{1 \leqslant i < j \leqslant 4} \frac{1}{(x_i^{-4} - 1)} \frac{1}{(x_j^{-4} - 1)} .$$

Nous utiliserons des transformations d'équations algébriques pour résoudre ce problème.

D'abord deux transformations quadratiques :

Posons $Q(X) = \prod_{i=1}^{4} (X - x_i^2)$, on trouve :

$$Q(X^2) = \prod_{i=1}^{4} (X^2 - x_i^2) = \prod_{i=1}^{4} (X - x_i) \times \prod_{i=1}^{4} (X + x_i) = P(X)\, P(-X) .$$

Ecrivons $P(X) = (X^4 - 3\,X^2 - 1) + 5\,X$, on voit que :

$$Q(X^2) = (X^4 - 3\,X^2 - 1)^2 - 25\,X^2 ,$$

d'où :

$$Q(X) = (X^2 - 3\,X - 1)^2 - 25\,X = X^4 - 6\,X^3 + 7\,X^2 - 19\,X + 1 .$$

Posons de manière analogue $R(X) = \prod_{i=1}^{4} (X - x_i^4)$, on trouve :

$$R(X^2) = \prod_{i=1}^{4} (X^2 - x_i^4) = Q(X)\, Q(-X) .$$

Comme $Q(X) = X^4 + 7\,X^2 + 1 - (6\,X^2 + 19)\,X$, on voit que :

$$R(X) = (X^2 + 7\,X + 1)^2 - (6\,X + 19)^2\,X = X^4 - 22\,X^3 - 177\,X^2 - 347\,X + 1 .$$

Nous en déduisons, à l'aide de la transformation par $1/X$, que :

$$S(X) = \prod_{i=1}^{4} (X - x_i^{-4}) = X^4 - 347\,X^3 - 177\,X^2 - 22\,X + 1$$

Par le calcul direct, ou en utilisant le schéma généralisé de Hörner :

$$S(X+1) = \prod_{i=1}^{4}(X - (x_i^{-4} - 1)) = X^4 - 343\,X^3 - 1212\,X^2 - 1413\,X - 544\ .$$

Nous obtenons finalement :

$$544\prod_{i=1}^{4}\left(X - \frac{1}{(x_i^{-4}-1)}\right) = 544\,X^4 + 1413\,X^3 + 1212\,X^2 + 343\,X - 1\ .$$

La fonction symétrique cherchée est :

$$f = \tilde{\sigma}_2 = \frac{1212}{544} = \frac{303}{136}\ .$$

Exercice 14 :

> Soit $(\alpha, \beta) \in \mathbb{C}^2$. Former l'équation de degré 9 ayant pour racines les nombres $\alpha \mathrm{j}^{\,k} + \beta \mathrm{j}^{\,l}$, $(k,l) \in [\![0,2]\!]^2$. ■

Pour $(k,l) \in [\![0,2]\!]^2$, posons $x = \alpha \mathrm{j}^{\,k} + \beta \mathrm{j}^{\,l}$. On voit que :

$$x^3 = (\alpha \mathrm{j}^{\,k})^3 + (\beta \mathrm{j}^{\,l})^3 + 3\,\mathrm{j}^{\,k+l}\,\alpha\beta\,(\alpha \mathrm{j}^{\,k} + \beta \mathrm{j}^{\,l}) = \alpha^3 + \beta^3 + 3\,\mathrm{j}^{\,k+l}\,\alpha\beta\,x\ .$$

On en déduit que les nombres $u_{k,l} = \alpha \mathrm{j}^{\,k} + \beta \mathrm{j}^{\,l}$, $(k,l) \in [\![0,2]\!]^2$, sont tous zéros du polynôme :

$$P = (X^3 - (\alpha^3 + \beta^3))^3 - 27\,\alpha^3\,\beta^3\,X^3\ .$$

Si on était sûr que les $(u_{k,l})$ soient distincts, le problème serait résolu.

Convenons que pour $u \in \mathbb{Z}/3\,\mathbb{Z} = \mathbb{Z}_3$, $\mathrm{j}^{\,u}$ désigne $\mathrm{j}^{\,n}$, où n est un représentant de u. On a bien sûr la propriété $\mathrm{j}^{\,u}\,\mathrm{j}^{\,v} = \mathrm{j}^{\,u+v}$ pour tout $(u,v) \in \mathbb{Z}_3^2$. Le polynôme dont les zéros sont les $(u_{k,l})$ s'écrit :

$$Q = \prod_{(u,v)\in\mathbb{Z}_3^2}(X - (\alpha \mathrm{j}^{\,u} + \beta \mathrm{j}^{\,v}))\ .$$

On peut dans $\mathbb{Z}_3^2$ faire le changement de variable $u = p + q$ et $v = p - q$, puisque l'application $(p,q) \mapsto (p+q, p-q)$ est bijective. On trouve alors :

$$Q = \prod_{(p,q)\in\mathbb{Z}_3^2}(X - (\alpha \mathrm{j}^{\,p+q} + \beta \mathrm{j}^{p-q})) = \prod_{p\in\mathbb{Z}_3}\prod_{q\in\mathbb{Z}_3}(X - \mathrm{j}^{\,p}\,(\alpha \mathrm{j}^{\,q} + \beta \mathrm{j}^{\,-q}))\ .$$

Calculons le produit :

$$A_0 = \big(X - (\alpha+\beta)\big)\big(X - (\mathrm{j}\,\alpha + \mathrm{j}^{-1}\beta)\big)\big(X - (\mathrm{j}^{-1}\alpha + \mathrm{j}\,\beta)\big)\ ,$$

on trouve :

$$A_0 = \big(X - (\alpha+\beta)\big)\big(X^2 + (\alpha+\beta)\,X + (\alpha^2 - \alpha\beta + \beta^2)\big)\ ,$$

d'où :

$$A_0 = X^3 - 3\alpha\beta X - (\alpha^3 + \beta^3)\ .$$

En remplaçant α et β par $\mathrm{j}^p\alpha$ et $\mathrm{j}^p\beta$, on trouve :

$$A_p = \prod_{q\in\mathbb{Z}_3} \big(X - \mathrm{j}^p(\alpha\,\mathrm{j}^q + \beta\,\mathrm{j}^{-q})\big) = X^3 - 3\mathrm{j}^{2p}\alpha\beta X - (\alpha^3+\beta^3)\ .$$

On voit finalement que :

$$Q = \prod_{p\in\mathbb{Z}_3} A_p = \prod_{p\in\mathbb{Z}_3} \big(X^3 - (\alpha^3+\beta^3) - 3\mathrm{j}^{2p}\alpha\beta X\big)\ ,$$

d'où, comme $2p$ décrit $\mathbb{Z}_3$:

$$Q = \big(X^3 - (\alpha^3+\beta^3)\big)^3 - 27\,\alpha^3\beta^3 X^3\ ,$$

ce qu'il fallait démontrer.

Exercice 19 :

Soit $\gamma \in \mathbb{Q}$ tel que le nombre $\Delta = \frac{4}{27}(\gamma-1)^3 + \gamma^2$ (relatif à l'équation $(x-1)(x^2+x+\gamma) = 0$) soit > 0. En utilisant les formules de Cardan, démontrer que $\sqrt{3} = \sqrt[3]{2\sqrt{7}+3\sqrt{3}} - \sqrt[3]{2\sqrt{7}-3\sqrt{3}}$ (*indication :* faire $\gamma = 2$). Vérifier directement cette égalité et en trouver d'autres analogues. ■

On trouve que :

$$P = (X-1)(X^2+X+\gamma) = X^3 + (\gamma-1)\,X - \gamma\ ,$$

polynôme de degré 3, auquel est associé le discriminant $\Delta > 0$. Le polynôme P a donc exactement un zéro réel qui est 1, et d'après les formules de Cardan, on a l'égalité :

$$1 = \sqrt[3]{\frac{\gamma+\sqrt{\Delta}}{2}} + \sqrt[3]{\frac{\gamma-\sqrt{\Delta}}{2}}\ .$$

Pour $\gamma = 2$, on trouve $\Delta = 4 \times 28/27 > 0$, dans ce cas :

$$1 = \sqrt[3]{1 + \frac{2\sqrt{7}}{3\sqrt{3}}} + \sqrt[3]{1 - \frac{2\sqrt{7}}{3\sqrt{3}}} ,$$

d'où en multipliant par $\sqrt{3}$:

$$\sqrt{3} = \sqrt[3]{3\sqrt{3} + 2\sqrt{7}} + \sqrt[3]{3\sqrt{3} - 2\sqrt{7}} .$$

On pouvait démontrer cette égalité directement. Posons $\alpha = \sqrt[3]{3\sqrt{3} + 2\sqrt{7}}$ et $\beta = \sqrt[3]{3\sqrt{3} - 2\sqrt{7}}$. On vérifie que α et β sont deux réels tels que $\alpha^3 + \beta^3 = 6\sqrt{3}$ et $\alpha\beta = \sqrt[3]{27 - 28} = -1$. Donc $x = \alpha + \beta$ est la seule racine réelle de l'équation $x^3 = 6\sqrt{3} - 3x$. Comme $\sqrt{3}$ est racine de cette équation, on en déduit l'égalité.

Soit $n \in \mathbb{N}$, et $a \in \mathbb{Z}$, on a l'égalité $n\sqrt{n} + a\sqrt{n} = (n + a)\sqrt{n}$, donc $\sqrt{n}$ est zéro réel du polynôme :

$$P = X^3 + aX - (n + a)\sqrt{n} .$$

Le discriminant associé à cette équation de degré 3, est $\Delta = \frac{4}{27}a^3 + n(n + a)^2 \in \mathbb{Q}$. Si ce discriminant est > 0, par exemple si $a > 0$, $\sqrt{n}$ est le seul zéro réel de P. On en déduit l'égalité :

$$\sqrt{n} = \sqrt[3]{\frac{(n + a)\sqrt{n} + \sqrt{\Delta}}{2}} + \sqrt[3]{\frac{(n + a)\sqrt{n} - \sqrt{\Delta}}{2}} .$$

On retrouve pour $n = 3$ et $a = 3$, l'égalité démontrée précédemment.

§ X.6 *ÉQUATIONS DE DEGRÉ 4, ÉQUATIONS PARTICULIÈRES*

Exercice 1 :

Résoudre l'équation $x^4 + \frac{2}{27}x - \frac{1}{108} = 0$ par la méthode de Ferrari. ■

Soit $\lambda \in \mathbb{C}$, l'équation s'écrit :

$$x^4 + \lambda x^2 + \frac{\lambda^2}{4} = \lambda x^2 - \frac{2}{27}x + \frac{1}{108} + \frac{\lambda^2}{4} .$$

Cherchons $\lambda \neq 0$ tel que le terme de droite soit un carré parfait, ce qui est vrai si, et seulement si :

$$\frac{1}{27^2} = \lambda \left(\frac{1}{108} + \frac{\lambda^2}{4} \right) \quad \text{soit} \quad 27^2 \lambda^3 + 27\lambda - 4 = 0 \, .$$

On trouve une solution rationnelle $\lambda = 1/9$. L'équation initiale s'écrit par conséquent sous la forme :

$$\left(x^2 + \frac{1}{2 \times 9} \right)^2 = \frac{1}{9} \left(x - \frac{1}{9 \times 27} \right)^2 \, .$$

Les solutions sont les solutions des équations :

$$x^2 - \frac{1}{3} x + \frac{1}{2 \times 9} + \frac{1}{3^6} = 0 \, ,$$

et :

$$x^2 + \frac{1}{3} x + \frac{1}{2 \times 9} - \frac{1}{3^6} = 0 \, .$$

On trouve 4 solutions :

$$x_1 = \frac{1}{6} + \frac{\mathrm{i}\sqrt{85}}{54} \quad x_2 = \frac{1}{6} - \frac{\mathrm{i}\sqrt{85}}{54} \quad x_3 = -\frac{1}{6} + \frac{\mathrm{i}\sqrt{77}}{54} \quad x_4 = -\frac{1}{6} - \frac{\mathrm{i}\sqrt{77}}{54} \, .$$

Exercice 3 :

Résoudre l'équation $X^4 - 2X^3 + 5X^2 - 6X + 3 = 0$, en cherchant un changement de variable $X = aY + b$ ($a \in \mathbb{C}^*$, $b \in \mathbb{C}$) qui la transforme en une équation réciproque. Préciser tous les couples (a, b) qui conviennent. ■

On obtient par calcul le polynôme transformé :

$$Q(Y) = a^4 Y^4 + 2a^3(2b-1) Y^3 + a^2(6b^2 - 6b + 5) Y^2 + \\ + 2a(2b^3 - 3b^2 + 5b - 3) Y + b^4 - 2b^3 + 5b^2 - 6b + 3 \, .$$

Ce polynôme est réciproque de deuxième espèce si, et seulement si :

$$\begin{aligned} 6b^2 - 6b + 5 &= 0 \\ a^2(2b-1) &= -(2b^3 - 3b^2 + 5b - 3) \\ a^4 &= -(b^4 - 2b^3 + 5b^2 - 6b + 3) \end{aligned}$$

Ces conditions sont incompatibles. On devrait avoir :

$$(b^4 - 2b^3 + 5b^2 - 6b + 3)(2b-1)^2 + (2b^3 - 3b^2 + 5b - 3$$

et $6b^2 - 6b + 5 = 0$; or en divisant le premier polynôme par le deuxième (division euclidienne), on trouve un reste qui est $-37/54$. Le complexe b ne peut donc pas être zéro commun de ces deux polynômes.

Le polynôme $Q(Y)$ ne peut donc être que réciproque de première espèce, et il l'est si, et seulement si,

$$a^2(2b-1) = (2b^3 - 3b^2 + 5b - 3)$$
$$a^4 = (b^4 - 2b^3 + 5b^2 - 6b + 3) .$$

Si ces conditions sont réalisées, alors b vérifie l'équation :

$$(b^4 - 2b^3 + 5b^2 - 6b + 3)(2b-1)^2 = (2b^3 - 3b^2 + 5b - 3)^2 .$$

Après calcul, on trouve que cette équation s'écrit :

$$4b^3 + 2b^2 - 12b + 6 = 2(b-1)(2b^2 + 3b - 3) = 0 .$$

Inversement, si b vérifie cette équation, on voit facilement que $b \neq 1/2$, et que pour tout complexe a tel que :

$$a^2 = \frac{2b^3 - 3b^2 + 5b - 3}{2b-1} ,$$

le polynôme $Q(Y)$ est réciproque.

Pour $b = 1$, on trouve $a^2 = 1$.
Pour b racine de l'équation $2b^2 + 3b - 3 = 0$, on trouve, en utilisant l'autre racine b', que :

$$a^2 = \frac{17b - 12}{2b-1} = \frac{(17b-12)(2b'-1)}{(2b-1)(2b'-1)} = \frac{3 - 7b}{2} .$$

Les valeurs possibles pour b étant :

$$b = \frac{-3 + \sqrt{33}}{4} \quad \text{et} \quad \frac{-3 - \sqrt{33}}{4} .$$

Résolvons maintenant l'équation initiale.
On obtient pour $a = b = 1$:

$$Q(Y) = Y^4 + 2Y^3 + 5Y^2 + 2Y + 1 .$$

On peut écrire :

$$Q(Y) = Y^2 \left(Y^2 + \frac{1}{Y^2} + 2\left(Y + \frac{1}{Y}\right) + 5 \right) =$$
$$= Y^2 \left(\left(Y + \frac{1}{Y}\right)^2 + 2\left(Y + \frac{1}{Y}\right) + 3 \right) = Y^2 \left(\left(Y + \frac{1}{Y} + 1\right)^2 + 2 \right)$$

soit enfin :

$$Q(Y) = (Y^2+Y+1)^2 + 2\,Y^2 = \\ = \left(Y^2 + (1+\mathrm{i}\sqrt{2})\,Y + 1\right)\left(Y^2 + (1-\mathrm{i}\sqrt{2})\,Y + 1\right) .$$

Les discriminants de ces polynômes de degré 2 sont $2\,\mathrm{i}\sqrt{2}-5$ et $-(5+2\,\mathrm{i}\sqrt{2})$. Les racines carrées de $2\,\mathrm{i}\sqrt{2}-5$ sont :

$$\varepsilon\left(\sqrt{\frac{\sqrt{33}-5}{2}} + \mathrm{i}\sqrt{\frac{\sqrt{33}+5}{2}}\right) \quad (\varepsilon \in \{-1,+1\}) ,$$

et celles de $-(5+2\,\mathrm{i}\sqrt{2}) = \overline{2\,\mathrm{i}\sqrt{2}-5}$ sont les conjuguées. Les zéros du polynôme Q sont donc :

$$y_1 = -\frac{1+\mathrm{i}\sqrt{2}}{2} + \frac{1}{2}\left(\sqrt{\frac{\sqrt{33}-5}{2}} + \mathrm{i}\sqrt{\frac{\sqrt{33}+5}{2}}\right)$$

$$y_2 = -\frac{1+\mathrm{i}\sqrt{2}}{2} - \frac{1}{2}\left(\sqrt{\frac{\sqrt{33}-5}{2}} + \mathrm{i}\sqrt{\frac{\sqrt{33}+5}{2}}\right) ,$$

et les zéros conjugués. Les racines de l'équation initiale sont les $x_i = y_i + 1$, pour $i \in [\![1,4]\!]$, soit :

$$x_1 = \frac{1-\mathrm{i}\sqrt{2}}{2} + \frac{1}{2}\left(\sqrt{\frac{\sqrt{33}-5}{2}} + \mathrm{i}\sqrt{\frac{\sqrt{33}+5}{2}}\right)$$

$$x_2 = \frac{1-\mathrm{i}\sqrt{2}}{2} - \frac{1}{2}\left(\sqrt{\frac{\sqrt{33}-5}{2}} + \mathrm{i}\sqrt{\frac{\sqrt{33}+5}{2}}\right) ,$$

et les racines conjuguées.

Exercice 5 :

> Soit $R(X)$ la résolvante, obtenue par la méthode d'Euler, de l'équation $P(X) = X^4 + b\,X^2 + c\,X + d = 0$ $(b,c,d) \in \mathbb{C}^3$). Etudier le rapport entre les multiplicités des zéros de R et les multiplicités des zéros de P. ■

La résolvante R est le polynôme :

$$R = X^3 + 8\,b\,X^2 + 16\,(b^2 - 4\,d)\,X - 64\,c^2 .$$

Rappelons le rapport entre les zéros de R et les zéros de P. Si g_1, g_2, g_3 est une liste des zéros de R, et que $\gamma_1, \gamma_2, \gamma_3$ sont des racines carrées de ces zéros telles que $\gamma_1\,\gamma_2\,\gamma_3 = -8\,c$, alors les complexes :

$$y_1 = \frac{\gamma_1 + \gamma_2 + \gamma_3}{4} \qquad y_2 = \frac{\gamma_1 - \gamma_2 - \gamma_3}{4}$$
$$y_3 = \frac{-\gamma_1 + \gamma_2 - \gamma_3}{4} \qquad y_4 = \frac{-\gamma_1 - \gamma_2 + \gamma_3}{4}$$

forment une liste des zéros du polynôme P.

Rappelons que si D_P et D_R sont les discriminants des polynômes P et R, on a la relation $D_R = 2^{12}\,D_P$. On voit donc que le polynôme R n'a que des zéros simples si, et seulement si, le polynôme P n'a que des zéros simples.

Supposons que R ait un zéro double g et un zéro simple $r \neq g$. On peut trouver une racine carrée γ de g, et une racine carrée ρ de r telles que $\gamma^2\,\rho = -8\,c$. Une liste des zéros de P est alors

$$y_1 = \frac{2\gamma + \rho}{4} \quad y_2 = -\frac{\rho}{4} \quad y_3 = -\frac{\rho}{4} \quad y_4 = \frac{-2\gamma + \rho}{4}\,.$$

On vérifie que $y_1 \neq y_2$, car $\gamma \neq -\rho$, et que $y_3 \neq y_4$, car $\gamma \neq \rho$. Si le zéro double g n'est pas nul, alors $y_1 \neq y_4$, et dans ce cas, le polynôme P a exactement un zéro double et deux zéros simples. Si le zéro double g est nul, alors le polynôme P a deux zéros doubles.

Supposons que R admette un zéro triple g, l'une des racines carrées γ de g est telle que $\gamma^3 = -8\,c$. Une liste des zéros de P est donc $3\gamma/4$, $-\gamma/4$, $-\gamma/4$, $-\gamma/4$. Si $g \neq 0$, ce qui équivaut à la condition $c \neq 0$, le polynôme P admet un zéro d'ordre 3 et un zéro simple, et si $c = 0$ le polynôme P admet 0 comme zéro à l'ordre 4 ; dans ce dernier cas, $R = X^3$ et $P = X^4$.

Récapitulons maintenant du point de vue de P.
Si P n'a que des zéros simples alors R n'a que des zéros simples ;
si P a un zéro double et deux zéros simples alors R a un zéro double non nul et un zéro simple ;
si P a deux zéros doubles, R a un zéro double nul et un zéro simple ;
si P a un zéro triple et un zéro simple, R a un zéro triple non nul ;
si P a un zéro d'ordre 4 (c'est alors X^4), alors $R = X^3$.

Exercice 7 :

Résoudre dans $\mathbb{C}$ l'équation $x^4 + \frac{7}{3}x^2 + 30\,x - \frac{100}{3} = 0$ en commençant par chercher une racine rationnelle (terminer avec les formules de Cardan). ■

On vérifie que 1 est une racine rationnelle. En divisant le polynôme $P = x^4+\frac{7}{3}x^2+30\,x-\frac{100}{3}$, par $x-1$, on trouve le polynôme $Q = x^3+x^2+\frac{10}{3}x+\frac{100}{3}$. On obtient :

$$R(y) = Q\left(y-\frac{1}{3}\right) = y^3+3\,y+\frac{872}{27}\ .$$

Le discriminant de ce polynôme de degré 3 est :

$$\Delta = \frac{763300}{729} \quad \text{on pose} \quad \delta = \frac{10}{27}\sqrt{7633}\ .$$

Le polynôme R a donc un zéro réel et deux zéros complexes conjugués. En appliquant les formules de Cardan on trouve :

$$\alpha = \sqrt[3]{\frac{-872+10\sqrt{7633}}{54}} = \frac{1}{3}\sqrt[3]{-436+5\sqrt{7633}}\ ,\ \beta = \frac{1}{3}\sqrt[3]{-436-5\sqrt{7633}}\ .$$

Les zéros de R sont $\alpha+\beta$, $\alpha\,\mathrm{j}+\beta\,\mathrm{j}^2$, $\alpha\,\mathrm{j}^2+\beta\,\mathrm{j}$. Les zéros du polynôme P sont donc :

$$x_1 = 1 \quad x_2 = -\frac{1}{3}+\alpha+\beta \quad x_3 = -\frac{1}{3}+\alpha\,\mathrm{j}+\beta\,\mathrm{j}^2 \quad x_4 = -\frac{1}{3}+\alpha\,\mathrm{j}^2+\beta\,\mathrm{j}\ .$$

Exercice 12 :

a) Soit $(\alpha,\beta)\in\mathbb{C}^2$ et $(p,q)\in\mathbb{C}^2$ tels que $\alpha^5+\beta^5 = -2\,q$ et $\alpha\,\beta = p$, et $f(X) = X^5-5\,p\,X^3+5\,p^2\,X+2\,q$. Montrer que les racines de l'équation $f(x) = 0$ sont : $(\zeta\,\alpha+\bar{\zeta}\,\beta)_{\zeta\in\mu_5}$.

b) En supposant $(p,q)\in\mathbb{R}_+\times\mathbb{R}$, montrer :
si $p^5 < q^2$, 4 des racines de f sont non réelles, et une est réelle,
si $p^5 > q^2$, toutes les racines de f sont réelles,
si $p^5 = q^2$, f est divisible par le carré d'un polynôme. ■

a) Il est assez facile ici de calculer les polynômes de Newton en les nombres $(\zeta\,\alpha+\bar{\zeta}\,\beta)_{\zeta\in\mu_5}$.

D'abord $S_1 = \sigma_1 = 0$, car la somme des racines $5^{\text{ième}}$ de 1 est nulle.

Pour tout $\zeta\in\mu_5$, $(\alpha\,\zeta+\beta\,\bar{\zeta})^2 = \alpha^2\,\zeta^2+2\alpha\,\beta+\beta^2\,\bar{\zeta}^2$. Comme ζ^2 décrit μ_5, on en déduit $S_2 = 10\,\alpha\,\beta$.

En utilisant des calculs analogues on trouve :

$$(\alpha\,\zeta+\beta\,\bar{\zeta})^3 = \alpha^3\,\zeta^3+3\,\alpha^2\,\beta\,\zeta+3\,\alpha\,\beta^2\,\bar{\zeta}+\beta^3\,\bar{\zeta}^3\ ,$$

d'où $S_3 = 0$.

Puis :

$$(\alpha\zeta + \beta\bar{\zeta})^4 = \alpha^4\zeta^4 + 4\alpha^3\beta\zeta^2 + 6\alpha^2\beta^2 + 4\alpha\beta^3\bar{\zeta}^2 + \beta^4\bar{\zeta}^4 ,$$

d'où $S_4 = 30\alpha^2\beta^2$.

Enfin à l'aide de calculs analogues on trouve facilement $S_5 = 5(\alpha^5 + \beta^5)$.

En utilisant les formules de Newton, on détermine les valeurs des polynômes symétriques élémentaires en les $(\zeta\alpha + \bar{\zeta}\beta)_{\zeta\in\mu_5}$.

Comme $10\alpha\beta = \sigma_1^2 - 2\sigma_2$, on en déduit $\sigma_2 = -5\alpha\beta$.

Comme $0 = S_3 = S_2\sigma_1 - S_1\sigma_2 + 3\sigma_3$, on voit que $\sigma_3 = 0$.

Comme $S_4 = 30\alpha^2\beta^2 = S_3\sigma_1 - S_2\sigma_2 + S_1\sigma_3 - 4\sigma_4$, on voit que $4\sigma_4 = -30\alpha^2\beta^2 + 50\alpha^2\beta^2 = 20\alpha^2\beta^2$, d'où $\sigma_4 = 5\alpha^2\beta^2$.

On trouve enfin :

$$S_5 = 5(\alpha^5 + \beta^5) = S_4\sigma_1 - S_3\sigma_2 + S_2\sigma_3 - S_1\sigma_4 + 5\sigma_5 = 5\sigma_5 ,$$

d'où $\sigma_5 = \alpha^5 + \beta^5$.

Nous obtenons en définitive l'égalité :

$$\prod_{\zeta\in\mu_5}(X - \zeta\alpha - \bar{\zeta}\beta) = X^5 - 5\alpha\beta X^3 + 5\alpha^2\beta^2 X - (\alpha^5 + \beta^5) ,$$

d'où :

$$\prod_{\zeta\in\mu_5}(X - \zeta\alpha - \bar{\zeta}\beta) = X^5 - 5pX^3 + 5p^2X + 2q = f(X) ,$$

puisque $\alpha\beta = p$ et que $\alpha^5 + \beta^5 = -2q$.

Remarquons que α^5 et β^5 sont les zéros du polynôme $Q = X^2 + 2qX + p^5$. Si le discriminant réduit $\Delta = q^2 - p^5$ de Q n'est pas nul, alors $\alpha^5 \neq \beta^5$, et les nombres $(\zeta\alpha + \bar{\zeta}\beta)_{\zeta\in\mu_5}$ sont distincts. Supposons en effet $\zeta\alpha + \bar{\zeta}\beta = \eta\alpha + \bar{\eta}\beta$, où ζ et η sont des éléments de μ_5, distincts. En multipliant des deux côtés par $\zeta\eta$, on trouve :

$$\zeta^2\eta\alpha + \eta\beta = \eta^2\zeta\alpha + \zeta\beta \quad \text{soit} \quad (\zeta - \eta)(\zeta\eta\alpha - \beta) = 0 .$$

On en déduit $\alpha^5 = \beta^5$, ce qui est contradictoire.

b) Les nombres p et q sont supposés ici réels.

Si $\Delta > 0$, c'est-à-dire si $p^5 < q^2$, le polynôme Q a deux zéros réels distincts a et b. Posons $\alpha = \sqrt[5]{a}$ et $\beta = \sqrt[5]{b}$, on voit que $\alpha^5 + \beta^5 = -2q$, $\alpha^5 \beta^5 = p^5$, et par conséquent (puisque p et $\alpha\beta$ sont réels), que $\alpha\beta = p$. Notons u une racine primitive d'ordre 5. Les zéros du polynôme f sont tous simples et s'écrivent $x_1 = \alpha+\beta$, $x_2 = u\alpha+\bar{u}\beta$, $x_3 = \bar{u}\alpha+u\beta$, $x_4 = u^2\alpha+\bar{u}^2\beta$, $x_5 = \bar{u}^2\alpha + u^2\beta$. On voit que x_1 est réel, que x_2 et x_3 sont conjugués et distincts donc non réels, et que de même x_4 et x_5 sont conjugués et non réels. Le polynôme f a donc dans ce cas 1 zéro réel et 4 zéros complexes non réels.

Si $\Delta < 0$, c'est-à-dire si $q^2 < p^5$, le polynôme Q a deux zéros complexes non réels conjugués, a et $\bar{a}$. Soit $\alpha \in \mathbb{C}$ tel que $\alpha^5 = a$, on voit que $\alpha^5 + \bar{\alpha}^5 = -2q$ et $\alpha^5\bar{\alpha}^5 = p^5$, et par conséquent que $\alpha\bar{\alpha} = p$. Notons de nouveau u une racine primitive de 1 d'ordre 5. Les zéros de f sont les complexes $\alpha+\bar{\alpha}$, $u\alpha+\bar{u}\bar{\alpha}$, $\bar{u}\alpha+u\bar{\alpha}$, $u^2\alpha+\bar{u}^2\bar{\alpha}$, $\bar{u}^2\alpha+u^2\bar{\alpha}$. Ce sont 5 réels distincts d'après ce qui a été démontré à la fin du *a*).

Si $\Delta = 0$, on peut prendre $\alpha = \beta = -\sqrt[5]{q}$. Une famille des zéros du polynôme f est $2\alpha, (u+\bar{u})\alpha, (\bar{u}+u)\alpha, (u^2+\bar{u}^2)\alpha, (\bar{u}^2+u^2)\alpha$. Dans ce cas le polynôme f a donc 3 zéros réels dont deux doubles. Les nombres $u+\bar{u}$ et $u^2+\bar{u}^2$ sont les zéros du polynôme X^2+X-1 (voir exemple 1, racines 5-ièmes de l'unité). On voit donc que :

$$f(X) = (X-2\alpha)\big(X-\alpha(u+\bar{u})\big)^2\big(X-\alpha(u^2+\bar{u}^2)\big)^2 = \\ = (X-2\alpha)(X^2+\alpha X-\alpha^2)^2 .$$

Le polynôme f est donc bien divisible par le carré d'un polynôme.

Exercice 14 :

Calculer $\lambda \in \mathbb{C}$ pour que deux des racines de $x^4-2x^2+\lambda x+3 = 0$ aient pour produit 1. Résoudre alors l'équation. ■

Le produit de deux des zéros du polynôme $P = X^4 - 2X^2 + \lambda X + 3$ est 1 si et seulement si, il est divisible par un polynôme de la forme $X^2+\alpha X+1$. Dans ce cas, le quotient exact est nécessairement $X^2-\alpha X+3$. Le polynôme P a donc deux zéros dont le produit est 1 si, et seulement si, il existe un complexe α tel que :

$$P = X^4 - 2X^2 + \lambda X + 3 = (X^2+\alpha X+1)(X^2-\alpha X$$

Cette égalité est vraie si, et seulement si $-2 = 4 - \alpha^2$ et $\lambda = 2\alpha$, soit $\alpha = \varepsilon\sqrt{6}$ et $\lambda = 2\varepsilon\sqrt{6}$, où $\varepsilon \in \{-1, +1\}$. Les racines de l'équation $P(x) = 0$ sont les zéros de $X^2 + \alpha X + 1$, de discriminant 2, et de $X^2 - \alpha X + 3$, de discriminant -6. Les zéros dans $\mathbb{C}$ du polynôme P sont donc :

$$x_1 = \frac{-\varepsilon\sqrt{6} + \sqrt{2}}{2} \quad x_2 = \frac{-\varepsilon\sqrt{6} - \sqrt{2}}{2}$$
$$x_3 = \frac{\varepsilon\sqrt{6} + \mathrm{i}\sqrt{6}}{2} \quad x_4 = \frac{\varepsilon\sqrt{6} - \mathrm{i}\sqrt{6}}{2}$$

On a $x_1 x_2 = 1$.

Chapitre XI

MATRICES

§ XI.1 *MATRICES DE TYPE (m, n)*

Exercice 3 :

> Soit n un entier $\geqslant 2$. Une matrice $M = [a_{i,j}] \in \mathfrak{M}_n(A)$ est dite *en damier* ssi $a_{i,j} = 0$ pour $j - i$ impair. Montrer que si $M \in \mathfrak{M}_n(A)$, et $N \in \mathfrak{M}_n(A)$ sont en damier, il en est de même de leur somme et de leur produit. Généraliser à des matrices en damier par blocs. ■

Nous noterons simplement $M(i,j)$ le terme de ligne i et de colonne j de la matrice M (ce qui correspond précisément à sa définition).

a) Soient $M \in \mathfrak{M}_n(K)$ et $N \in \mathfrak{M}_n(K)$ deux matrices en damier.
Pour tout $(i,j) \in [\![1,n]\!]^2$ tel que $j - i$ est impair :

$$(M+N)(i,j) = M(i,j) + N(i,j) = 0 .$$

La matrice $M+N$ est donc en damier.
Pour tout $(i,k) \in [\![1,n]\!]^2$:

$$(M \times N)(i,k) = \sum_{j=1}^{n} M(i,j)\, N(j,k) . \qquad (1)$$

Si $k - i$ et impair, alors k et i n'ont pas la même parité ; pour tout $j \in [\![1,n]\!]$, j n'a pas la même parité que i ou j n'a pas la même parité que k. On voit donc que dans la somme (1) ci-dessus, chaque terme $M(i,j)\,N(j,k)$ est nul, et par conséquent que $(M \times N)(i,k) = 0$. La matrice $M \times N$ est donc en damier.

b) Soit $(n_1, n_2, \ldots, n_p)$ une suite d'entiers $\geqslant 1$, tels que $n_1 + n_2 + \ldots + n_p = n$. On pose aussi $n_0 = 0$, $s_0 = 0$, et pour tout $i \in [\![1,p]\!]$, $s_i = n_1 + \ldots + n_i$. On note I_i l'intervalle $[\![s_{i-1}+1, s_i]\!]$, pour $i \in [\![1,p]\!]$. Si M

sa sous-matrice $\mathfrak{M}_{I_i,I_j}(M)$, où $(i,j) \in [\![1,p]\!]^2$, est notée aussi $\mathrm{BL}_{i,j}(M)$; on remarque que $\mathrm{BL}_{i,j}(M) \in \mathfrak{M}_{n_i,n_j}$. Le théorème XI.1.2, dans ce cas particulier, permet d'affirmer que si M et N sont des éléments de $\mathfrak{M}_n(K)$, pour tout $(i,k) \in [\![1,p]\!]^2$:

$$\mathrm{BL}_{i,k}(M \times N) = \sum_{j=1}^{p} \mathrm{BL}_{i,j}(M) \times \mathrm{BL}_{j,k}(N) \,. \tag{2}$$

Nous dirons que $M \in \mathfrak{M}_n(K)$ est en damier par blocs, relativement à la suite $(n_1,\ldots,n_p)$, si pour tout $(i,j) \in [\![1,p]\!]^2$ tel que $i-j$ est impair, $\mathrm{BL}_{i,j}(M) = 0$. En utilisant l'égalité (2), on voit facilement comme dans le a), que le produit de deux matrices en damier par blocs est en damier par blocs. Il est d'autre part évident que leur somme est aussi en damier par blocs.

§ XI.2 *MATRICES CARRÉES*

Exercice 1 :

Le corps de base est $\mathbb{R}$. Soit $M = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2,\mathbb{R})$ et $N = {}^tM$. Montrer : quels que soient $n \in \mathbb{N}^*$, et $(\alpha_1,\alpha_2,\ldots,\alpha_n) \in \mathbb{N}^n$, $(\beta_1,\beta_2,\ldots,\beta_n) \in \mathbb{N}^n$, la relation :

$$M^{\alpha_1} N^{\beta_1} M^{\alpha_2} N^{\beta_2} \ldots M^{\alpha_n} N^{\beta_n} = I_2$$

entraîne $\alpha_1 = \alpha_2 = \ldots = \alpha_n = 0 = \beta_1 = \beta_2 = \ldots = \beta_n = 0$. ■

Posons $R_0 = I_2$ et pour tout $k \in [\![1,n]\!]$

$$R_k = M^{\alpha_1} N^{\beta_1} M^{\alpha_2} N^{\beta_2} \ldots M^{\alpha_k} N^{\beta_k} = \begin{pmatrix} a_k & b_k \\ c_k & d_k \end{pmatrix} .$$

Pour tout $k \in [\![0,n-1]\!]$ on a l'égalité :

$$R_{k+1} = \begin{pmatrix} a_k & b_k \\ c_k & d_k \end{pmatrix} \begin{pmatrix} 1 & 2\alpha_{k+1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2\beta_{k+1} & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} a_k & b_k \\ c_k & d_k \end{pmatrix} \begin{pmatrix} 1+4\beta_{k+1}\alpha_{k+1} & 2\alpha_{k+1} \\ 2\beta_{k+1} & 1 \end{pmatrix} .$$

On a donc pour tout $k \in [\![0,n-1]\!]$ les relations de récurrence :

$$(1) \quad a_{k+1} = (1+4\beta_{k+1}\alpha_{k+1})\,a_k + 2\beta_{k+1}\,b_k$$

$$(2) \quad b_{k+1} = 2\alpha_{k+1}\,a_k + b_k$$

$$(3) \quad c_{k+1} = (1+4\beta_{k+1}\alpha_{k+1})\,c_k + 2\beta_{k+1}\,d_k$$

$$(4) \quad d_{k+1} = 2\alpha_{k+1}\,c_k + d_k$$

Il est clair par récurrence que les suites (a_k), (b_k), (c_k) et (d_k) sont des suites dans $\mathbb{N}$. Comme les suites (α_k) et (β_k) sont aussi $\geqslant 0$, on voit que les suites (a_k), (b_k), (c_k) et (d_k) sont croissantes. Puisque $R_0 = I_2 = R_n$, il est clair que ces suites sont constantes, d'où pour tout $k \in [\![0, n]\!]$, $a_k = d_k = 1$ et $b_k = c_k = 0$. Des égalités (2) et (3) nous déduisons enfin que pour tout $k \in [\![0, n-1]\!]$, $\alpha_{k+1} = \beta_{k+1} = 0$, ce qu'il fallait démontrer.

Exercice 2 :

a) K est un corps commutatif. Soit $n \in \mathbb{N}^*$ et $T : \mathfrak{M}_n(K) \to \mathfrak{M}_n(K)^*$ qui associe, à chaque matrice $M \in \mathfrak{M}_n(K)$, la forme linéaire $T_M : X \mapsto \mathrm{Tr}(M\,X)$ sur $\mathfrak{M}_n(K)$. Démontrer que T est un isomorphisme de K-ev.

b) Soit $\varphi \in (\mathfrak{M}_n(K))^*$ telle que $\varphi(M\,N) = \varphi(N\,M)$ pour toutes matrices M, N de $\mathfrak{M}_n(K)$. On note M_0 la matrice élément de $\mathfrak{M}_n(K)$ telle que $\varphi = T_{M_0}$ (cf. *a*)). Démontrer que $(\forall M \in \mathfrak{M}_n(K))\quad M_0\,M = M\,M_0$. En déduire que $\varphi = \lambda\,\mathrm{Tr}$ pour un $\lambda \in K$. En déduire que le sous-K-ev de $\mathfrak{M}_n(K)$ engendré par les matrices $M\,N - N\,M$ ($M \in \mathfrak{M}_n(K)$, $N \in \mathfrak{M}_n(K)$) est un hyperplan $\mathscr{H}$. ■

Nous noterons $E_{i,j}$, pour $(i,j) \in [\![1, n]\!]^2$, la matrice élément de $\mathfrak{M}_n(K)$ dont tous les termes sont nuls, sauf le terme de ligne i et de colonne j qui est 1. On rappelle que la famille $(E_{i,j})_{(i,j)\in[\![1,n]\!]^2}$ est une base de $\mathfrak{M}_n(K)$ (c'est la base dite canonique). Calculons les valeurs des produits de deux éléments de la base canonique. Nous utiliserons le symbole de Kronecker : $\delta_{i,j} = 0$ si $i \neq j$ et $\delta_{i,j} = 1$ si $i = j$.

Pour tous entiers i, j, h, k, p, q dans $[\![1, n]\!]$, on a :

$$(E_{i,j} \times E_{h,k})(p,q) = \sum_{r=1}^{n} E_{i,j}(p,r)\,E_{h,k}(r,q) = \sum_{r=1}^{n} \delta_{i,p}\,\delta_{j,r}\,\delta_{h,r}\,\delta_{k,q}\ .$$

Dans cette somme le terme d'indice r n'est pas nul si, et seulement si, $i = p$, $r = j = h$ et $k = q$. On en déduit que si $j \neq h$, $E_{i,j} \times E_{h,k} = 0$.
Si $j = h$, un seul terme de la somme peut ne pas être nul :

$$(E_{i,j} \times E_{j,k})(p,q) = \sum_{r=1}^{n} \delta_{i,p}\,\delta_{j,r}\,\delta_{k,q} = \delta_{i,p}\,\delta_{k,q} = E_{i,k}(p,q)\ .$$

On voit donc que $E_{i,j} \times E_{j,k} = E_{i,k}$.

a) L'application $M \mapsto T_M$ est évidemment linéaire ; démontrons qu'elle est bijective.
La forme linéaire φ, élément de $(\mathfrak{M}_n(K))^*$, coïncide avec T_M si et seulement si, pour tout $(i,j) \in [\![1,n]\!]^2$, $T_M(E_{i,j}) = \varphi(E_{i,j})$ (puisque la famille $(E_{i,j})_{(i,j)\in[\![1,n]\!]^2}$ est une base de $\mathfrak{M}_n(K)$). Cette condition s'écrit :

$$(\forall (i,j) \in [\![1,n]\!]^2) \quad \mathrm{Tr}\,(M \times E_{i,j}) = \varphi(E_{i,j})\ .$$

Or $M = \sum_{h,k} M(h,k)\, E_{h,k}$, donc, d'après les formules établies en introduction, $M \times E_{i,j} = \sum_{h=1}^{n} M(h,i)\, E_{h,j}$, et $\mathrm{Tr}\,(M \times E_{i,j}) = M(j,i)$. Cela démontre l'existence et l'unicité de la forme linéaire φ. On a précisément, pour toute matrice $N \in \mathfrak{M}_n(K)$:

$$\varphi(N) = \sum_{(i,j)\in[\![1,n]\!]^2} N(i,j)\,\varphi(E_{i,j}) = \sum_{(i,j)\in[\![1,n]\!]^2} N(i,j)\,M(j,i)\ .$$

b) Pour toutes matrices M et N dans $\mathfrak{M}_n(K)$, on a l'égalité :

$$\mathrm{T}_{M_0}(N\,M) = \mathrm{T}_{M_0}(M\,N) \quad \text{soit} \quad \mathrm{Tr}\,((M_0\,N)\,M) = \mathrm{Tr}\,(M_0\,M\,N)\ ,$$

d'où :

$$\mathrm{Tr}\,(M\,(M_0\,N)) = \mathrm{Tr}\,(M_0\,M\,N) \quad \text{soit} \quad \mathrm{T}_{M\,M_0 - M_0\,M}(N) = 0\ .$$

Nous en déduisons, pour toute matrice $M \in \mathfrak{M}_n(K)$, $\mathrm{T}_{M\,M_0 - M_0\,M} = 0$, donc d'après *a*), $M\,M_0 - M_0\,M = 0$. D'après le théorème IX.6.3, nous pouvons en déduire : $\exists \lambda \in K \mid M_0 = \lambda\, I_n$, d'où $\varphi = \lambda\,\mathrm{Tr}$.

Soit $\mathcal{H}$ un hyperplan contenant le sous-ev G engendré par les matrices de la forme $M\,N - N\,M$, où M et N sont dans $\mathfrak{M}_n(K)$. L'hyperplan $\mathcal{H}$ est noyau d'une forme linéaire φ telle que pour toutes matrices M et N dans $\mathfrak{M}_n(K)$, $\varphi(M\,N) = \varphi(N\,M)$. D'après ce qui précède, il existe un scalaire $\lambda \in K$ tel que $\varphi = \lambda\,\mathrm{Tr}$. Il y a donc un seul hyperplan qui contienne l'espace G, l'hyperplan formé par les matrices de trace nulle. Or dans un K-ev de dimension finie, un sous-espace est intersection des hyperplans qui le contiennent (Théorème IX.5.1, Corollaire 2) ; nous en déduisons $G = \mathcal{H}$, ce qu'il fallait démontrer.

Exercice 4 :

K est un corps commutatif, n un entier fixé $\geqslant 2$.
a) Trouver les idéaux bilatères $\mathfrak{b}$ de la K-algèbre $\mathfrak{S}$

sont *maximaux* pour l'inclusion.

b) Trouver dans $\mathcal{T}_+(n,K)$ un idéal bilatère non nul *minimal*. ■

Nous reprendrons les résultats de l'exercice précédent sur les matrices $E_{i,j}$, qui forment la base canonique de $\mathfrak{M}_n(K)$.

a) On sait que si M et N sont deux matrices trigonales supérieures d'éléments diagonaux $(\lambda_1,\dots,\lambda_n)$ et $(\mu_1,\dots,\mu_n)$, alors la matrice $M\times N$ est trigonale supérieure d'éléments diagonaux $(\lambda_1\,\mu_1,\dots,\lambda_n\,\mu_n)$. Il est donc clair que pour tout $i\in[\![1,n]\!]$ l'application $\mathcal{T}_+(n,K)\to K$, $M\mapsto M(i,i)$, est un homomorphisme d'algèbres. Nous en déduisons que pour tout $i\in[\![1,n]\!]$, l'ensemble $\mathfrak{I}_i=\{M\in\mathcal{T}_+(n,K)\mid M(i,i)=0\}$, est un idéal bilatère de l'algèbre $\mathcal{T}_+(n,K)$.

Montrons que ces idéaux bilatères sont maximaux pour l'inclusion parmi les idéaux stricts de l'algèbre $\mathcal{T}_+(n,K)$. Soit $i\in[\![1,n]\!]$ et $\mathfrak{I}$ un idéal bilatère de l'algèbre $\mathcal{T}_+(n,K)$ tel que $\mathfrak{I}_i\subset\mathfrak{I}$. Si $\mathfrak{I}\neq\mathfrak{I}_i$, alors il existe un élément $M\in\mathfrak{I}\setminus\mathfrak{I}_i$, c'est-à-dire tel que $M(i,i)\neq 0$. La matrice $N=M-M(i,i)\,I_n$ est un élément de $\mathfrak{I}_i$, donc de $\mathfrak{I}$, et par conséquent $M(i,i)\,I_n\in\mathfrak{I}$. Comme $M(i,i)\neq 0$, nous en déduisons $I_n\in\mathfrak{I}$, et donc finalement $\mathfrak{I}=\mathcal{T}_+(n,K)$. Les idéaux $\mathfrak{I}_i$ sont donc bien maximaux.

Montrons que ce sont les seuls idéaux maximaux. Soit $\mathfrak{M}$ un idéal bilatère maximal de l'algèbre $\mathcal{T}_+(n,K)$. Si $\mathfrak{M}$ n'est inclus dans aucun des idéaux $\mathfrak{I}_i$, où $i\in[\![1,n]\!]$, alors pour tout $i\in[\![1,n]\!]$, il existe une matrice M telle que $M\in\mathfrak{M}$, et $M(i,i)\neq 0$; la matrice $(M(i,i))^{-1}E_{i,i}\times M$ est aussi dans l'idéal $\mathfrak{M}$ et cette matrice est en fait la matrice $E_{i,i}$. Nous en déduisons que si $\mathfrak{M}$ n'est inclus dans aucun des idéaux $\mathfrak{I}_i$, où $i\in[\![1,n]\!]$, alors pour tout $i\in[\![1,n]\!]$, $E_{i,i}\in\mathfrak{M}$, donc $I_n=\sum_{i=1}^{n}E_{i,i}\in\mathfrak{M}$, ce qui implique $\mathfrak{M}=\mathcal{T}_+(n,K)$; ceci est exclu, puisque $\mathfrak{M}$ est un idéal bilatère strict. Il existe donc un entier $i\in[\![1,n]\!]$ tel que $\mathfrak{M}\subset\mathfrak{I}_i$; mais comme $\mathfrak{M}$ est un idéal maximal et que $\mathfrak{I}_i$ est un idéal strict, on en déduit $\mathfrak{M}=\mathfrak{I}_i$. Les idéaux bilatères maximaux de l'algèbre $\mathcal{T}_+(n,K)$ sont donc bien les idéaux $\mathfrak{I}_i$, où $i\in[\![1,n]\!]$.

b) Montrons que le sous-K-espace vectoriel de $\mathcal{T}_+(n,K)$ engendré par $E_{1,n}$, est aussi un idéal de cette algèbre. Notons $\mathfrak{I}$ cette droite vectorielle.

Pour tout $M\in\mathcal{T}_+(n,K)$:

$$M\times E_{1,n}=\sum_{i\leqslant j}M(i,j)\,E_{i,j}\times E_{1,n}=\sum_{i\leqslant 1}M(i,1)\,E_{i,n}=M(1,1)\,E_{1,n}\in\mathfrak{I}\,.$$

et :

$$E_{1,n} \times M = \sum_{i \leqslant j} M(i,j)\, E_{1,n} \times E_{i,j} = \sum_{n \leqslant j} M(n,j)\, E_{1,j} = M(n,n)\, E_{1,n} \in \Im\ .$$

Le sous-K-espace vectoriel $\Im$ est bien un idéal de l'algèbre $\mathcal{T}_+(n,K)$, et comme c'est un sous-K-espace vectoriel de dimension 1, il est évidemment minimal parmi les idéaux non nuls, qui sont aussi des sous-K-espaces vectoriels de $\mathcal{T}_+(n,K)$.

Exercice 8 *(matrices bistochastiques)* **:**

a) Soit E et F deux ensembles finis non vides et $\varphi : E \to \mathcal{P}(F)$, une application qui satisfait l'hypothèse

$$(\mathcal{H}) \qquad \forall X \subset E\ , \quad \operatorname{card}\left(\bigcup_{x \in X} \varphi(x)\right) \geqslant \operatorname{card}(X)\ .$$

Montrer qu'il existe $f : E \to F$ *injective* telle que $f(x) \in \varphi(x)$ pour tout $x \in E$ ("Lemme des mariages", ainsi nommé parce qu'il constitue la condition nécessaire et suffisante pour que, si chacun des Messieurs $x \in E$ connaît l'ensemble $\varphi(x)$ de Dames, alors chacun d'eux puisse épouser une dame de sa connaissance).

b) Soit $n \in \mathbb{N}$ $(n \geqslant 2)$; on note S l'ensemble des matrices $M = [a_{ij}] \in \mathfrak{M}_n(\mathbb{R})$ telles que :

$$(\forall (i,j) \in [\![1,n]\!]^2)\ \sum_{k=1}^{n} a_{ik} = 1\ ,\ \sum_{k=1}^{n} a_{kj} = 1 \text{ et } a_{ij} \in \mathbb{R}_+\ .$$

Déduire de *a*) que si $M = [a_{ij}] \in S$, il existe $\sigma \in \mathfrak{S}_n$ telle que $a_{\sigma(i)\,i} > 0$ pour tout $i \in [\![1,n]\!]$.

c) Un élément $M \in S$ est dit *extrémal* ssi les relations $M_1 \in S$, $M_2 \in S$ et $M = \frac{1}{2}(M_1 + M_2)$ entraînent $M_1 = M_2 = M$. Montrer que toute *matrice de permutation*, i.e. du type

$$M = [\delta_{\sigma^{-1}(i)\,j}]_{(i,j) \in [\![1,n]\!]^2} = P_\sigma$$

pour une $\sigma \in \mathfrak{S}_n$, ($\delta$: symbole de Kronecker) est élément extrémal de S.

d) Soit M un élément *extrémal* de S. Montrer que pour tout réel $\lambda > 1$, et toute matrice $N \in S$, $N \neq M$, on a $\lambda M + (1-\lambda) N \notin S$. En déduire que pour $\lambda > 1$ et $N \in S$, $N \neq M$, l'un au moins des coefficients de $\lambda M + (1-\lambda) N$ est < 0. En déduire que si P_σ ($\sigma \in \mathfrak{S}_n$) est une matrice de permutation distincte de M, posant $M = [a_{ij}]$, alors il existe $(k,l) \in [\![1,n]\!]^2$ tel que $a_{kl} = 0$ et $\sigma^{-1}(k) = l$. Comparer ce rés

Conclure enfin : les éléments extrémaux de S sont exactement les $(P_\sigma)_{\sigma\in\mathfrak{S}_n}$. ■

a) Soit R la relation entre E et F dont le graphe est l'ensemble des couples (x,y) tels que $x\in E$ et $y\in\varphi(x)$; on écrira $(x,y)\in R$ à la place de $x\in E$ et $y\in\varphi(x)$ (en identifiant R et son graphe). Si $X\subset E$, l'ensemble $\{y\in F \mid \exists x\in X\ ,(x,y)\in R\}$, sera dit image (directe) de X par la relation R et noté $R(X)$. On a bien sûr l'égalité $R(X)=\bigcup_{x\in X}\varphi(x)(\subset F)$.
Nous utiliserons deux propriétés de cette notation :
- si $X\subset X'\subset E$ alors $R(X)\subset R(X')$,
- si $X\subset E$ et $X'\subset E$, $R(X\cup X')=R(X)\cup R(X')$.
La démonstration de ces propriétés élémentaires ne pose pas de difficulté.
La propriété à démontrer devient :
Soient E et F deux ensembles finis et R une relation entre E et F, si R est telle que :

$$(\forall X\subset E)\quad \mathrm{card}\,(R(X))\geqslant \mathrm{card}\,(X)\ ,$$

alors il existe une injection $f: E\to F$ telle que pour tout $x\in E$, $(x,f(x))\in R$. Nous démontrerons cette propriété par récurrence sur le cardinal de E.

La propriété est évidemment vraie si $\mathrm{card}\,(E)=1$. Supposons qu'elle soit vraie si $\mathrm{card}\,(E)\leqslant n$, où $n\in\mathbb{N}$, $n\geqslant 1$. Soit E un ensemble fini de cardinal $n+1$, F un ensemble fini, et R une relation entre E et F telle que :

$$(\forall X\subset E)\quad \mathrm{card}\,(R(X))\geqslant \mathrm{card}\,(X)\ .$$

Supposons d'abord que pour toute partie X de E, $X\neq\emptyset$ et $X\neq E$, $\mathrm{card}\,(R(X))>\mathrm{card}\,(X)$. Soit $a\in E$, et $b\in F$ tels que $(a,b)\in R$ ($R(\{a\})$ n'est pas vide d'après l'hypothèse). Soit R' la relation obtenue en restreignant R à $E\setminus\{a\}$ pour le départ, et à $F\setminus\{b\}$ pour l'arrivée. Si $X=\emptyset$, alors $\mathrm{card}\,(R'(X))=\mathrm{card}\,(X)=0$; si X est une partie non vide de $E\setminus\{a\}$ alors $R'(X)=R(X)\setminus\{b\}$, mais comme $\mathrm{card}\,(R(X))>\mathrm{card}\,(X)$ on voit que $\mathrm{card}\,(R'(X))\geqslant\mathrm{card}\,(X)$. D'après l'hypothèse de récurrence, il existe une injection $f': E\setminus\{a\}\to F\setminus\{b\}$, telle que pour tout $x\in E\setminus\{a\}$, $(x,f'(x))\in R'$, soit $(x,f'(x))\in R$. Posons pour $x\in E$, $f(x)=f'(x)$ si $x\neq a$, et $f(a)=b$; il est clair que f est une injection $E\to F$ telle que pour tout $x\in E$, $(x,f(x))\in R$.

Supposons maintenant qu'il existe une partie A de E, $A\neq\emptyset$ et $A\neq E$, telle que $\mathrm{card}\,(R(A))=\mathrm{card}\,(A)$. Considérons la restriction R' de R à A pour ensemble de départ et à $R(A)$ pour ensemble d'arrivée. Pour toute partie $X\subset A$, $R(X)\subset R(A)$, d'où $R'(X)=R(X)$. On voit donc que pour toute partie $X\subset A$, $\mathrm{card}\,(R'(X))\geqslant\mathrm{card}\,(X)$. Nous en déduisons, en utilisant l'hypothèse de récurrence, qu'il existe une injection f'

telle que pour tout $x \in A$, $(x, f'(x)) \in R'$, soit $(x, f'(x)) \in R$.
Notons B le complémentaire de A dans E. C'est une partie stricte et non vide de E. Considérons la restriction R'' de R, à B pour l'ensemble de départ et à $F \setminus R(A)$ pour l'ensemble d'arrivée. Soit $Y \subset B$,

$$R(A \cup Y) = R(A) \cup R(Y) = R(A) \cup (R(Y) \setminus R(A)) = R(A) \cup R''(Y) .$$

Comme $\text{card}\,(R(A \cup Y)) \geqslant \text{card}\,(A \cup Y) = \text{card}\,(A) + \text{card}\,(Y)$ on en déduit :

$$\begin{aligned} \text{card}\,(R''(Y)) &= \text{card}\,(R(A \cup Y) - \text{card}\,(R(A)) \geqslant \\ &\geqslant \text{card}\,(Y) + \text{card}\,(A) - \text{card}\,(R(A)) = \text{card}\,(Y) . \end{aligned}$$

D'après l'hypothèse de récurrence, il existe une injection $f'' : B \to F \setminus R(A)$, telle que pour tout $x \in B$, $(x, f''(x)) \in R''$, soit $(x, f''(x)) \in R$.
Posons pour $x \in E$, $f(x) = f'(x)$ si $x \in A$, et $f(x) = f''(x)$ si $x \in B$; il est clair que comme f' et f'' ont des images disjointes, on définit ainsi une injection $f : E \to F$, telle que pour tout $x \in E$, $(x, f(x)) \in R$.

La propriété est donc démontrée pour tout ensemble E de cardinal $n+1$, ce qui termine la démonstration par récurrence.

b) Soit R la relation sur $[\![1, n]\!]$ dont le graphe est :

$$G = \left\{ (i, j) \in [\![1, n]\!]^2 \mid a_{ij} > 0 \right\} .$$

Montrons que R vérifie les hypothèses de la question *a*). Soit $I \subset [\![1, n]\!]$, on voit que :

$$\sum_{i \in I,\ (i,j) \in G} a_{ij} \leqslant \sum_{j \in R(I)} \sum_{i=1}^{n} a_{ij} = \sum_{j \in R(I)} 1 = \text{card}\,(R(I)) ,$$

et, puisque si $(i, j) \notin G$, $a_{ij} = 0$:

$$\sum_{i \in I,\ (i,j) \in G} a_{ij} = \sum_{i \in I, j \in [\![1,n]\!]} a_{ij} = \sum_{i \in I} 1 = \text{card}\,(I) .$$

Il existe donc une injection $\sigma : [\![1, n]\!] \to [\![1, n]\!]$, telle que pour tout $i \in [\![1, n]\!]$, $a_{i\,\sigma(i)} > 0$. L'injection σ est évidemment une permutation de $[\![1, n]\!]$. C'est ce qu'il fallait démontrer, en remplaçant σ par σ^{-1}.

c) Nous supposerons connu dans ce qui suit un certain nombre de résultats de géométrie convexe. Des démonstrations élémentaires sont toujours possibles et faciles, mais la notion de point extrémal n'aurait pas de

Nous supposerons connues les propriétés et notions suivantes :
- application affine, barycentre ;
- convexe d'un $\mathbb{R}$-espace affine ;
- les variétés linéaires affines d'un $\mathbb{R}$-espace affine sont des convexes ;
- les convexes de $\mathbb{R}$ sont les intervalles ;
- l'intersection d'une famille de parties convexes est convexe ;
- l'image directe et l'image réciproque d'un convexe par une application affine est convexe.

D'après ces résultats, il est clair que l'intersection d'un convexe $\mathscr{C}$ et d'une droite D qui passe par $A \in \mathscr{C}$, est un intervalle de cette droite, contenant A. On voit que A est, d'après la définition donnée par l'énoncé, un élément extrémal du convexe $\mathscr{C}$ si, et seulement si, A est toujours l'une des extrémités de l'intervalle $D \cap \mathscr{C}$.

Montrons que l'ensemble S est un convexe du $\mathbb{R}$-espace affine $\mathfrak{M}_n(\mathbb{R})$. Pour tout $i \in [\![1, n]\!]$, l'application qui à la matrice $M = [a_{ij}] \in \mathfrak{M}_n(\mathbb{R})$ fait correspondre $\sum_{k=1}^{n} a_{ik}$ est linéaire ; nous en déduisons que l'ensemble E_i des matrices $M = [a_{ij}] \in \mathfrak{M}_n(\mathbb{R})$ telles que $\sum_{k=1}^{n} a_{ik} = 1$, est une variété linéaire affine de $\mathfrak{M}_n(\mathbb{R})$. De manière analogue, pour tout $j \in [\![1, n]\!]$, l'ensemble F_j des matrices $M = [a_{ij}] \in \mathfrak{M}_n(\mathbb{R})$ telles que $\sum_{k=1}^{n} a_{kj} = 1$, est une variété linéaire affine de $\mathfrak{M}_n(\mathbb{R})$. Enfin comme pour tout $(i, j) \in [\![1, n]\!]^2$, l'application qui à $M = [a_{ij}] \in \mathfrak{M}_n(\mathbb{R})$ fait correspondre a_{ij} est linéaire, l'ensemble G_{ij} des matrices $M = [a_{ij}] \in \mathfrak{M}_n(\mathbb{R})$ telles que $a_{ij} \in \mathbb{R}_+$, est un convexe de $\mathfrak{M}_n(\mathbb{R})$. L'ensemble S est un convexe de $\mathfrak{M}_n(\mathbb{R})$ car :

$$S = \left(\bigcap_{i=1}^{n} E_i\right) \cap \left(\bigcap_{j=1}^{n} F_j\right) \cap \left(\bigcap_{(i,j)\in[\![1,n]\!]^2} G_{i,j}\right) .$$

L'ensemble S est aussi un fermé de $\mathfrak{M}_n(\mathbb{R})$.

Montrons maintenant que les matrices de permutation sont des éléments extrémaux de S. Ce sont bien entendu des éléments de S, la vérification en est immédiate. Soit $\sigma \in \mathfrak{S}_n$, supposons que les matrices $M = [a_{ij}]$ et $M' = [a'_{ij}]$, soient des éléments de S telles que $(M + M')/2 = P_\sigma$, soit pour tout $(i, j) \in [\![1, n]\!]^2$:

$$\frac{a_{ij} + a'_{ij}}{2} = \delta_{i,\sigma(j)} .$$

Pour tout (i, j) tel que $i \neq \sigma(j)$, $a_{ij} + a'_{ij} = 0$, et comme ces réels sont $\geqslant 0$, on en déduit $a_{ij} = a'_{ij} = 0$. Comme la somme des éléments d'une ligne ou d'une colonne de M et de M' est toujours 1, on voit

$a'_{\sigma(j)\,j} = 1$. Finalement on en déduit que nécessairement, $M = M' = P_\sigma$. La matrice P_σ est donc bien un élément extrémal de S.

d) Soit M un élément extrémal de S et N un élément quelconque de S différent de M. La droite D qui passe par M et N coupe le convexe S suivant un intervalle contenant M et N, mais puisque M est extrémal, M est nécessairement une des extrémités de cet intervalle. Nous en déduisons que pour tout $\lambda > 1$, $\lambda M + (1-\lambda) N \notin S$, mais comme les ensembles E_i, pour $i \in [\![1, n]\!]$, et F_j, pour $j \in [\![1, n]\!]$ sont des variétés linéaires affines, elles contiennent $\lambda M + (1-\lambda) N$; il faut donc qu'il existe $(i, j) \in [\![1, n]\!]^2$ tel que $\lambda M + (1-\lambda) N \notin G_{i,j}$, c'est-à-dire $\lambda M(i,j) + (1-\lambda) N(i,j) < 0$. Appliquons ce résultat dans le cas où $N = P_\sigma$, en supposant $P_\sigma \neq M$. Pour tout $\lambda > 1$, il existe $(i, j) \in [\![1, n]\!]^2$ tel que $\lambda M(i,j) < (\lambda - 1)\,\delta_{i,\sigma(j)}$; mais comme $M(i,j) \geqslant 0$, nécessairement $\delta_{i,\sigma(j)} > 0$, d'où $i = \sigma(j)$. On trouve donc que pour tout $\lambda > 1$, il existe $j \in [\![1, n]\!]$ tel que $\lambda M(\sigma(j), j) < (\lambda - 1)$. Si les n réels $M(\sigma(j), j)$ étaient tous > 0, il existerait un réel $\varepsilon > 0$ tel que pour tout $j \in [\![1, n]\!]$, $M(\sigma(j), j) \geqslant \varepsilon$; mais alors, pour tout $\lambda > 1$, on aurait $\varepsilon < \lambda\varepsilon < \lambda - 1$, ce qui est évidemment impossible. Il existe donc $j \in [\![1, n]\!]$ tel que $M(\sigma(j), j) = 0$.
Supposons que M, élément extrémal de S ne soit aucune des matrices P_σ, où $\sigma \in \mathfrak{S}_n$. On pourrait alors appliquer ce qui précède pour tout $\sigma \in \mathfrak{S}_n$. Il existerait donc pour tout $\sigma \in \mathfrak{S}_n$ un entier $j \in [\![1, n]\!]$ tel que $M(\sigma(j), j) = 0$. Cela est en contradiction avec ce qui avait été démontré dans le *b*) : si $M \in S$, alors il existe $\sigma \in \mathfrak{S}_n$, tel que pour tout $i \in [\![1, n]\!]$, $M(\sigma(i), i) > 0$.
Nous en déduisons que si M est un élément extrémal du convexe S, alors c'est l'une des matrices P_σ, où $\sigma \in \mathfrak{S}_n$. L'ensemble des éléments extrémaux de S est donc l'ensemble des matrices de permutation.

Exercice 13 :

Soit K un corps commutatif. On se propose d'étudier des *groupes de matrices* pour la multiplication des matrices.

a) Montrer que les matrices éléments d'un tel groupe sont nécessairement carrées et de même ordre.

b) Vérifier qu'une matrice carrée *idempotente* (c'est-à-dire telle que $M^2 = M$) constitue un tel groupe à elle seule. En donner un exemple.

c) En déduire que l'élément neutre d'un groupe de matrices n'est pas nécessairement I_n (matrice unité d'ordre n).

d) Montrer que, soit aucune des matrices du groupe n'est inversible dans $\mathfrak{M}_n(K)$, soit elles le sont toutes (dans

ser l'unité du groupe et l'inverse dans le groupe d'une matrice donnée du groupe). (Voir aussi exercice 7 du § XI.6.) ■

a) Soit G un tel groupe, et $M \in \mathfrak{M}_{p,q}(K)$ élément de G. Comme M est composable avec elle-même, on voit que $p = q$. Les éléments de G sont donc nécessairement des matrices carrées. Soient $M \in \mathfrak{M}_p(K)$ et $N \in \mathfrak{M}_q(K)$, deux éléments de G (p, q entiers > 0). Comme les matrices M et N sont composables, on en déduit $p = q$. Il existe donc un entier $n > 0$ tel que $G \subset \mathfrak{M}_n(K)$.

b) *c*) Soit $M \in \mathfrak{M}_n(K)$ idempotente ; posons $G = \{M\}$. L'ensemble G est stable par la multiplication des matrices ; la restriction à G de la multiplication des matrices est toujours associative, elle a bien un élément neutre M, et tout élément (le seul est M) a un inverse bilatère dans G. L'ensemble G muni de la multiplication des matrices est bien un groupe (attention : ce n'est pas un sous-groupe de $\mathrm{GL}_n(K)$, sauf si $M = I_n$). On peut prendre pour M toute matrice diagonale dont les coefficients diagonaux sont 0 ou 1. De manière générale, si A est un anneau, le singleton $\{0_A\}$ muni de la restriction de la multiplication de l'anneau, est un groupe (multiplicatif) ; son élément neutre est 0_A, et $0_A \neq 1_A$, sauf si $A = \{0_A\}$ (en effet si $1_A = 0_A$ alors pour tout $x \in A$, $0_A = x \times 0_A = x \times 1_A = x$).

d) Soit G un tel groupe de matrices d'élément neutre M_0. Si M est une matrice régulière élément de G, comme $M \times M_0 = M = M \times I_n$, par régularité de M dans l'anneau $\mathfrak{M}_n(K)$, on en déduit $M_0 = I_n$. Pour toute matrice $M \in G$, comme M est inversible dans G, il existe $N \in G$ telle que $M \times N = N \times M = M_0 = I_n$. Tout élément de G est donc inversible dans $\mathfrak{M}_n(K)$, et son inverse dans $\mathfrak{M}_n(K)$ est le même que dans G. Dans ce cas, G est un sous-groupe de $\mathrm{GL}_n(K)$.

Voir aussi l'exercice 3 du chapitre IX.6.

§ XI.3 *MATRICES ET APPLICATIONS LINÉAIRES*

Exercice 1 :

Le corps de base est de caractéristique 0. Soit $\varphi_1, \varphi_2, \ldots, \varphi_r$ ($r \geqslant 2$), des projecteurs d'un K-ev E de dimension finie $n \geqslant 1$ tels que $\varphi_1 + \varphi_2 + \ldots + \varphi_r = \mathrm{Id}_E$. Montrer que $E = \bigoplus_{i=1}^{r} \mathrm{Im}\,(\varphi_i)$, et que les φ_i sont deux à deux permutables. ■

Soit φ un projecteur, on remarque que $\mathrm{Tr}\,(\varphi) = \mathrm{rg}(\varphi)\cdot 1_K$. Comme $\varphi_1 + \varphi_2 + \ldots + \varphi_r = \mathrm{Id}_E$, on en déduit :

$$n\cdot 1_K = \sum_{i=1}^{r} \mathrm{Tr}\,(\varphi_i) = \sum_{i=1}^{r} \mathrm{rg}(\varphi_i)\cdot 1_k\ ,$$

et puisque K est de caractéristique 0, $n = \sum_{i=1}^{r} \mathrm{rg}(\varphi_i)$. D'autre part, puisque $\varphi_1 + \varphi_2 + \ldots + \varphi_r = \mathrm{Id}_E$, il est clair que $E = \sum_{i=1}^{n} \mathrm{Im}\,(\varphi_i)$.

Montrons par récurrence sur $r \in \mathbb{N}$, $r \geqslant 2$, que si $(E_1, \ldots, E_r)$ est une famille de sous-espaces vectoriels de E, alors $\dim\left(\sum_{i=1}^{r} E_i\right) \leqslant \sum_{i=1}^{r} \dim E_i$, et qu'il n'y a égalité que si les espaces E_i sont indépendants (i.e. la somme est directe). Si A et B sont deux sous-espaces de E, alors $\dim(A+B) = \dim A + \dim B - \dim(A\cap B)$, donc $\dim(A+B) \leqslant \dim A + \dim B$, et il n'y a égalité que si $A\cap B = \{0\}$, i.e. que si A et B sont indépendants. La propriété est donc vraie pour $r = 2$. Supposons qu'elle soit vraie pour r. Soit $(E_1, \ldots, E_{r+1})$ une famille de sous-espaces de E. Posons $E' = E_1 + \ldots + E_r$. En utilisant l'hypothèse de récurrence, on obtient les inégalités :

$$\dim\left(\sum_{i=1}^{r+1} E_i\right) = \dim\,(E' + E_{r+1}) \leqslant \dim E' + \dim E_{r+1} \leqslant$$

$$\leqslant \sum_{i=1}^{r} \dim E_i + \dim E_{r+1} = \sum_{i=1}^{r+1} \dim E_i\ .$$

S'il y a égalité, alors :

$$\dim\,(E' + E_{r+1}) = \dim E' + \dim E_{r+1} \quad \text{et} \quad \dim E' = \sum_{i=1}^{r} \dim E_i\ .$$

Nous en déduisons que les espaces E' et E_{r+1} sont indépendants, et que les espaces $(E_1, \ldots, E_r)$ sont indépendants (hypothèse de récurrence). Les espaces $(E_1, \ldots, E_r, E_{r+1})$ sont donc indépendants.
La proposition est donc démontrée par récurrence.

Nous pouvons appliquer cette proposition générale dans le cas particulier de l'exercice. Les espaces $\mathrm{Im}\,(E_i)$, pour $i \in [\![1, r]\!]$, sont donc indépendants, c'est-à-dire :

(1) $$E = \bigoplus_{i=1}^{r} \mathrm{Im}\,(\varphi_i)\ .$$

Pour tout $x \in E$, on a :

$$x = \sum_{i=1}^{r} \varphi_i(x) \ ;$$

par conséquent, pour tout $i \in [\![1, r]\!]$, $\varphi_i(x)$ est la projection de x sur l'espace $\mathrm{Im}\,(\varphi_i)$, dans la somme directe (1), autrement dit pour tout $i \in [\![1, r]\!]$, φ_i est le projecteur sur l'espace $\mathrm{Im}\,(\varphi_i)$ dans la somme directe (1). Nous en déduisons que pour tout $(i, j) \in [\![1, r]\!]^2$, $i \neq j$, $\varphi_i \circ \varphi_j = 0 = \varphi_j \circ \varphi_j$. Les endomorphismes φ_i sont donc des projecteurs commutables (Voir aussi l'exercice 7 du §IX.2).

Exercice 3 :

Le corps de base est $\mathbb{C}$. Soit E un $\mathbb{C}$-ev de dimension $n \geqslant 2$. On considère une base $(\Phi_{ij})_{(i,j)\in[\![1,n]\!]^2}$ de $\mathrm{Hom}_{\mathbb{C}}(E)$ possédant les propriétés suivantes :

(I) $\displaystyle\sum_{i=1}^{n} \Phi_{ii} = \mathrm{Id}_E$

(II) $(\forall (i, j, k, l) \in [\![1, n]\!]^4)$ $\Phi_{ij}\,\Phi_{kl} = \delta_{jk}\,\Phi_{il}$.

(δ est le symbole de Kronecker)

Démontrer qu'il existe une base $\mathcal{B} = (e_1, \ldots, e_n)$ de E telle que (Φ_{ij}) soit la base de $\mathrm{Hom}_{\mathbb{C}}(E)$ canoniquement associée à $\mathcal{B}$ (i.e. $\Phi_{ij}(e_k) = \delta_{kj} e_i$ pour tous i, j, k dans $[\![1, n]\!]$). ■

Il est clair d'après l'égalité (II) que les endomorphismes Φ_{ii}, où $i \in [\![1, n]\!]$ sont des projecteurs et que si $i \neq j$:

$$\Phi_{ii}\,\Phi_{jj} = 0 = \Phi_{jj}\,\Phi_{ii} \ .$$

Comme d'autre part $\displaystyle\sum_{i=1}^{n} \Phi_{ii} = \mathrm{Id}_E$, les endomorphismes Φ_{ii}, où $i \in [\![1, n]\!]$ sont les projecteurs dans la somme directe :

$$E = \bigoplus_{i=1}^{n} \mathrm{Im}\,(\Phi_{ii}) \ .$$

Les espaces $E_i = \mathrm{Im}\,(\Phi_{ii})$ sont tous non nuls (puisque pour tout $i \in [\![1, n]\!]$, Φ_{ii} est élément d'une base), et comme la somme de leurs dimensions est n, ils sont tous de dimension 1. Les endomorphismes Φ_{ii}, où $i \in [\![1, n]\!]$, sont donc tous de rang 1. Il en est de même pour les Φ_{ij}. En effet, si $(i, j) \in [\![1, n]\!]^2$, $\Phi_{ii}\,\Phi_{ij} = \Phi_{ij}$, et $\Phi_{ij}\,\Phi_{ji} = \Phi_{ii}$, donc $\mathrm{Im}\,(\Phi_{ii}) = \mathrm{Im}\,(\Phi_{ij}) = E_i$. Choisissons pour tout $i \in [\![1, n]\!]$ un élément non nul a_i dans la droite E_i. D'après ce qui précède, pour tout $i \in [\![1, n]\!]$; $\Phi_{ii}(a_i) = a_i$,

$j \neq i$, $\Phi_{ii}(a_j) = 0$. Nous en déduisons que pour tout $(i,j) \in [\![1,n]\!]^2$, pour tout $h \neq j$, $\Phi_{ij}(a_h) = \Phi_{ij}\,\Phi_{jj}(a_h) = 0$; et $\Phi_{ij}(a_j) = \Phi_{ii}(\Phi_{ij}(a_j))$, donc $\Phi_{ij}(a_j) \in E_i$.
Posons pour tout $(i,j) \in [\![1,n]\!]^2$, $\Phi_{ij}(a_j) = \lambda_{ij}\,a_i$, où $\lambda_{ij} \in \mathbb{C}$ ($\lambda_{ij} \neq 0$, sinon $\Phi_{ij} = 0$). Pour tout $(i,j,h) \in [\![1,n]\!]^3$:

$$\Phi_{ij}\,\Phi_{jh}(a_h) = \Phi_{ij}(\lambda_{jh}\,a_j) = \lambda_{ij}\,\lambda_{jh}\;a_i = \Phi_{ih}(a_h) = \lambda_{ih}\,a_i\ ,$$

d'où $\lambda_{ij}\,\lambda_{jh} = \lambda_{ih}$.

Posons pour tout $i \in [\![1,n]\!]$, $e_i = \lambda_{i1}\,a_i$. Pour tout $(i,j) \in [\![1,n]\!]^2$, pour tout $h \neq j$, $\Phi_{ij}(e_h) = 0$, et :

$$\Phi_{ij}(e_j) = \lambda_{j1}\,\Phi_{ij}(a_j) = \lambda_{j1}\,\lambda_{ij}\,a_i = \lambda_{i1}\,a_i = e_i\ .$$

La base $(\Phi_{ij})_{(i,j)\in[\![1,n]\!]^2}$ du $\mathbb{C}$-espace $\mathrm{Hom}_{\mathbb{C}}(E)$, est donc associée à la base $(e_1,\ldots,e_n)$ de E.

Exercice 5 :

Soit K un corps commutatif de caractéristique 0 et E un K-ev de dimension finie $n \geqslant 1$. Soit $q \in \mathbb{N}^*$ et $u \in \mathrm{Hom}_K(E)$ tel que $u^q = \mathrm{Id}_E$. On pose $E_1 = \mathrm{Ker}\,(u - \mathrm{Id}_E)$. En utilisant $v = \dfrac{1}{q}\sum_{i=0}^{q-1} u^i$, démontrer : $\dim_K(E_1) = \dfrac{1}{q}\sum_{i=0}^{q-1} \mathrm{Tr}\,(u^i)$. On prouvera d'abord que $E_1 = \mathrm{Im}\,(v)$. ■

Remarquons que :

$$q\,(u - \mathrm{Id}_E) \circ v = (u - \mathrm{Id}_E) \circ (\mathrm{Id}_E + u + \ldots + u^{q-1}) = u^q - \mathrm{Id}_E^q = 0\ ,$$

et donc que $\mathrm{Im}\,(v) \subset E_1$.
Supposons $x \in E_1$, i.e. $u(x) = x$; on voit que pour tout $i \in \mathbb{N}$, $u^i(x) = x$, d'où $v(x) = x$.
L'endomorphisme v est donc un projecteur d'image E_1, et par conséquent :

$$\dim E_1 \cdot 1_K = \mathrm{rg}(v) \cdot 1_K = \mathrm{Tr}(v) = \frac{1}{q}\sum_{i=0}^{q-1} \mathrm{Tr}\,(u^i)\ .$$

Exercice 8 :

Le corps de base est $\mathbb{R}$. On donne $n \in \mathbb{N}^*$, et on cherche les matrices $M = [a_{ij}] \in \mathfrak{M}_n(\mathbb{R})$ *inversibles* et

$M^{-1} = [b_{ij}]$, on ait :

$$(\forall (i,j) \in [\![1,n]\!]^2) \quad a_{ij} \geqslant 0 \quad \text{et} \quad b_{ij} \geqslant 0 .$$

a) Soit $\sigma \in \mathfrak{S}_n$ et $c_1, \ldots, c_n$ des réels > 0. Montrer que $M = [c_j\, \delta_{i\,\sigma(j)}]$ convient.

b) Soit M une matrice du type cherché et $u \in \mathrm{GL}_{\mathbb{R}}(\mathbb{R}^n)$ l'endomorphisme dont la matrice est M dans la base canonique $\mathcal{B} = (e_1, \ldots, e_n)$. On note $\Omega = \mathbb{R}^n_+$. Montrer que $u(\Omega) = \Omega$. Soit $\mathcal{D}_k = \mathbb{R}\, e_k$; montrer que si $x \in \mathcal{D}_k \setminus \{0\}$, les relations $y \in \Omega$, $z \in \Omega$ et $x = \frac{1}{2}(y+z)$ entraînent $y \in \mathcal{D}_k$ et $z \in \mathcal{D}_k$, et que $\left(\bigcup_{k=1}^{n} \mathcal{D}_k\right) \setminus \{0\}$ est l'ensemble des $x \in \Omega$ possédant cette propriété. En déduire que u permute les $\mathcal{D}_k$, et que M est du type trouvé dans le *a*). ■

a) Il est clair que les coefficients de la matrice $M = [c_j\, \delta_{i\,\sigma(j)}]$ sont tous $\geqslant 0$. Montrons que l'inverse de la matrice M est la matrice $N = [c_i^{-1}\, \delta_{\sigma(i)\,j}]$, matrice à coefficients tous $\geqslant 0$. En effet, pour tout $(i,h) \in [\![1,n]\!]^2$:

$$(M \times N)(i,h) = \sum_{j=1}^{n} c_j\, \delta_{i\,\sigma(j)}\, c_j^{-1}\, \delta_{\sigma(j)\,h} .$$

Le terme $\delta_{i\,\sigma(j)}\, \delta_{\sigma(j)\,h}$ ne peut être non nul que si $i = \sigma(j) = h$. On voit donc que si $i \neq h$, $(M \times N)(i,h) = 0$, et que $(M \times N)(i,i) = 1$; donc $M \times N = I_n$, et $N = M^{-1}$.

b) Soit $x = (x_1, \ldots, x_n) \in \Omega$, et $u(x) = (y_1, \ldots, y_n)$; pour tout $j \in [\![1,n]\!]$, $y_j = \sum_{i=1}^{n} a_{ij}\, x_i$. Comme pour tout $i \in [\![1,n]\!]$, $x_i \geqslant 0$ et que pour tout $(i,j) \in [\![1,n]\!]^2$, $a_{ij} \geqslant 0$, on voit que pour tout $j \in [\![1,n]\!]$, $y_j \geqslant 0$. Nous en déduisons $u(\Omega) \subset \Omega$. De manière analogue on démontrerait $u^{-1}(\Omega) \subset \Omega$, d'où $\Omega \subset u(\Omega)$, et finalement $\Omega = u(\Omega)$.

Soit $x \in \mathcal{D}_k$, $x \neq 0$, et y et z éléments de Ω tels que $x = \frac{1}{2}(y+z)$. Pour tout $i \neq k$, $0 = y_i + z_i$, et comme $y_i \geqslant 0$ et $z_i \geqslant 0$, on voit que $y_i = z_i = 0$, donc $y \in \mathcal{D}_k$ et $z \in \mathcal{D}_k$.

Nous supposerons connues dans ce qui suit, les mêmes propriétés des parties convexes des $\mathbb{R}$-espaces affines, que dans la résolution de l'exercice 8 du §XI.2. Il est clair que Ω est un convexe de $\mathbb{R}^n$. Les éléments de l'en

$\bigcup_{k=1}^{n} \mathcal{D}_k \setminus \{0\}$ ne sont pas extrémaux dans Ω, mais pour tout $x \in A$, il existe une et une seule droite D passant par x telle que x soit intérieur à l'intervalle $D \cap \Omega$ de la droite D. Inversement, soit $x \in \Omega$ vérifiant cette propriété que nous désignerons par $\mathcal{A}$; supposons que deux des coordonnées de $x = (x_1, \ldots, x_n)$ soient $\neq 0$, donc > 0, posons $x_i > 0$ et $x_j > 0$, où $i \neq j$. Il est clair que les droites passant par x et dirigées par les vecteurs e_i, et respectivement e_j, coupent le convexe Ω suivant un intervalle dans lequel x est intérieur. On voit donc que si $x \in \Omega$ possède la propriété $\mathcal{A}$, x ne peut avoir au plus qu'une coordonnée non nulle ; x ne pouvant pas être 0, c'est un élément de l'ensemble A. L'ensemble des éléments de Ω qui vérifient la propriété $\mathcal{A}$ est donc l'ensemble A.

Comme Ω est stable par l'application linéaire u, il est clair qu'un élément $x \in \Omega$ vérifie la propriété $\mathcal{A}$ si, et seulement si, $u(x)$ vérifie la propriété $\mathcal{A}$. L'ensemble $A = \bigcup_{k=1}^{n} \mathcal{D}_k \setminus \{0\}$ est donc stable par u.

Posons pour tout $j \in [\![1, n]\!]$, $u(e_j) = \lambda_j e_{k(j)}$, où $\lambda_j \in \mathbb{R}_+^*$, et $k(j) \in [\![1, n]\!]$. Comme l'application linéaire u est injective, elle transforme les sous-espaces indépendants $(E_j)_{j \in [\![1,n]\!]}$, en sous-espaces indépendants. Il est donc clair que l'application $j \mapsto k(j)$ est une permutation de $[\![1, n]\!]$. Notons cette permutation σ. Le terme de ligne i et de colonne j de la matrice M est la coordonnée i du vecteur $u(e_j)$, c'est-à-dire $\lambda_j \delta_{i\,\sigma(j)}$.
L'ensemble des $M \in \mathfrak{M}_n(\mathbb{R})$ dont tous les coefficients sont $\geqslant 0$, et dont les coefficients de l'inverse sont tous $\geqslant 0$, est donc l'ensemble des matrices de la forme $M = [c_j \delta_{i\,\sigma(j)}]$.

Autre démonstration.
Supposons que les matrices $M = [a_{ij}]$ et $N = [b_{ij}]$ soient à coefficients $\geqslant 0$, et inverses l'une de l'autre. Pour tout $(i, j) \in [\![1, n]\!]^2$, $i \neq j$, $\sum_{h=1}^{n} b_{ih}\, a_{hj} = 0$. Comme les termes de la somme sont tous $\geqslant 0$, ils sont tous nuls. On en déduit que pour tout $h \in [\![1, n]\!]$, $b_{ih} = 0$ ou $a_{hj} = 0$.
Soit $j \in [\![1, n]\!]$, supposons qu'il y ait sur la colonne j de M deux éléments > 0, $a_{h_1 j}$ et $a_{h_2 j}$; alors tous les termes $b_{i h_1}$ et $b_{i h_2}$ des colonnes d'indices h_1 et h_2 de la matrice N sont nuls, sauf peut-être le terme de ligne j ; les colonnes d'indices h_1 et h_2 de la matrice N seraient liées, ce qui est exclu. Il ne peut donc y avoir, sur une colonne de la matrice M, qu'au plus un terme non nul (il y en a exactement 1). Les termes non nuls, sur deux colonnes différentes, ne peuvent pas être sur la même ligne, sinon les deux colonnes seraient liées. Il existe donc une permutation $\sigma \in \mathfrak{S}_n$ telle que pour tout $j \in [\![1, n]\!]$, le seul terme non nul de la colonne de M d'indice j est le terme $a_{\sigma(j),j}$; en posant $c_j = a_{\sigma(j)\,j}$, on obtient finalement la forme prévue : pour tout $(i, j) \in [\![1, n]\!]^2$, $a_{ij} = c_j \delta_{i\,\sigma(j)}$.

§ XI.4 *RANG D'UNE MATRICE*

Exercice 2 :

a) soit $n \in \mathbb{N}^*$. Montrer qu'une matrice $M = [a_{ij}] \in \mathfrak{M}_n(K)$ est de rang 1 ssi on a $(b_1, \ldots, b_n) \in K^n$ et $(a_1, \ldots, a_n) \in K^n$ non nuls tels que $(\forall i, j)\ a_{ij} = b_i c_j$.

Application : $M = [\alpha^{i-j}]$, $\alpha \neq 0$.

b) $M = [a_{ij}] \in \mathfrak{M}_n(K)$ est de rang 1 et symétrique ssi on a $\rho \in K^*$ et $(b_1, \ldots, b_n) \in K^n \setminus \{0\}$ tels que $(\forall i, j)\ a_{ij} = \rho\, b_i\, b_j$.

c) Si $K = \mathbb{C}$, les matrices de rang 1 et symétriques dans $\mathfrak{M}_n(\mathbb{C})$ sont les $M(a_1, \ldots, a_n) = [a_i\, a_j]$, où $(a_1, \ldots, a_n) \in \mathbb{C}^n \setminus \{0\}$. Etudier les $(a_1, \ldots, a_n) \in \mathbb{C}^n \setminus \{0\}$ tels que $M(a_1, \ldots, a_n)$ soit une matrice symétrique de rang 1 donnée. ■

a) Supposons qu'il existe dans K^n des n-uplets non nuls $(b_1, \ldots, b_n)$ et $(c_1, \ldots, c_n)$ tels que pour tout $(i, j) \in [\![1, n]\!]^2$, $M(i, j) = b_i c_j$. Soit B la matrice colonne élément de $\mathfrak{M}_{n,1}(K)$ dont les coordonnées sont $(b_1, \ldots, b_n)$. Les colonnes de la matrice M sont $c_1 B, c_2 B, \ldots, c_n B$. La matrice M est donc de rang au plus 1. Comme les n-uplets $(b_1, \ldots, b_n)$ et $(c_1, \ldots, c_n)$, sont non nuls, il existe $(i, j) \in [\![1, n]\!]^2$, tel que $b_i \neq 0$ et $c_j \neq 0$, d'où $b_i c_j \neq 0$. La matrice M n'est donc pas nulle, et son rang est 1.

Supposons maintenant que $M \in \mathfrak{M}_n(K)$ soit de rang 1. Le sous-K-ev E engendré par les colonnes de la matrice M est donc de dimension 1. Soit $B \in E$, $B \neq 0$. Les colonnes de M sont toutes proportionnelles à B ; il existe donc des scalaires $(c_1, \ldots, c_n)$ tels que les colonnes de M soient $(c_1 B, \ldots, c_n B)$. Les scalaires $(c_1, \ldots, c_n)$ ne sont pas tous nuls, sinon M serait nulle. Notons $(b_1, \ldots, b_n)$ les coordonnées de B dans la base canonique de $\mathfrak{M}_{n,1}(K)$, on voit que pour tout $(i, j) \in [\![1, n]\!]^2$, le terme (i, j) de la matrice M est $c_j b_i$. C'est ce qu'il fallait démontrer.

En particulier, on voit que la matrice $M = [\alpha^{i-j}] = [\alpha^i\, \alpha^{-j}]$ ($\alpha \neq 0$) est de rang 1.

b) S'il existe un n-uplet non nul $(b_1, \ldots, b_n)$, et un scalaire $\rho \neq 0$, tels que pour tout $(i, j) \in [\![1, n]\!]^2$, $M(i, j) = \rho\, b_i\, b_j$, il est clair que la matrice M est symétrique et, d'après le *a*), qu'elle est de rang 1.

Inversement, supposons que la matrice M soit symétrique et de rang 1. D'après le *a*), il existe deux n-uplets non nuls $(b_1, \ldots, b_n)$ et

tels que pour tout $(i,j) \in [\![1,n]\!]^2$, $M(i,j) = b_i\, c_j$. La matrice colonne dont les coordonnées sont $(b_1,\dots,b_n)$ est une base du sous-K-ev engendré par les colonnes de M. Comme la matrice M est symétrique, pour tout $(i,j) \in [\![1,n]\!]^2$, $M(i,j) = M(j,i) = b_j\, c_i = c_i\, b_j$. On voit donc que la matrice colonne C dont les coordonnées dans la base canonique de $\mathfrak{M}_{n,1}(K)$ sont $(c_1,\dots,c_n)$ est aussi une base du sous-K-ev engendré par les colonnes de M. Les matrices C et B sont donc proportionnelles, i.e. il existe un scalaire $\rho \neq 0$ tel que pour tout $i \in [\![1,n]\!]$, $c_i = \rho\, b_i$. On voit donc que pour tout $(i,j) \in [\![1,n]\!]^2$, $M(i,j) = \rho\, b_i\, b_j$, ce qu'il fallait démontrer.

c) Les matrices de la forme $M(a_1,\dots,a_n) = [a_i\, a_j]$, où $(a_1,\dots,a_n) \in \mathbb{C}^n \setminus \{0\}$ sont, d'après le *b*), symétriques et de rang 1.

Inversement, si M est symétrique et de rang 1, d'après *b*), il existe un n-uplet non nul $(b_1,\dots,b_n)$, et un scalaire $\rho \neq 0$, tels que pour tout $(i,j) \in [\![1,n]\!]^2$, $M(i,j) = \rho\, b_i\, b_j$. Soit $\lambda \in \mathbb{C}$ tel que $\lambda^2 = \rho$. Posons pour tout $i \in [\![1,n]\!]$, $a_i = \lambda\, b_i$; on voit que pour tout $(i,j) \in [\![1,n]\!]^2$, $M(i,j) = a_i\, a_j$, donc $M = M(a_1,\dots,a_n)$. Cela répond à la première partie de la question posée.

Soit $M \in \mathfrak{M}_n(\mathbb{C})$ symétrique et de rang 1. D'après ce qui précède, il existe un n-uplet non nul $(a_1,\dots,a_n)$ tel que pour tout $(i,j) \in [\![1,n]\!]^2$, $M(i,j) = a_i\, a_j$. La matrice colonne A dont les coordonnées dans la base canonique de $\mathfrak{M}_{n,1}(\mathbb{C})$ sont $(a_1,\dots,a_n)$, est une base du sous-K-ev engendré par les colonnes de la matrice M. Si $(a'_1,\dots,a'_n)$ est un autre n-uplet non nul tel que $M = M(a'_1,\dots,a'_n)$, alors la matrice colonne A' dont les coordonnées dans la base canonique de $\mathfrak{M}_{n,1}(\mathbb{C})$ sont $(a'_1,\dots,a'_n)$, sera une autre base du sous-K-ev engendré par les colonnes de la matrice M. Les matrices A et A' seront donc nécessairement proportionnelles. Il existe donc nécessairement un scalaire $\rho \neq 0$ tel que pour tout $i \in [\![1,n]\!]$, $a'_i = \rho\, a_i$. Mais alors $M = M(a'_1,\dots,a'_n)$ si, et seulement si, pour tout $(i,j) \in [\![1,n]\!]^2$, $\rho^2\, a_i\, a_j = a_i\, a_j$. Comme le n-uplet $(a_1,\dots,a_n)$ n'est pas nul, c'est vrai si, et seulement si, $\rho^2 = 1$. Il y a donc toujours exactement deux n-uplets $(a_1,\dots,a_n)$ tels que M, symétrique de rang 1, soit $M(a_1,\dots,a_n)$.

Exercice 5 :

a) Soit $M = [a_{ij}] \in \mathfrak{M}_n(\mathbb{C})$ $(n \geqslant 2)$ telle que

$$(\forall i \in [\![1,n]\!]) \quad |a_{ii}| > \sum_{j \neq i} |a_{ij}|\,.$$

Prouver que M est inversible.

b) Soit $M = [a_{ij}] \in \mathfrak{M}_n(\mathbb{C})$. On suppose :

(I) $\quad (\forall i \in [\![1,n]\!]) \quad |a_{ii}| \geqslant \sum_{j \neq i} |a_{ij}|$

(II) $\quad (\exists i \in [\![1,n]\!]) \quad |a_{ii}| > \sum_{j \neq i} |a_{ij}|$

(III) $\quad \forall (i,j) \in [\![1,n]\!]^2 \ , \ \exists m \in \mathbb{N}^* \ , \ \exists (k_1, \ldots, k_m) \in [\![1,n]\!]^m$

$$a_{i\,k_1}\, a_{k_1\,k_2} \ldots, a_{k_m\,j} \neq 0 \, .$$

Montrer que M est inversible (Hadamard). ■

a) En divisant chaque ligne de la matrice M par son élément diagonal, nous pouvons nous ramener au cas où les termes diagonaux de la matrice M sont tous 1. On peut alors écrire $M = I_n - N$, où la matrice $N = [b_{ij}]$ est telle que pour tout $i \in [\![1,n]\!]$, $\sum_{j=1}^{n} |b_{ij}| < 1$ (le terme diagonal est nul, mais ce n'est pas essentiel). Posons :

$$r = \sup \left\{ \sum_{j=1}^{n} |b_{ij}| \ , i \in [\![1,n]\!] \right\} .$$

On a bien sûr $r < 1$. Pour $X \in \mathfrak{M}_{n,1}(\mathbb{C})$, dont les coordonnées dans la base canonique sont $(x_1, \ldots, x_n)$, on notera $\|X\| = \sup \{|x_i| \ , i \in [\![1,n]\!]\}$ la norme de X. Les coordonnées de NX sont $(y_1, \ldots, y_n)$, où pour tout $i \in [\![1,n]\!]$:

$$y_i = \sum_{j=1}^{n} b_{i,j}\, x_j \ ,$$

d'où :

$$|y_i| \leqslant \sum_{j=1}^{n} |b_{i,j}|\, \|X\| \leqslant r\, \|X\| \ .$$

Nous en déduisons finalement $\|NX\| \leqslant r\, \|X\|$.

Supposons $MX = 0$, c'est-à-dire $X = NX$, alors $X = 0$, car $r < 1$. La matrice M est donc régulière, et par conséquent inversible.

Le lecteur pourra vérifier que l'inverse de la matrice $M = I_n - N$ est la somme de la série de terme général N^k, $k \in \mathbb{N}$, série géométrique absolument convergente. Cela donne un moyen concret de calcul de l'inverse de M, ou simplement de résolution de l'équation en $X \in \mathfrak{M}_{n,1}(\mathbb{C})$, $MX = Y$, dans le cas où M vérifie cette condition.

b) Soit $X \in \mathfrak{M}_{n,1}(\mathbb{C})$, de coordonnées $(x_1, \ldots, x_n)$ tel que $MX = 0$. Posons :

$$I = \{ i \in [\![1,n]\!] \mid |x_i| = \|X\| \} \ .$$

Par définition $I \neq \emptyset$, et si $j \notin I$ (s'il en existe), $|x_j| < \|X\|$.
Pour tout $i \in I$, $a_{ii}\, x_i = -\sum_{j \neq i} a_{ij}\, x_j$, d'où d'après (I) :

$$|a_{ii}|\ |x_i| \leqslant \sum_{j \neq i} |a_{ij}|\ |x_j| \leqslant \sum_{j \neq i} |a_{ij}|\ |x_i| \leqslant |a_{ii}|\ |x_i| \ .$$

Nous en déduisons que pour tout $j \neq i$, $|a_{ij}|\ (|x_i| - |x_j|) = 0$, et donc que pour tout $j \notin I$ (s'il en existe), $|a_{ij}| = 0$.
Soit $i \in I$ quelconque (il en existe), et $j \in [\![1, n]\!]$, d'après l'hypothèse (III), il existe un entier $m \in \mathbb{N}^*$, et un m-uplet $(k_1, \ldots, k_m)$ d'éléments de $[\![1, n]\!]$, tels que $a_{i\,k_1}\, a_{k_1\,k_2} \ldots, a_{k_m\,j} \neq 0$. D'après ce qui précède, on voit que nécessairement $k_1 \in I$, puis $k_2 \in I$, etc., $k_m \in I$, et finalement $j \in I$. Cela démontre $I = [\![1, n]\!]$; toutes les coordonnées de X ont par conséquent même module.
Soit $i \in [\![1, n]\!]$ tel que $a_{ii} > \sum_{j \neq i} |a_{ij}|$, si X n'était pas nul on aurait les inégalités :

$$|a_{ii}|\ |x_i| \leqslant \sum_{j \neq i} |a_{ij}|\ |x_j| = \sum_{j \neq i} |a_{ij}|\ |x_i| < |a_{ii}|\ |x_i| \ ,$$

ce qui est contradictoire. Nous en déduisons $X = 0$.

La matrice M est donc régulière et par conséquent inversible.

Exercice 6 :

On considère la matrice $C = [A : B]$ obtenue en juxtaposant une (m, n_1)-matrice A et une (m, n_2)-matrice B. Montrer que $\mathrm{rg}\,(C) \leqslant \mathrm{rg}\,(A) + \mathrm{rg}\,(B)$. ■

Notons r le rang de la matrice A et s le rang de la matrice B. On peut trouver des indices $(i_1, \ldots, i_r)$, $i_1 < \ldots < i_r$, dans $[\![1, n_1]\!]$, tels que les colonnes d'indices $i_1, \ldots, i_r$ de A forment une base du sous-K-ev engendré par les colonnes de A. On peut de même trouver des indices $(j_1, \ldots, j_s)$, $j_1 < \ldots < j_s$, dans $[\![1, n_2]\!]$, tels que les colonnes d'indices $j_1, \ldots, j_s$ de B forment une base du sous-K-ev engendré par les colonnes de B. Il est clair que les colonnes d'indices $i_1, \ldots, i_r$ et $n_1 + j_1, \ldots, n_1 + j_s$ de C sont bien distinctes, et forment une famille génératrice du sous-K-ev engendré par les colonnes de C. La dimension de ce sous-K-ev, qui est le rang de la matrice C, est donc $\leqslant r + s$, ce qu'il fallait démontrer.

Exercice 7 :

Soit $A \in \mathfrak{M}_n(K)$, $B \in \mathfrak{M}_n(K)$ de rangs respecti

Montrer que le rang r de AB vérifie : $r_2 \geqslant r \geqslant r_1 + r_2 - n$ (inégalité de Sylvester). ■

Considérons les applications linéaires $f : \mathfrak{M}_{n,1}(K) \to \mathfrak{M}_{n,1}(K)$, $X \mapsto AX$, et $g : \mathfrak{M}_{n,1}(K) \to \mathfrak{M}_{n,1}(K)$, $X \mapsto BX$. Les matrices de ces endomorphismes de $\mathfrak{M}_{n,1}(K)$ dans la base canonique de $\mathfrak{M}_{n,1}(K)$, sont respectivement A et B ; donc $\mathrm{rg}(f) = \mathrm{rg}(A) = r_1$, $\mathrm{rg}(g) = \mathrm{rg}(B) = r_2$, et $\mathrm{rg}(f \circ g) = \mathrm{rg}(AB) = r$, puisque la matrice de $f \circ g$ est AB. Nous sommes donc ramenés à démontrer l'inégalité :

$$\mathrm{rg}(g) \geqslant \mathrm{rg}(f \circ g) \geqslant \mathrm{rg}(f) + \mathrm{rg}(g) - n .$$

Posons $E = \mathfrak{M}_{n,1}(K)$, et $G = \mathrm{Im}(g)$, sous-K-ev de dimension r_2. Considérons la restriction f_1 de f à G, $f_1 : G \to E$. Il est clair que :

$$\mathrm{rg}(f \circ g) = \dim(f(g(E))) = \dim(f_1(G)) = \mathrm{rg}(f_1) \leqslant \dim G = \mathrm{rg}(g) .$$

On a aussi l'égalité :

$$\mathrm{rg}(f_1) + \dim(\mathrm{Ker}(f_1)) = \dim G = \mathrm{rg}(g) .$$

Comme :

$$\mathrm{Ker}(f_1) = \mathrm{Ker}(f) \cap \mathrm{Im}(g) \subset \mathrm{Ker}(f) ,$$

on en déduit :

$$\begin{aligned} \mathrm{rg}(f \circ g) = \mathrm{rg}(f_1) &= \mathrm{rg}(g) - \dim(\mathrm{Ker}(f_1)) \geqslant \\ &\geqslant \mathrm{rg}(g) - \dim(\mathrm{Ker}(f)) = r_2 - (n - r_1) = r_2 + r_1 - n . \end{aligned}$$

D'où finalement :

$$r_2 \geqslant r \geqslant r_1 + r_2 - n ,$$

ce qu'il fallait démontrer.

§ XI.5 *OPÉRATIONS ÉLÉMENTAIRES*

Exercice 3 :

Soit K un corps commutatif, $n \in \mathbb{N}^*$ et $\mathscr{H}$ un hyperplan du K-ev $\mathfrak{M}_n(K)$. Montrer que $\mathscr{H}$ rencontre $\mathrm{GL}(n, K)$. ■

Le résultat est évidemment faux si $n = 1$, nous supposerons donc $n \geqslant 2$.
Nous utiliserons la base canonique de $\mathfrak{M}_n(K)$: $(E_{ij})_{(i,j)\in[\![1,n]\!]^2}$.
L'hyperplan $\mathscr{H}$ est le noyau d'une forme linéaire non nulle φ.

tout $(i,j) \in [\![1,n]\!]^2$, $\varphi(E_{ij}) = u_{ij}$ $(\in K)$.
Soit $M = [a_{ij}]$, $M \in \mathcal{H}$ si, et seulement si :

$$\varphi(M) = \sum_{(i,j)\in[\![1,n]\!]^2} a_{ij}\varphi(E_{ij}) = \sum_{(i,j)\in[\![1,n]\!]^2} a_{ij}\,u_{ij} = 0 \ .$$

Supposons qu'il existe $(p,q) \in [\![1,n]\!]^2$, $p \neq q$, tel que $u_{pq} \neq 0$. Pour tout $\lambda \in K$, on a :

$$\varphi(I_n + \lambda\, E_{pq}) = \left(\sum_{i=1}^{n} u_{ii}\right) + \lambda\, u_{pq} \ .$$

Les matrices $I_n + \lambda\, E_{pq}$ (matrices de transvexion) sont toutes inversibles, et l'une d'elle est dans $\mathcal{H}$.
Supposons maintenant que pour tout $(p,q) \in [\![1,n]\!]^2$, si $p \neq q$ alors $u_{pq} = 0$; on a donc :

$$\varphi(M) = \sum_{i=1}^{n} a_{ii}\,u_{ii} \ .$$

On peut trouver, si $n \geqslant 2$, des matrices inversibles dont tous les éléments diagonaux sont nuls ; par exemple la matrice de permutation associée au cycle $\langle 1, 2, \ldots, n\rangle$; ces matrices sont dans l'hyperplan $\mathcal{H}$.

Dans tous les cas il existe donc des matrices inversibles dans l'hyperplan $\mathcal{H}$, ce qu'il fallait démontrer.

Exercice 4 :

> K est un corps commutatif quelconque. Soit r , p et n des entiers vérifiant $p > r \geqslant 1$, $n > r$. On considère dans $\mathfrak{M}_{p,n}(K)$ l'ensemble $\mathcal{E}_r$ des matrices M de rang r dont la sous-matrice $M_r = \mathcal{M}_{[\![1,r]\!]\times[\![1,r]\!]}(M)$ soit inversible. Construire une bijection de $\mathrm{GL}\,(r,K) \times K^{r\,(p+n-2\,r)}$ sur $\mathcal{E}_r$. ■

Nous utiliserons la notation par blocs des matrices.
Soit $M \in \mathcal{E}_r$, que nous écrivons :

$$M = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \ ,$$

où :

$$A \in \mathrm{GL}\,(r,K) \ , \ B \in \mathfrak{M}_{r,n-r}(K) \ , \ C \in \mathfrak{M}_{p-r,r}(K) \ , \ D \in \mathfrak{M}_p$$

Comme la matrice M est exactement de rang r, les colonnes de la matrice $\begin{bmatrix} B \\ D \end{bmatrix}$ sont des combinaisons linéaires des colonnes de la matrice $\begin{bmatrix} A \\ C \end{bmatrix}$. Il existe donc une matrice $T \in \mathfrak{M}_{r,n-r}(K)$ telle que :

$$\begin{bmatrix} B \\ D \end{bmatrix} = \begin{bmatrix} A \\ C \end{bmatrix} \times T \ ,$$

d'où $B = AT$ et $D = CT$. La matrice M est donc de la forme :

$$M = \begin{bmatrix} A & AT \\ C & CT \end{bmatrix} \ .$$

Inversement, une telle matrice est bien dans $\mathscr{E}_r$.
Avec les notations initiales, nous voyons que nécessairement $T = A^{-1}B$.

Nous venons en fait d'établir que l'application :

$$(A, C, T) \mapsto \begin{bmatrix} A & AT \\ C & CT \end{bmatrix} \ ,$$

dont l'ensemble de départ est $\mathrm{GL}(r, K) \times \mathfrak{M}_{p-r,r}(K) \times \mathfrak{M}_{r,n-r}(K)$, est à valeurs dans $\mathscr{E}_k$, et y est surjective. Elle est bien sûr injective ; il s'agit donc d'une bijection dont la réciproque est l'application :

$$M \mapsto (A, C, A^{-1}B) \ .$$

L'ensemble $\mathscr{E}_r$ est donc en bijection avec l'ensemble $\mathrm{GL}(r, K) \times \mathfrak{M}_{p-r,r}(K) \times \mathfrak{M}_{r,n-r}(K)$, lui-même en bijection avec l'ensemble $\mathrm{GL}(r, K) \times K^q$, où $q = (p-r)r + r(n-r) = r(p+n-2r)$.

On trouve une application de ce résultat dans l'exercice 11 du §X.5 du tome 1 d'analyse.

§ XI.6 *SIMILITUDE D'ENDOMORPHISMES OU DE MATRICES*

Exercice 1 :

a) Soit n un entier $\geqslant 2$ et $u \in \mathrm{Hom}_K(K^n)$. Si u n'est pas une homothétie, on a e_1 et e_2 dans K^n tels que $u(e_1) = e_2$ et (e_1, e_2) linéairement indépendants.

b) Utiliser *a*) pour prouver : si $M \in \mathfrak{M}_n(K)$ est *de trace nulle*, et si K est de caractéristique 0, alors M est sem

‖ matrice $[a_{ij}]$ telle que $a_{ii} = 0$ pour $1 \leqslant i \leqslant n$. ■

a) Soit $(\varepsilon_1, \ldots, \varepsilon_n)$ la base canonique de K^n . Si l'un des éléments ε_i de cette base n'est pas colinéaire à son image par u , on peut poser $e_1 = \varepsilon_i$.
Si tous les éléments de cette base sont colinéaires à leur image par u , posons $u(\varepsilon_i) = \lambda_i \varepsilon_i$, où pour tout $i \in [\![1, n]\!]$, $\lambda_i \in K$. On a :

$$u(\varepsilon_1 + \ldots + \varepsilon_n) = \sum_{i=1}^{n} \lambda_i \varepsilon_i \ .$$

Si le vecteur $\varepsilon_1 + \ldots + \varepsilon_n$ était colinéaire à son image par u , il existerait un scalaire $\lambda \in K$, tel que :

$$\lambda_1 \varepsilon_1 + \ldots + \lambda_n \varepsilon_n = \lambda \varepsilon_1 + \ldots + \lambda \varepsilon_n \ .$$

Dans ce cas, pour tout $i \in [\![1, n]\!]$, $\lambda_i = \lambda$, et l'application linéaire u est une homothétie, ce qui a été exclu.
On peut donc dans tous les cas, si u n'est pas une homothétie, trouver un vecteur e_1 dans K^n tel que $(e_1, u(e_1))$ soit libre.

b) Montrons par récurrence sur $n \geqslant 1$, que si $M \in \mathfrak{M}_n(K)$ est de trace nulle, elle est semblable à une matrice dont tous les termes diagonaux sont nuls. C'est évidemment vrai pour $n = 1$. Supposons cette propriété vraie pour l'entier $n \geqslant 1$. Soit $M \in \mathfrak{M}_{n+1}(K)$, et u l'endomorphisme de K^{n+1} dont la matrice dans la base canonique est M .
Si u est une homothétie de rapport $\lambda \in K$, alors $\mathrm{Tr}\,(M) = \mathrm{Tr}\,(u) = (n+1)\,\lambda = 0$; donc, puisque K est de caractéristique 0, $\lambda = 0$, et $M = 0$.
Si u n'est pas une homothétie, il existe d'après le *a*) ($n+1 \geqslant 2$), un vecteur $e_1 \in K^{n+1}$ tel que $(e_1, u(e_1))$ est libre. D'après le théorème de la base incomplète, il existe une base $(e_1, u(e_1), e_3, \ldots, e_{n+1})$ dans l'espace K^{n+1} .
La matrice M' de u dans cette base est semblable à la matrice M , et elle est de la forme :

$$M' = \left[\begin{array}{c|c} 0 & L \\ \hline V & N \end{array}\right]$$

où $V \in \mathfrak{M}_{n,1}(K)$, $L \in \mathfrak{M}_{1,n}(K)$, et $N \in \mathfrak{M}_n(K)$.
D'après l'hypothèse de récurrence, la matrice N , qui est de trace nulle et de dimension n , est semblable à une matrice $N' \in \mathfrak{M}_n(K)$ dont tous les termes diagonaux sont nuls. Soit $Q \in \mathrm{GL}\,(n, K)$ telle que N'

On obtient :

$$\left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & Q^{-1} \end{array}\right] \times \left[\begin{array}{c|c} 0 & L \\ \hline V & N \end{array}\right] \times \left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & Q \end{array}\right] = \left[\begin{array}{c|c} 0 & LQ \\ \hline Q^{-1}V & Q^{-1}NQ \end{array}\right]$$

Comme les termes diagonaux de la matrice $N' = Q^{-1}NQ$ sont nuls, on voit que la matrice M' est semblable à une matrice M'' dont les termes diagonaux sont nuls. Par transitivité il en est de même pour la matrice M, ce qui termine la démonstration par récurrence.

Exercice 6 (*Application de l'exercice 7, du §IX.4*) **:**

Soit $M \in \mathfrak{M}_n(K)$ $(n \geqslant 2)$; on suppose M non inversible et non nilpotente (donc $M^k \neq 0$ pour tout $k \in \mathbb{N}$).

Démontrer que M est semblable à une matrice du type suivant (écriture par blocs) :

$$\left[\begin{array}{c|c} G & 0 \\ \hline 0 & N \end{array}\right],$$

avec $G \in \mathrm{GL}_s(K)$ pour s convenable $(1 \leqslant s \leqslant n-1)$ et $N \in \mathfrak{M}_{n-s}(K)$, N *nilpotente.* ■

Soit u l'endomorphisme du K-ev K^n dont la matrice dans la base canonique est M. On démontre dans l'exercice 7 du § IX.4, qu'il existe deux sous-K-ev supplémentaires J et F, stables par u, tels que l'endomorphisme induit par u sur J est un automorphisme, et l'endomorphisme induit par u sur F est nilpotent. Comme M n'est ni inversible ni nilpotente, il en est de même pour u, et par conséquent les sous-K-ev J et F sont ici non nuls. Si $(e_1, \ldots, e_s)$ est une base de J, et $(e_{s+1}, \ldots, e_n)$ une base de F, la matrice de u dans cette base est de la forme :

$$M' = \left[\begin{array}{c|c} G & 0 \\ \hline 0 & N \end{array}\right],$$

où $G \in \mathrm{GL}_s(K)$ est la matrice dans la base $(e_1, \ldots, e_s)$ de l'endomorphisme induit par u sur J, et où N est la matrice dans la base $(e_{s+1}, \ldots, e_n)$ de l'endomorphisme induit par u sur F. Comme l'endomorphisme induit par u sur F est nilpotent, la matrice N est nilpotente. La matrice M' étant semblable à M, cela démontre la proposition de l'énoncé.

Exercice 7 *(suite de l'exercice 13 du §XI.2).* **:**

On donne un entier $n \geqslant 2$; on appellera *groupe de matrices* dans $\mathfrak{M}_n(K)$ tout sous-ensemble non vide de matrices qui, pour le produit des matrices, est un groupe. L'élément neutre d'un tel groupe n'est pas forcément I_n .

a) Si un groupe de matrices contient une matrice inversible dans $\mathfrak{M}_n(K)$, alors ce groupe est un sous-groupe de $\mathrm{GL}(n,K)$ (et donc son élément neutre est I_n).

b) Soit $\mathcal{G}$ un groupe de matrices non inversibles et J son élément neutre. Montrer que tous les éléments de $\mathcal{G}$ ont le même rang r .

c) Soit $r \in [\![1, n-1]\!]$; montrer que l'ensemble Γ_r formé des matrices du type :

$$\left[\begin{array}{c|c} G & 0 \\ \hline 0 & 0 \end{array}\right] \in \mathfrak{M}_n(K) ,$$

avec $G \in \mathrm{GL}(r,K)$, est un groupe de matrices, et en préciser l'élément neutre J_r .

d) On reprend un groupe $\mathcal{G}$ comme en *b*) et on suppose le rang commun r des matrices de $\mathcal{G}$ tel que $1 \leqslant r \leqslant n-1$. Montrer que J est semblable à J_r .

Si $P \in \mathrm{GL}(n,K)$ est tel que $J = P J_r P^{-1}$, démontrer que l'application $M \mapsto P^{-1} M P$ définit un homomorphisme injectif de $\mathcal{G}$ dans le groupe Γ_r . Conclure en décrivant tous les groupes de matrices dans $\mathfrak{M}_n(K)$. ■

a) Le groupe de matrices sera noté $\mathcal{G}$ et son neutre J , comme dans les questions suivantes. Soit $M \in \mathcal{G}$, une matrice inversible dans $\mathfrak{M}_n(K)$. On a :

$$M \times J = M = M \times I_n ,$$

mais puisque la matrice M est régulière dans $\mathfrak{M}_n(K)$, on en déduit $J = I_n$. Toute matrice $M \in \mathcal{G}$ a un inverse N dans $\mathcal{G}$ qui est tel que $M \times N = N \times M = J = I_n$; les éléments de $\mathcal{G}$ sont donc tous inversibles dans $\mathfrak{M}_n(K)$, et l'inverse de $M \in \mathcal{G}$ dans le groupe $\mathrm{GL}(n,K)$ est le même que son inverse dans $\mathcal{G}$. L'ensemble $\mathcal{G}$ est donc un sous-groupe de $\mathrm{GL}(n,K)$.

b) Nous utiliserons le fait que le rang du produit de deux matrices composables est inférieur ou égal au rang de chacune des matrices. O

une proposition analogue pour les applications linéaires (voir § IX.4 Exercice 3).

Soit $M \in \mathcal{G}$; on a $M \times J = M$, donc $\operatorname{rg}(J) \geqslant \operatorname{rg}(M)$; la matrice M a un inverse N dans $\mathcal{G}$, qui vérifie $M \times N = J$, d'où $\operatorname{rg}(J) \leqslant \operatorname{rg}(M)$. Finalement nous en déduisons que tous les éléments de $\mathcal{G}$ ont le même rang que l'élément neutre J de $\mathcal{G}$.

c) Introduisons l'application $\varphi : \mathfrak{M}_r(K) \to \mathfrak{M}_n(K)$, définie par :

$$N \mapsto \left[\begin{array}{c|c} N & 0 \\ \hline 0 & 0 \end{array}\right].$$

Il est clair que cette application linéaire est injective et qu'elle est, d'après les règles de multiplication des matrices par blocs, un homomorphisme pour la multiplication. L'image de $\mathrm{GL}(r, K)$ par φ est donc un groupe pour la multiplication, dont l'élément neutre J_r est l'image par φ de la matrice I_r.

d) Soit u un endomorphisme de K^n dont la matrice dans la base canonique est J. Comme $J \times J = J$, on voit que u est un projecteur. Le rang de u est aussi le rang de J, soit r. Si $(e_1, \ldots, e_r)$ est une base de l'image du projecteur u, et $(e_{r+1}, \ldots, e_n)$ une base de son noyau, la matrice de u dans la base $(e_1, \ldots, e_r, e_{r+1}, \ldots, e_n)$ de K^n est visiblement la matrice $\varphi(I_r) = J_r$ (voir *c*)). Cette matrice est donc semblable à la matrice J, qui est la matrice de u dans la base canonique.

Soit $P \in \mathrm{GL}(n, K)$ telle que $J_r = P^{-1} J P$. Montrons que pour tout $M \in \mathcal{G}$, $M' = P^{-1} M P \in \Gamma_r$. La matrice M' est telle que :

$$M' J_r = P^{-1} M J P = P^{-1} M P = M' = P^{-1} J M P = J_r M' .$$

En distinguant dans M' des blocs de tailles convenables on obtient :

$$M' = \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right] = \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right] \times \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right] = \left[\begin{array}{c|c} A & 0 \\ \hline C & 0 \end{array}\right]$$

d'où $B = D = 0$. De manière analogue :

$$M' = \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right] = \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right] \times \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right] = \left[\begin{array}{c|c} A & B \\ \hline 0 & 0 \end{array}\right]$$

d'où $C = D = 0$.
La matrice M est inversible dans $\mathcal{G}$, il existe donc une matrice $N \in \mathcal{G}$ telle que $MN = NM = J$. Posons $N' = P^{-1}NP$. On voit que $M'N' = N'M' = J_r$, et par conséquent, que la matrice A est inversible dans $\mathfrak{M}_r(K)$. La matrice $M' = P^{-1}MP$ est donc bien dans le groupe Γ_r.

Nous en déduisons que si $\mathcal{G}$ est un groupe, non réduit à $\{0\}$, de matrices non inversibles, il existe une matrice inversible P et un entier $r \in [\![1, n-1]\!]$, tels que l'application $M \mapsto P^{-1}MP$ soit un isomorphisme de groupes, entre $\mathcal{G}$ et un sous-groupe du groupe Γ_r. La réciproque est immédiate. On trouve donc ainsi tous les groupes de matrices.
Voir aussi l'exercice 3 du §IX.6.

Exercice 9 :

On donne un entier $n \geqslant 2$; on appellera *algèbre de matrices* dans $\mathfrak{M}_n(K)$ tout sous-ensemble non vide $\mathcal{A}$ de $\mathfrak{M}_n(K)$ qui est un sous-K-ev stable pour le produit et qui, muni de cette structure de K-ev et de ce produit, est une K-algèbre.

a) Soit $r \in [\![1, n-1]\!]$; montrer que l'ensemble $\mathcal{A}_r$ formé des matrices du type :

$$\left[\begin{array}{c|c} M & 0 \\ \hline 0 & 0 \end{array}\right] \in \mathfrak{M}_n(K)$$

avec $M \in \mathfrak{M}_r(K)$, est une algèbre non nulle de matrices, préciser son élément neutre J_r ($J_r =$ *unité* de $\mathcal{A}_r$).

b) Soit $\mathcal{A}$ une algèbre non nulle de matrices et E son élément unité ; montrer que $\operatorname{rg}(M) \leqslant r = \operatorname{rg}(E)$ pour toute $M \in \mathcal{A}$.
Montrer que si $r = n$, alors $E = I_n$ et $\mathcal{A}$ est une sous-algèbre de $\mathfrak{M}_n(K)$.

c) Avec les notations du *b*), on suppose $r \in [\![1, n-1]\!]$. En reprenant la méthode de l'exercice 7 *b*), montrer que E est semblable à J_r, et que, si $P \in \mathrm{GL}(n, K)$ vérifie $E = PJ_rP^{-1}$, l'application $M \mapsto P^{-1}MP$ définit un homomorphisme de K-algèbres injectif de $\mathcal{A}$ dans $\mathcal{A}_r$. Conclure en décrivant toutes les algèbres de matrices dans $\mathfrak{M}_n(K)$. ■

a) Introduisons l'application $\varphi : \mathfrak{M}_r(K) \to \mathfrak{M}_n(K)$, définie par :

$$N \mapsto \left[\begin{array}{c|c} N & 0 \\ \hline 0 & 0 \end{array}\right].$$

Il est clair que cette application linéaire est injective et qu'elle est, d'après les règles de multiplication des matrices par blocs, un homomorphisme pour la multiplication. L'image de $\mathfrak{M}_r(K)$ par φ est donc une algèbre de matrices, dont l'élément unité J_r est l'image par φ de la matrice I_r ; donc $J_r \neq 0$.

b) Nous utiliserons le fait que le rang du produit de deux matrices composables est inférieur ou égal au rang de chacune des matrices. On a d'ailleurs une proposition analogue pour les applications linéaires (voir §IX.4 Exercice 3).

Soit $M \in \mathscr{A}$; on a $M \times E = M$, donc $\operatorname{rg}(E) \geqslant \operatorname{rg}(M)$.
Si $r = n$, la matrice E est inversible dans $\mathfrak{M}_n(K)$, et comme $E \times E = E = E \times I_n$, on en déduit $E = I_n$. Dans ce cas, $\mathscr{A}$ est par définition une sous-algèbre de $\mathfrak{M}_n(K)$.

c) Comme $E \times E = E$, on démontrerait comme dans l'exercice 7 *d*), que E est la matrice d'un projecteur (non nul et différent de Id_E), et qu'elle est par conséquent semblable à la matrice J_r, où $r = \operatorname{rg}(E) \in [\![1, n-1]\!]$. Soit $P \in \mathrm{GL}(n, K)$ telle que $J_r = P^{-1} E P$. Pour $M \in \mathscr{A}$, posons $M' = P^{-1} M P$. Comme $M' = P^{-1} M E P = M' J_r$ et que de même $M' = J_r M'$, on démontrerait comme dans l'exercice 7 *d*), que la matrice M' est dans $\mathscr{A}_r$.

Nous en déduisons que si $\mathscr{A}$ est une algèbre non nulle de matrices dans $\mathfrak{M}_n(K)$ qui n'est pas une sous-algèbre de $\mathfrak{M}_n(K)$ (i.e. qui ne contient pas I_n mais qui est quand même unitaire), il existe une matrice inversible $P \in \mathrm{GL}(n, K)$, et un entier $r \in [\![1, n-1]\!]$ tels que l'application $M \mapsto P^{-1} M P$ soit un isomorphisme entre l'algèbre $\mathscr{A}$ et une sous-algèbre de l'algèbre $\mathscr{A}_r$. La réciproque est immédiate. On obtient donc ainsi toutes les algèbres non nulles de matrices qui ne sont pas des sous-algèbres de $\mathfrak{M}_n(K)$.

Chapitre XII

DUALITÉ. ESPACES VECTORIELS QUOTIENTS

§ XII.1 *DUAL ; FORME BILINÉAIRE CANONIQUE*

Exercice 2 :

> Soit I un ensemble non vide, et E le K-ev K^I, F son sous-K-ev $K^{(I)}$. On note $(e_i)_{i\in I}$ la base canonique de $K^{(I)}$. Soit, pour $i \in I$, φ_i la forme linéaire sur F telle que $(\forall j)\ \varphi_i(e_j) = \delta_{ij}\,1_K$ (δ symbole de Kronecker).
>
> *a*) Prouver que l'application $F^* \to E$, $\varphi \mapsto (\varphi(e_i))_{i\in I}$ est un isomorphisme de K-ev ; quel est le sous-K-ev de F^* engendré par les $(\varphi_i)_{i\in I}$?
>
> *b*) On prend $K = \mathbb{Q}$ et $I = \mathbb{N}$. Montrer que $\mathbb{Q}^{(\mathbb{N})}$ est dénombrable, que $\mathbb{Q}^{\mathbb{N}}$ ne l'est pas, et que le $\mathbb{Q}$-ev $\mathbb{Q}^{(\mathbb{N})}$ n'est pas de dimension finie. En déduire que $\mathbb{Q}^{(\mathbb{N})}$ n'est isomorphe au dual d'aucun $\mathbb{Q}$-ev. ■

a) Notons Φ l'application $\varphi \mapsto (\varphi(e_i))_{i\in I}$.
Soit $(\lambda_i)_{i\in I}$ une famille de scalaires, d'après le théorème VI.3.2 (théorème de la base), il existe une et une seule application linéaire $\varphi : F \to K$, telle que pour tout $i \in I$, $\varphi(e_i) = \lambda_i$. L'application Φ est donc bijective. Comme elle est visiblement K-linéaire, c'est un isomorphisme de K-ev.

On vérifie que pour tout $i \in I$, $\Phi(\varphi_i) = (\delta_{ij}\,1_K)_{j\in I} = e_i$. L'image par Φ du sous-K-ev engendré par la famille $(\varphi_i)_{i\in I}$, est donc le sous-K-ev engendré par la famille $(e_i)_{i\in I}$, c'est-à-dire le sous-K-ev $K^{(I)}$.

b) Pour $n \in \mathbb{N}$ notons E_n le sous-K-ev de $\mathbb{Q}^{(\mathbb{N})}$ engendré par la famille $(e_i)_{i\in[\![0,n]\!]}$. Le $\mathbb{Q}$-ev E_n est de dimension $n+1$, il est donc

$\mathbb{Q}^{n+1}$, et est par conséquent dénombrable. On voit que $\mathbb{Q}^{(\mathbb{N})} = \bigcup_{n\in\mathbb{N}} E_n$, et donc que $\mathbb{Q}^{(\mathbb{N})}$ est dénombrable.
Si l'ensemble $\mathbb{Q}^{\mathbb{N}}$ était dénombrable, l'ensemble $\{0,1\}^{\mathbb{N}}$ le serait ; or ce n'est pas le cas, car $\{0,1\}^{\mathbb{N}}$ est équipotent à l'ensemble $\mathcal{P}(\mathbb{N})$ qui n'est pas dénombrable (Théorème de Cantor §II.3).
Le $\mathbb{Q}$-ev $\mathbb{Q}^{(\mathbb{N})}$ n'est pas de dimension finie, car il contient une famille libre $(e_i)_{i\in\mathbb{N}}$ indexée par un ensemble infini.

Soit maintenant A un $\mathbb{Q}$-ev. Si A est de dimension finie, son dual A^* est de dimension finie. Il ne peut donc pas être isomorphe au $\mathbb{Q}$-ev $\mathbb{Q}^{(\mathbb{N})}$.
Si A n'est pas de dimension finie, admettons qu'il a une base $(e_i)_{i\in I}$, où I est un ensemble infini. Si I n'est pas dénombrable, A et A^* ne sont pas dénombrables car ils contiennent des familles libres indexées par I ; le $\mathbb{Q}$-ev A^* n'est donc pas isomorphe au $\mathbb{Q}$-ev $\mathbb{Q}^{(\mathbb{N})}$. Si I est dénombrable, on peut supposer par changement d'indices que c'est $\mathbb{N}$. Alors A est isomorphe au $\mathbb{Q}$-ev $\mathbb{Q}^{(\mathbb{N})} = F$, donc A^* est isomorphe au $\mathbb{Q}$-ev F^* ; or on a vu dans le *a*), que F^* est isomorphe à $\mathbb{Q}^{\mathbb{N}}$, donc dans ce cas A^* est isomorphe à $\mathbb{Q}^{\mathbb{N}}$, et n'est donc pas isomorphe à $\mathbb{Q}^{(\mathbb{N})}$, puisqu'il ne lui est pas équipotent.
Le $\mathbb{Q}$-ev $\mathbb{Q}^{(\mathbb{N})}$ n'est donc isomorphe au dual d'aucun $\mathbb{Q}$-ev.

Exercice 3 :

> Soit E un K-ev, supposé muni d'une base $\mathcal{B} = (e_i)_{i\in I}$. Démontrer que l'application canonique $J_E : E \to E^{**}$ est injective (lorsque I est infini, on peut prouver que J_E n'est pas surjective, mais cela déborde le cadre de cet ouvrage). ■

Pour $i \in I$, notons φ_i la forme linéaire qui à un vecteur $v \in E$ fait correspondre sa coordonnée sur le vecteur e_i dans la base $(e_j)_{j\in I}$. Si $v \neq 0$, alors il existe $i \in I$ tel que $\varphi_i(v) \neq 0$, ce qu'on écrit aussi : $J_E(v)(\varphi_i) = \varphi_i(v) \neq 0$; l'application linéaire $J_E(v)$ n'est donc pas nulle. Nous en déduisons que $J_E(v) = 0$ si, et seulement si, $v = 0$, et par conséquent que J_E est injective.

Exercice 6 :

> Soit E un ensemble non vide muni d'une loi interne notée $+$, et d'une loi externe de domaine K notée $(\lambda, x) \mapsto \lambda \cdot x$, $K \times E \to E$. On note F l'ensemble des $\varphi \in \mathcal{F}(E, K)$ telles que $\forall (x, y) \in E^2$, $\forall \lambda \in K \quad \varphi(x + y) = \varphi(x) + \varphi(y)$ et $\varphi(\lambda \cdot x) = \lambda\, \varphi(x)$. On suppose que $(\forall (x, y) \in E^2),\ (x \neq y) \Rightarrow \exists \varphi \in F \mid \varphi(x) \neq \varphi(y)$. Montrer que $(E, +, \cdot)$ est un K-ev (ENS *de Sèvres*.

Remarquons d'abord que d'après l'hypothèse :

$$(\forall (x,y) \in E^2) \quad x = y \Longleftrightarrow (\forall \varphi \in \mathcal{F}(E,K)) \ \ \varphi(x) = \varphi(y) \ .$$

Montrons que $(E,+)$ est un groupe abélien.
Associativité.
Soit $(x,y,z) \in E^3$, pour tout $\varphi \in F$, on a :

$$\varphi\big((x+y)+z\big) = \varphi(x+y) + \varphi(z) = \varphi(x) + \varphi(y) + \varphi(z) \ .$$

On obtient de même :

$$\varphi\big(x+(y+z)\big) = \varphi(x) + \varphi(y+z) = \varphi(x) + \varphi(y) + \varphi(z) \ .$$

D'après la remarque préliminaire, nous en déduisons $(x+y)+z = x+(y+z)$.

Commutativité.
Soit $(x,y) \in E^2$, pour tout $\varphi \in F$, on a :

$$\varphi(x+y) = \varphi(x) + \varphi(y) = \varphi(y) + \varphi(x) = \varphi(x+y) \ .$$

Nous en déduisons $x + y = y + x$.

Neutre.
Soit $x_0 \in E$ ($E \neq \emptyset$), et $y \in E$. Pour tout $\varphi \in F$ on a :

$$\varphi(0 \cdot x_0 + y) = 0\,\varphi(x_0) + \varphi(y) = \varphi(y) \ .$$

Nous en déduisons $0 \cdot x_0 + y = y$. On voit donc que $0 \cdot x_0$ est élément neutre.

Opposé.
Soit $x \in E$, pour tout $\varphi \in F$, on a :

$$\varphi((-1) \cdot x + x) = (-1)\,\varphi(x) + \varphi(x) = 0 = \varphi(0 \cdot x_0) \ .$$

Nous en déduisons $(-1) \cdot x + x = 0 \cdot x_0$, élément neutre. Donc $(-1) \cdot x$ est l'opposé de x.
L'ensemble E muni de la loi interne $+$ est donc un groupe abélien.

Montrons maintenant que $(E,+,\cdot)$ est un K-ev.
Soient $(x,y) \in E^2$ et $\lambda \in K$. Pour toute application $\varphi \in F$:

$$\begin{aligned} \varphi(\lambda \cdot (x+y)) &= \lambda\,\varphi(x+y) = \lambda\,(\varphi(x) + \varphi(y)) = \\ &= \lambda\,\varphi(x) + \lambda\,\varphi(y) = \varphi(\lambda \cdot x) + \varphi(\lambda \cdot y) = \varphi(\lambda \cdot x + \lambda \cdot y) \ . \end{aligned}$$

Nous en déduisons $\lambda \cdot (x+y) = \lambda \cdot x + \lambda \cdot y$.

Soit $x \in E$ et $(\lambda, \mu) \in K^2$. Pour toute application $\varphi \in F$:

$$\varphi((\lambda + \mu) \cdot x) = (\lambda + \mu)\,\varphi(x) = \lambda\,\varphi(x) + \mu\,\varphi(x) = \\ = \varphi(\lambda \cdot x) + \varphi(\mu \cdot x) = \varphi(\lambda \cdot x + \mu \cdot x) \ .$$

Nous en déduisons $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$.

Soit $x \in E$ et $(\lambda, \mu) \in K^2$. Pour toute application $\varphi \in F$:

$$\varphi(\lambda \cdot (\mu \cdot x)) = \lambda\,\varphi(\mu \cdot x) = \lambda\,\mu\,\varphi(x) = \varphi((\lambda\,\mu) \cdot x) \ .$$

Nous en déduisons $\lambda \cdot (\mu \cdot x)) = (\lambda\,\mu) \cdot x$.

Soit $x \in E$, pour toute application $\varphi \in F$:

$$\varphi(1 \cdot x) = 1\,\varphi(x) = \varphi(x) \ ,$$

donc $1 \cdot x = x$.
Cela démontre que $(E, +, \cdot)$ est un K-ev.

§ XII.2 *DUALITÉ EN DIMENSION FINIE*

Exercice 2 :

Soit E un K-ev de dimension finie $n \geqslant 1$. Si $x \in E$ et $y \in E$, avec $x \neq y$, il existe $\varphi \in E^*$ telle que $\varphi(x) \neq \varphi(y)$ (on dit que E^* *sépare* les points de E).

Réciproquement, soit $V \subset E^*$ un sous-K-ev de E^* qui sépare les points de E, *i.e.* $\forall (x, y) \in E^2,\ (x \neq y) \Rightarrow \exists \varphi \in V \mid \varphi(x) \neq \varphi(y)$. Montrer que $V = E^*$. ■

La propriété du sous-K-ev V est équivalente à :

$$(\forall (x, y) \in E^2) \quad x = y \Longleftrightarrow (\forall \varphi \in V) \ \ \varphi(x) = \varphi(y) \ .$$

Comme les applications φ sont des formes linéaires, cette propriété s'écrit encore :

$$(\forall x \in E) \quad x = 0 \Longleftrightarrow (\forall \varphi \in V) \ \ \varphi(x) = 0 \ .$$

Cette propriété est donc ${}^0V = \{0\}$. On en déduit $V = ({}^0V)^0 = \{0\}^0 = E^*$.

Exercice 3 :

Soit E et F deux K-ev de dimensions finies $n \geqslant$

Pour chaque couple $(\varphi, x) \in E^* \times F$, on définit $u = \varphi \otimes x \in \mathrm{Hom}_K(E,F)$ par la condition :

$$(\forall z \in E) \quad u(z) = \varphi(z)\, x\,.$$

a) Montrer que l'application $\zeta : E^* \times F \to \mathrm{Hom}_K(E,F)$, $(\varphi, x) \mapsto \varphi \otimes x$, est bilinéaire, et que, si $\mathscr{B} = (e_1, \ldots, e_n)$ est une base de E, de base duale $\mathscr{B}^* = (e_1^*, \ldots, e_n^*)$, et si $(f_1, \ldots, f_p)$ est une base de F, alors $(e_i^* \otimes f_j)_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]}$ est une base de $\mathrm{Hom}_K(E,F)$. Reconnaître cette base.

b) Montrer : pour tout K-ev G, et toute application *bilinéaire* $f : E^* \times F \to G$, il existe une, et une seule, application *linéaire* $\bar{f} : \mathrm{Hom}_K(E,F) \to G$ telle que $\bar{f} \circ \zeta = f$.

c) Soit $g : E^* \times F \to K$, $(\varphi, x) \mapsto \varphi(x) =< x, \varphi >$. Montrer que $\bar{g}(u) = \mathrm{Tr}\,(u)$ pour tout $u \in \mathrm{Hom}_K(E)$ (on peut ainsi définir la trace d'un endomorphisme d'une façon *intrinsèque*). ■

a) Soit $\varphi \in E^*$, $(x,y) \in F^2$ et $\lambda \in K$; pour tout $z \in E$, on a :

$$\begin{aligned}\big(\varphi \otimes (x + \lambda y)\big)(z) &= \varphi(z)\,(x + \lambda y) = \varphi(z)\, x + \lambda \varphi(z)\, y = \\ &= (\varphi \otimes x)(z) + \lambda\,(\varphi \otimes y)(z) = (\varphi \otimes x + \lambda \varphi \otimes y)(z)\,.\end{aligned}$$

Nous en déduisons :

$$\varphi \otimes (x + \lambda y) = \varphi \otimes x + \lambda \varphi \otimes y\,.$$

Soient $(\varphi, \psi) \in E^{*2}$, $\lambda \in K$, et $x \in F$; pour tout $z \in E$, on a :

$$\begin{aligned}\big((\varphi + \lambda \psi) \otimes x\big)(z) &= (\varphi + \lambda \psi)(z)\, x = \varphi(z)\, x + \lambda \psi(z)\, x = \\ &= (\varphi \otimes x)(z) + \lambda\,(\psi \otimes x)(z) = (\varphi \otimes x + \lambda \psi \otimes x)(z)\,.\end{aligned}$$

Nous en déduisons :

$$(\varphi + \lambda \psi) \otimes x = \varphi \otimes x + \lambda \psi \otimes x\,.$$

L'application ζ est donc bilinéaire.

Pour tout $(i,j) \in [\![1,n]\!] \times [\![1,p]\!]$, pour tout $h \in [\![1,n]\!]$, on a :

$$(e_i^* \otimes f_j)(e_h) = e_i^*(e_h)\, f_j = \delta_{i,h}\, f_j\,,$$

où δ est le symbole de Kronecker. On reconnaît donc dans $e_i^* \otimes f_j$, l'élément $u_{j,i}$ de la base de $\mathrm{Hom}_K(E,F)$ associée aux bases $\mathcal{B}$ de E et $(f_1,\ldots,f_p)$ de F (voir la démonstration du théorème IX.4.6).

b) Si l est une application linéaire $\mathrm{Hom}_K(E,F) \to G$, les applications $l \circ \zeta$ et f sont des applications bilinéaires $E^* \times F \to G$; elles sont donc égales si, et seulement si, elles coïncident sur les couples (e_i^*, f_j), où $(i,j) \in [\![1,n]\!] \times [\![1,p]\!]$, donc si, et seulement si, pour tout $(i,j) \in [\![1,n]\!] \times [\![1,p]\!]$, $l(e_i^* \otimes f_j) = f(e_i, f_j)$. Comme la famille $(e_i^* \otimes f_j)_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]}$ est une base du K-ev $\mathrm{Hom}_K(E,F)$, il est clair d'après le Théorème VI.3.2 qu'il existe une et une seule application linéaire $l : \mathrm{Hom}_K(E,F) \to G$, qui vérifie cette condition.

c) Nous appliquons ici les résultats de la question *b*) dans le cas où $E = F$, et par conséquent $n = p$. On prendra $(f_1,\ldots,f_p) = (e_1,\ldots,e_n)$.

Par définition, pour tout $(i,j) \in [\![1,n]\!]^2$:

$$\bar{g}(u_{j,i}) = \bar{g}(e_i^* \otimes e_j) = g(e_i^*, e_j) = e_i^*(e_j) = \delta_{i,j} \ .$$

Soit $u \in \mathrm{Hom}_K(E,F)$, posons $u = \sum_{(i,j)\in[\![1,n]\!]^2} \lambda_{j,i}\, u_{j,i}$, où pour tout $(i,j) \in [\![1,n]\!]^2$, $\lambda_{j,i} \in K$; on obtient :

$$\bar{g}(u) = \sum_{(i,j)\in[\![1,n]\!]^2} \lambda_{j,i}\, \bar{g}(u_{j,i}) = \sum_{(i,j)\in[\![1,n]\!]^2} \lambda_{j,i}\, \delta_{i,j} = \sum_{i=1}^{n} \lambda_{i,i} = \mathrm{Tr}\,(u) \ .$$

Exercice 4 :

> Soit E la K-algèbre $\mathcal{F}(K,K)$. On considère des éléments f_1, $\ldots$, f_n de E linéairement indépendants. En raisonnant par dualité, montrer qu'il existe $a_1,\ldots,a_n$ dans K tels que la matrice $[f_i(a_j)]_{(i,j)\in[\![1,n]\!]^2}$ soit inversible. ■

Soit F le sous-K-ev de E engendré par la famille $(f_1,\ldots,f_n)$ $(n \geqslant 1)$. Pour tout $a \in K$, on note $\delta_a : F \to K$ l'application $f \mapsto f(a)$ ($\delta_a \in F^*$).

Soit V le sous-K-ev de F^* engendré par la famille $(\delta_a)_{a\in K}$. On voit que :

$${}^0V = \{f \in F \mid (\forall a \in K)\ f(a) = 0\} = \{0\} \ .$$

Comme F est de dimension finie, nous en déduisons $V = F^*$. La famille $(\delta_a)_{a\in K}$ est donc génératrice de F^*, et on peut en extraire une base. Il existe par conséquent une famille $(a_1,\dots,a_n) \in K^n$, telle que la famille $(\delta_{a_1},\dots,\delta_{a_n})$ soit une base du K-ev F^*. Considérons la base $(f_1^*,\dots,f_n^*)$ de F^*, base duale de la base $(f_1,\dots,f_n)$ de F. Le terme (i,j) de la matrice de passage de la base $(f_1^*,\dots,f_n^*)$ vers la base $(\delta_{a_1},\dots,\delta_{a_n})$ de F^*, est la i-ième coordonnée dans la base $(f_1^*,\dots,f_n^*)$ de la forme linéaire δ_{a_j} ; c'est donc la valeur de cette forme linéaire sur le vecteur f_i, c'est-à-dire $\delta_{a_j}(f_i) = f_i(a_j)$. La matrice $[f_i(a_j)]_{(i,j)\in[\![1,n]\!]^2}$ est donc une matrice de passage et est par conséquent inversible.

Exercice 5 :

> Soit $n \in \mathbb{N}^*$. Pour chaque $d \in \mathbb{N}^*$, on note $\mathcal{H}_d$ le $\mathbb{C}$-ev des polynômes homogènes de degré d à n lettres $X_1,\dots,X_n$ sur $\mathbb{C}$. On fixe $p \geqslant 1$. Montrer que l'ensemble $\{\varphi^p\}_{\varphi\in\mathcal{H}_1}$ engendre le $\mathbb{C}$-ev $\mathcal{H}_p$, en étudiant son orthogonal dans $\mathcal{H}_p^*$. ■

Soit $\mathcal{S} = \{(\alpha_1,\dots,\alpha_n) \in \mathbb{N}^n \mid \alpha_1 + \dots + \alpha_n = p\}$.

Soit ψ une forme linéaire $\mathcal{H}_p \to \mathbb{C}$, nulle sur l'espace V engendré par l'ensemble $\{\varphi^p\}_{\varphi\in\mathcal{H}_1}$; c'est-à-dire :

$$(\forall(\lambda_1,\dots,\lambda_n) \in \mathbb{C}^n) \quad \psi\left((\lambda_1 X_1 + \dots + \lambda_n X_n)^p\right) = 0 .$$

En utilisant la formule du multinôme on obtient :

$$(\forall(\lambda_1,\dots,\lambda_n) \in \mathbb{C}^n) \quad \psi\left(\sum_{\alpha\in\mathcal{S}} \frac{p!}{\alpha_1!\dots\alpha_n!}\lambda_1^{\alpha_1}\dots\lambda_n^{\alpha_n}\, X_1^{\alpha_1}\dots X_n^{\alpha_n}\right) = 0 .$$

Comme pour tout $\alpha \in \mathcal{S}$, le monôme $X_1^{\alpha_1}\dots X_n^{\alpha_n}$ est homogène de degré p, on peut écrire :

$$(\forall(\lambda_1,\dots,\lambda_n) \in \mathbb{C}^n) \quad \sum_{\alpha\in\mathcal{S}} \frac{p!}{\alpha_1!\dots\alpha_n!}\lambda_1^{\alpha_1}\dots\lambda_n^{\alpha_n}\psi(\, X_1^{\alpha_1}\dots X_n^{\alpha_n}) = 0 .$$

L'application polynomiale $Q : \mathbb{C}^n \to \mathbb{C}$:

$$(\lambda_1,\dots,\lambda_n) \mapsto \sum_{\alpha\in\mathcal{S}} \frac{p!}{\alpha_1!\dots\alpha_n!}\psi(\, X_1^{\alpha_1}\dots X_n^{\alpha_n})\,\lambda_1^{\alpha_1}\dots\lambda_n^{\alpha_n} ,$$

est donc identiquement nulle. Nous pouvons en déduire :

$$(\forall\alpha \in \mathcal{S}) \quad \frac{p!}{\alpha_1!\dots\alpha_n!}\,\psi(\, X_1^{\alpha_1}\dots X_n^{\alpha_n}) = 0 ,$$

d'où :

$$(\forall \alpha \in \mathcal{S}) \quad \psi(X_1^{\alpha_1} \dots X_n^{\alpha_n}) = 0 ,$$

puisque $\mathbb{C}$ est de caractéristique 0. Comme la famille $(X_1^{\alpha_1} \dots X_n^{\alpha_n})_{\alpha \in \mathcal{S}}$ est une base de l'espace $\mathcal{H}_p$, nous en déduisons $\psi = 0$.

Nous avons démontré $V^0 = \{0\}$, et par conséquent $V = \mathcal{H}_p$.

Exercice 7 :

Soit E un K-ev de dimension finie $n \geqslant 1$.
a) Si $u \in \mathrm{Hom}_K(E)$, soit $T_u \in (\mathrm{Hom}_K(E))^*$ tel que $T_u(v) = \mathrm{Tr}(u\,v)$ pour $v \in \mathrm{Hom}_K(E)$. Montrer que l'application $u \mapsto T_u$, $\mathrm{Hom}_K(E) \to (\mathrm{Hom}_K(E))^*$ est un isomorphisme.
b) Pour u et α éléments de $\mathrm{Hom}_K(E)$, on pose

$$[u, \alpha] = u\,\alpha - \alpha\,u , \text{ et } \mathcal{C}_\alpha = \{u \in \mathrm{Hom}_K(E) \mid [u, \alpha] = 0\} .$$

Montrer, pour tous α, β dans $\mathrm{Hom}_K(E)$ et $\gamma \in \mathcal{C}_\alpha$:

$$\mathrm{Tr}([\alpha, \beta]\,\gamma) = 0 .$$

c) Soit α et u dans $\mathrm{Hom}_K(E)$ tels que T_u s'annule sur $\mathcal{C}_\alpha$. Montrer qu'il existe $\beta \in \mathrm{Hom}_K(E)$ tel que $u = [\alpha, \beta]$. ■

Soit $(e_1, \dots, e_n)$ une base de E. Pour tout $(i, j) \in [\![1, n]\!]^2$, nous noterons $u_{i,j}$ l'endomorphisme de E tel que pour tout $k \in [\![1, n]\!]$, $u_{i,j}(e_k) = \delta_{j\,k}\,e_i$. On sait que la famille $(u_{i,j})_{(i,j) \in [\![1,n]\!]^2}$ est une base du K-ev $\mathrm{Hom}_K(E)$ (voir théorème IX.4.6). Pour tous entiers i, j, h, k dans $[\![1, n]\!]$, on établit sans peine l'égalité :

$$u_{i,j} \circ u_{h,k} = \delta_{j,h}\,u_{i,k} .$$

On remarque aussi que pour tout $(i, j) \in [\![1, n]\!]^2$, $\mathrm{Tr}(u_{i,j}) = \delta_{i,j}$.
Enfin, rappelons que si u et v sont des éléments de $\mathrm{Hom}_K(E)$, $\mathrm{Tr}(u\,v) = \mathrm{Tr}(v\,u)$.

a) Il est clair que l'application $u \mapsto T_u$ est linéaire. Montrons qu'elle est injective.
Soit $u \in \mathrm{Hom}_K(E)$, écrivons $u = \sum_{(i,j) \in [\![1,n]\!]^2} \lambda_{i,j}\,u_{i,j}$, où pour tout $(i, j) \in [\![1, n]\!]^2$, $\lambda_{i,j} \in K$. Pour tout $(h, k) \in [\![1, n]\!]^2$, on obtient :

$$T_u(u_{h,k}) = \mathrm{Tr}\left(\sum_{i,j} \lambda_{i,j}\,u_{i,j}\,u_{h,k}\right) = \mathrm{Tr}\left(\sum_{i=1}^{n} \lambda_{i,h} u_{i,k}\right) =$$

$$= \sum_{i=1}^{n} \lambda_{i,h} \mathrm{Tr}(u_{i,k}) = \lambda_{\cdot} .$$

On voit donc que si $T_u = 0$, alors pour tout $(h,k) \in [\![1,n]\!]^2$, $\lambda_{k,h} = 0$, donc $u = 0$. L'application $u \mapsto T_u$ est donc injective, et comme les K-espaces $\mathrm{Hom}_K(E)$ et $(\mathrm{Hom}_K(E))^*$ sont tous les deux de dimension finie égale à n^2, nous en déduisons que $u \mapsto T_u$ est un isomorphisme.

On peut remarquer que $T_u(u_{h,k}) = \lambda_{k,h}$, est la coordonnée de T_u sur l'élément $u^*_{h,k}$ de la base $(u^*_{i,j})_{(i,j)\in[\![1,n]\!]^2}$ de l'espace $(\mathrm{Hom}_K(E))^*$, base duale de la base $(u_{i,j})$ de $\mathrm{Hom}_K(E)$. Donc si $u = \sum_{(i,j)\in[\![1,n]\!]^2} \lambda_{i,j}\, u_{i,j}$, alors $T_u = \sum_{(i,j)\in[\![1,n]\!]^2} \lambda_{j,i}\, u^*_{i,j}$.

L'application $T : \mathrm{Hom}_K(E) \to (\mathrm{Hom}_K(E))^*$ est donc l'application linéaire telle que pour tout $(h,k) \in [\![1,n]\!]^2$, $T_{u_{k,h}} = u^*_{h,k}$.

b) On obtient :

$$[\alpha,\beta]\,\gamma = \alpha\beta\gamma - \beta\alpha\gamma = \alpha\beta\gamma - \beta\gamma\alpha\ ,$$

puisque γ commute avec α. Nous en déduisons :

$$\mathrm{Tr}\,([\alpha,\beta]\,\gamma) = \mathrm{Tr}\,(\alpha\,(\beta\gamma) - (\beta\gamma)\,\alpha) = 0\ .$$

c) Pour $\alpha \in \mathrm{Hom}_K(E)$ fixé, posons $V = \{[\alpha,\beta]\ ,\ \beta \in \mathrm{Hom}_K(E)\}$. Comme l'application $\beta \mapsto [\alpha,\beta]$ est linéaire, on voit que V est un sous-K-ev de $\mathrm{Hom}_K(E)$. On a démontré dans le *b*), que pour tout $u \in V$, et pour tout $\gamma \in \mathscr{C}_\alpha$, $T_u(\gamma) = 0$, soit encore pour tout $u \in V$, $T_u \in \mathscr{C}^0_\alpha$.

Le sous-K-ev V est l'image de l'application $\beta \mapsto \alpha\beta - \beta\alpha$, dont le noyau est par définition $\mathscr{C}_\alpha$, donc $\dim V = \mathrm{Codim}\mathscr{C}_\alpha = \dim \mathscr{C}^0_\alpha$. Comme $u \mapsto T_u$ est un isomorphisme linéaire, l'ensemble $\{T_u\ ,\ u \in V\}$ est un sous-K-ev de dimension $\dim V = \dim \mathscr{C}^0_\alpha$ de $(\mathrm{Hom}_K(E))^*$. D'après ce qui précède, $\{T_u\ ,\ u \in V\} \subset \mathscr{C}^0_\alpha$, on voit donc que $\{T_u\ ,\ u \in V\} = \mathscr{C}^0_\alpha$.

Cela implique que si la forme linéaire T_u est nulle sur $\mathscr{C}_\alpha$, alors $u \in V$, c'est-à-dire :

$$(\exists \beta \in \mathrm{Hom}_K(E)) \quad u = [\alpha,\beta]\ .$$

C'est ce qu'il fallait démontrer.

Exercice 8 :

‖ Soit E un K-ev de dimension finie $n \geqslant 2$ et λ_1

tincts dans K. On considère une base $\mathcal{B} = (e_1, \ldots, e_n)$ de E, et $\alpha \in \mathrm{Hom}_K(E)$ tel que

$$\mathrm{Mat}_{\mathcal{B}}(\alpha) = \mathrm{Diag}(\lambda_1, \ldots, \lambda_n).$$

a) Montrer que $\mathcal{C}_\alpha$ est un sous-K-ev de dimension n du K-ev $\mathrm{Hom}_K(E)$, et que $(\mathrm{Id}, \alpha, \ldots, \alpha^{n-1})$ en est une base. (On reprend les notations de l'exercice 7).

b) En déduire : si $v \in \mathrm{Hom}_K(E)$, pour qu'il existe un endomorphisme $u \in \mathrm{Hom}_K(E)$ tel que $[\alpha, u] = v$, il faut et il suffit que $\mathrm{Tr}(v\,\alpha^k) = 0$ pour $k \in [\![0, n-1]\!]$.

c) Soit $v \in \mathrm{Hom}_K(E)$ et $[a_{i,j}]$ sa matrice dans $\mathcal{B}$. Pour qu'il existe $u \in \mathrm{Hom}_K(E)$ tel que $[\alpha, u] = v$, il faut et il suffit que $a_{i,i} = 0$ pour tout i. ■

a) Montrons que $\mathcal{C}_\alpha$ est l'ensemble des éléments $u \in \mathrm{Hom}_K(E)$ dont la matrice dans la base $\mathcal{B}$ est diagonale. Il clair que si u vérifie cette condition, alors u commute avec α. Inversement si u commute avec α pour tout $i \in [\![1, n]\!]$, $\alpha(u(e_i)) = u(\alpha(e_i)) = u(\lambda_i\, e_i) = \lambda_i\, u(e_i)$; le vecteur $u(e_i)$ est donc dans l'espace propre de α relatif à la valeur propre λ_i ; comme cet espace propre est de dimension 1 engendré par e_i, on en déduit qu'il existe $\mu_i \in K$, tel que $u(e_i) = \mu_i\, e_i$. Ceci étant vrai pour tout $i \in [\![1, n]\!]$, on voit que la matrice de u dans la base $\mathcal{B}$ est diagonale. L'ensemble $\mathcal{C}_\alpha$ est donc le sous-K-ev des endomorphismes de E dont la matrice dans la base $\mathcal{B}$ est diagonale. Ce sous-K-ev est évidemment de dimension n.

Soit $u \in \mathcal{C}_\alpha$, posons $u(e_i) = \mu_i\, e_i$ pour $i \in [\![1, n]\!]$. Il existe un polynôme P, $P \in K_{n-1}[X]$, tel que pour tout $i \in [\![1, n]\!]$, $P(\lambda_i) = \mu_i$ (polynôme d'interpolation de Lagrange). L'endomorphisme $P(\alpha)$ a pour matrice dans la base $\mathcal{B}$ la matrice $\mathrm{Diag}(P(\lambda_1), \ldots, P(\lambda_n)) = \mathrm{Diag}(\mu_1, \ldots, \mu_n)$, et par conséquent $u = P(\alpha)$. On voit donc que $\mathcal{C}_\alpha$ est inclus dans le sous-K-ev engendré par la famille $(\mathrm{Id}, \alpha, \ldots, \alpha^{n-1})$. Comme $\mathcal{C}_\alpha$ est de dimension n, il y a égalité, et la famille $(\mathrm{Id}, \alpha, \ldots, \alpha^{n-1})$ est une base de $\mathcal{C}_\alpha$.

b) D'après le *a*), la condition : $(\forall k \in [\![0, n-1]\!])$ $\mathrm{Tr}(v\,\alpha^k) = 0$, est réalisée si, et seulement si, T_v est nulle sur $\mathcal{C}_\alpha$. D'après l'exercice 7 *c*), cette condition est équivalente à la condition $\exists u \in \mathrm{Hom}_K(E)$, $v = [\alpha, u]$.

c) D'après l'exercice 7 *c*), la condition : $\exists u \in \mathrm{Hom}_K(E)$, $v = [\alpha, u]$, est réalisée si, et seulement si, T_v est nulle sur $\mathcal{C}_\alpha$. Comme $\mathcal{C}_\alpha$ est engendré par les $u_{h,h}$, où $h \in [\![1, n]\!]$, cette condition s'écrit encore :

$$(\forall h \in [\![1, n]\!]) \quad \mathrm{Tr}(v\,u_{h,h}) = a_{h,h} = 0,$$

ce qu'il fallait démontrer.

§ XII.3 *QUOTIENTS D'ESPACES VECTORIELS*

Exercice 2 :

Soit E, F, G trois K-ev, $u \in \mathrm{Hom}_K(E,F)$ et $v \in \mathrm{Hom}_K(F,G)$. On suppose F de dimension finie. Démontrer :

$$\mathrm{rg}\, v = \mathrm{rg}\,(v \circ u) + \mathrm{Codim}_F(\mathrm{Im}\,(u) + \mathrm{Ker}\,(v))\,. \blacksquare$$

Soit v_1 la restriction de v à $\mathrm{Im}\,(u)$, $v_1 \in \mathrm{Hom}_K(\mathrm{Im}\,(u), G)$. On a la relation :

$$(1) \qquad \begin{aligned} \mathrm{rg}\,(v \circ u) = \mathrm{rg}\, v_1 &= \dim(\mathrm{Im}\, u) - \dim(\mathrm{Ker}\, v_1) = \\ &= \dim(\mathrm{Im}\, u) - \dim(\mathrm{Ker}\, v \cap \mathrm{Im}\, u)\ . \end{aligned}$$

Comme $\mathrm{Ker}\, v$ et $\mathrm{Im}\, u$ sont deux sous-K-ev de F, on a aussi l'égalité :

$$\dim(\mathrm{Ker}\, v + \mathrm{Im}\, u) = \dim(\mathrm{Ker}\, v) + \dim(\mathrm{Im}\, u) - \dim(\mathrm{Ker}\, v \cap \mathrm{Im}\, u)\ ,$$

soit :

$$\dim(\mathrm{Ker}\, v + \mathrm{Im}\, u) - \dim(\mathrm{Ker}\, v) = \dim(\mathrm{Im}\, u) - \dim(\mathrm{Ker}\, v \cap \mathrm{Im}\, u)\ ,$$

soit encore :

$$\mathrm{Codim}_F(\mathrm{Ker}\, v) - \mathrm{Codim}_F(\mathrm{Ker}\, v + \mathrm{Im}\, u) = \dim(\mathrm{Im}\, u) - \dim(\mathrm{Ker}\, v \cap \mathrm{Im}\, u)\ ,$$

et finalement :

$$\mathrm{rg}\, v - \mathrm{Codim}_F(\mathrm{Ker}\, v + \mathrm{Im}\, u) = \dim(\mathrm{Im}\, u) - \dim(\mathrm{Ker}\, v \cap \mathrm{Im}\, u)\ .$$

En utilisant l'égalité (1) on obtient :

$$\mathrm{rg}\,(v \circ u) = \mathrm{rg}\, v - \mathrm{Codim}_F(\mathrm{Ker}\, v + \mathrm{Im}\, u)\ ,$$

d'où finalement :

$$\mathrm{rg}\, v = \mathrm{rg}\,(v \circ u) + \mathrm{Codim}_F(\mathrm{Ker}\, v + \mathrm{Im}\, u)\ ,$$

ce qu'il fallait démontrer.

Exercice 8 :

Soit E un K-ev de dimension finie $n \geqslant 1$, et $V_1, \ldots, V_r$ des sous-K-ev de codimensions $\mu_1, \ldots, \mu_r$ $(r \leqslant n)$.

a) Montrer d'abord que $\text{Codim}\,(\cap V_i) \leqslant \sum \mu_i$.

b) Prouver ensuite l'équivalence des quatre conditions suivantes :

(I) $\forall i \in [\![1, r]\!]$, $\text{Codim}_E\left(\bigcap_{j=1}^{i} V_j\right) = \sum_{j=1}^{i} \mu_j$.

(II) Les $(V_j^0)_{j\in[\![1,r]\!]}$ sont linéairement indépendants.

(III) Il existe une décomposition $E = F \oplus W_1 \oplus \ldots \oplus W_r$ telle que $(\forall j)$ $V_j = F \oplus \left(\bigoplus_{k\neq j} W_k\right)$.

(IV) Si $F = \bigcap_{j=1}^{r} V_j$, alors $\text{Codim}_E(F) = \sum_{j=1}^{r} \mu_j$.

c) Cas où les V_j sont des hyperplans ? ■

Etablissons d'abord quelques résultats sur les orthogonaux.

Lemme 1 :

Soit E un K-ev et U et V des sous-K-ev de E^* , ${}^0(U+V) = {}^0U \cap {}^0V$. ■

Soit $x \in E$, $x \in {}^0U \cap {}^0V$ si, et seulement si, l'ensemble $\{\varphi \in E^* \mid \varphi(x) = 0\}$ contient U et contient V ; comme cet ensemble de formes linéaires est un sous-K-ev de E^* , c'est vrai si, et seulement si, $\{\varphi \in E^* \mid \varphi(x) = 0\}$ contient $U + V$, donc si, et seulement si, $x \in {}^0(U+V)$.

Lemme 2 :

Soit E un K-ev et A et B des sous-K-ev de E , $(A+B)^0 = A^0 \cap B^0$. ■

Soit $\varphi \in E^*$, $\varphi \in A^0 \cap B^0$ si, et seulement si, l'ensemble $\{x \in E \mid \varphi(x) = 0\}$ contient A et contient B ; comme cet ensemble est un sous-K-ev de E , c'est vrai si, et seulement si, $\{x \in E \mid \varphi(x) = 0\}$ contient $A + B$, donc si, et seulement si, $\varphi \in (A+B)^0$.

Lemme 3 :

Soit E un K-ev de dimension finie, A un sous-K-ev de E et U un sous-K-ev de E^* , alors $A = {}^0U$ si, et seulement si, $A^0 = U$. ■

Si $A = {}^0U$, alors $A^0 = \left({}^0U\right)^0 = U$. Si $A^0 = U$, alors $A = {}^0\left(A^0\right) = {}^0U$.

Lemme 4 :

Soit E un K-ev de dimension finie, et A et B des sous-K-ev de E , alors $(A \cap B)^0 = A^0 + B^0$. ■

En utilisant le lemme 1, on trouve :

$$A \cap B = {}^0(A^0) \cap {}^0(B^0) = {}^0(A^0 + B^0) \ .$$

En utilisant le lemme 3, on en déduit :

$$(A \cap B)^0 = A^0 + B^0 \ .$$

Lemme 5 :

Soit E un K-ev de dimension finie, et $f \in \mathrm{Hom}_K(E^*)$, il existe un et un seul $h \in \mathrm{Hom}_K(E)$ tel que ${}^t h = f$ ■

Cette proposition est évidente matriciellement. On peut aussi dire, en identifiant E et son bidual, que $h = {}^t f$.

Rappelons aussi deux résultats.

Résultat 1 :

La dimension d'une somme de sous-K-ev est inférieure ou égale à la somme des dimensions, et elle est égale si, et seulement si, la somme est directe. Exercice 1 du §XI.4. ■

Résultat 2 :

Si E est un K-ev et $p_1, \ldots, p_r$ des projecteurs de E, $E = \bigoplus_{i=1}^{r} \mathrm{Im}\, p_i$ si, et seulement si, $\sum_{i=1}^{r} p_i = \mathrm{Id}_E$, et $(\forall (i,j) \in [\![1,r]\!]^2)$ $(i \neq j) \Rightarrow p_i \circ p_j = 0$. Voir exercice 7 du §IX.2. ■

a) Nous pouvons écrire l'égalité :

$$\mathrm{Codim}_E\left(\bigcap_{j=1}^{r} V_j\right) = \dim\left(\left(\bigcap_{j=1}^{r} V_j\right)^0\right) = \dim\left(\sum_{j=1}^{r} V_j^0\right) \ ,$$

d'après le lemme 4. D'après le Résultat 1, on peut affirmer :

$$\mathrm{Codim}_E\left(\bigcap_{j=1}^{r} V_j\right) \leqslant \sum_{j=1}^{r} \dim\left(V_j^0\right) = \sum_{j=1}^{r} \mu_j \ .$$

b) L'implication (I) $\Rightarrow$ (IV) est évidente.

Montrons (IV) $\Rightarrow$ (II). Si (IV) est vraie, d'après les calculs du a) :

$$\dim\left(\sum_{j=1}^{r} V_j^0\right) = \sum_{j=1}^{r} \dim\left(V_j^0\right) .$$

D'après le Résultat 1, nous en déduisons que les espaces $(V_j^0)_{j\in[\![1,r]\!]}$ sont indépendants.

Montrons (II) $\Rightarrow$ (I). Si (II) est vrai, pour tout $i \in [\![1,r]\!]$, les espaces $(V_j^0)_{j\in[\![1,i]\!]}$ sont indépendants, et par conséquent :

$$\operatorname{Codim}_E\left(\bigcap_{j=1}^{i} V_j\right) = \dim\left(\left(\bigcap_{j=1}^{i} V_j\right)^0\right) =$$

$$= \dim\left(\bigoplus_{j=1}^{i} V_j^0\right) = \sum_{j=1}^{r} \dim\left(V_j^0\right) = \sum_{j=1}^{i} \mu_j .$$

Les propriétés (I), (II) et (IV) sont donc équivalentes. Montrons maintenant qu'elles sont équivalentes à la propriété (III).

Supposons que (III) soit vraie. Notons p le projecteur sur F et p_j le projecteur sur W_j, pour $j \in [\![1,r]\!]$, dans la somme directe $E = F \oplus W_1 \oplus \ldots \oplus W_r$. Il est clair que pour tout $j \in [\![1,r]\!]$, $V_j = F \oplus \left(\bigoplus_{k\neq j} W_k\right) = \operatorname{Ker} p_j$. Par conséquent, $\bigcap_{j=1}^{r} V_j = \bigcap_{j=1}^{r} \operatorname{Ker} p_j = F$, et $\operatorname{Codim}_E(F) = \sum_{j=1}^{r} \dim W_j = \sum_{j=1}^{r} \dim \operatorname{Im}(p_j) = \sum_{j=1}^{r} \operatorname{Codim}_E\left(\operatorname{Ker}(p_j)\right) = \sum_{j=1}^{r} \operatorname{Codim}_E(V_j)$, ce qui est la propriété (IV).

Supposons que (II) soit vraie. L'espace $\bigoplus_{j=1}^{r} V_j^0$ a un supplémentaire dans E^*, qui est l'orthogonal d'un sous-K-ev G de E. On peut donc écrire $E^* = G^0 \oplus \left(\bigoplus_{j=1}^{r} V_j^0\right)$. Soit f le projecteur dans E^* sur G^0 et pour tout $j \in [\![1,r]\!]$, f_j le projecteur sur V_j^0 dans cette somme directe. Ces endomorphismes de E^* sont les transposés d'endomorphismes de E (Lemme 5) ; soit $p \in \operatorname{Hom}_K(E)$ tel que ${}^t p = f$, et pour tout $j \in [\![1,r]\!]$, $p_j \in \operatorname{Hom}_K(E)$, tel que ${}^t p_j = f_j$. On voit que p et p_j, pour tout $j \in [\![1,r]\!]$, sont des projecteurs, que ${}^t(p + p_1 + \ldots + p_r) = f + f_1 + \ldots + f_r = \mathrm{Id}_{E^*}$, et par conséquent que $p + p_1 + \ldots + p_r = \mathrm{Id}_E$. On voit aussi que pour tout $(i,j) \in [\![1,r]\!]^2$, $i \neq j$, ${}^t(p_i \circ p_j) = {}^t p_j \circ {}^t p_i = f_j \circ f_i = 0$, et par conséquent que $p_i \circ p_j = 0$. Les projecteurs $p, p_1, \ldots, p_r$ sont donc les projecteurs associés dans la somme directe de leur images (Résultat 2).

Or $(\operatorname{Im} p)^0 = \operatorname{Ker}({}^t p) = \operatorname{Ker}(f)$ (Théorème XII.1.1), et donc $(\operatorname{Im} p)^0 = \bigoplus_{j=1}^{r} V_j^0 = \left(\bigcap_{j=1}^{r} V_j\right)^0$, donc $\operatorname{Im} p = \bigcap_{j=1}^{r} V_j = F$.

Notons, pour $j \in [\![1,r]\!]$, $W_j = \operatorname{Im} p_j$, de telle sorte que $E = F \oplus W_1 \oplus \ldots \oplus W_r$. Pour tout $j \in [\![1,r]\!]$, on a $W_j^0 = \operatorname{Ker}({}^t p_j) = \operatorname{Ker}(f_j)$, et pour tout $i \in [\![1,r]\!]$:

$$V_i^0 = \operatorname{Ker} f \cap \bigcap_{j \neq i} \operatorname{Ker} f_j = F^0 \cap \bigcap_{j \neq i} W_j^0 = \left(F \oplus \left(\bigoplus_{j \neq i} W_j\right)\right)^0 ,$$

d'après le lemme 2 ; donc finalement, pour tout $i \in [\![1,r]\!]$:

$$V_i = F \oplus \left(\bigoplus_{j \neq i} W_j\right) .$$

Nous avons démontré (II) $\Rightarrow$ (III).

Les propositions (I), (II), (III) et (IV) sont donc bien équivalentes.

c) Si les V_j, pour $j \in [\![1,r]\!]$, sont des hyperplans, les espaces V_j^0 sont des droites vectorielles, elles sont indépendantes si, et seulement si, elles sont engendrées par des formes linéaires linéairement indépendantes. Dans ce cas les propriétés (I), (II), (III) et (IV) sont vérifiées, et les projecteurs f_j sur V_j^0, où $j \in [\![1,r]\!]$, sont de rang 1 ; puisque ${}^t p_j = f_j$, les projecteurs p_j sont de rang 1. Les espaces W_j, où $j \in [\![1,r]\!]$ sont donc des droites vectorielles.

Exercice 11 (cas particulier du "lemme de Zassenhaus") **:**

> Soit V, V', W, W' quatre sous-K-ev d'un K-ev E, tels que $V' \subset V$, $W' \subset W$. Démontrer que le K-ev quotient
> $Q = V \cap W / (V \cap W' + V' \cap W)$ est canoniquement isomorphe aux K-ev quotients $Q' = (V' + V \cap W)/(V' + V \cap W')$ et $Q'' = (W' + V \cap W)/(W' + V' \cap W)$. ■

Posons $F = V \cap W$ et $G = V' + V \cap W'$. On voit que $F + G = V' + V \cap W$. Montrons $F \cap G = V' \cap W + V \cap W'$. On vérifie d'abord $F \cap G = V \cap W \cap G = W \cap G$, puisque $G \subset V$. Comme $G \supset V' \cap W + V \cap W'$ et $W \supset V' \cap W + V \cap W'$, on en déduit $G \cap W \supset V' \cap W + V \cap W'$. Inversement, si $w \in W \cap G$, on peut écrire $w = v' + w'$, ou $v' \in V'$ et $w' \in V \cap W'$; mais alors $v' = w - w' \in W$, donc $v' \in V' \cap W$ et $w = v' + w' \in V' \cap$

nous en déduisons $W \cap G \subset V' \cap W + V \cap W'$. On obtient donc l'égalité $F \cap G = W \cap G = V' \cap W + V \cap W'$.

On sait que les K-ev quotient $(F+G)/_G$ et $F/_{F \cap G}$ sont isomorphes (isomorphisme de Noether), d'après ce qui précède cela signifie ici que le K-ev quotient $Q' = (V' + V \cap W)/_{(V' + V \cap W')}$ est isomorphe au K-ev quotient $Q = V \cap W/_{(V \cap W' + V' \cap W)}$. On obtient l'autre isomorphisme en intervertissant V et W, et V' et W'.

Exercice 16 :

Soit E et E' deux K-ev et F (resp. F') un sous-K-ev de E (resp. de E'). On note $\varphi : E \mapsto E/_F$ et $\varphi' : E' \mapsto E'/_{F'}$ les applications canoniques. On suppose connus des supplémentaires de F dans E et de F' dans E'.

a) Soit $\alpha : \mathrm{Hom}_K(E, E') \to \mathrm{Hom}_K\left(F, E'/_{F'}\right)$, $u \mapsto \varphi' \circ (u|_F)$.

Montrer que α est surjective et que son noyau est le sous-K-ev :

$$\mathscr{E} = \{u \in \mathrm{Hom}_K(E, E') \mid u(F) \subset F'\} \text{ (cf. exercice 6)}$$

b) Montrer que l'espace quotient $\mathscr{E}/_{\mathrm{Hom}_K(E, F')}$ est isomorphe au K-ev $\mathrm{Hom}_K(E/_F, E'/_{F'})$.

Conclure si F et F' sont de codimension finie dans E et E' respectivement. ■

Nous noterons i_F l'injection canonique $F \to E$. Avec cette notation, pour tout $u \in \mathrm{Hom}_K(E, E')$, $\alpha(u) = \varphi' \circ u \circ i_F$. Soit S un supplémentaire de F dans E, nous noterons p_F la projection sur F parallèlement à S.

Soit S' un supplémentaire de F' dans E'. La restriction de φ' à S' est un isomorphisme (Théorème XII.3.6). Nous poserons $j' = i_{S'} \circ (\varphi'_{|S'})^{-1}$. On vérifie que j' est une application linéaire injective $E'/_{F'} \to E'$ telle que $\varphi' \circ j'$ est l'identité de l'espace quotient $E'/_{F'}$.

a) Comme $\mathrm{Ker}(\varphi') = F'$, on voit que le sous-$K$-ev $\mathrm{Ker}(\alpha)$ est l'ensemble $\mathscr{E} = \{u \in \mathrm{Hom}_K(E, E') \mid u(F) \subset F'\}$. Montrons que α est surjective. Soit $v \in \mathrm{Hom}_K(F, E'/_{F'})$. Posons $u = j' \circ v \circ p_F$ ($u \in \mathrm{Hom}_K(E, E')$). On vérifie : $\varphi' \circ u \circ i_F = \varphi' \circ j' \circ v \circ p_F \circ i_F = v$. L'application linéaire α est donc surjective.

b) Soit $u \in \mathscr{E}$, on voit que $F \subset \mathrm{Ker}(\varphi' \circ u)$. Il existe donc une et une seule application linéaire $v : E/_F \to E'/_{F'}$ telle que $v \circ \varphi = \varphi' \circ u$

factorisation), et il est clair que l'application $\Phi : \mathscr{C} \to \mathrm{Hom}_K(E/_F, E'/_{F'})$, $u \mapsto v$, est K-linéaire.
Déterminons le noyau de Φ. On voit que :

$$\mathrm{Ker}\,(\Phi) = \{u \in \mathscr{C} \mid \varphi' \circ u = 0\} = \mathrm{Hom}_K(E, F') \ .$$

Montrons que Φ est surjective. Soit $v \in \mathrm{Hom}_K(E/_F, E'/_{F'})$, posons $u = j' \circ v \circ \varphi$ ($u \in \mathrm{Hom}_K(E, E')$). On voit que :

$$\varphi' \circ u = \varphi' \circ j' \circ v \circ \varphi = v \circ \varphi \ , \tag{1}$$

et que :

$$\varphi' \circ u \circ i_F = v \circ \varphi \circ i_F = 0 \ . \tag{2}$$

L'égalité (2) prouve $u \in \mathscr{C}$, et l'égalité (1) prouve $\Phi(u) = v$. L'application Φ est donc bien surjective.
L'application linéaire Φ induit donc un isomorphisme de K-ev :

$$\overline{\Phi} : {}^{\mathscr{C}}/_{\mathrm{Hom}_K(E, F')} \to \mathrm{Hom}_K(E/_F, E'/_{F'}) \ .$$

Si F est de codimension finie dans E, et que F' est de codimension finie dans E', alors $\mathrm{Hom}_K(E, F')$ est de codimension finie dans $\mathscr{C}$ et on a l'égalité :

$$\mathrm{Codim}_{\mathscr{C}}\big(\mathrm{Hom}_K(E, F')\big) = \mathrm{Codim}_E(F) \times \mathrm{Codim}_{E'}(F') \ .$$

Exercice 17 :

> Soit E un K-ev et F un sous-K-ev de codimension finie dans E. On donne $u \in \mathrm{GL}_K(E)$ tel que $u(F) \subset F$. Montrer que $u(F) = F$. Donner un exemple où cette propriété tombe en défaut lorsque F n'est pas de codimension finie. ■

Soit $p : E \to E/_F$ l'application linéaire canonique. On voit que $F \subset \mathrm{Ker}\,(p \circ u)$; il existe par conséquent une et une seule application linéaire $v : E/_F \to E/_F$, telle que $v \circ p = p \circ u$. Comme les applications linéaires p et u sont surjectives, nous en déduisons que v est surjective. Comme v est un endomorphisme surjectif du K-ev de dimension finie $E/_F$, v est aussi injectif. Nous en déduisons $F = \mathrm{Ker}\,(p) = \mathrm{Ker}\,(v \circ p) = \mathrm{Ker}\,(p \circ u) = u^{-1}(F)$. On voit donc que $u(F) = u\big(u^{-1}(F)\big) = F$, puisque u est surjective.

Soit $E = K^{\mathbb{Z}}$. Considérons sur E l'application δ qui à une suite $(s(n))_{n\in\mathbb{Z}}$ fait correspondre la suite $(s(n+1))_{n\in\mathbb{Z}}$. Il est clair qu'il s'agit d'un automorphisme linéaire de E dont l'automorphisme réciproque est

qui à une suite $(s(n))_{n\in\mathbb{Z}}$ fait correspondre la suite $(s(n-1))_{n\in\mathbb{Z}}$. Le sous-$K$-ev $F = \{s \in E \mid (\forall n \leqslant 0) \quad s(n) = 0\}$ est bien stable par δ mais n'est égal à $\delta(F)$.

§ XII.4 *QUOTIENTS, PRODUITS ET SOMMES DIRECTES*

Exercice 2 :

Soit E un K-ev, et deux sous-K-ev V et W de E. On note $\varphi : E/_{V\cap W} \to E/_V$ et $\psi : E/_{V\cap W} \to E/_W$ les applications naturelles (obtenues à partir des applications canoniques $E \to E/_V$ et $E \to E/_W$ par application du théorème XII.3.1). On définit de la même manière les applications canoniques $\alpha : E/_V \to E/_{(V+W)}$ et $\beta : E/_W \to E/_{(V+W)}$.

Soit

$$u : E/_{V\cap W} \to E/_V \times E/_W\,,\ x \mapsto (\varphi(x), \psi(x))$$

et $\quad v : E/_V \times E/_W \to E/_{(V+W)}\,,\ (y,z) \mapsto \alpha(y) - \beta(z)$.

Démontrer que u est injective, que v est surjective, et que $\mathrm{Im}\,(u) = \mathrm{Ker}\,(v)$. En déduire que, si V et W sont de codimension finie, $V\cap W$ l'est encore (ainsi, bien sûr, que $V+W$), et qu'on a :

$$\mathrm{Codim}_E(V) + \mathrm{Codim}_E(W) = \\ = \mathrm{Codim}_E(V\cap W) + \mathrm{Codim}_E(V+W)\,.\ \blacksquare$$

Si A est un sous-K-ev de E, nous noterons $\pi_A : E \to E/_A$, l'application linéaire canonique.

Les applications linéaires φ et ψ sont telles que :

$$\varphi \circ \pi_{V\cap W} = \pi_V \quad \text{et} \quad \psi \circ \pi_{V\cap W} = \pi_W\,.$$

Montrons que u est injective. Un élément $\pi_{V\cap W}(a)$, où $a \in E$, est dans le noyau de u si, et seulement si, $\varphi \circ \pi_{V\cap W}(a) = \pi_V(a) = 0$ et $\psi \circ \pi_{V\cap W}(a) = \pi_W(a) = 0$, donc si, et seulement si, $a \in V$ et $a \in W$, soit encore si, et seulement si, $a \in V\cap W$, ce qui s'écrit $\pi_{V\cap W}(a) = 0$. Comme $\pi_{V\cap W}$ est surjective, cela prouve que le noyau de u est $\{0\}$, et par conséquent que u est injective.

Les applications α et β sont telles que :

$$\alpha \circ \pi_V = \pi_{V+W} \quad \text{et} \quad \beta \circ \pi_W = \pi_{V+W}\,.$$

L'application π_{V+W} étant surjective, les applications α et β sont surjectives ; il est alors clair que l'application $v : (y,z) \mapsto \alpha(y) - \beta(z)$ est surjective.

Caractérisons $\mathrm{Im}\,(u)$:

$$\mathrm{Im}\,(u) = \mathrm{Im}\,(u \circ \pi_{V\cap W}) = \{(\pi_V(x), \pi_W(x)) \ , \ x \in E\} \ .$$

Caractérisons $\mathrm{Ker}\,(v)$.

$$\mathrm{Ker}\,(v) = \left\{(y,z) \in E/_V \times E/_W \mid \alpha(y) = \beta(z)\right\} \ ,$$

soit encore, puisque π_V et π_W sont surjectives :

$$\begin{aligned}\mathrm{Ker}\,(v) &= \left\{(\pi_V(a), \pi_W(b)) \mid (a,b) \in E^2 \text{ et } \alpha(\pi_V(a)) = \beta(\pi_W(b))\right\} = \\ &= \left\{(\pi_V(a), \pi_W(b)) \mid (a,b) \in E^2 \text{ et } \pi_{V+W}(a) = \pi_{V+W}(b)\right\} \\ &= \left\{(\pi_V(a), \pi_W(b)) \mid (a,b) \in E^2 \text{ et } a - b \in V + W\right\} \ .\end{aligned}$$

L'inclusion $\mathrm{Im}\,(u) \subset \mathrm{Ker}\,(v)$ est donc évidente. Inversement, si $(x,y) \in \mathrm{Ker}\,(v)$, écrivons $x = \pi_V(a)$ et $y = \pi_W(b)$, où $a - b \in V + W$; il existe $v \in V$ et $w \in W$ tels que $a - b = v + w$; posons $a' = a - v = b + w$, on voit que $x = \pi_V(a')$ et $y = \pi_W(a')$, donc $(x,y) = (\pi_V(a'), \pi_W(a')) \in \mathrm{Im}\,(u)$. Cela démontre l'inclusion $\mathrm{Ker}\,(v) \subset \mathrm{Im}\,(u)$. D'où l'égalité $\mathrm{Ker}\,(v) = \mathrm{Im}\,(u)$.

Si les sous-K-ev V et W sont de codimension finie, le K-ev $E/_V \times E/_W$ est de dimension finie. Puisque $v : E/_V \times E/_W \to E/_{V+W}$ est surjective, on en déduit que le K-ev quotient $E/_{V+W}$ est de dimension finie, donc que le sous-K-ev $V+W$ est de codimension finie. Puisque $u : E/_{V\cap W} \to E/_V \times E/_W$ est injective, on voit que le K-ev quotient $E/_{V\cap W}$ est de dimension finie, et donc que le sous-K-ev $V \cap W$ est de codimension finie. Comme $\mathrm{rg}\, v = \mathrm{Codim}_E(V+W)$, et $\dim \mathrm{Ker}\,(v) = \dim \mathrm{Im}\,(u) = \mathrm{Codim}_E(V \cap W)$, l'égalité :

$$\mathrm{rg}\, v + \dim \mathrm{Ker}\,(v) = \dim\left(E/_V \times E/_W\right) = \mathrm{Codim}_E(V) + \mathrm{Codim}_E(W) \ ,$$

s'écrit :

$$\mathrm{Codim}_E(V+W) + \mathrm{Codim}_E(V \cap W) = \mathrm{Codim}_E(V) + \mathrm{Codim}_E(W) \ ,$$

ce qu'il fallait démontrer.

Chapitre XIII

DÉTERMINANTS

§ XIII.1 *APPLICATIONS MULTILINÉAIRES*

Exercice 5 :

On donne un K-ev E et $n \in \mathbb{N}^*$; K est supposé de caractéristique 0. Pour $u \in E$, si f est une application de E dans K, on note $T_u(f)$ l'application $E \to K$, $x \mapsto f(x+u)$ et $\Delta_u(f)$ l'application $x \mapsto f(x+u)-f(x)$ ($\Delta_u(f) = T_u(f)-f$).

a) Soit $s \in S_n(E)$. On note $\tilde{s}$ l'application $E \to K$, $x \mapsto s(\overbrace{x, x, \ldots, x}^{n\text{fois}})$. Si $(u_1, \ldots, u_n) \in E^n$, montrer que l'application $(\Delta_{u_1} \circ \Delta_{u_2} \circ \ldots \circ \Delta_{u_n})\,\tilde{s} : E \to K$ est *constante*, sa valeur étant $n!\, s(u_1, u_2, \ldots, u_n)$.

b) En déduire la *formule de restitution :* si $s \in S_n(E)$, pour $(u_1, \ldots, u_n) \in E^n$,

$$s(u_1, \ldots, u_n) = \frac{1}{n!}[(\Delta_{u_1} \circ \Delta_{u_2} \circ \ldots \circ \Delta_{u_n})\,\tilde{s}](0) =$$

$$= \frac{1}{n!} \sum_{k=0}^{n} (-1)^{n-k} \sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} \tilde{s}(u_{i_1} + u_{i_2} + \ldots + s_{u_{i_k}}) .$$

En déduire que $s \mapsto \tilde{s}$ est *injective*.

c) On suppose maintenant E de dimension finie $N \geqslant 1$. Montrer que si $s \in S_n(E)$, $\tilde{s}$ est *polynomiale homogène* de degré n sur E. On note $\mathcal{H}_n(E)$ le K-ev des fonctions polynomiales homogènes de degré n sur E. Si $P \in \mathcal{H}_n(E)$, montrer que l'application : $\widehat{P} : E^n \to K$, $(u_1, \ldots, u_n) \mapsto$

$$\frac{1}{n!} \sum_{k=0}^{n} (-1)^{n-k} \sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} P(u_{i_1} + \ldots + u_{i_k}) ,$$

est dans $S_n(E)$. En déduire que $s \mapsto \tilde{s}$ est un *isomorphisme* de K-ev $S_n(E)$ sur $\mathcal{H}_n(E)$, et en particulier, que

$\left\| \binom{N+n-1}{N-1} \right.$.

N.B. Si $P \in \mathscr{H}_n(E)$, $\widehat{P}$ s'appelle la *polarisée* de P. ■

Le lecteur pourra consulter la fin du §IX.3 pour trouver une définition des fonctions polynomiales sur un K-ev.

a) Montrons le résultat par récurrence sur $n \in \mathbb{N}^*$. La proposition est vraie pour $n = 1$, en effet, pour tout $s \in S_1(E) = E^*$, pour tout $u_1 \in E$, et pour tout $x \in E$,

$$[(\Delta_{u_1})\,\tilde{s}](x) = s(x+u_1) - s(x) = s(u_1)\ .$$

Soit $n > 1$; supposons que la proposition soit vérifiée pour tout $k \in \mathbb{N}^*$, $k < n$. Soit $s \in S_n(E)$, $x \in E$ et $(u_1, \ldots, u_n) \in E^n$; comme l'application $(x_1, \ldots, x_n) \mapsto s(x_1, \ldots, x_n)$ est n-linéaire et symétrique, on peut développer l'expression $s(x+u_n, \ldots, x+u_n)$ comme on développerait un produit $(x+u_n)^n$, mutatis mutandis. On obtient une formule analogue à celle du binôme de Newton :

$$s(x+u_n, \ldots, x+u_n) =$$

$$= s(u_n, \ldots, u_n) + \sum_{k=1}^{n-1} \binom{n}{k} s(\overbrace{x, \ldots, x}^{k \text{ fois}}, \overbrace{u_n, \ldots, u_n}^{n-k \text{ fois}}) + s(x, \ldots, x)\ .$$

Le vecteur u_n étant fixé, posons pour $k \in [\![1, n-1]\!]$, $\varphi_k : E^k \to K$,

$$(x_1, \ldots, x_k) \mapsto s(x_1, \ldots, x_k, \overbrace{u_n, \ldots, u_n}^{n-k \text{ fois}})\ ;$$

il est clair que φ_k est k-linéaire symétrique. On note aussi φ_0 la constante $s(u_n, \ldots, u_n)$. On obtient donc l'égalité :

$$[(\Delta_{u_n})\,\tilde{s}](x) = \varphi_0 + \sum_{k=1}^{n-1} \binom{n}{k} \tilde{\varphi}_k(x)\ .$$

Si $k < n-1$, $(\Delta_{u_1} \circ \Delta_{u_2} \circ \ldots \circ \Delta_{u_{n-1}})\,\tilde{\varphi}_k = 0$, car en appliquant à $\tilde{\varphi}_k$ successivement k opérateurs de différence, on obtient d'après l'hypothèse de récurrence une fonction constante, et on obtient donc 0 si on lui applique un nombre $> k$ d'opérateurs de différence. Ce résultat est aussi vrai pour $k = 0$, puisque $n > 1$. On obtient donc :

$$[(\Delta_{u_1} \circ \Delta_{u_2} \circ \ldots \circ \Delta_{u_n})\,\tilde{s}](x) = \binom{n}{n-1} [(\Delta_{u_1} \circ \Delta_{u_2} \circ \ldots \circ \Delta_{u_{n-}}$$

soit, en utilisant l'hypothèse de récurrence :

$$[(\Delta_{u_1} \circ \Delta_{u_2} \circ \ldots \circ \Delta_{u_n})\,\tilde{s}](x) = \\ = n\,(n-1)!\,\varphi_{n-1}(u_1, \ldots, u_{n-1}) = n!\; s(u_1, \ldots, u_{n-1}, u_n)\ ,$$

ce qu'il fallait démontrer. La proposition est donc vraie pour tout n.

b) Les opérateurs T_u, où $u \in E$, commutant tous entre eux, on obtient pour tout $(u_1, \ldots, u_n) \in E^n$ l'égalité :

$$\Delta_{u_1} \circ \Delta_{u_2} \circ \ldots \circ \Delta_{u_n} = \\ = (T_{u_1} - \mathrm{Id}_E) \circ \ldots \circ (T_{u_n} - \mathrm{Id}_E) = \sum_{I \subset [\![1,n]\!]} \prod_{i \in I} T_{u_i} \circ \prod_{i \notin I} (-\mathrm{Id}_E)\ .$$

Le symbole $\prod$ se rapporte à la composition des endomorphismes. Pour $k \in [\![1, n]\!]$, nous noterons $\mathcal{P}_k$ l'ensemble des parties de $[\![1, n]\!]$ de cardinal k. En faisant dans la somme ci-dessus un partage suivant le cardinal de I, nous obtenons :

$$\Delta_{u_1} \circ \Delta_{u_2} \circ \ldots \circ \Delta_{u_n} = \sum_{k=0}^{n} \sum_{I \in \mathcal{P}_k} (-1)^{n-k} \prod_{i \in I} T_{u_i} = \sum_{k=0}^{n} \sum_{I \in \mathcal{P}_k} (-1)^{n-k} T_{S_I}\ ,$$

où pour $I \subset [\![1, n]\!]$, $S_I = \sum_{i \in I} u_i$. On vérifie que pour $I = \emptyset$,

$$\prod_{i \in I} T_{u_i} = \mathrm{Id}_E = T_0 \quad \text{et} \quad \sum_{i \in I} u_i = 0\ .$$

Nous en déduisons l'égalité :

$$[(\Delta_{u_1} \circ \Delta_{u_2} \circ \ldots \circ \Delta_{u_n})\tilde{s}](0) = \\ = \sum_{k=0}^{n} \sum_{I \in \mathcal{P}_k} (-1)^{n-k} [T_{S_I}(\tilde{s})]\ (0) = \sum_{k=0}^{n} \sum_{I \in \mathcal{P}_k} (-1)^{n-k} \tilde{s}(S_I)\ ,$$

d'où, d'après le *a*), l'égalité :

$$n!\, s(u_1, \ldots, u_n) = \sum_{k=0}^{n} \sum_{I \in \mathcal{P}_k} (-1)^{n-k} \tilde{s}(S_I)\ .$$

C'est, aux notations près, l'égalité à démontrer. Comme le corps K est de caractéristique 0, on voit que $\tilde{s} = 0$ implique $s = 0$. L'application $s \mapsto \tilde{s}$ est donc injective.

c) Soit $(e_1, \ldots, e_N)$ une base de E et $\varphi_1, \ldots, \varphi_N$, les formes linéaires coordonnées dans cette base. Pour tout $x \in E$, on peut écrire :

$$\tilde{s}(x) = s\left(\sum_{i_1=1}^{N} \varphi_{i_1}(x)\, e_{i_1}, \ldots, \sum_{i_n=1}^{N} \varphi_{i_n}(x)\, e_{i_n}\right) =$$
$$= \sum_{(i_1,\ldots,i_n)\in[\![1,N]\!]^n} s(e_{i_1}, \ldots, e_{i_n})\ \varphi_{i_1}(x) \ldots \varphi_{i_n}(x)\ .$$

On voit donc que $\tilde{s}$ est une fonction polynomiale homogène de degré n sur E.

En remontant les calculs faits dans le *b*), on voit que :

$$\widehat{P} = \frac{1}{n!}[(\Delta_{u_1} \circ \Delta_{u_2} \circ \ldots \circ \Delta_{u_n})\, P](0)\ .$$

On remarque que si Q est une fonction polynomiale de degré k sur E, pour tout $u \in E$, $\Delta_u(Q)$ est une fonction polynomiale sur E de degré $< k$ (ou nulle). Il suffit (par linéarité) de le prouver pour tout monôme de degré k, de la forme $\varphi_{i_1}(x) \ldots \varphi_{i_k}(x)$, où $(i_1, \ldots, i_k) \in [\![1, N]\!]^k$. On a pour tout $x \in E$ l'égalité :

$$\varphi_{i_1}(x+u) \ldots \varphi_{i_k}(x+u) = \sum_{I \subset [\![1,k]\!]} \prod_{j\in I} \varphi_{i_j}(x) \prod_{j\notin I} \varphi_{i_j}(u)\ .$$

En retranchant de cette somme le terme $\varphi_{i_1}(x) \ldots \varphi_{i_k}(x)$ qui correspond à la partie $I = [\![1, k]\!]$, il ne reste que des monômes de degré $\leqslant k-1$.
On voit donc que pour tout $(u_2, \ldots, u_n) \in E^{n-1}$, $(\Delta_{u_2} \circ \ldots \circ \Delta_{u_n})\, P$ est une fonction polynomiale sur E de degré $\leqslant 1$ (mais pas nécessairement homogène) donc de la forme :

$$(\Delta_{u_2} \circ \ldots \circ \Delta_{u_n})\, P = \alpha + \sum_{i=1}^{N} \lambda_i\, \varphi_i\ ,$$

où $\alpha \in K$ et $(\lambda_1, \ldots, \lambda_N) \in K^N$. On obtient donc pour tout $x \in E$ l'égalité :

$$[(\Delta_{u_1} \circ \Delta_{u_2} \circ \ldots \circ \Delta_{u_n})\, P](x) =$$
$$= \alpha + \sum_{i=1}^{N} \lambda_i\, \varphi_i(x+u_1) - \alpha - \sum_{i=1}^{N} \lambda_i\, \varphi_i(x) = \sum_{i=1}^{N} \lambda_i\, \varphi_i(u_1)\ .$$

Il est alors clair que, $u_2, \ldots, u_n$ étant fixés dans E, l'application :

$$u_1 \mapsto \frac{1}{n!}\,[(\Delta_{u_1} \circ \Delta_{u_2} \circ \ldots \circ \Delta_{u_n})\, P](0) = \widehat{P}(u_1, \ldots, u$$

est une forme linéaire sur E. Comme les opérateurs Δ_u, où $u \in E$, commutent entre eux, on voit que $\widehat{P}$ est linéaire par rapport à chaque variable, les autres étant fixées, c'est-à-dire est n-linéaire. Le même argument prouve que $\widehat{P}$ est symétrique. On a donc bien démontré $\widehat{P} \in S_n(E)$.

D'après le début de cette question c), on peut considérer que l'application $s \mapsto \tilde{s}$, est une application (linéaire injective d'après a)) $\Phi : S_n(E) \to \mathscr{H}_n(E)$. Notons Ψ l'application $P \mapsto \widehat{P}$. On vient de démontrer que Ψ est une application (linéaire) $\mathscr{H}_n(E) \to S_n(E)$. La formule de restitution s'écrit alors $\Psi \circ \Phi = \mathrm{Id}_{S_n(E)}$. Vérifions l'égalité $\Phi \circ \Psi = \mathrm{Id}_{\mathscr{H}_n(E)}$.
Soit $P \in \mathscr{H}_n(E)$, $\Phi(\Psi(P))$ est la fonction polynomiale sur E, homogène de degré n,

$$x \mapsto \widehat{P}(\overbrace{x, \ldots, x}^{n \text{ fois}}) .$$

Par définition on a l'égalité :

$$\widehat{P}(\overbrace{x, \ldots, x}^{n \text{ fois}}) = \frac{1}{n!} \sum_{k=0}^{n} (-1)^{n-k} \sum_{I \in \mathscr{P}_k} P(S_I) ,$$

où pour tout $I \subset [\![1, n]\!]$, $S_I = \sum_{i \in I} x = \mathrm{card}\,(I)\, x$, soit $S_I = k\, x$ si $I \in \mathscr{P}_k$.
Comme P est homogène de degré n, on obtient finalement, pour tout $x \in E$:

$$\widehat{P}(\overbrace{x, \ldots, x}^{n \text{ fois}}) = \frac{1}{n!} \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k^n P(x) .$$

Nous avons démontré dans l'exercice 13 du §VII.4 c), l'égalité :

$$\sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k^n = n! .$$

On a donc bien $\Phi \circ \Psi = \mathrm{Id}_{\mathscr{H}_n(E)}$. Les applications linéaires Φ et Ψ sont donc bijectives et réciproques l'une de l'autre, ce que nous voulions démontrer. On a donc :

$$\dim S_n(E) = \dim \mathscr{H}_n(E) = \binom{N + n - 1}{N - 1} .$$

Exercice 6 (suite de l'exercice 5) **:**

> E est supposé de dimension finie $N \geqslant 1$ et on le munit d'une base $\mathscr{B} = (e_1, \ldots, e_N)$ et l'on note $(x_1, \ldots, x_N)$ sa base duale. On notera $\mathscr{S}_n$ l'ensemble des N-uplets d'entiers, $(\alpha_1, \ldots, \alpha_N)$ tels que $\|\alpha\| = \alpha_1 + \ldots + \alpha_N = n$.

a) Soit $P = \sum_{\alpha \in \mathcal{S}_n} c_\alpha x_1^{\alpha_1} \dots x_N^{\alpha_N} \in \mathcal{H}_n(E)$. Montrer que la polarisée $\widehat{P}$ de P peut s'exprimer de la manière suivante : pour chaque $\alpha = (\alpha_1, \dots, \alpha_N) \in \mathcal{S}_n$, soit $\mathcal{C}_\alpha$ l'ensemble des applications $\varphi : [\![1, n]\!] \to [\![1, N]\!]$ telles que $\operatorname{card}(\varphi^{-1}(i)) = \alpha_i$ pour tout i. Alors, si $(u_1, \dots, u_n) \in E^n$, $u_i = \sum_{j=1}^{N} u_{j,i} e_j$, on a :

$$\widehat{P}(u_1, \dots, u_n) = \frac{1}{n!} \sum_{\alpha \in \mathcal{S}_n} \alpha_1 ! \dots \alpha_N ! c_\alpha \left(\sum_{\varphi \in \mathcal{C}_\alpha} u_{\varphi(1),1} \dots u_{\varphi(n),n} \right).$$

Expliciter cette formule pour $n = 2$ et $n = 3$.

b) On donne $p \in [\![1, n-1]\!]$ et on pose $q = n - p$. Soit $x = \sum_{i=1}^{N} x_i e_i$ et $y = \sum_{i=1}^{N} y_i e_i$ éléments de E. Démontrer : si $u_i = x$ pour $1 \leqslant i \leqslant q$ et $u_i = y$ pour $q+1 \leqslant i \leqslant n$, alors

$$\frac{n!}{(n-p)!} \widehat{P}(u_1, \dots, u_n) = \sum_{\alpha \in \mathcal{S}_p} \frac{p!}{\alpha_1 ! \dots \alpha_N !} \frac{\partial^p P(x)}{\partial x_1^{\alpha_1} \dots \partial x_N^{\alpha_N}} y_1^{\alpha_1} \dots y_N^{\alpha_N} . \blacksquare$$

a) Pour démontrer cette égalité il suffit de la vérifier pour les monômes de degré n. Soit $\alpha \in \mathcal{S}_n$. Montrons que $\widehat{\mathcal{M}}_\alpha$ coïncide avec l'application $S_\alpha : E^n \to K$, définie pour tout $(u_1, \dots, u_n) \in E^n$ par :

$$S_\alpha(u_1, \dots, u_n) = \frac{\alpha_1 ! \dots \alpha_N !}{n!} \sum_{\varphi \in \mathcal{C}_\alpha} u_{\varphi(1),1} \dots u_{\varphi(n),n} .$$

Il est clair que l'application S_α est n-linéaire (par exemple le vecteur u_1 n'apparaît que dans le premier facteur de chaque produit $u_{\varphi(1),1} \dots u_{\varphi(n),n}$). Montrons qu'elle est symétrique. Soit $\sigma \in \mathfrak{S}_n$, si $\varphi \in \mathcal{C}_\alpha$, alors $\varphi \circ \sigma \in \mathcal{C}_\alpha$, et l'application $\varphi \mapsto \varphi \circ \sigma$, est une bijection de l'ensemble $\mathcal{C}_\alpha$ sur lui-même. Par définition, pour tout $(u_1, \dots, u_n) \in E^n$:

$$S_\alpha(u_{\sigma(1)}, \dots, u_{\sigma(n)}) = \frac{\alpha_1 ! \dots \alpha_N !}{n!} \sum_{\varphi \in \mathcal{C}_\alpha} u_{\varphi(1),\sigma(1)} \dots u_{\varphi(n),\sigma(n)} .$$

En permutant dans chaque terme de la somme les facteurs du produit on obtient :

$$S_\alpha(u_{\sigma(1)}, \dots, u_{\sigma(n)}) = \frac{\alpha_1 ! \dots \alpha_N !}{n!} \sum_{\varphi \in \mathcal{C}_\alpha} u_{\varphi(\sigma^{-1}(1)),1} \dots u_{\varphi(\sigma^{-1}(n)),n} .$$

donc :

$$S_\alpha(u_{\sigma(1)}, \dots, u_{\sigma(n)}) = S_\alpha(u_1, \dots, u_n) \ .$$

L'application S_α est bien n-linéaire symétrique. Pour démontrer que S_α est la polarisée du monôme $\mathcal{M}_\alpha$, il suffit maintenant de vérifier $\tilde{S}_\alpha = \mathcal{M}_\alpha$ (cf. exercice 5 *c*)).
Pour tout $x \in E$ on a :

$$\tilde{S}_\alpha(x) = S_\alpha(x, \dots, x) = \frac{\alpha_1 ! \dots \alpha_N !}{n!} \sum_{\varphi \in \mathscr{C}_\alpha} x_{\varphi(1)} \dots x_{\varphi(n)} \ .$$

Si $\varphi \in \mathscr{C}_\alpha$, φ prend α_1 fois la valeur 1, α_2 fois la valeur 2, etc., α_N fois la valeur N ; donc $x_{\varphi(1)} \dots x_{\varphi(n)} = x_1^{\alpha_1} \dots x_N^{\alpha_N}$. On en déduit :

$$\tilde{S}_\alpha(x) = \frac{\alpha_1 ! \dots \alpha_N !}{n!} \operatorname{card}(\mathscr{C}_\alpha)\, x_1^{\alpha_1} \dots x_N^{\alpha_N} = x_1^{\alpha_1} \dots x_N^{\alpha_N} \ ,$$

ce qu'il fallait démontrer.

Les monômes de degré 2 sont les monômes x_i^2, où $i \in [\![1, N]\!]$, et les monômes $x_i\, x_j$, où $(i, j) \in [\![1, N]\!]^2$, $(i \neq j)$.
La polarisée du monôme x_i^2 est la forme bilinéaire symétrique :

$$(u_1, u_2) \mapsto u_{i,1}\, u_{i,2} \ .$$

La polarisée du monôme $x_i\, x_j$ est la forme bilinéaire symétrique :

$$(u_1, u_2) \mapsto \frac{1}{2}(u_{i,1}\, u_{j,2} + u_{j,1}\, u_{i,2}) \ .$$

On retrouve l'identité de polarisation d'une forme quadratique.

Les monômes de degré 3 sont les monômes x_i^3, où $i \in [\![1, N]\!]^3$, $x_i^2\, x_j$, où $(i, j) \in [\![1, N]\!]^2$, $(i \neq j)$, et $x_i\, x_j\, x_k$, où (i, j, k) est un triplet d'éléments de $[\![1, N]\!]$ distincts.
La polarisée du monôme x_i^3 est la forme 3-linéaire symétrique :

$$(u_1, u_2, u_3) \mapsto u_{i,1}\, u_{i,2}\, u_{i,3} \ .$$

La polarisée du monôme $x_i^2\, x_j$ est la forme 3-linéaire symétrique :

$$(u_1, u_2, u_3) \mapsto \frac{2}{6}(u_{j,1}\, u_{i,2}\, u_{i,3} + u_{i,1}\, u_{j,2}\, u_{i,3} + u_{i,1}\, u_{i,2}\, u_{j,3}) \ .$$

En effet, $\mathscr{C}_\alpha$ est ici constitué des applications $[\![1, 3]\!] \to [\![1, N]\!]$ qui prennent 2 fois la valeur i, et 1 fois la valeur j.
La polarisée du monôme $x_i\, x_j\, x_k$ est la forme 3-linéaire symétrique :

$$(u_1, u_2, u_3) \mapsto \frac{1}{3!}(u_{i,1}\, u_{j,2}\, u_{k,3} + u_{j,1}\, u_{k,2}\, u_{i,3} + u_{k,1}\, u_{i,2}\, u_{j,3} +$$
$$+ u_{i,1}\, u_{k,2}\, u_{j,3} + u_{k,1}\, u_{j,2}\, u_{i,3} + u_{j,1}$$

En effet, $\mathscr{E}_\alpha$ est ici constitué des applications $[\![1,3]\!] \to [\![1,N]\!]$ qui prennent exactement une fois chaque valeur i, j et k sur $[\![1,3]\!]$.

b) Par linéarité, il suffit de démontrer l'égalité de l'énoncé pour tous les monômes $\mathcal{M}_\beta$, où $\beta \in \mathcal{S}_n$. D'après le *a*), on a pour tout $(u_1, \ldots, u_n) \in E^n$ l'égalité :

$$\widehat{\mathcal{M}}_\beta(u_1, \ldots, u_n) = \frac{\beta_1 ! \ldots \beta_N !}{n !} \sum_{\varphi \in \mathscr{E}_\beta} u_{\varphi(1),1} \ldots u_{\varphi(n),n} .$$

L'ensemble $\mathscr{E}_\beta$ est l'ensemble des applications $[\![1,n]\!] \to [\![1,N]\!]$ qui prennent β_1 fois la valeur 1, etc., β_N fois la valeur N. Soit $\mathcal{S}'_p$ l'ensemble des éléments α de $\mathcal{S}_p$ tels que $(\forall i \in [\![1,N]\!])\ \alpha_i \leqslant \beta_i$, et pour tout $\alpha \in \mathcal{S}'_p$, soit $\mathscr{F}_\alpha$ l'ensemble des applications $\varphi : [\![1,n]\!] \to [\![1,N]\!]$ qui prennent pour tout $i \in [\![1,N]\!]$, β_i fois la valeur i dont α_i fois sur $[\![q+1,n]\!]$. On voit que la famille $(\mathscr{F}_\alpha)$, pour α variant dans $\mathcal{S}'_p$, est un partage de $\mathscr{E}_\beta$. On a donc, pour tout $(u_1, \ldots, u_n) \in E^n$, l'égalité :

$$\widehat{\mathcal{M}}_\beta(u_1, \ldots, u_n) = \frac{\beta_1 ! \ldots \beta_N !}{n !} \sum_{\alpha \in \mathcal{S}'_p} \sum_{\varphi \in \mathscr{F}_\alpha} u_{\varphi(1),1} \ldots u_{\varphi(n),n} .$$

Dans le cas particulier où :

$$(u_1, \ldots, u_n) = (\overbrace{x, \ldots, x}^{q \text{ fois}}, \overbrace{y, \ldots, y}^{p \text{ fois}}) ,$$

pour tout $\alpha \in \mathcal{S}'_p$ et tout $\varphi \in \mathscr{F}_\alpha$, on a l'égalité :

$$u_{\varphi(1),1} \ldots u_{\varphi(n),n} = x_1^{\beta_1 - \alpha_1} \ldots x_N^{\beta_N - \alpha_N} y_1^{\alpha_1} \ldots y_N^{\alpha_N} .$$

On voit assez facilement que le cardinal de l'ensemble $\mathscr{F}_\alpha$ est :

$$\frac{p !}{\alpha_1 ! \ldots \alpha_N !} \frac{q !}{(\beta_1 - \alpha_1) ! \ldots (\beta_N - \alpha_N) !} ,$$

puisque les éléments de $\mathscr{F}_\alpha$ sont les applications $[\![1,n]\!] \to [\![1,N]\!]$ qui prennent,
- sur $[\![1,q]\!]$, $\beta_i - \alpha_i$ fois la valeur i, pour tout $i \in [\![1,N]\!]$,
- sur $[\![q+1,n]\!]$ (de cardinal p), α_i fois la valeur i, pour tout $i \in [\![1,N]\!]$.

Nous en déduisons finalement l'égalité :

$$\frac{n !}{\beta_1 ! \ldots \beta_N !} \widehat{\mathcal{M}}_\beta(\overbrace{x, \ldots, x}^{q \text{ fois}}, \overbrace{y, \ldots, y}^{p \text{ fois}}) =$$

$$= \sum_{\alpha \in \mathcal{S}'_p} \frac{p !}{\alpha_1 ! \ldots \alpha_N !} \frac{q !}{(\beta_1 - \alpha_1) ! \ldots (\beta_N - \alpha_N) !} x_1^{\beta_1 - \alpha_1} \ldots x_N^{\beta_N - \alpha_N} y_1^{\alpha_1} \ldots y_N^{\alpha_N} .$$

D'autre part, pour tout $\alpha \in \mathcal{S}_p$, si $\exists i \in [\![1, N]\!] \mid \alpha_i > \beta_i$ on a :

$$\frac{\partial^p (x_1^{\beta_1} \dots x_N^{\beta_N})}{\partial x_1^{\alpha_1} \dots \partial x_N^{\alpha_N}} = 0 \ ,$$

et si $\alpha \in \mathcal{S}'_p$:

$$\frac{\partial^p (x_1^{\beta_1} \dots x_N^{\beta_N})}{\partial x_1^{\alpha_1} \dots \partial x_N^{\alpha_N}} = \frac{\beta_1 ! \dots \beta_N !}{(\beta_1 - \alpha_1) ! \dots (\beta_N - \alpha_N) !} x_1^{\beta_1 - \alpha_1} \dots x_N^{\beta_N - \alpha_N} \ .$$

On voit donc que :

$$\sum_{\alpha \in \mathcal{S}_p} \frac{p!}{\alpha_1 ! \dots \alpha_N !} \frac{\partial^p (x_1^{\beta_1} \dots x_N^{\beta_N})}{\partial x_1^{\alpha_1} \dots \partial x_N^{\alpha_N}} y_1^{\alpha_1} \dots y_N^{\alpha_N} =$$

$$= \sum_{\alpha \in \mathcal{S}'_p} \frac{p!}{\alpha_1 ! \dots \alpha_N !} \frac{\beta_1 ! \dots \beta_N !}{(\beta_1 - \alpha_1) ! \dots (\beta_N - \alpha_N) !} x_1^{\beta_1 - \alpha_1} \dots x_N^{\beta_N - \alpha_N} y_1^{\alpha_1} \dots y_N^{\alpha_N} \ .$$

Nous en déduisons enfin l'égalité :

$$\frac{n!}{q!} \widehat{\mathcal{M}}_\beta (\overbrace{x, \dots, x}^{q \text{ fois}}, \overbrace{y, \dots, y}^{p \text{ fois}}) =$$

$$= \sum_{\alpha \in \mathcal{S}_p} \frac{p!}{\alpha_1 ! \dots \alpha_N !} \frac{\partial^p (x_1^{\beta_1} \dots x_N^{\beta_N})}{\partial x_1^{\alpha_1} \dots \partial x_N^{\alpha_N}} y_1^{\alpha_1} \dots y_N^{\alpha_N} \ ,$$

ce qu'il fallait démontrer.

§ XIII.2 *FORMES n-LINÉAIRES ALTERNÉES SUR E DE DIMENSION n*

Exercice 1 :

> Soit E un K-ev et deux sous-K-ev F et G de E supplémentaires : $E = F \oplus G$. On note φ le projecteur associé à (F, G) d'image F. Si $f \in \Lambda_k^*(F)$, vérifier que l'application $E^k \to K$, $(x_1, \dots, x_k) \mapsto f(\varphi(x_1), \dots, \varphi(x_k))$ appartient à $\Lambda_k^*(E)$. Lorsque E est de dimension finie, en déduire que, pour tout $k \in [\![1, \dim(E)]\!]$, l'espace $\Lambda_k^*(E)$ est non nul. ■

Notons $g : E^k \to K$, l'application $(x_1, \dots, x_k) \mapsto f(\varphi(x_1), \dots, \varphi(x_k))$. Pour tout $i \in [\![1, k]\!]$, les vecteurs x_j pour $j \neq i$ étant fixés,

$x_i \mapsto f(\varphi(x_1), \ldots, \varphi(x_i), \ldots, \varphi(x_k))$, de E dans K, est linéaire car composée de deux applications linéaires. L'application g est donc une forme k-linéaire.
Pour tout $(i,j) \in [\![1,k]\!]^2$, $i \neq j$, et pour tout k-uplet $(x_1, \ldots, x_k)$, si $x_i = x_j$, alors $\varphi(x_i) = \varphi(x_j)$, donc $f(\varphi(x_1), \ldots, \varphi(x_k)) = 0$. L'application g est donc une forme k-linéaire alternée sur E.

On pose $n = \dim(E)$. Soit $k \in [\![1,n]\!]$. On peut trouver un sous-K-ev F de E tel que $\dim(F) = k$, et un sous-K-ev G de E tel que $E = F \oplus G$. Nous noterons comme ci-dessus φ le projecteur sur F dans la somme directe $E = F \oplus G$. Soit enfin une base $\mathcal{B} = (e_1, \ldots, e_k)$ de F. L'application :

$$(x_1, \ldots, x_k) \mapsto \det_{\mathcal{B}}(\varphi(x_1), \ldots, \varphi(x_k)) ,$$

est, d'après le début de cet exercice, une forme k-linéaire alternée sur E. Elle n'est pas nulle car l'image de $(e_1, \ldots, e_k)$ par cette application est 1. L'espace $\Lambda_k^*(E)$ n'est donc pas nul.

§ XIII.3 *DÉTERMINANT DE n VECTEURS DANS UNE BASE; DÉTERMINANT D'UN ENDOMORPHISME*

Exercice 1 :

Le corps K est supposé de caractéristique nulle. Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base d'un K-ev E ($n \geqslant 1$). Pour $i \in [\![1,n]\!]$ on pose $\varepsilon_i = e_i - \sum_{j \neq i} e_j$. Démontrer que

$$\det_{\mathcal{B}}(\varepsilon_1, \ldots, \varepsilon_n) = -2^{n-1}(n-2) . \blacksquare$$

Soit $s = \sum_{i=1}^{n} e_i$; on a pour tout $i \in [\![1,n]\!]$, $\varepsilon_i = 2e_i - s$. Le déterminant cherché est donc ;

$$D_n = \det_{\mathcal{B}}(2e_1 - s, \ldots, 2e_n - s) .$$

En développant ce déterminant par n-linéarité, on obtient une somme de 2^n termes, mais les termes où apparaît au moins 2 fois s sont nuls. Il reste donc :

$$D_n = \det_{\mathcal{B}}(2e_1, \ldots, 2e_n) + \sum_{i=1}^{n} \det_{\mathcal{B}}(2e_1, \ldots, 2e_{i-1}, -s, 2e_{i+1} \ldots, 2e_n) =$$

$$= 2^n - 2^{n-1} \sum_{i=1}^{n} \det_{\mathcal{B}}(e_1, \ldots, e_{i-1}, \sum_{j=1}^{n} e_j, e_{i+1} \ldots, e_n) = 2^n - 2^{n-1} n .$$

On obtient finalement $D_n = -2^{n-1}(n-2)$.

On peut remarquer que D_n est le déterminant de la matrice M telle que pour tout $(i,j) \in [\![1,n]\!]^2$, $M_{i,j} = 1$ si $i = j$ et $M_{i,j} = -1$ si $i \neq j$. On a par définition l'égalité :

$$D_n = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) M_{\sigma(1),1} \dots M_{\sigma(n),n} .$$

Pour $\sigma \in \mathfrak{S}_n$ notons $k(\sigma)$ le nombre de points fixes de σ. On voit facilement que $M_{\sigma(1),1} \dots M_{\sigma(n),n} = (-1)^{n-k(\sigma)}$. On obtient finalement :

$$D_n = (-1)^n \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma)(-1)^{k(\sigma)} .$$

Notons, comme dans l'exercice 10 du chapitre §VIII.5, S_n le nombre des permutations paires dont le nombre de points fixes est pair, et T_n le nombre de permutations impaires dont le nombre de points fixes est impair. Notons aussi S'_n le nombre de permutations paires dont le nombre de points fixes est impair, et T'_n le nombre de permutations impaires dont le nombre de points fixes est pair. On voit que pour tout $n \geqslant 1$:

$$D_n = (-1)^n (S_n + T_n - S'_n - T'_n) = (-1)^n (2\,S_n + 2\,T_n - n!) .$$

On doit donc avoir l'égalité :

$$2\,(S_n + T_n) - n! = (-1)^{n-1}\, 2^{n-1}\, (n-2) ,$$

ce qu'on observe en effet (cf. exercice 10, §VIII.5).

Rappelons que pour tout $n \geqslant 2$ ($S_0 = 1, S_1 = 0$) :

$$S_n = \frac{1}{4}\left(n! + (-1)^{n-1} 2^{n-1}(n-2) + n! \sum_{q=0}^{n} (-1)^q \frac{2^q}{q!} \right) ,$$

et que pour tout $n \geqslant 2$ ($T_0 = T_1 = 0$) :

$$T_n = \frac{1}{4}\left(n! + (-1)^{n-1} 2^{n-1}(n-2) - n! \sum_{q=0}^{n} (-1)^q \frac{2^q}{q!} \right) .$$

Exercice 3 :

Le corps commutatif K est supposé fini, de cardinal q. Soit E un K-ev de dimension $n \in \mathbb{N}^*$, calculer card (SL_K

L'application det : $(\mathrm{GL}_K(E), \circ) \to (K \setminus \{0\}, \times)$ est un homomorphisme de groupes dont le noyau est $\mathrm{SL}_K(E)$. Cet homomorphisme de groupes est bien surjectif : $\det(\mathrm{Diag}(\lambda, 1, \ldots, 1)) = \lambda$, pour tout $\lambda \in K \setminus \{0\}$. Nous en déduisons :

$$\mathrm{card}(\mathrm{SL}_K(E)) = \frac{\mathrm{card}(\mathrm{GL}_K(E))}{q-1} .$$

Nous avons vu dans l'exercice 3 du §IX.3 que le nombre d'automorphismes de E est :

$$\mathrm{card}(\mathrm{GL}_K(E)) = (q^n - 1)(q^n - q)\ldots(q^n - q^{n-1}) .$$

On obtient donc l'égalité :

$$\mathrm{card}(\mathrm{SL}_K(E)) = \frac{(q^n - 1)(q^n - q)\ldots(q^n - q^{n-1})}{q-1} .$$

§ XIII.4 *DÉTERMINANT D'UNE MATRICE CARRÉE*

Exercice 1 :

Soit $D = |a_{i,j}|_{(i,j)\in[\![1,n]\!]^2}$, n entier $\geqslant 1$ et $x \in K$. On considère la matrice M de terme général $a_{i,j} + x$.

a) Calculer $\det(M)$.

b) On suppose en particulier que $a_{i,i} \neq 0$ pour tout $i \in [\![1,n]\!]$, $x \neq 0$ et $a_{i,j} = 0$ pour $i \neq j$. Montrer que :

$$\begin{vmatrix} a_{1,1}+x & x & \ldots & x \\ x & a_{2,2}+x & \ldots & x \\ \vdots & \vdots & \vdots & \vdots \\ x & x & \ldots & a_{n,n}+x \end{vmatrix} =$$

$$= a_{1,1}\, a_{2,2} \ldots a_{n,n}\, x \left(\frac{1}{x} + \frac{1}{a_{1,1}} + \ldots + \frac{1}{a_{n,n}} \right) . \blacksquare$$

a) En retranchant la dernière colonne des précédentes, et en développant le déterminant par rapport à la dernière colonne, on voit que ce déterminant est une fonction polynomiale du premier degré en x.
Plus précisément, notons V le vecteur colonne dont toutes les coordonnées sont 1 et $C_1, \ldots, C_n$ les colonnes de la matrice $(a_{i,j})_{(i,j)\in[\![1,n]\!]^2}$. La base canonique de $\mathfrak{M}_{n,1}(K)$ sera notée $\mathfrak{B}$. On voit que :

$$\det(M) = \det_{\mathfrak{B}}(C_1 + x\,V, \ldots, C_n + x\,V) .$$

En développant ce déterminant par multilinéarité, on obtient une somme de 2^n déterminants ; comme $\det_{\mathcal{B}}$ est une forme n-linéaire alternée on trouve :

$$\det(M) = \det_{\mathcal{B}}(C_1, \ldots, C_n) + x \sum_{i=1}^{n} \det_{\mathcal{B}}(C_1, \ldots, C_{i-1}, V, C_{i+1}, \ldots, C_n) \ .$$

b) Dans ce cas particulier, en notant $(e_1, \ldots, e_n)$ la base canonique de $\mathfrak{M}_{n,1}(K)$, on a pour tout $i \in [\![1, n]\!]$, $C_i = a_{i,i}\, e_i$. Donc pour tout $i \in [\![1, n]\!]$:

$$\begin{aligned}
&\det_{\mathcal{B}}(C_1, \ldots, C_{i-1}, V, C_{i+1}, \ldots, C_n) = \\
&\quad = \det_{\mathcal{B}}(a_{1,1}\, e_1, \ldots, a_{i-1,i-1}\, e_{i-1}, \sum_{j=1}^{n} e_j, a_{i+1,i+1}\, e_{i+1}, \ldots, a_{n,n}\, e_n) = \\
&\quad = \prod_{j \neq i} a_{j,j} \ .
\end{aligned}$$

On obtient donc :

$$\det(M) = \prod_{j=1}^{n} a_{j,j} + x \sum_{i=1}^{n} \prod_{j \neq i} a_{j,j} \ .$$

En supposant $x \neq 0$, et pour tout $i \in [\![1, n]\!]$ $a_{i,i} \neq 0$, on obtient le résultat proposé :

$$\det(M) = a_{1,1}\, a_{2,2} \ldots a_{n,n}\, x \left(\frac{1}{x} + \frac{1}{a_{1,1}} + \ldots + \frac{1}{a_{n,n}} \right) \ .$$

Exercice 4 :

Le corps de base est $\mathbb{C}$.

a) Calculer

$$D = \det \begin{bmatrix} 0 & c & b & d \\ c & 0 & a & e \\ b & a & 0 & f \\ d & e & f & 0 \end{bmatrix},$$

(par exemple à l'aide de la formule de Laplace).

b) Dans $\mathbb{C}[X, Y, Z]$, factoriser en facteurs de degré 1 le polynôme

$$X^4 + Y^4 + Z^4 - 2(Y^2 Z^2 + Z^2 X^2 + X^2 Y^2) \ .$$

c) En déduire une factorisation en facteurs de degré 2 de :

$$\Delta = \det \begin{bmatrix} 0 & \gamma^2 & \beta^2 & \delta^2 \\ \gamma^2 & 0 & \alpha^2 & \varepsilon^2 \\ \beta^2 & \alpha^2 & 0 & \varphi^2 \\ \delta^2 & \varepsilon^2 & \varphi^2 & 0 \end{bmatrix} . \blacksquare$$

a) Le développement du déterminant d'une matrice $M \in \mathfrak{M}_4(K)$ par la formule de Laplace est explicité dans l'exemple 4 du §XIII.4. L'application de la formule obtenue donne :

$$D = \begin{vmatrix} 0 & c \\ c & 0 \end{vmatrix} \begin{vmatrix} 0 & f \\ f & 0 \end{vmatrix} - \begin{vmatrix} 0 & b \\ c & a \end{vmatrix} \begin{vmatrix} a & f \\ e & 0 \end{vmatrix} + \begin{vmatrix} 0 & d \\ c & e \end{vmatrix} \begin{vmatrix} a & 0 \\ e & f \end{vmatrix} + \\ + \begin{vmatrix} c & b \\ 0 & a \end{vmatrix} \begin{vmatrix} b & f \\ d & 0 \end{vmatrix} - \begin{vmatrix} c & d \\ 0 & e \end{vmatrix} \begin{vmatrix} b & 0 \\ d & f \end{vmatrix} + \begin{vmatrix} b & d \\ a & e \end{vmatrix} \begin{vmatrix} b & a \\ d & e \end{vmatrix} .$$

Soit :

$$D = c^2 f^2 - c b e f - c d a f - c a d f - c e b f + (b e - a d)^2 = \\ = a^2 d^2 + b^2 e^2 + c^2 f^2 - 2 a b d e - 2 a c d f - 2 b c e f .$$

b) Dans le cas où $a = d$, $b = e$ et $c = f$, on obtient :

$$D = a^4 + b^4 + c^4 - 2(a^2 b^2 + a^2 c^2 + b^2 c^2) ,$$

qui est le déterminant de la matrice :

$$M = \begin{bmatrix} 0 & c & b & a \\ c & 0 & a & b \\ b & a & 0 & c \\ a & b & c & 0 \end{bmatrix} .$$

Posons :

$$A = \begin{bmatrix} 0 & c \\ c & 0 \end{bmatrix} \quad \text{et} \quad B = \begin{bmatrix} b & a \\ a & b \end{bmatrix} .$$

En écrivant la matrice M à l'aide des blocs A et B on voit que :

$$\det(M) = \begin{vmatrix} A & B \\ B & A \end{vmatrix} = \begin{vmatrix} A-B & B-A \\ B & A \end{vmatrix} = \begin{vmatrix} A-B & 0 \\ B & B+A \end{vmatrix} = \\ = \det(A-B) \det(A+B) ,$$

ce qui donne la factorisation :

$$a^4 + b^4 + c^4 - 2(a^2 b^2 + a^2 c^2 + b^2 c^2) = \begin{vmatrix} -b & c-a \\ c-a & -b \end{vmatrix} \begin{vmatrix} b & c+a \\ c+a & b \end{vmatrix} = \\ = \big((a-c)^2 - b^2\big)\big((a+c)^2 - b^2\big) = \\ = -(a+b+c)(a+b-c)(a-b+c)(-$$

Cette identité est bien entendu vraie dans tout anneau commutatif, en particulier dans l'anneau $\mathbb{C}[X,Y,Z]$. On a donc la factorisation :

$$X^4+Y^4+Z^4-2(X^2Y^2+X^2Z^2+Y^2Z^2) = \\ =-(X+Y+Z)(X+Y-Z)(X-Y+Z)(-X+Y+Z)\ .$$

c) En appliquant la formule démontrée dans le *a*), on trouve :

$$\Delta=\alpha^4\delta^4+\beta^4\varepsilon^4+\gamma^4\varphi^4-2\alpha^2\beta^2\delta^2\varepsilon^2-2\alpha^2\gamma^2\delta^2\varphi^2-2\beta^2\gamma^2\varepsilon^2\varphi^2\ .$$

On peut poser $a=\alpha\delta$, $b=\beta\varepsilon$ et $c=\gamma\varphi$. On obtient alors :

$$\Delta=a^4+b^4+c^4-2a^2b^2-2a^2c^2-2b^2c^2\ .$$

En utilisant la factorisation démontrée dans le *b*), on obtient :

$$\Delta= \\ -(\alpha\delta+\beta\varepsilon+\gamma\varphi)(\alpha\delta+\beta\varepsilon-\gamma\varphi)(\alpha\delta-\beta\varepsilon+\gamma\varphi)(-\alpha\delta+\beta\varepsilon+\gamma\varphi)\ ,$$

ce qui est une factorisation en produit de facteurs homogènes de degré 2.

§ XIII.5 *EXEMPLES DE DÉTERMINANTS*

Exercice 5 :

‖ Calculer $\det\left[(i+j-1)^2\right]_{(i,j)\in[\![1,n]\!]^2}$. ■

Pour $n=1$, le déterminant vaut 1.
Pour $n=2$, le déterminant vaut :

$$\begin{bmatrix}1&4\\4&9\end{bmatrix}=-7\ .$$

Pour $n\geqslant 3$ nous utiliserons une méthode générale.

Soient K un corps, n polynômes $P_1,\dots,P_n$ dans $K_{n-1}[X]$, et un n-uplet $(a_1,\dots,a_n)$ d'éléments de K. Notons aussi $\mathcal{B}$ la base canonique $(1,X,\dots,X^{n-1})$ de $K_{n-1}[X]$. Montrons que le déterminant de la matrice M telle que pour tout $(i,j)\in[\![1,n]\!]^2$, $M_{i,j}=P_j(a_i)$, est :

$$|P_j(a_i)|=\det_{\mathcal{B}}(P_1,\dots,P_n)\,V_n(a_1,\dots,a_n)\ ,$$

où $V_n(a_1,\ldots,a_n)$ désigne le déterminant de Vandermonde de la suite de scalaires $(a_1,\ldots,a_n)$.

Posons, pour tout $j \in [\![1,n]\!]$, $P_j(X) = \sum_{h=1}^{n} \lambda_{h,j} X^{h-1}$. On a donc pour tout $(i,j) \in [\![1,n]\!]^2$, $P_j(a_i) = \sum_{h=1}^{n} \lambda_{h,j}\, a_i^{h-1} = \sum_{h=1}^{n} a_i^{h-1}\, \lambda_{h,j}$. On reconnaît que la matrice M est le produit de la matrice A telle que pour tout $(i,h) \in [\![1,n]\!]^2$, $A_{i,h} = a_i^{h-1}$, et de la matrice N telle que pour tout $(h,j) \in [\![1,n]\!]^2$, $N_{h,j} = \lambda_{h,j}$. Il est clair que :

$$\det(A) = V_n(a_1,\ldots,a_n) \quad \text{et} \quad \det(N) = \det_{\mathcal{B}}(P_1,\ldots,P_n)\,.$$

On obtient donc l'égalité :

$$|P_j(a_i)| = \det_{\mathcal{B}}(P_1,\ldots,P_n)\, V_n(a_1,\ldots,a_n)\,.$$

Dans le cas particulier de l'exercice, on pose pour tout $i \in [\![1,n]\!]$, $a_i = i-1$, et pour tout $j \in [\![1,n]\!]$ $P_j(X) = (X+j)^2$. Pour $n > 3$ on voit que la famille $(P_1,\ldots,P_n)$ est liée ; le déterminant est donc nul. Pour $n = 3$, on pourrait bien entendu calculer le déterminant directement, on peut aussi résoudre le problème de manière générale.

Soit une famille $(b_1,\ldots,b_n)$ d'éléments de K, et $P \in K_{n-1}[X]$. On pose pour tout $j \in [\![1,n]\!]$ $P_j(X) = P(X+b_j)$. En utilisant la formule de Taylor (on supposera pour la commodité que la caractéristique du corps est 0), on obtient pour tout $j \in [\![1,n]\!]$:

$$P_j(X) = P(b_j+X) = P(b_j) + \frac{P'(b_j)}{1\,!}\,X + \ldots + \frac{P^{(n-1)}(b_j)}{(n-1)\,!}\,X^{n-1}\,.$$

Posons pour tout $i \in [\![1,n]\!]$:

$$Q_i = \frac{P^{(i-1)}}{(i-1)\,!}\,.$$

On voit que :

$$\det_{\mathcal{B}}(P_1,\ldots,P_n) = \det[Q_i(b_j)] = \det_{\mathcal{B}}(Q_1,\ldots,Q_n)\, V_n(b_1,\ldots,b_n)\,.$$

Pour tout $h \in [\![1,n]\!]$, le polynôme Q_h est de degré $\leqslant n-h$; en notant c_h le coefficient du monôme de degré $n-h$ dans Q_h, et a le coefficient de degré $n-1$ dans P, on voit que :

$$c_h = a\,\frac{(n-1)\ldots(n-h+1)}{(h-1)\,!} = a\,\frac{(n-1)\,!}{(n-h)\,!\,(h-1)\,!} = a\cdot\binom{n-1}{}$$

La matrice des polynômes $Q_1, \ldots, Q_n$ dans la base $\mathcal{B}$ est de la forme :

$$\begin{bmatrix} | & | & & c_n \\ | & | & \iddots & 0 \\ | & \iddots & \iddots & \vdots \\ c_1 & 0 & \ldots & 0 \end{bmatrix}$$

La matrice des polynômes $Q_n, \ldots, Q_1$ dans la base $\mathcal{B}$ est donc trigonale supérieure de coefficients diagonaux $(c_n, \ldots, c_1)$. Comme le nombre d'inversions de la permutation $\begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ n & n-1 & \ldots & 2 & 1 \end{pmatrix}$ est $\binom{n}{2}$, on trouve :

$$\det_{\mathcal{B}}(Q_1, \ldots, Q_n) =$$
$$= (-1)^{\frac{n(n-1)}{2}} \det_{\mathcal{B}}(Q_n, \ldots, Q_1) = (-1)^{\frac{n(n-1)}{2}} a^n \prod_{h=1}^{n} \binom{n-1}{h-1} .$$

On obtient finalement la formule générale suivante :

$$\det[P(a_i + b_j)] = (-1)^{\frac{n(n-1)}{2}} a^n \prod_{k=0}^{n-1} \binom{n-1}{k} V_n(a_1, \ldots, a_n)\, V_n(b_1, \ldots, b_n) .$$

Dans le cas particulier de l'exercice, et si $n = 3$, on peut poser $P = (X+1)^2$, et pour tout $(i,j) \in [\![1,3]\!]^2$, $a_i = i - 1$ et $b_j = j - 1$. La valeur du déterminant est donc :

$$(-1)^3\, 1^3 \binom{2}{0} \binom{2}{1} \binom{2}{2} V_3^2(0,1,2) = -8 ,$$

ce qu'on peut vérifier par calcul direct.

Exercice 6 :

Le corps de base est $\mathbb{C}$.

a) Pour $(a_1, \ldots, a_n) \in \mathbb{C}^n$, calculer $\det(M_n)$, où $M_n = [b_{i,j}]$, avec $b_{i,j} = 1 + \delta_{i,j}\, a_i$ (δ est le symbole de Kronecker).

b) Etudier le cas particulier où $a_1 = a_2 = \ldots = a_n = a$.

c) On développe le déterminant D_n suivant : $D_n = \det[c_{i,j}]$ où $c_{i,i} = -x_{i,i}$ pour $i \in [\![1,n]\!]$ et $c_{i,j} = x_{i,j}$ pour $i \neq j$, les $(x_{i,j})$ étant des indéterminées sur $\mathbb{C}$. Le développement est du type $\sum \varepsilon\, \mu(x)$ où les $\mu(x)$ sont des monômes en les $x_{i,j}$ et $\varepsilon \in \{-1, +1\}$. Calculer le nombre de termes de ce dé

pour lesquels $\varepsilon = +1$. ■

a) On peut appliquer ici l'égalité démontrée dans l'exercice 1 du §XIII.4. On obtient :

$$\det(M_n) = \prod_{i=1}^{n} a_i + \sum_{j=1}^{n} \prod_{i \neq j} a_i \ .$$

b) Avec la méthode utilisée dans le *a*) on trouve :

$$\det(M_n) = a^n + n\,a^{n-1} \ .$$

c) Par définition :

$$D_n = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma)\, c_{\sigma(1),1} \cdots c_{\sigma(n),n} \ .$$

Pour $\sigma \in \mathfrak{S}_n$ notons $k(\sigma)$ le nombre de points fixes de la permutation σ. On voit que :

$$D_n = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma)(-1)^{k(\sigma)} x_{\sigma(1),1} \cdots x_{\sigma(n),n} \ .$$

En remplaçant tous les $x_{i,j}$ par 1, on obtient $D_n = (-2)^n + n\,(-2)^{n-1}$ (cf. *b*) avec $a = -2$). En notant p le nombre de termes affectés du signe $+$ et ν le nombre de termes affectés du signe $-$, on a $p - \nu = (-2)^{n-1}(n-2)$. Comme $p + \nu = n!$, nous en déduisons :

$$p = \frac{n!}{2} + (-1)^{n-1}\, 2^{n-2}\,(n-2) \ .$$

Exercice 7 :

On suppose acquise la formule de l'exemple 4 donnant la factorisation du déterminant d'une matrice circulante sur $\mathbb{C}$.

a) En déduire, pour $(x, y, z) \in \mathbb{C}^3$:

$x^3 + y^3 + z^3 - 3\,x\,y\,z = (x+y+z)\,(x+\mathrm{j}\,y+\mathrm{j}^2\,z)\,(x+\mathrm{j}^2\,y+\mathrm{j}\,z)$.

b) Pour $n \geqslant 3$ et $x \in \mathbb{C}$, calculer le déterminant circulant :

$D_n =$

$$\det \begin{bmatrix} 0 & 1 & 2x & 3x^2 & \dots & (n-1)x^{n-2} \\ (n-1)x^{n-2} & 0 & 1 & 2x & \dots & (n-2)x^{n-3} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 2x & 3x^2 & \dots & \dots & 0 \end{bmatrix}.$$

c) Calculer sous forme de nombre rationnel le déterminant circulant $\Gamma(1,2,\dots,n)$, avec les notations de l'exemple 4.

d) Dans $\mathbb{C}[X,Y,Z]$, démontrer en utilisant un déterminant circulant :

$$\prod_{\zeta\in\mu_5}(X+\zeta Y+\bar{\zeta}Z) = X^5+Y^5+Z^5-5XYZ(X^2-YZ)\,.\ \blacksquare$$

a) En utilisant la règle de Sarrus on trouve :

$$\Gamma(x,y,z) = \begin{vmatrix} x & y & z \\ z & x & y \\ y & z & x \end{vmatrix} = x^3+y^3+z^3-3xyz\,.$$

On obtient donc (d'après la formule donnant le déterminant d'une matrice circulante) :

$$x^3+y^3+z^3-3xyz = (x+y+z)(x+\mathrm{j}\,y+\mathrm{j}^2 z)(x+\mathrm{j}^2 y+\mathrm{j}^4 z)\,,$$

ce qu'il fallait démontrer.

b) On voit que :

$$D_n = \Gamma(0,1,2x,3x^2,\dots,(n-1)x^{n-2})\,.$$

En appliquant la formule donnant le déterminant d'une matrice circulante, l'ensemble des indices étant l'ensemble des racines n-ièmes de 1 :

$$D_n = \prod_{\zeta\in\mu_n}(0\,\zeta^0+\zeta+2x\zeta^2+3x^2\zeta^3+\dots+(n-1)x^{n-2}\zeta^{n-1})\,.$$

Notons P_n le polynôme $1+2X+3X^2+\dots+(n-1)X^{n-2}$. Avec cette notation on a :

$$D_n = \left(\prod_{\zeta\in\mu_n}\zeta\right)\prod_{\zeta\in\mu_n}P_n(\zeta x) = (-1)^{n-1}\prod_{\zeta\in\mu_n}P_n(\zeta x)\,.$$

Dans $\mathbb{C}(X)$ on a l'égalité :

$$\frac{X^n-1}{X-1} = 1+X+X^2+\dots+X^{n-1}\,,$$

d'où en dérivant :

$$\frac{n\,X^{n-1}(X-1)-(X^n-1)}{(X-1)^2}=\frac{(n-1)\,X^n-n\,X^{n-1}+1}{(X-1)^2}=P_n\ .$$

Pour tout $\zeta\in\mu_n$ on a donc :

$$P_n(\zeta\,X)=\frac{(n-1)\,X^n-n\,\zeta^{-1}\,X^{n-1}+1}{(\zeta\,X-1)^2}\ ,$$

et par conséquent :

$$\prod_{\zeta\in\mu_n}P(\zeta\,X)=\frac{\displaystyle\prod_{\zeta\in\mu_n}\left[\left((n-1)\,X^n+1\right)-\zeta^{-1}\,n\,X^{n-1}\right]}{\left(\displaystyle\prod_{\zeta\in\mu_n}(1-\zeta\,X)\right)^2}\ .$$

Pour tous polynômes A et B dans $\mathbb{C}[X]$ on a l'égalité :

$$\prod_{\zeta\in\mu_n}(A-\zeta\,B)=A^n-B^n=\prod_{\zeta\in\mu_n}(A-\zeta^{-1}\,B)\ .$$

On obtient donc :

$$\prod_{\zeta\in\mu_n}P(\zeta\,X)=\frac{\left((n-1)\,X^n+1\right)^n-n^n\,X^{n(n-1)}}{(1-X^n)^2}\ .$$

Pour tout $x\in\mathbb{C}$ tel que $x^n\neq 1$, on peut donc écrire :

$$D_n=(-1)^{n-1}\,\frac{\left((n-1)\,x^n+1\right)^n-n^n\,x^{n(n-1)}}{(1-x^n)^2}\ .$$

Posons $Q_n(Y)=\left((n-1)\,Y+1\right)^n-n^n\,Y^{n-1}$. On trouve :

$$Q_n'(Y)=n(n-1)\left(\left((n-1)\,Y+1\right)^{n-1}-n^{n-1}\,Y^{n-2}\right)\ ,$$

et

$$Q_n''(Y)=n(n-1)\left((n-1)^2\left((n-1)\,Y+1\right)^{n-2}-n^{n-1}(n-2)\,Y^{n-3}\right)\ .$$

On vérifie facilement que $Q_n(1)=Q_n'(1)=0$, et donc que $Q_n(Y)$ est divisible par $(Y-1)^2$. Notons $R_n(Y)$ le quotient exact de $Q_n(Y)$ par $(Y-1)^2$; on a dans $\mathbb{C}(X)$ l'égalité :

$$\prod_{\zeta\in\mu_n}P(\zeta\,X)=\frac{Q_n(X^n)}{(1-X^n)^2}=R_n(X^n)\ ,$$

d'où pour tout $x \in \mathbb{C}$:

$$D_n = (-1)^{n-1} \prod_{\zeta \in \mu_n} P(\zeta\, x) = (-1)^{n-1}\, R_n(x^n)\ .$$

En particulier, si $x^n = 1$, $D_n = R_n(1)$. Comme :

$$Q_n(Y) = (Y-1)^2\, R_n(Y)\ ,$$

en dérivant deux fois on trouve (formule de Leibnitz) :

$$Q_n''(Y) = 2\, R_n(Y) + 4\,(Y-1)\, R_n'(Y) + (Y-1)^2\, R_n''(Y)\ ,$$

et en particulier :

$$R_n(1) = \frac{1}{2}\, Q_n''(1) = \frac{1}{2}\, n(n-1)\big((n-1)^2\, n^{n-2} - n^{n-1}\,(n-2)\big) = \\ = \frac{1}{2}\,(n-1)\, n^{n-1}\ .$$

On a donc, si $x^n = 1$, $D_n = \dfrac{(-1)^{n-1}}{2}\,(n-1)\, n^{n-1}$.

c) On trouve ici :

$$\Gamma(1, 2, \ldots, n) = \prod_{\zeta \in \mu_n} (1 + 2\zeta + 3\zeta^2 + \ldots + n\,\zeta^{n-1}) = \prod_{\zeta \in \mu_n} P_n(\zeta)\ ,$$

où $P_n(X) = 1 + 2\,X + \ldots + n\,X^{n-1}$. On a dans $\mathbb{C}(X)$ l'égalité :

$$\frac{X^{n+1} - 1}{X - 1} = 1 + X + \ldots + X^n\ ,$$

d'où en dérivant :

$$\frac{(n+1)\, X^n\,(X-1) - (X^{n+1} - 1)}{(X-1)^2} = \frac{n\, X^{n+1} - (n+1)\, X^n + 1}{(X-1)^2} = P_n\ .$$

On a donc $P_n(1) = \frac{n(n+1)}{2}$, et pour tout $\zeta \in \mu_n$, $\zeta \neq 1$:

$$P_n(\zeta) = \frac{n\,\zeta - n}{(\zeta - 1)^2} = \frac{n}{\zeta - 1}\ .$$

On voit facilement que :

$$Q_n(X) = \prod_{\zeta \neq 1} (X - \zeta) = 1 + X + \ldots + X^{n-1}\ ,$$

d'où $Q_n(1) = n$. On a donc :

$$\Gamma(1,2,\ldots,n) = \frac{n(n+1)}{2}(-1)^{n-1}\frac{n^{n-1}}{n} = (-1)^{n-1}\frac{n+1}{2}n^{n-1}\ .$$

d) On voit que :

$$D = \prod_{\zeta\in\mu_5}(X+\zeta Y+\bar{\zeta}Z) = \prod_{\zeta\in\mu_5}(X+\zeta Y+0\,\zeta^2+0\,\zeta^3+\zeta^4 Z) = \Gamma(X,Y,0,0,Z)\ .$$

Par conséquent :

$$D = \begin{vmatrix} X & Y & 0 & 0 & Z \\ Z & X & Y & 0 & 0 \\ 0 & Z & X & Y & 0 \\ 0 & 0 & Z & X & Y \\ Y & 0 & 0 & Z & X \end{vmatrix}\ .$$

On peut calculer ce déterminant, d'abord en développant par rapport à la première colonne. On obtient (on a remplacé les majuscules par des minuscules) :

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

On peut ensuite développer chaque déterminant par rapport à la première ligne :

$$D = x^2\begin{vmatrix} x & y & 0 \\ z & x & y \\ 0 & z & x \end{vmatrix} - xy\begin{vmatrix} z & y & 0 \\ 0 & x & y \\ 0 & z & x \end{vmatrix} - zy\begin{vmatrix} x & y & 0 \\ z & x & y \\ 0 & z & x \end{vmatrix}$$
$$+ z^2\begin{vmatrix} z & x & y \\ 0 & z & x \\ 0 & 0 & z \end{vmatrix} + y^2\begin{vmatrix} y & 0 & 0 \\ x & y & 0 \\ z & x & y \end{vmatrix} - yz\begin{vmatrix} x & y & 0 \\ z & x & y \\ 0 & z & x \end{vmatrix}\ .$$

En appliquant la règle de Sarrus on obtient :

$$\begin{vmatrix} x & y & 0 \\ z & x & y \\ 0 & z & x \end{vmatrix} = x^3 - 2xyz = x(x^2 - 2yz)\ .$$

Les autres déterminants se calculent facilement. On trouve :

$$D = (x^2 - 2yz)\,x\,(x^2 - 2yz) - xyz\,(x^2 - yz) + z^5 +$$

soit après développement et simplifications :

$$D = x^5 + y^5 + z^5 - 5\,x\,y\,z\,(x^2 - y\,z)\ .$$

Exercice 9 :

On suppose connu le déterminant de Vandermonde :

$$\det\left[(x_i)^{j-1}\right]_{(i,j)\in[\![1,n]\!]^2} = \prod_{i<j}(x_j - x_i)\,,$$

où les (x_i) sont dans $\mathbb{C}$.

a) Soit $P_k(X) \in \mathbb{C}_k[X]$ un polynôme *normalisé* de degré k pour $k \in [\![0, n-1]\!]$, avec $n \geqslant 2$. Donc

$$P_0 = 1, \ldots, P_k = X^k + a_{k,1}X^{k-1} + \ldots + a_{k,k}\,.$$

Démontrer que

$$\det\left[P_{j-1}(x_i)\right]_{(i,j)\in[\![1,n]\!]^2} = \prod_{1\leqslant i<j\leqslant n}(x_j - x_i)\,.$$

b) Calculer ensuite $\det\left[\binom{x_i}{j-1}\right]_{(i,j)\in[\![1,n]\!]^2}$ où $\binom{x_i}{k}$ désigne le coefficient binomial généralisé :

$$\binom{x_i}{k} = \frac{x_i\,(x_i-1)\ldots(x_i-k+1)}{k\,!}\,.$$

c) En déduire que si $(a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n$, avec $a_1 < a_2 < \ldots < a_n$, alors le rationnel $\displaystyle\prod_{1\leqslant i<j\leqslant n}\frac{a_j - a_i}{j-i}$ est un entier. ■

a) D'après l'identité établie dans la résolution de l'exercice 4, on a :

$$\det\left[P_{j-1}(x_i)\right]_{(i,j)\in[\![1,n]\!]^2} = \det_{\mathcal{B}}(P_0, \ldots, P_{n-1})\,V_n(x_1, \ldots, x_n)\ ,$$

où $\mathcal{B}$ désigne la base canonique de $K_{n-1}[X]$. La matrice des polynômes $P_0, \ldots, P_{n-1}$ dans la base canonique est ici trigonale supérieure, de coefficients diagonaux égaux à 1 ; son déterminant est donc 1. On a donc l'égalité :

$$\det\left[P_{j-1}(x_i)\right]_{(i,j)\in[\![1,n]\!]^2} = V_n(x_1, \ldots, x_n) = \prod_{1\leqslant i<j\leqslant n}(x_j - x_i)\ .$$

b) Notons, pour $k \in \mathbb{N}^*$

$$P_k(X) = \frac{X\,(X-1)\ldots(X-k+1)}{k\,!}\ ,$$

en convenant $P_0 = 1$; le polynôme P_k est de degré k. Pour tout $m \in \mathbb{Z}$, si $m \geqslant k$, $P_k(m) = \binom{m}{k} \in \mathbb{Z}$, si $m \in [\![0, k-1]\!]$, $P_k(m) = 0$, et si $m < 0$, $P_k(m) = (-1)^k \binom{-m+k-1}{k} \in \mathbb{Z}$. Le polynôme P_k prend donc des valeurs entières sur $\mathbb{Z}$.

Le déterminant à calculer ici est :

$$\det\left[P_{j-1}(x_i)\right]_{(i,j)\in[\![1,n]\!]^2} =$$

$$= \det_{\mathcal{B}}(P_0, \ldots, P_{n-1})\, V_n(x_1, \ldots, x_n) = \frac{\prod\limits_{1\leqslant i<j\leqslant n}(x_j - x_i)}{0!\,1!\ldots(n-1)!} ,$$

car la matrice des polynômes $(P_0, \ldots, P_{n-1})$ dans la base canonique est trigonale supérieure, de coefficients diagonaux $(0!, 1!, \ldots, (n-1)!)$.

c) Nous pouvons écrire les deux égalités :

$$\det\left[P_{j-1}(a_i)\right]_{(i,j)\in[\![1,n]\!]^2} = \det_{\mathcal{B}}(P_0, \ldots, P_{n-1})\, V_n(a_1, \ldots, a_n) ,$$

et

$$\det\left[P_{j-1}(i-1)\right]_{(i,j)\in[\![1,n]\!]^2} = \det_{\mathcal{B}}(P_0, \ldots, P_{n-1})\, V_n(0, 1, \ldots, n-1) .$$

Nous avons remarqué que si $j > i$, alors $P_{j-1}(i-1) = 0$; d'autre part, pour tout $k \in \mathbb{N}$, $P_k(k) = 1$. On voit que la matrice $(P_{j-1}(i-1))_{(i,j)\in[\![1,n]\!]^2}$ est trigonale inférieure, de coefficients diagonaux tous égaux à 1 ; son déterminant est donc 1. Nous en déduisons :

$$\det\left[P_{j-1}(a_i)\right]_{(i,j)\in[\![1,n]\!]^2} = \frac{V_n(a_1, \ldots, a_n)}{V_n(0, 1, \ldots, n-1)} .$$

Remarquons que :

$$V_n(0, 1, \ldots, n-1) = \prod_{1\leqslant i<j\leqslant n}((j-1) - (i-1)) = V_n(1, 2, \ldots, n) .$$

Comme pour tout $(i, j) \in [\![1, n]\!]^2$, $P_{j-1}(a_i) \in \mathbb{Z}$, on a aussi :

$$\frac{V_n(a_1, \ldots, a_n)}{V_n(1, 2, \ldots, n)} = \det\left[P_{j-1}(a_i)\right]_{(i,j)\in[\![1,n]\!]^2} \in \mathbb{Z} .$$

Enfin, si on suppose de plus $a_1 < a_2 < \ldots < a_n$, il est clair qu'alors :

$$\frac{V_n(a_1, \ldots, a_n)}{V_n(1, 2, \ldots, n)} = \prod_{1\leqslant i<j\leqslant n} \frac{a_j - a_i}{j - i} \in \mathbb{N}^* .$$

Exercice 17 :

Soit $n \in \mathbb{N}$, ($n \geqslant 2$). On désigne par φ *l'indicateur d'Euler* sur $\mathbb{N}^*$ (cf. §IV.5).

a) Démontrer que

$$\det\left([\operatorname{pgcd}(i,j)]_{(i,j)\in[\![1,n]\!]^2}\right) = \varphi(1)\,\varphi(2)\ldots\varphi(n)\,.$$

b) Généraliser au calcul de

$$\det\left(\left[(\operatorname{pgcd}(i,j))^\lambda\right]_{(i,j)\in[\![1,n]\!]^2}\right) \text{ pour } \lambda \in \mathbb{C}\,. \blacksquare$$

a) Rappelons la formule d'Euler-Gauss, démontrée dans l'exercice 15 du §IV.5. Pour tout $n \in \mathbb{N}$, $n \geqslant 2$:

$$n = \sum_{d\,|\,n} \varphi(d)\,.$$

Pour h et k entiers > 0, posons ici $\delta_{h,k} = 0$ si h ne divise pas k et $\delta_{h,k} = 1$ si h divise k. Pour tout $(i,j) \in [\![1,n]\!]^2$, on peut écrire :

$$\operatorname{pgcd}(i,j) = \sum_{d\,|\,\operatorname{pgcd}(i,j)} \varphi(d) = \sum_{d\,|\,i \text{ et } d\,|\,j} \varphi(d)\,.$$

Les diviseurs des entiers $\leqslant n$ étant $\leqslant n$, pour tout $(i,j) \in [\![1,n]\!]^2$:

$$\operatorname{pgcd}(i,j) = \sum_{d=1}^{n} \delta_{d,i}\,\delta_{d,j}\,\varphi(d)\,.$$

La matrice M telle que, pour tout $(i,j) \in [\![1,n]\!]^2$, $M_{i,j} = \operatorname{pgcd}(i,j)$, est donc le produit de la matrice D dont le terme (i,d) est, pour tout $(i,d) \in [\![1,n]\!]^2$, $D_{i,d} = \delta_{d,i}$, et de la matrice Φ dont le terme (d,j) est, pour tout $(d,j) \in [\![1,n]\!]^2$, $\Phi_{d,j} = \delta_{d,j}\,\varphi(d)$. Il est clair que si $h > k$, h ne divise pas k, et par conséquent $\delta_{h,k} = 0$. La matrice D est donc trigonale inférieure, de coefficients diagonaux tous égaux à 1. La matrice Φ est elle trigonale supérieure, de coefficients diagonaux $(\varphi(1),\ldots,\varphi(n))$. On en déduit :

$$\det\left([\operatorname{pgcd}(i,j)]_{(i,j)\in[\![1,n]\!]^2}\right) = \det(D)\,\det(\Phi) = \varphi(1)\,\varphi(2)\ldots\varphi(n)\,.$$

b) Nous utiliserons ici la formule d'inversion utilisant la fonction de Möbius (notée μ), démontrée dans l'exercice 12 du §IX.7, et déjà utilisée dans l'exercice 13 du §IX.7.

Posons pour $m \in \mathbb{N}^*$:

$$\varphi_\lambda(m) = \sum_{d \mid m} \mu(d) \left(\frac{m}{d}\right)^\lambda .$$

D'après la formule d'inversion (avec les notations additives), pour tout $m \in \mathbb{N}^*$:

$$m^\lambda = \sum_{d \mid m} \varphi_\lambda(d) .$$

En remplaçant dans le a), φ par φ_λ, on trouve de même que :

$$\det\left(\left[(\text{pgcd}\,(i,j))^\lambda\right]_{(i,j)\in[\![1,n]\!]^2}\right) = \varphi_\lambda(1)\,\varphi_\lambda(2)\ldots\varphi_\lambda(n) .$$

Soit $m \in \mathbb{N}^*$, $m = \prod_{i=1}^{k} p_i^{r_i}$, où $p_1, \ldots, p_k$ sont des nombres premiers distincts et $r_1, \ldots, r_k$ des entiers > 0 ($k \in \mathbb{N}$). D'après la définition de la fonction de Möbius μ, on a l'égalité :

$$\varphi_\lambda(m) = \sum_{I \subset [\![1,k]\!]} (-1)^{\text{card}(I)} \left(\frac{m}{\prod_{i\in I} p_i}\right)^\lambda = m^\lambda \sum_{I \subset [\![1,k]\!]} \prod_{i\in I} \left(\frac{-1}{p_i^\lambda}\right) .$$

On reconnaît ci-dessus le développement d'un produit. On obtient :

$$\varphi_\lambda(m) = m^\lambda \prod_{i=1}^{k} \left(1 - \frac{1}{p_i^\lambda}\right) .$$

Exercice 20 :

Soit m, n dans $\mathbb{N}^*$. On donne des matrices $A_{i,j} \in \mathfrak{M}_m(K)$ ($(i,j) \in [\![1,n]\!]^2$) *deux à deux permutables.* Soit $M \in \mathfrak{M}_{mn}(K)$ la matrice qui s'écrit : $M = [A_{i,j}]_{(i,j)\in[\![1,n]\!]^2}$, par blocs carrés d'ordre m. Démontrer :

$$\det(M) = \det\left(\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma)\, A_{\sigma(1),1}\, A_{\sigma(2),2} \ldots A_{\sigma(n),n}\right) . \blacksquare$$

Les matrices $(A_{i,j})$ étant deux à deux permutables dans $\mathfrak{M}_m(K)$, on peut considérer que ce sont des éléments d'une sous-algèbre unitaire et commutative $\mathcal{A}$ de $\mathfrak{M}_m(K)$, $\mathcal{A}$ étant par exemple le sous-K-ev de $\mathfrak{M}_m(K)$ engendré par les monômes en les $(A_{i,j})$. L'écriture : $A = [A_{i,j}]_{(i,j)\in[\![1,n]\!]^2}$ désignera la matrice à coefficients dans $\mathcal{A}$ dont le terme (i,j), pour tout $(i,$

est $A_{i,j}$, élément de $\mathscr{A}$. La matrice élément de $\mathfrak{M}_{nm}(K)$, constituée des blocs $(A_{i,j})$, sera elle notée $M = \mathscr{B}(A)$. Avec ces notations, la propriété à démontrer s'énonce :

$$\det_K(\mathscr{B}(A)) = \det_K(\det_{\mathscr{A}}(A)) \ .$$

Pour éviter toute ambiguïté l'anneau de base est indiqué en indice du symbole det.

Montrons par récurrence sur n que la propriété est vraie (elle est vraie pour $n = 1$). Supposons la propriété vraie pour $n-1$, où $n \geqslant 2$, et ceci pour tout corps de base. Nous reprenons les notations de l'énoncé. Nous allons transformer le problème par une manipulation élémentaire sur les blocs qui ressemble à la méthode du pivot de Gauss. Nous aurons besoin pour cela de pouvoir inverser la matrice $A_{n,n}$, ce qui n'est pas toujours directement possible. Aussi introduisons pour tout $(i,j) \in [\![1,n]\!]^2$, $B_{i,j} \in \mathfrak{M}_m(K(X))$ dont les coefficients sont ceux de $A_{i,j} \in \mathfrak{M}_m(K)$ si $(i,j) \neq (n,n)$, et si $(i,j) = (n,n)$, $B_{n,n} = A_{n,n} - X\,I_m$. La matrice $B_{n,n}$ est bien inversible dans $\mathfrak{M}_m(K(X))$, puisque son déterminant dans $K(X)$, qui est le polynôme caractéristique de $A_{n,n}$, n'est pas nul. Il est clair que les matrices $B_{i,j}$, éléments de $\mathfrak{M}_m(K(X))$, sont deux à deux permutables, $I_m (\in \mathfrak{M}_m(K(X))$ commutant avec toute matrice. Soit $\mathscr{C}$ une sous-$K(X)$-algèbre commutative de $\mathfrak{M}_m(K(X))$ contenant toutes les matrices $B_{i,j}$, $(i,j) \in [\![1,n]\!]^2$. Nous noterons $B \in \mathfrak{M}_n(\mathscr{C})$, la matrice dont le terme (i,j) est $B_{i,j}$, pour tout $(i,j) \in [\![1,n]\!]^2$.

Introduisons la matrice auxiliaire suivante, élément de $\mathfrak{M}_n(\mathscr{C})$:

$$D = \begin{bmatrix} I_m & 0 & \dots & \dots & 0 & -B_{1,n}\,B_{n,n}^{-1} \\ 0 & I_m & \ddots & & \vdots & -B_{2,n}\,B_{n,n}^{-1} \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & \ddots & 0 & \vdots \\ \vdots & & & \ddots & I_m & -B_{n-1,n}\,B_{n,n}^{-1} \\ 0 & \dots & & \dots & 0 & I_m \end{bmatrix}$$

On voit que la matrice $D\,B$ est de la forme (calcul dans $\mathfrak{M}_n(\mathscr{C})$) :

$$D\,B = \begin{bmatrix} B'_{1,1} & \dots & \dots & B'_{1,n-1} & 0 \\ \vdots & & & \vdots & \vdots \\ \vdots & & & \vdots & \vdots \\ B'_{n-1,1} & \dots & \dots & B'_{n-1,n-1} & 0 \\ B_{n,1} & \dots & \dots & B_{n,n-1} & B_{n,n} \end{bmatrix},$$

où les $(B'_{i,j})_{(i,j)\in[\![1,n-1]\!]^2}$ sont éléments de l'anneau commutatif $\mathscr{C}$. Notons B' l'élément de $\mathfrak{M}_{n-1}(\mathscr{C})$, dont le terme (i,j) est $B'_{i,j}$, pour tout $(i,j)\in[\![1,n-1]\!]^2$.

On voit que :

$$\det_{\mathscr{C}}(B) = B_{n,n}\det_{\mathscr{C}}B' ,$$

d'où :

$$\det_{K(X)}(\det_{\mathscr{C}}(B)) = \det_{K(X)}(B_{n,n})\det_{K(X)}(\det_{\mathscr{C}}B') .$$

En utilisant la récurrence, on trouve que :

$$\det_{K(X)}(\det_{\mathscr{C}}(B)) = \det_{K(X)}(B_{n,n})\det_{K(X)}(\mathscr{B}(B')) . \tag{1}$$

Les propriétés du produit par blocs des matrices nous permettent d'affirmer :

$$\mathscr{B}(D\,B) = \mathscr{B}(D)\,\mathscr{B}(B) ,$$

et comme il est clair que $\det_{K(X)}(\mathscr{B}(D)) = 1$, nous en déduisons :

$$\det_{K(X)}(\mathscr{B}(B)) = \det_{K(X)}(\mathscr{B}(D\,B)) . \tag{2}$$

Enfin, vu les propriétés des déterminants des matrices trigonales par blocs :

$$\det_{K(X)}(\mathscr{B}(D\,B)) = \det_{K(X)}(B_{n,n})\det_{K(X)}(\mathscr{B}(B')) . \tag{3}$$

En comparant les égalités (1), (2) et (3), nous en déduisons finalement :

$$\det_{K(X)}(\mathscr{B}(B)) = \det_{K(X)}(\det_{\mathscr{C}}(B)) . \tag{4}$$

Il reste à démontrer cette propriété sur la matrice initiale A, c'est-à-dire à justifier le remplacement de X par 0 dans l'égalité ci-dessus. Une telle "substitution" ne va pas de soi, l'égalité (4) n'étant pas clairement "polynomiale" ; on ne peut pas appliquer un théorème de substitution. Nous allons justifier explicitement cette manipulation.

Considérons l'application $\varphi : \mathfrak{M}_m(K[X]) \to \mathfrak{M}_m(K)$ telle que pour tout $M\in\mathfrak{M}_m(K[X])$, et tout $(i,j)\in[\![1,m]\!]^2$, $\varphi(M)_{i,j} = M_{i,j}(0)$. La matrice $\varphi(M)$ est donc obtenue en substituant 0 à X dans chaque coefficient de M. Cette application est visiblement K-linéaire, et l'image du neutre multiplicatif de l'algèbre $\mathfrak{M}_m(K[X])$ est le neutre multiplicatif de l'algèbre $\mathfrak{M}_m(K)$. D'autre part, pour tout M et N dans $\mathfrak{M}_m(K[X])$, et pour tout $(i,j)\in[\![1,m]\!]^2$:

$$(M\,N)_{i,j} = \sum_{h=1}^{m} M_{i,h}\,N_{h,j} ,$$

donc par application du théorème de substitution :

$$\varphi(M\,N)_{i,j} = \big((M\,N)_{i,j}\big)(0) =$$
$$= \sum_{h=1}^{m} M_{i,h}(0)\,N_{h,j}(0) = \sum_{h=1}^{m} \varphi(M)_{i,h}\,\varphi(N)_{h,j} = \big(\varphi(M)\,\varphi(N)\big)_{i,j}\ ,$$

c'est-à-dire $\varphi(M\,N) = \varphi(M)\,\varphi(N)$. L'application φ est donc un homomorphisme d'algèbres unitaires.

On voit aussi que si $M \in \mathfrak{M}_m(K[X])$:

$$\det_{K[X]}(M) = \sum_{\sigma\in\mathfrak{S}_m} \varepsilon(\sigma) M_{\sigma(1),1} \dots M_{\sigma(m),m}\ ,$$

et par conséquent, en appliquant le théorème de substitution :

$$\big(\det_{K[X]}(M)\big)(0) = \sum_{\sigma\in\mathfrak{S}_m} \varepsilon(\sigma) M_{\sigma(1),1}(0) \dots M_{\sigma(m),m}(0) = \det_K(\varphi(M))\ .$$

Nous noterons Φ l'application analogue à φ, mais de $\mathfrak{M}_{mn}(K[X])$ vers $\mathfrak{M}_{mn}(K)$. On voit facilement que $\Phi(\mathfrak{B}(B)) = \mathfrak{B}(A)$. Nous en déduisons :

$$\det_{K[X]}(\mathfrak{B}(B))(0) = \det_K(\Phi(\mathfrak{B}(B))) = \det_K(\mathfrak{B}(A))\ .$$

L'égalité (4) s'écrit aussi :

$$\det_{K[X]}(\mathfrak{B}(B)) = \det_{K[X]}\left(\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) B_{\sigma(1),1} \dots B_{\sigma(n),n}\right)\ ,$$

d'où, en prenant les valeurs en 0 de ces deux polynômes :

$$\det_K(\mathfrak{B}(A)) = \det_K\left(\varphi\left(\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) B_{\sigma(1),1} \dots B_{\sigma(n),n}\right)\right) =$$
$$= \det_K\left(\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) \varphi(B_{\sigma(1),1}) \dots \varphi(B_{\sigma(n),n})\right)\ ,$$
$$= \det_K\left(\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) A_{\sigma(1),1} \dots A_{\sigma(n),n})\right)$$

ce qu'il fallait démontrer.

La proposition est donc démontrée par récurrence sur l'entier r

Comme le montre l'exemple ci-dessous, il est indispensable de supposer que les matrices $A_{i,j}$ commutent entre elles.
On prend $n = m = 2$, $K = \mathbb{Q}$ et les quatre éléments de $\mathfrak{M}_2(\mathbb{Q})$ suivants :

$$A_{1,1} = A_{2,2} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad A_{2,1} = A_{1,2} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} .$$

On a alors :

$$D = \sum_{\sigma \in \mathfrak{S}_2} \varepsilon(\sigma)\, A_{\sigma(1),1}\, A_{\sigma(2),2} = A_{1,1}\, A_{2,2} - A_{2,1}\, A_{1,2} = 2\, I_2 ,$$

et $\det(D) = 4$. Mais la matrice :

$$M = \begin{bmatrix} 0 & 1 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} ,$$

est singulière, donc $\det(M) = 0$.

Exercice 23 :

Soit m et n dans $\mathbb{N}^*$, $m \leqslant n$. On donne $M \in \mathfrak{M}_{m,n}(K)$ et $N \in \mathfrak{M}_{n,m}(K)$ ($M = [a_{i,j}]$, $N = [b_{i,j}]$).

a) Démontrer :

$$\det(M\,N) = \sum_{I \in \mathcal{P}_m} \Delta_{[\![1,m]\!],I}(M)\, \Delta_{I,[\![1,m]\!]}(N) ,$$

où $\mathcal{P}_m$ désigne l'ensemble des parties de $[\![1,n]\!]$ de cardinal m.

b) Pour $M \in \mathfrak{M}_{m,n}(K)$, en déduire $\det(M\,{}^tM)$.

c) Soit $n \in \mathbb{N}$, $n \geqslant 2$, et $(p,q) \in (\mathbb{N}^*)^2$ tels que $p+q = m \leqslant n$. On suppose $K = \mathbb{R}$. On donne $N = [A \vdots B] \in \mathfrak{M}_{n,m}(\mathbb{R})$, avec $A \in \mathfrak{M}_{n,p}(\mathbb{R})$ et $B \in \mathfrak{M}_{n,q}(\mathbb{R})$. Démontrer :

$$\det({}^tN\,N) \leqslant \det({}^tA\,A)\, \det({}^tB\,B) .$$

d) Soit $M \in \mathfrak{M}_n(\mathbb{R})$, de colonnes $C_1, C_2, \ldots, C_n$. Démontrer que

$$\big(\det(M)\big)^2 \leqslant \prod_{i=1}^{n} ({}^tC_i\, C_i) \qquad \text{(inégalité de Hadamard).} \blacksquare$$

a) Par définition :

$$\det(M\,N) = \sum_{\sigma \in \mathfrak{S}_m} \varepsilon(\sigma) \left(\sum_{i_1=1}^{n} a_{\sigma(1),i_1}\, b_{i_1,1} \right) \cdots \left(\sum_{i_m=1}^{n} a_{\sigma(m),i_m}\, b_{i_m,m} \right) =$$

$$= \sum_{(i_1,\ldots,i_m) \in [\![1,n]\!]^m} \left(\sum_{\sigma \in \mathfrak{S}_m} \varepsilon(\sigma)\, a_{\sigma(1),i_1} \cdots a_{\sigma(m),i_m} \right) b_{i_1,1} \cdots b_{i_m,m} .$$

En notant, pour tout $i \in [\![1,n]\!]$, C_i la i-ième colonne de la matrice M, et $\mathcal{B}$ la base canonique de $\mathfrak{M}_{m,1}(K)$, on voit que pour tout $(i_1,\dots,i_m) \in [\![1,n]\!]^m$:

$$\sum_{\sigma\in\mathfrak{S}_m} \varepsilon(\sigma)\, a_{\sigma(1),i_1}\dots a_{\sigma(m),i_m} = \det_{\mathcal{B}}(C_{i_1},\dots,C_{i_m})\ .$$

Ce terme est donc nul si les entiers $(i_1,\dots,i_m)$ ne sont pas distincts. On peut donc ne garder, dans la somme donnant $\det(M\,N)$, que les termes correspondant à des m-uplets injectifs. On peut alors faire un partage dans la somme suivant l'image du m-uplet, $P = \{i_1,\dots,i_m\} \in \mathcal{P}_m([\![1,n]\!])$. En notant $B_m(P)$ l'ensemble des bijections de $[\![1,m]\!]$ dans P, on obtient l'égalité :

$$\det(M\,N) = \sum_{P\in\mathcal{P}_m}\ \sum_{i\in B_m(P)} \det_{\mathcal{B}}(C_{i(1)},\dots,C_{i(m)})\, b_{i(1),1}\dots b_{i(m),m}\ .$$

Pour $P \in \mathcal{P}_m([\![1,n]\!])$, notons i_P la seule bijection strictement croissante de $[\![1,m]\!]$ vers P. Quand σ décrit $\mathfrak{S}_m$, alors $i_P\circ\sigma$ décrit l'ensemble des bijections de $[\![1,m]\!]$ dans P, ensemble que nous avons noté $B_m(P)$. Par changement d'indice on obtient :

$$\begin{aligned}&\det(M\,N) = \\ &\quad = \sum_{P\in\mathcal{P}_m}\ \sum_{\sigma\in\mathfrak{S}_m} \det_{\mathcal{B}}(C_{i_P(\sigma(1))},\dots,C_{i_P(\sigma(m))})\, b_{i_P(\sigma(1)),1}\dots b_{i_P(\sigma(m)),m}\ .\end{aligned}$$

En utilisant la propriété d'antisymétrie du déterminant :

$$\begin{aligned}&\det(M\,N) = \\ &\quad = \sum_{P\in\mathcal{P}_m}\ \sum_{\sigma\in\mathfrak{S}_m} \varepsilon(\sigma)\det_{\mathcal{B}}(C_{i_P(1)},\dots,C_{i_P(m)})\, b_{i_P(\sigma(1)),1}\dots b_{i_P(\sigma(m)),m} = \\ &\quad = \sum_{P\in\mathcal{P}_m} \det_{\mathcal{B}}(C_{i_P(1)},\dots,C_{i_P(m)}) \sum_{\sigma\in\mathfrak{S}_m} \varepsilon(\sigma) b_{i_P(\sigma(1)),1}\dots b_{i_P(\sigma(m)),m}\ .\end{aligned}$$

Notons enfin $(L_1,\dots,L_n)$ les lignes de N ; on voit que pour tout $P \in \mathcal{P}_m([\![1,n]\!])$, le déterminant de la sous-matrice de N constituée par les lignes $(L_{i_P(1)},\dots,L_{i_P(m)})$ est, en utilisant les notations de l'énoncé :

$$\Delta_{P,[\![1,m]\!]}(N) = \sum_{\sigma\in\mathfrak{S}_m} \varepsilon(\sigma) b_{i_P(\sigma(1)),1}\dots b_{i_P(\sigma(m)),m}\ .$$

De manière analogue :

$$\Delta_{[\![1,m]\!],P}(M) = \det_{\mathcal{B}}(C_{i_P(1)},\dots,C_{i_P(m)})\ .$$

On obtient donc l'égalité à démontrer :

$$\det(M\,N) = \sum_{P\in\mathcal{P}_m} \Delta_{[\![1,m]\!],P}(M)\,\Delta_{P,[\![1,m]\!]}(N)\ .$$

b) Nous déduisons du *a*) l'égalité :

$$\det(M\,{}^tM) = \sum_{P\in\mathcal{P}_m} \Delta_{[\![1,m]\!],P}(M)\,\Delta_{P,[\![1,m]\!]}({}^tM) = \\ = \sum_{P\in\mathcal{P}_m} \left(\Delta_{[\![1,m]\!],P}(M)\right)^2\ ,$$

car pour tout $P\in\mathcal{P}_m([\![1,n]\!])$, la sous-matrice de ${}^tM$ constituée par les lignes dont l'indice est dans P, est la transposée de la sous-matrice de M constituée par les colonnes dont l'indice est dans P.

c) On voit donc que pour toute matrice $N\in\mathfrak{M}_{n,m}(\mathbb{R})$, $\det({}^tN\,N)\geqslant 0$, et que ce déterminant est nul si, et seulement si, tous les mineurs d'ordre m dans N sont nuls, donc si, et seulement si, $\mathrm{rg}N < m$. Si les colonnes de N sont $C_1,\ldots,C_m$, éléments de $\mathfrak{M}_{n,1}(\mathbb{R})$, pour tout $(i,j)\in[\![1,m]\!]^2$, le terme (i,j) de la matrice ${}^tN\,N$ est ${}^tC_i\times C_j$, c'est-à-dire le produit scalaire des vecteurs C_i et C_j pour la structure euclidienne canonique du $\mathbb{R}$-espace $\mathfrak{M}_{n,1}(\mathbb{R})$. La matrice ${}^tN\,N$ est appelée *matrice de Gram* des vecteurs $(C_1,\ldots,C_m)$, et son déterminant est le *déterminant de Gram* de ces vecteurs.

Nous supposerons que la matrice N est de rang m, car dans le cas contraire, d'après les remarques faites ci-dessus, $\det({}^tN\,N)=0$ et l'inégalité est vérifiée. Notons $C_1,\ldots,C_p$ les colonnes de la matrice A, $C_{p+1},\ldots,C_{p+q}$ les colonnes de la matrice B. Soit F le sous-$\mathbb{R}$-ev engendré dans $\mathfrak{M}_{n,1}(\mathbb{R})$ par les colonnes de A et G le sous-$\mathbb{R}$-ev engendré par les colonnes de A et celles de B, de telle sorte que $F\subset G\subset\mathfrak{M}_{n,1}(\mathbb{R})$. Soit $(e_1,\ldots,e_p)$ une base orthonormée de F, $(e_{p+1},\ldots,e_{p+q})$ une base orthonormée de l'orthogonal de F dans G, et $(e_{m+1},\ldots,e_n)$ une base orthonormée de l'orthogonal de G (si cet orthogonal n'est pas nul). On voit que $(e_1,\ldots e_n)$ est une base orthonormée de $\mathfrak{M}_{n,1}(\mathbb{R})$. Notons P la matrice de passage de la base canonique de $\mathfrak{M}_{n,1}(\mathbb{R})$ vers cette nouvelle base orthonormée ; la matrice P est orthogonale. Soit N' la matrice dont les colonnes sont les vecteurs colonnes des coordonnées des colonnes de N dans la nouvelle base, c

$N = P\,N'$ et N' s'écrit par blocs sous la forme :

$$N' = \left[\begin{array}{c|c} A'_1 & B'_1 \\ \hline 0 & B'_2 \\ \hline 0 & 0 \end{array}\right]$$

où $A'_1 \in \mathfrak{M}_p(\mathbb{R})$, $B'_1 \in \mathfrak{M}_{p,q}(\mathbb{R})$ et $B'_2 \in \mathfrak{M}_q(\mathbb{R})$.

Soit $A' \in \mathfrak{M}_{n,p}$ telle que $A = P\,A'$ et $B' \in \mathfrak{M}_{n,q}$ telle que $B = P\,B'$. Les colonnes de A' sont les p premières colonnes de N' et les colonnes de B' les q dernières. Remarquons que :

$$^tN\,N = {}^tN'\,{}^tP\,P\,N' = {}^tN'\,N' \ ,$$

et de même $^tA\,A = {}^tA'\,A'$ et $^tB\,B = {}^tB'\,B'$, car la matrice P est orthogonale. On a aussi :

$$^tA\,A = {}^tA'\,A' = \left[{}^tA'_1 \middle|\, 0\right] \times \left[\frac{A'_1}{0}\right] = {}^tA'_1\,A'_1 \ .$$

Enfin, en utilisant l'égalité du *b*) en remplaçant la matrice M par la matrice $^tB'$, on voit que $\det({}^tB'\,B')$ est une somme de carrés de déterminants de sous-matrices carrées de taille q, dont $\left(\det B'_2\right)^2$, et que par conséquent :

$$\det\left(B'_2\right)^2 \leqslant \det\left({}^tB'\,B'\right) = \det\left({}^tB\,B\right) \ .$$

Remarquons l'égalité :

$$^tN\,N = {}^tN'\,N' =$$

$$= \left[\begin{array}{c|c|c} {}^tA'_1 & 0 & 0 \\ \hline {}^tB'_1 & {}^tB'_2 & 0 \end{array}\right] \left[\begin{array}{c|c} A'_1 & B'_1 \\ \hline 0 & B'_2 \\ \hline 0 & 0 \end{array}\right] = \left[\begin{array}{c|c} {}^tA'_1 & 0 \\ \hline {}^tB'_1 & {}^tB'_2 \end{array}\right] \left[\begin{array}{c|c} A'_1 & B'_1 \\ \hline 0 & B'_2 \end{array}\right] \ ,$$

et par conséquent :

$$\det\left({}^tN\,N\right) = \det\left({}^tA'_1\right)\det\left({}^tB'_2\right)\det\left(A'_1\right)\det\left(B'_2\right) =$$
$$= \det^2\left(A'_1\right)\det^2\left(B'_2\right) = \det\left({}^tA\,A\right)\,\det^2\left(B'_2\right) \leqslant \det\left({}^tA\,A\right)\,\det\left({}^tB\,B\right) \ ,$$

ce qu'il fallait démontrer.

d) Montrons par récurrence sur l'entier $m \leqslant n$, que la sous-matrice A_m formée par les m premières colonnes de M, est telle que :

$$\det\left({}^t A_m\, A_m\right) \leqslant \prod_{i=1}^{m} ({}^t C_i\, C_i)\ .$$

C'est évidemment vrai pour $m = 1$. Supposons que la propriété soit vraie pour l'entier m, avec $m < n$. Nous pouvons appliquer le résultat du *c*) aux matrices $A = A_m$ et $B = C_m$. Nous obtenons :

$$\det\left({}^t A_{m+1}\, A_{m+1}\right) \leqslant \det\left({}^t A_m\, A_m\right)\ ({}^t C_{m+1}\, C_{m+1})\ ,$$

puisque ${}^t C_{m+1}\, C_{m+1}$ est une matrice scalaire. Nous déduisons de l'hypothèse de récurrence l'inégalité :

$$\det\left({}^t A_{m+1}\, A_{m+1}\right) \leqslant ({}^t C_1\, C_1) \ldots ({}^t C_m\, C_m)\, ({}^t C_{m+1}\, C_{m+1})\ ,$$

ce qui prouve que la propriété est vraie pour $m+1$. La propriété est donc vraie pour l'entier n, et comme $A_n = M$ est une matrice carrée, nous obtenons :

$$\left(\det(M)\right)^2 \leqslant \prod_{i=1}^{n} ({}^t C_i\, C_i)\ ,$$

ce qu'il fallait démontrer.

Exercice 25 :

Soit $(n, p) \in \mathbb{N}^2$, $1 \leqslant p < n$. On donne $M \in \mathfrak{M}_{n,p}(K)$ et $N \in \mathfrak{M}_{p,n}(K)$. Montrer :

$$(\forall x \in K) \quad \det(M\,N + x\,I_n) = x^{n-p} \det(N\,M + x\,I_p)\ . \blacksquare$$

Nous constatons les deux égalités suivantes (produits par blocs) :

$$\left[\begin{array}{c|c} x\,I_p & -N \\ \hline M & I_n \end{array}\right] \times \left[\begin{array}{c|c} I_p & N \\ \hline 0 & x\,I_n \end{array}\right] = \left[\begin{array}{c|c} x\,I_p & 0 \\ \hline M & M\,N + x\,I_n \end{array}\right]\ ,$$

et :

$$\left[\begin{array}{c|c} I_p & N \\ \hline 0 & x\,I_n \end{array}\right] \times \left[\begin{array}{c|c} x\,I_p & -N \\ \hline M & I_n \end{array}\right] = \left[\begin{array}{c|c} x\,I_p + N\,M & 0 \\ \hline x\,M & x\,I_n \end{array}\right]\ .$$

Notons :

$$D = \det \left[\begin{array}{c|c} x\,I_p & -N \\ \hline M & I_n \end{array}\right] .$$

En calculant les déterminants on trouve :

$$D\,x^n = x^p \det(M\,N + x\,I_n) \quad \text{et} \quad x^n\,D = \det(x\,I_p + N\,M)\,x^n .$$

Nous en déduisons, pour tout $x \in K$, $x \neq 0$, l'égalité :

$$\det(M\,N + x\,I_n) = x^{n-p} \det(N\,M + x\,I_p) .$$

Cette égalité est vraie aussi si $x = 0$, car la matrice $M\,N$, élément de $\mathfrak{M}_{n,n}(K)$, est de rang au plus p, et est par conséquent singulière.

Exercice 26 :

a) Soit $(a_1, \ldots, a_n) \in K^n$ et $(b_1, \ldots, b_n) \in K^n$ ($n \geqslant 2$), avec $\forall (i,j),\ a_i + b_j \neq 0$. Démontrer :

$$\det\left(\left[\frac{1}{a_i + b_j}\right]_{(i,j)\in[\![1,n]\!]^2}\right) = \frac{\prod\limits_{1\leqslant i<j\leqslant n} (a_j - a_i)(b_j - b_i)}{\prod\limits_{(i,j)\in[\![1,n]\!]^2} (a_i + b_j)} .$$

(déterminant de Cauchy). Achever le calcul pour $a_i = b_i = i$ ($1 \leqslant i \leqslant n$).

b) Soit $(\rho_1, \rho_2, \ldots, \rho_{n+1}) \in (\mathbb{C}^*)^{n+1}$. On pose,

pour $1 \leqslant i \leqslant n$, $x_{i,i} = \dfrac{(\rho_i + \rho_{n+1})^2}{\rho_i^2\,\rho_{n+1}^2}$,

et pour $i \neq j$, $x_{i,j} = \dfrac{(\rho_i + \rho_{n+1})(\rho_j + \rho_{n+1}) - 2\,\rho_{n+1}^2}{\rho_i\,\rho_j\,\rho_{n+1}^2}$.

Démontrer : $\det\left([x_{i,j}]_{(i,j)\in[\![1,n]\!]^2}\right) =$

$$\frac{2^{n-1}}{\rho_1^2\,\rho_2^2 \cdots \rho_{n+1}^2}\left[\left(\sum_{i=1}^{n+1} \rho_i\right)^2 - (n-1)\sum_{i=1}^{n+1} \rho_i^2\right] .$$

c) *Application géométrique :* Soit E un espace euclidien de dimension $n - 1 \geqslant 2$. On donne des sphères $\mathcal{S}_1, \mathcal{S}_2 \ldots, \mathcal{S}_{n+1}$ dans E telles que chacune d'elles est tangente à toutes les autres en des points distincts. On note $\Omega_1, \ldots, \Omega_{n+1}$ leurs centres, $R_1, \ldots, R_{n+1}$ leurs rayons et $\rho_1, \ldots, \rho_{n+1}$ leurs courbures ($\rho_i = 1/R_i$). Prouver d'abord que : ou bien toutes les sphères sont tangentes extérieurement, ou bien l'une contient toutes les autres. Si on est dans le premier cas, les R_i seront pris

le second cas, si on suppose que c'est la sphère $\mathcal{S}_{n+1}$ qui contient toutes les autres, son rayon sera pris < 0. Poser ensuite $\overrightarrow{V_i} = \overrightarrow{\Omega_{n+1}\Omega_i}$ $(1 \leqslant i \leqslant n)$. On adopte les notations du b). Prouver que $(\overrightarrow{V_i} \mid \overrightarrow{V_j}) = (x_{i,j})$ $((i,j) \in [\![1,n]\!]^2)$. En s'aidant du résultat du b), montrer la relation :

$$\left(\sum_{i=1}^{n+1} \rho_i\right)^2 = (n-1)\sum_{i=1}^{n+1} \rho_i^2 .$$

(*Référence :* W.S. Brown, in Math Monthly, Juin 1969.) ■

a) Pour chaque $i \in [\![1,n]\!]$, multiplions la ligne i de la matrice par le scalaire $\prod_{h=1}^{n} (a_i + b_h)$. On multiplie par conséquent le déterminant initial D par $\prod_{(i,h)\in[\![1,n]\!]^2} (a_i + b_h)$. La matrice obtenue a pour terme de ligne i et de colonne j, le scalaire $\prod_{h\neq j} (a_i + b_h) = P_j(a_i)$, si on note P_j, pour $j \in [\![1,n]\!]$, le polynôme $P_j = \prod_{h\neq j} (X + b_h)$. Pour tout $j \in [\![1,n]\!]$, $P_j \in K_{n-1}[X]$, et on peut donc utiliser l'égalité démontrée dans la résolution de l'exercice 5. Nous en déduisons :

$$D \times \prod_{(i,h)\in[\![1,n]\!]^2} (a_i + b_h) = \det_{\mathcal{B}}(P_1, \ldots, P_n)\, V_n(a_1, \ldots, a_n) ,$$

où $\mathcal{B}$ désigne la base canonique de $K_{n-1}[X]$ et $V_n(a_1, \ldots, a_n)$ le déterminant de Vandermonde de la suite $(a_1, \ldots, a_n)$.

Soit N la matrice dont le terme (i,j) est $P_j(-b_i)$. Il est clair que N est la matrice diagonale dont les coefficients diagonaux sont $N_{j,j} = \prod_{h\neq j} (b_h - b_j)$ $(j \in [\![1,n]\!])$, et par conséquent :

$$\prod_{j\neq h} (b_h - b_j) = \det(N) = \det_{\mathcal{B}}(P_1, \ldots, P_n)\, V(-b_1, \ldots, -b_n) .$$

Nous en déduisons :

$$\det_{\mathcal{B}}(P_1, \ldots, P_n) = \frac{\prod_{j\neq h} (b_h - b_j)}{\prod_{h<j} (b_h - b_j)} = \prod_{1\leqslant j<h\leqslant n} (b_h - b_j) = V_n(b_1, \ldots, b_n) .$$

Nous obtenons enfin :

$$D = \frac{V_n(a_1, \ldots, a_n)\, V_n(b_1, \ldots, b_n)}{\prod_{(i,j)\in[\![1,n]\!]^2} (a_i + b_j)} .$$

Dans le cas particulier où $a_i = b_i = i$, pour tout $i \in [\![1,n]\!]$, on trouve :

$$\prod_{(i,j)\in[\![1,n]\!]^2} (i+j) = 2.3\ldots(n+1) \times 3.4\ldots(n+2) \times \ldots \times (n+1)\ldots(2n) =$$

$$= \frac{(n+1)!}{1!}\,\frac{(n+2)!}{2!}\cdots\frac{(2n)!}{n!}\ .$$

Comme d'autre part :

$$V_n(1,2,\ldots,n) = (n-1)!\,(n-2)!\ldots 1!\ ,$$

nous en déduisons :

$$D = \frac{1}{n+1}\,\frac{\left(1!\,2!\ldots(n-1)!\right)^3}{(n+2)!\ldots(2n)!}\ .$$

b) Notons D le déterminant à calculer. En multipliant chaque ligne d'indice i, pour $i \in [\![1,n]\!]$, par $\rho_i\,\rho_{n+1}$, et chaque colonne d'indice j, pour $j \in [\![1,n]\!]$, par $\rho_j\,\rho_{n+1}$, on trouve un déterminant D' tel que $D' = \rho_1^2 \ldots \rho_n^2\,\rho_{n+1}^{2\,n}\,D$, qui est le déterminant de la matrice $[y_{i,j}]$ telle que, pour tout $i \in [\![1,n]\!]$, $y_{i,i} = (\rho_i + \rho_{n+1})^2$, et pour tout $(i,j) \in [\![1,n]\!]^2$ $i \neq j$, $y_{i,j} = (\rho_i + \rho_{n+1})(\rho_j + \rho_{n+1}) - 2\,\rho_{n+1}^2$. Posons pour tout $i \in [\![1,n]\!]$, $\mu_i = (\rho_i + \rho_{n+1})$. On a, pour tout $i \in [\![1,n]\!]$, $y_{i,i} = \mu_i^2$, et pour tout $(i,j) \in [\![1,n]\!]^2$, $i \neq j$, $y_{i,j} = \mu_i\,\mu_j - 2\,\rho_{n+1}^2$. La matrice :

$$M\,N = \begin{bmatrix} \mu_1 & \rho_{n+1} \\ \vdots & \vdots \\ \vdots & \vdots \\ \mu_n & \rho_{n+1} \end{bmatrix} \times \begin{bmatrix} \mu_1 & \cdots & \cdots & \mu_n \\ -2\,\rho_{n+1} & \cdots & \cdots & -2\,\rho_{n+1} \end{bmatrix}\ ,$$

a pour coefficient d'indice (i,j), le scalaire $\mu_i\,\mu_j - 2\rho_{n+1}^2$. On voit donc que $D' = \det\left(M\,N + 2\rho_{n+1}^2\,I_n\right)$. D'après l'exercice 25, on a :

$$D' = (2\,\rho_{n+1}^2)^{n-2}\det\left(N\,M + 2\rho_{n+1}^2\,I_2\right)\ .$$

On calcule facilement :

$$N\,M = \begin{bmatrix} \mu_1 & \cdots & \cdots & \mu_n \\ -2\,\rho_{n+1} & \cdots & \cdots & -2\,\rho_{n+1} \end{bmatrix} \times \begin{bmatrix} \mu_1 & \rho_{n+1} \\ \vdots & \vdots \\ \vdots & \vdots \\ \mu_n & \rho_{n+1} \end{bmatrix} =$$

$$= \begin{bmatrix} \sum_{i=1}^{n} \mu_i^2 & \rho_{n+1}\sum_{i=1}^{n} \mu_i \\ -2\,\rho_{n+1}\sum_{i=1}^{n} \mu_i & -2\,n\,\rho_{n+1}^2 \end{bmatrix}\ .$$

Calculons les termes de la matrice $N\,M + 2\,\rho_{n+1}^2\,I_2$, en faisant apparaître les sommes :

$$S_1 = \sum_{i=1}^{n+1} \rho_i \quad \text{et} \quad S_2 = \sum_{i=1}^{n+1} \rho_i^2 \ .$$

Le coefficient d'indice $(1,1)$ est :

$$\begin{aligned} a_{1,1} = 2\,\rho_{n+1}^2 + \sum_{i=1}^{n} (\rho_i + \rho_{n+1})^2 = \\ = (n+2)\,\rho_{n+1}^2 + S_2 - \rho_{n+1}^2 + 2\,\rho_{n+1}(S_1 - \rho_{n+1}) = \\ = S_2 + 2\,\rho_{n+1}\,S_1 + (n-1)\,\rho_{n+1}^2 \ . \end{aligned}$$

Le coefficient d'indice $(1,2)$ est :

$$a_{1,2} = \rho_{n+1}(S_1 + (n-1)\,\rho_{n+1}) = \rho_{n+1}\,S_1 + (n-1)\rho_{n+1}^2 \ .$$

On voit que $a_{2,1} = -2\,a_{1,2}$, et que $a_{2,2} = -2\,(n-1)\,\rho_{n+1}^2$. On a donc l'égalité :

$$\begin{aligned} &\det(N\,M + 2\,\rho_{n+1}^2\,I_2) = \\ &\quad = \begin{vmatrix} S_2 + 2\,\rho_{n+1}\,S_1 + (n-1)\,\rho_{n+1}^2 & \rho_{n+1}\,S_1 + (n-1)\,\rho_{n+1}^2 \\ -2\big(\rho_{n+1}\,S_1 + (n-1)\,\rho_{n+1}^2\big) & -2\,(n-1)\,\rho_{n+1}^2 \end{vmatrix} \ . \end{aligned}$$

En divisant la deuxième ligne par 2, et en ajoutant la deuxième ligne à la première, on obtient :

$$\det(N\,M + 2\,\rho_{n+1}^2\,I_2) = 2 \begin{vmatrix} S_2 + \rho_{n+1}\,S_1 & \rho_{n+1}\,S_1 \\ -\rho_{n+1}\,S_1 - (n-1)\,\rho_{n+1}^2 & -(n-1)\,\rho_{n+1}^2 \end{vmatrix} \ .$$

En retranchant la deuxième colonne à la première, on obtient :

$$\det(N\,M + 2\,\rho_{n+1}^2\,I_2) = 2 \begin{vmatrix} S_2 & \rho_{n+1}\,S_1 \\ -\rho_{n+1}\,S_1 & -(n-1)\,\rho_{n+1}^2 \end{vmatrix} \ .$$

Nous en déduisons l'égalité :

$$D' = (2\,\rho_{n+1}^2)^{n-2} \det\left(N\,M + 2\rho_{n+1}^2\,I_2\right) = 2^{n-1}\,\rho_{n+1}^{2n-2}\big(S_1^2 - (n-1)\,S_2\big) \ .$$

D'où enfin :

$$D = \frac{D'}{\rho_1^2 \cdots \rho_n^2\,\rho_{n+1}^{2n}} = 2^{n-1}\,\frac{S_1^2 - (n-1)\,S_2}{\rho_1^2 \cdots \rho_{n+1}^2} \ ,$$

ce qu'il fallait démontrer.

c) Supposons que trois sphères $\mathcal{S}$, $\mathcal{S}'$, $\mathcal{S}''$ soient tangentes deux à deux, $\mathcal{S}$ intérieurement à $\mathcal{S}'$, et $\mathcal{S}'$ intérieurement $\mathcal{S}''$. Dans ce cas, $\mathcal{S}$ est incluse dans la sphère $\mathcal{S}''$ et les trois sphères sont tangentes au même point. D'après les hypothèses, cette situation est exclue pour trois des sphères $\mathcal{S}_i$, donc s'il existe $(i,j) \in [\![1, n+1]\!]^2$, $i \neq j$, tel que $\mathcal{S}_i$ soit tangente intérieurement à $\mathcal{S}_j$, pour tout $h \in [\![1, n+1]\!]$, $h \neq i$ et $h \neq j$, la sphère $\mathcal{S}_h$ ne peut pas être tangente intérieurement à $\mathcal{S}_i$, ni tangente extérieurement à $\mathcal{S}_j$; elle est donc tangente intérieurement à $\mathcal{S}_j$, et tangente extérieurement à $\mathcal{S}_i$. On voit donc que, soit les sphères sont toutes tangentes deux à deux extérieurement, soit il existe $j \in [\![1, n+1]\!]$, tel que pour tout $i \in [\![1, n+1]\!]$, $i \neq j$, $\mathcal{S}_i$ est tangente intérieurement à $\mathcal{S}_j$, et tel que toutes les sphères $\mathcal{S}_i$, $i \neq j$, sont tangentes extérieurement deux à deux. Nous pouvons supposer dans ce cas que la sphère qui contient toutes les autres est $\mathcal{S}_{n+1}$.

Notons $d_{i,j}$, pour tout $(i,j) \in [\![1, n+1]\!]^2$, la distance entre les centres des sphères $\mathcal{S}_i$ et $\mathcal{S}_j$.
Soit les sphères sont toutes deux à deux tangentes extérieurement ; dans ce cas, pour tout $(i,j) \in [\![1, n+1]\!]^2$, $i \neq j$, $d_{i,j} = R_i + R_j$;
soit la sphère $\mathcal{S}_{n+1}$ est tangente extérieurement aux sphères $\mathcal{S}_i$ ($i \leqslant n$), et les sphères $\mathcal{S}_i$ ($i \leqslant n$), sont tangentes deux à deux extérieurement ; dans ce cas pour tout $i \in [\![1, n]\!]$ $d_{i,n+1} = R_{n+1} - R_i$, et pour tout $(i,j) \in [\![1, n]\!]^2$, $i \neq j$, $d_{i,j} = R_i + R_j$.
En remplaçant dans le deuxième cas R_{n+1} par $-R_{n+1}$, on voit que dans tous les cas, pour tout $(i,j) \in [\![1, n+1]\!]^2$, $i \neq j$, $d_{i,j}^2 = (R_i + R_j)^2$. On a donc l'égalité, pour tout $(i,j) \in [\![1, n]\!]^2$, $i \neq j$:

$$(R_i + R_j)^2 = \overrightarrow{\Omega_i\Omega_j}^2 = \left(\overrightarrow{V_j} - \overrightarrow{V_i}\right)^2 = d_{n+1,j}^2 + d_{n+1,i}^2 - 2\left(\overrightarrow{V_j} \middle| \overrightarrow{V_i}\right),$$

d'où :

$$\begin{aligned} 2\left(\overrightarrow{V_j} \middle| \overrightarrow{V_i}\right) &= (R_{n+1} + R_i)^2 + (R_{n+1} + R_j)^2 - (R_i + R_j)^2 = \\ &= 2\left(R_{n+1}^2 + R_{n+1}\,R_j + R_{n+1}\,R_i - R_i\,R_j\right). \end{aligned}$$

On obtient donc, pour tout $(i,j) \in [\![1, n]\!]^2$, $i \neq j$:

$$\begin{aligned} \left(\overrightarrow{V_j} \middle| \overrightarrow{V_i}\right) &= R_{n+1}^2\,R_j\,R_i(\rho_j\,\rho_i + \rho_{n+1}\,\rho_i + \rho_{n+1}\,\rho_j - \rho_{n+1}^2) = \\ &= \frac{(\rho_{n+1} + \rho_i)\,(\rho_{n+1} + \rho_j) - 2\,\rho_{n+1}^2}{\rho_i\,\rho_j\,\rho_{n+1}^2}. \end{aligned}$$

On a aussi, pour tout $i \in [\![1, n]\!]$,

$$\left(\overrightarrow{V_i} \middle| \overrightarrow{V_i}\right) = d_{n+1,i}^2 = (R_{n+1} + R_i)^2 = R_{n+1}^2\,R_i^2(\rho_i + \rho_{n+1})^2 = \frac{(\rho_{n+1} + \rho_i)^2}{}$$

On voit donc que pour tout $(i,j) \in [\![1,n]\!]^2$, $(\overrightarrow{V_i}|\overrightarrow{V_j}) = x_{i,j}$ (cf. b)).

Le déterminant $|x_{i,j}|_{(i,j)\in[\![1,n]\!]^2}$ est donc le déterminant de Gram des n vecteurs $(V_1,\ldots,V_n)$, dans l'espace euclidien E de dimension $n-1$. La famille $(V_1,\ldots,V_n)$ est liée et son déterminant de Gram est nul (si V_n par exemple est combinaison linéaire des vecteurs précédents, alors la dernière colonne du déterminant est combinaison linéaire des colonnes précédentes). En appliquant l'égalité trouvée dans le b), nous en déduisons :

$$\left(\sum_{i=1}^{n+1}\rho_i\right)^2 = (n-1)\sum_{i=1}^{n+1}\rho_i^2 \ .$$

Chapitre XIV

ÉQUATIONS LINÉAIRES SUR UN CORPS

§ XIV.1 LANGAGE DE LA GÉOMÉTRIE AFFINE DANS UN ESPACE VECTORIEL

Exercice 3 :

> On suppose K de caractéristique $\neq 2$. Soit $\mathscr{V}$ une partie non vide d'un K-ev E. Pour que $\mathscr{V}$ soit une s.v.l.a. de E, il faut et il suffit que :
>
> $$(\forall (x,y) \in \mathscr{V}^2,\ \forall \lambda \in K) \quad \lambda x + (1-\lambda) y \in \mathscr{V}\,. \blacksquare$$

Ecartons le cas où $\mathscr{V}$ est vide. Soit $x_0 \in \mathscr{V}$, montrons que la partie de E définie par $V = \{x - x_0,\ x \in \mathscr{V}\}$, est un sous-$K$-ev de E.

La partie V n'est pas vide car $0_E = x_0 - x_0 \in V$.
Soit $u \in V$ et $\lambda \in K$. Ecrivons $u = x - x_0$, où $x \in \mathscr{V}$. Comme $y = \lambda x + (1-\lambda) x_0 \in \mathscr{V}$, nous en déduisons $\lambda u = y - x_0 \in V$. La partie V est donc stable par les homothéties.
Soient u et v dans V, il existe des vecteurs x et y dans $\mathscr{V}$ tels que $u = x - x_0$ et $v = y - x_0$. Comme $z = \dfrac{x+y}{2} \in \mathscr{V}$, nous en déduisons $\dfrac{u+v}{2} = z - x_0 \in V$, donc, d'après ce qui précède, $u + v = 2\dfrac{u+v}{2} \in V$.

La partie V de E est donc un sous-K-ev de E, et comme $\mathscr{V} = x_0 + V$, $\mathscr{V}$ est une sous-variété linéaire affine de E.

§ XIV.2 ÉQUATIONS LINÉAIRES SUR UN CORPS ; CAS D'UN SYSTÈME DE CRAMER

Exercice 4 :

> Le corps de base est quelconque. Soit $n \in \mathbb{N}$ $(n \geqslant 2)$, et trois familles $(\alpha_1, \ldots, \alpha_n)$, $(\beta_1, \ldots, \beta_n)$ et $(b_1, \ldots, b_n$

On suppose les (α_i) tous distincts, les (β_j) tous distincts et $(\forall (i,j) \in [\![1,n]\!]^2)\ \alpha_i + \beta_j \neq 0$. Résoudre le système linéaire

$$\sum_{j=1}^{n} \frac{1}{\alpha_i + \beta_j} x_j = b_i \ ;\ 1 \leqslant i \leqslant n\,,$$

et en déduire un calcul de la matrice inverse de $M = \left[\frac{1}{\alpha_i + \beta_j}\right]$.

Application : Soit $M = \left[\frac{1}{i+j-1}\right]$. Vérifier que M^{-1} est à coefficients dans $\mathbb{Z}$. ■

On sait que le système est de Cramer (cf. exercice 26, §XIII.5). Les scalaires $(b_1, \ldots, b_n)$ étant donnés, il existe donc un et un seul n-uplet $(x_1, \ldots, x_n)$ solution du système d'équations. Soit $P \in K_{n-1}[X]$ tel que pour tout $j \in [\![1,n]\!]$ on ait l'égalité :

$$P(\beta_j) = x_j \prod_{k \neq j} (\beta_j - \beta_k)\ .$$

Il existe un et un seul polynôme P qui vérifie ces conditions (polynôme d'interpolation de Lagrange), c'est le polynôme :

$$P = \sum_{j=1}^{n} x_j \prod_{k \neq j} (X - \beta_k)\ .$$

Nous en déduisons :

$$\frac{P(X)}{\prod_{k=1}^{n} (X - \beta_k)} = \sum_{j=1}^{n} \frac{x_j}{X - \beta_j}\ .$$

Pour tout $i \in [\![1,n]\!]$, ceci est vrai en $-\alpha_i$, d'où :

$$\frac{P(-\alpha_i)}{\prod_{k=1}^{n} (-\alpha_i - \beta_k)} = -\sum_{j=1}^{n} \frac{x_j}{\alpha_i + \beta_j} = -b_i\ ,$$

d'où, pour tout $i \in [\![1,n]\!]$,

$$P(-\alpha_i) = b_i\,(-1)^{n-1} \prod_{k=1}^{n} (\alpha_i + \beta_k)\ .$$

D'après le théorème d'interpolation de Lagrange, ces relations déterminent le polynôme P ; on a l'égalité :

$$P(X) = \sum_{i=1}^{n} P(-\alpha_i) \prod_{h \neq i} \frac{X + \alpha_h}{\alpha_h - \alpha_i}\ ,$$

soit par conséquent :

$$P(X) = \sum_{i=1}^{n} \left(b_i \, (-1)^{n-1} \prod_{k=1}^{n} (\alpha_i + \beta_k) \prod_{h \neq i} \frac{X + \alpha_h}{\alpha_h - \alpha_i} \right) .$$

Ceci nous permet de trouver les valeurs des x_j , en fonction des b_i . En effet, pour tout $j \in [\![1, n]\!]$:

$$x_j = \frac{P(\beta_j)}{\prod\limits_{k \neq j} (\beta_j - \beta_k)} = \sum_{i=1}^{n} (-1)^{n-1} \, b_i \frac{\prod\limits_{k=1}^{n} (\alpha_i + \beta_k) \prod\limits_{h \neq i} (\beta_j + \alpha_h)}{\prod\limits_{k \neq j} (\beta_j - \beta_k) \prod\limits_{h \neq i} (\alpha_h - \alpha_i)} ,$$

soit encore :

$$x_j = \sum_{i=1}^{n} \frac{b_i}{\alpha_i + \beta_j} \frac{\prod\limits_{k=1}^{n} (\alpha_i + \beta_k) \prod\limits_{h=1}^{n} (\beta_j + \alpha_h)}{\prod\limits_{k \neq j} (\beta_k - \beta_j) \prod\limits_{h \neq i} (\alpha_h - \alpha_i)} .$$

Le coefficient (j, i) de la matrice M^{-1} est donc le scalaire :

$$\frac{\prod\limits_{k=1}^{n} (\alpha_i + \beta_k) \prod\limits_{h=1}^{n} (\beta_j + \alpha_h)}{\prod\limits_{k \neq j} (\beta_k - \beta_j) \prod\limits_{h \neq i} (\alpha_h - \alpha_i)} \frac{1}{\alpha_i + \beta_j} .$$

Dans le cas particulier où pour tout $i \in [\![1, n]\!]$, $\alpha_i = i$, et pour tout $j \in [\![1, n]\!]$, $\beta_j = j - 1$, nous obtenons les résultats suivants :
Pour tout i fixé :

$$\prod_{k=1}^{n} (\alpha_i + \beta_k) = i \, (i+1) \ldots (i+n-1) ,$$

et :

$$\prod_{h \neq i} (\alpha_h - \alpha_i) = \prod_{h \neq i} (h - i) = (1-i) \ldots (-1) \, 1 \ldots (n-i) = (-1)^{i-1} (i-1)! \, (n-i)! .$$

Pour tout j fixé :

$$\prod_{h=1}^{n} (\beta_j + \alpha_h) = j \, (j+1) \ldots (j+n-1) ,$$

et :

$$\prod_{k \neq j} (\beta_k - \beta_j) = \prod_{k \neq j} (k - j) = (-1)^{j-1} (j-1) \, ! \, (n-j) \, ! .$$

Le coefficient $u_{j,i}$ de la matrice M^{-1} est donc le rationnel :

$$u_{j,i} = \frac{i\,(i+1)\dots(i+n-1)\times j(j+1)\dots(j+n-1)}{1.2\dots(i-1)\times 1.2\dots(n-i)\times 1.2\dots(j-1)\times 1.2\dots(n-j)}\,\frac{(-1)^{i+j}}{i+j-1}\,.$$

En permutant les facteurs au numérateur, de façon à faire apparaître des coefficients du binôme, on obtient l'égalité :

$$u_{j,i} = \frac{j(j+1)\dots(j+i-2)}{1.2\dots(i-1)}\,(j+i-1)\,\frac{(j+i)\dots(j+n-1)}{1.2\dots(n-i)}\times$$
$$\times\,\frac{i(i+1)\dots(i+j-2)}{1.2\dots(j-1)}\,(i+j-1)\,\frac{(i+j)\dots(i+n-1)}{1.2\dots(n-j)}\,\frac{(-1)^{i+j}}{i+j-1}\,.$$

On voit que dans chacune des quatre fractions, le nombre de facteurs au numérateur est égal au nombre de facteurs au dénominateur. Le résultat est donc entier, plus précisément :

$$u_{j,i} = (-1)^{i+j}\,(i+j-1)\binom{j+i-2}{i-1}\binom{j+n-1}{n-i}\binom{i+j-2}{j-1}\binom{i+n-1}{n-j}\,.$$

Exercice 5 :

Le corps K est une extension de $\mathbb{C}$. On donne $n \in \mathbb{N}$ ($n \geqslant 2$).

a) On considère la matrice circulante (cf. §XIII.5, exemple 4) :

$$M = \Gamma(a_0,\dots,a_{n-1}) = \left[a_{\overline{j-i}}\right]_{(i,j)\in[\![1,n]\!]^2},$$

où $(a_0,\dots,a_{n-1}) \in K^n$. On suppose $\det(M) \neq 0$. Inverser M par la méthode du système linéaire.

b) Appliquer aux cas : $K = \mathbb{C}(X)$ et $a_i = X^i$ ($0 \leqslant i \leqslant n-1$), et K extension quelconque de $\mathbb{C}$ avec $a_k = \alpha + k\beta$, α et β donnés ($0 \leqslant k \leqslant n-1$). ■

a) Désignons par f l'endomorphisme de K^n dont la matrice dans la base canonique $\mathcal{B}$ est la matrice M.
Soit $(x_1,\dots,x_n) \in K^n$, posons $(y_1,\dots,y_n) = f(x_1,\dots,x_n)$. On a donc pour tout $i \in [\![1,n]\!]$ l'égalité :

$$y_i = \sum_{j=1}^{n} a_{\overline{j-i}}\,x_j\,.$$

Soit $\zeta \in \mu_n$ quelconque, pour tout $(i,j) \in [\![1,n]\!]^2$, on voit que $\zeta^{\overline{j-i}} = \zeta^{j-i}$. On a donc l'égalité :

$$\sum_{i=1}^{n} \zeta^{1-i} y_i = \sum_{(i,j)\in[\![1,n]\!]^2} a_{\overline{j-i}} \zeta^{j-i} \zeta^{1-j} x_j =$$

$$= \sum_{j=1}^{n} \left(\sum_{i=1}^{n} a_{\overline{j-i}} \zeta^{\overline{j-i}} \right) \zeta^{1-j} x_j \ .$$

Comme pour tout $j \in [\![1,n]\!]$ fixé, l'application $i \mapsto \overline{j-i}$ est une bijection $[\![1,n]\!] \to [\![0,n-1]\!]$, nous en déduisons :

$$\sum_{i=1}^{n} \zeta^{1-i} y_i = \sum_{j=1}^{n} \left(\sum_{h=0}^{n-1} a_h \zeta^h \right) \zeta^{1-j} x_j = Q(\zeta) \sum_{j=1}^{n} \zeta^{1-j} x_j \ ,$$

en posant $Q(X) = \sum_{h=0}^{n-1} a_h X^h$.

S'il existait $\zeta \in \mu_n$ tel que $Q(\zeta) = 0$, alors pour tout $(x_1, \ldots, x_n) \in K^n$, le n-uplet $(y_1, \ldots, y_n) = f(x_1, \ldots, x_n)$ vérifierait l'équation $\sum_{i=1}^{n} \zeta^{1-i} y_i = 0$. L'application linéaire f ne serait donc pas bijective, et sa matrice M ne serait pas inversible. Nous en déduisons que pour tout $\zeta \in \mu_n$ $Q(\zeta) \neq 0$, et que :

$$\sum_{j=1}^{n} \zeta^{1-j} x_j = \frac{1}{Q(\zeta)} \sum_{i=1}^{n} \zeta^{1-i} y_i \ .$$

Pour tout $h \in \mathbb{Z}$ posons $S_h = \sum_{\zeta\in\mu_n} \zeta^h$. On sait que $S_h = 0$ si h n'est pas divisible par n, et que $S_h = n$ si h est divisible par n. Nous poserons ici, pour tout $(i,j) \in \mathbb{Z}^2$, $\delta_{i,j}^{(n)} = 0$ si $i \not\equiv j \bmod n$, et $\delta_{i,j}^{(n)} = 1$ si $i \equiv j \bmod n$. On a pour tout $k \in [\![1,n]\!]$ l'égalité :

$$\sum_{\zeta\in\mu_n} \zeta^{k-1} \left(\sum_{j=1}^{n} \zeta^{1-j} x_j \right) = \sum_{j=1}^{n} \left(\sum_{\zeta\in\mu_n} \zeta^{k-j} \right) x_j = n\, x_k \ .$$

Par conséquent, pour tout $k \in [\![1,n]\!]$:

$$x_k = \frac{1}{n} \sum_{\zeta\in\mu_n} \frac{\zeta^{k-1}}{Q(\zeta)} \left(\sum_{i=1}^{n} \zeta^{1-i} y_i \right) = \frac{1}{n} \sum_{i=1}^{n} \left(\sum_{\zeta\in\mu_n} \frac{\zeta^{k-i}}{Q(\zeta)} \right) y_i \ .$$

Le coefficient d'indice (k,i) la matrice M^{-1} est donc :

$$\left(M^{-1}\right)_{k,i} = \frac{1}{n} \sum_{\zeta\in\mu_n} \frac{\zeta^{k-i}}{Q(\zeta)} \ .$$

b) On suppose que pour tout $h \in [\![0, n-1]\!]$, $a_h = X^h$.
Pour tout $\zeta \in \mu_n$ l'égalité :

$$Q(\zeta) = 1 + \zeta X + \zeta^2 X^2 + \ldots + \zeta^{n-1} X^{n-1} = \frac{\zeta^n X^n - 1}{\zeta X - 1} = \frac{X^n - 1}{\zeta X - 1} .$$

Pour tout $(k, i) \in [\![1, n]\!]^2$, le coefficient d'indice (k, i) de la matrice M^{-1} est donc :

$$\left(M^{-1}\right)_{k,i} = \frac{1}{n} \sum_{\zeta \in \mu_n} \frac{\zeta^{k-i}(\zeta X - 1)}{X^n - 1} = \frac{\delta^{(n)}_{k+1,i} X - \delta^{(n)}_{k,i}}{X^n - 1} .$$

La matrice dont le terme (k, i) est, pour tout $(k, i) \in [\![1, n]\!]^2$, $\delta^{(n)}_{k+1,i}$, est la matrice :

$$C = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & & & \ddots & 1 \\ 1 & 0 & \ldots & \ldots & 0 \end{bmatrix}$$

Avec cette notation on a l'égalité :

$$M^{-1} = \frac{1}{X^n - 1} (X C - I_n) .$$

On suppose que pour tout $h \in [\![0, n-1]\!]$, $a_h = \alpha + h\beta$.
Pour tout $\zeta \in \mu_n$ on a l'égalité :

$$Q(\zeta) = \alpha + (\alpha + \beta)\zeta + \ldots + \left(\alpha + (n-1)\beta\right)\zeta^{n-1} .$$

Pour $\zeta = 1$, on a $Q(\zeta) = n\alpha + \frac{n(n-1)}{2}\beta$. Nous supposerons $\alpha + \frac{n-1}{2}\beta \neq 0$.
En dérivant l'identité :

$$1 + X + \ldots + X^{n-1} = \frac{X^n - 1}{X - 1} ,$$

on obtient :

$$1 + 2X + \ldots + (n-1)X^{n-2} = \frac{(n-1)X^n - nX^{n-1} + 1}{(X-1)^2} ,$$

d'où :

$$X + 2X^2 + \ldots + (n-1)X^{n-1} = \frac{(n-1)X^{n+1} - nX^n + X}{(X-1)^2}$$

Nous en déduisons que pour tout $\zeta \in \mu_n$, $\zeta \neq 1$:

$$Q(\zeta) = \alpha \frac{\zeta^n - 1}{\zeta - 1} + \beta \frac{(n-1)\zeta^{n+1} - n\zeta^n + \zeta}{(\zeta - 1)^2} = \beta \frac{n}{\zeta - 1} .$$

Nous supposerons $\beta \neq 0$. Pour tout $(k,i) \in [\![1,n]\!]^2$, le coefficient (k,i) de la matrice M^{-1} est :

$$\left(M^{-1}\right)_{k,i} = \frac{1}{n} \sum_{\zeta \in \mu_n} \frac{\zeta^{k-i}}{Q(\zeta)} = \frac{1}{n} \left[\frac{1}{Q(1)} + \sum_{\zeta \neq 1} \frac{\zeta^{k-i}(\zeta - 1)}{n\beta} \right] =$$

$$= \frac{1}{n} \left[\frac{1}{Q(1)} + \sum_{\zeta \in \mu_n} \frac{\zeta^{k-i}(\zeta - 1)}{n\beta} \right] = \frac{1}{n} \left[\frac{1}{Q(1)} + \frac{1}{\beta} \left(\delta^{(n)}_{k+1,i} - \delta^{(n)}_{k,i} \right) \right] .$$

Notons $J \in \mathfrak{M}_n(K)$ la matrice dont tous les coefficients sont 1, on voit que :

$$M^{-1} = \frac{1}{n^2} \frac{1}{\alpha + \frac{n-1}{2}\beta} J + \frac{1}{n\beta} (C - I_n) .$$

Exercice 10 :

On considère $\lambda_1, \ldots, \lambda_n$ distincts dans $K \setminus \{0\}$ ($n \geqslant 2$). On posera

$\Lambda = \prod_{i=1}^{n} \lambda_i$, $\Lambda_i = \dfrac{\Lambda}{\lambda_i}$ et on suppose que $D = \Lambda + \sum_{j=1}^{n} \Lambda_j \neq 0$.

a) Résoudre le système linéaire $\sum_{j=1}^{n} (1 + \delta_{i,j}\lambda_i) x_j = A_i$ où la famille $(A_1, \ldots, A_n) \in K^n$ est donnée (δ = symbole de Kronecker). Donner l'inverse de la matrice M du système.

b) Soit X une indéterminée sur K.

On pose $\Phi(X) = \prod_{i=1}^{n} (\lambda_i - X)$ et on note $\mathfrak{D}(X)$ le polynôme obtenu à partir des $\lambda_i + X$ de la même façon que D est obtenu à partir des λ_i. Enfin soit $\Delta(X) = \det[1 + \delta_{i,j}(\lambda_i + X)]$ avec $(i,j) \in [\![1,n]\!]^2$. Montrer que :

$$(\forall i) \quad \Delta(-\lambda_i) = \mathfrak{D}(-\lambda_i) = -\Phi'(\lambda_i) .$$

En déduire $\mathfrak{D}(X) = \Delta(X)$, et en particulier : $\det(M) = D$. Retrouver ce résultat par un calcul direct.

c) En appliquant les formules de Cramer, déduire de ce qui précède la valeur, pour $i \in [\![1,n]\!]$, du détermina

matrice dont les colonnes Γ_j sont $\mathscr{C}_j(M)$ si $j \neq i$ et $\Gamma_i = (A_1, \ldots, A_n)$. ■

a) Nous poserons pour tout $i \in [\![1, n]\!]$, $\mu_i = \frac{1}{\lambda_i}$. Cherchons les n-uplets solutions du système dont la somme est fixée, égale au paramètre s . Les conditions s'écrivent :

$$\begin{array}{llll} \lambda_1 x_1 + & x_1 + \ldots + x_n & = A_1 \\ \lambda_2 x_2 + & x_1 + \ldots + x_n & = A_2 \\ \vdots & \vdots \quad \vdots & \vdots \\ \lambda_n x_n + & x_1 + \ldots + x_n & = A_n \\ & x_1 + \ldots + x_n & = s \end{array}$$

Un système équivalent est le système :

$$\begin{array}{rcl} x_1 & = & \mu_1 A_1 - \mu_1 s \\ x_2 & = & \mu_2 A_2 - \mu_2 s \\ \vdots & = & \vdots \\ x_n & = & \mu_n A_n - \mu_n s \\ x_1 + \ldots + x_n & = & s \end{array}$$

Ce système a des solutions si, et seulement si, le paramètre s vérifie la condition :

$$\sum_{i=1}^{n} \mu_i A_i - \sum_{i=1}^{n} \mu_i \, s = s \ ,$$

soit si, et seulement si :

$$\sum_{i=1}^{n} \mu_i A_i = \left(1 + \sum_{i=1}^{n} \mu_i\right) s \ .$$

On vérifie que :

$$1 + \sum_{i=1}^{n} \mu_i = 1 + \sum_{i=1}^{n} \frac{1}{\lambda_i} = \frac{\Lambda + \sum\limits_{i=1}^{n} \Lambda_i}{\Lambda} = \frac{D}{\Lambda} \neq 0 \ .$$

Le paramètre s prenant la seule valeur possible, on obtient une et une seule solution pour le n-uplet $(x_1, \ldots, x_n)$:

$$(\forall j \in [\![1, n]\!]) \quad x_j = \mu_j A_j - \mu_j \left(\frac{\sum\limits_{i=1}^{n} \mu_i A_i}{1 + \sum\limits_{i=1}^{n} \mu_i} \right) = \frac{1}{\lambda_j} \left(A_j - \frac{\sum\limits_{i=1}^{n} \Lambda_i A_i}{D} \right) \ .$$

On voit donc que le système initial est de Cramer et que sa matrice M est inversible. Pour tout $(j,i) \in [\![1,n]\!]^2$, le coefficient (j,i) de la matrice M^{-1}, est :

$$u_{j,i} = \frac{1}{\lambda_j}\left(\delta_{i,j} - \frac{\Lambda_i}{D}\right) .$$

b) On obtient facilement l'expression du polynôme $\mathcal{D}(X)$:

$$\mathcal{D}(X) = \prod_{i=1}^{n}(\lambda_i + X) + \sum_{j=1}^{n}\prod_{h\neq j}(\lambda_h + X) .$$

On a donc pour tout $i \in [\![1,n]\!]$ l'égalité :

$$\mathcal{D}(-\lambda_i) = \prod_{h\neq i}(\lambda_h - \lambda_i) .$$

D'autre part, par dérivation on obtient :

$$\Phi'(X) = -\sum_{j=1}^{n}\prod_{h\neq j}(\lambda_h - X) ,$$

d'où, pour tout $i \in [\![1,n]\!]$,

$$\mathcal{D}(-\lambda_i) = \prod_{h\neq i}(\lambda_h - \lambda_i) = -\Phi'(\lambda_i) .$$

Justifions que pour tout $h \in [\![1,n]\!]$, $\Delta(-\lambda_h)$ est le déterminant de la matrice $[1 + \delta_{i,j}(\lambda_i - \lambda_h)]_{(i,j)\in[\![1,n]\!]^2}$. De manière générale le lecteur pourra vérifier que si $\varphi : A \to B$ est un homomorphisme d'anneaux (commutatifs), et $\Phi : \mathfrak{M}_n(A) \to \mathfrak{M}_n(B)$ l'application qui à $M \in \mathfrak{M}_n(A)$ fait correspondre la matrice dont le coefficient d'indice (i,j) est l'image par φ du coefficient d'indice (i,j) de M (pour tout $(i,j) \in [\![1,n]\!]^2$), Φ est un homomorphisme d'anneaux tel que pour tout $M \in \mathfrak{M}_n(A)$:

$$\varphi(\det_A(M)) = \det_B(\Phi(M)) .$$

On applique ici cette propriété à l'homomorphisme de substitution $K[X] \to K$, $P \mapsto P(-\lambda_h)$.

Soit $\mathcal{B} = (\varepsilon_1, \ldots, \varepsilon_n)$ la base canonique de $\mathfrak{M}_n(K)$, et $V = \sum_{j=1}^{n}\varepsilon_j$. On voit que pour tout $i \in [\![1,n]\!]$, $\Delta(-\lambda_i)$ est le déterminant dans la base $\mathcal{B}$ de la famille de vecteurs colonnes $(V + (\lambda_h - \lambda_i)\,\varepsilon_h)_{h\in[\![1,n]\!]}$. Le vecte

étant V, on peut le retrancher des autres colonnes. On en déduit, pour tout $i \in [\![1, n]\!]$, l'égalité :

$$\Delta(-\lambda_i) =$$
$$\det_{\mathcal{B}}\big((\lambda_1 - \lambda_i)\varepsilon_1, \ldots, (\lambda_{i-1} - \lambda_i)\varepsilon_{i-1}, V, (\lambda_{i+1} - \lambda_i)\varepsilon_{i+1}, \ldots, (\lambda_n - \lambda_i)\varepsilon_n\big) ,$$

d'où :

$$\Delta(-\lambda_i) = \det_{\mathcal{B}}(\varepsilon_1, \ldots, \varepsilon_{i-1}, V, \varepsilon_{i+1}, \ldots, \varepsilon_n) \prod_{h \neq i}(\lambda_h - \lambda_i) =$$
$$= \prod_{h \neq i}(\lambda_h - \lambda_i) = D(-\lambda_i) .$$

Les polynômes $\mathcal{D}$ et Δ coïncidant en les n scalaires $(-\lambda_1, \ldots, -\lambda_n)$ distincts, leur différence est divisible par le polynôme $(X + \lambda_1) \ldots (X + \lambda_n)$. Or on remarque que ces deux polynômes sont de degré n, de même coefficient dominant égal à 1. Ils sont donc égaux. En particulier, $\mathcal{D}(0) = D = \Delta(0) = \det(M)$.

On peut retrouver ce résultat directement, sans supposer que les scalaires $(\lambda_1, \ldots, \lambda_n)$ soient distincts et non nuls. En effet, en reprenant les mêmes notations que ci-dessus, on a l'égalité :

$$\det(M) = \det_{\mathcal{B}}(V + \lambda_1 \varepsilon_1, \ldots, V + \lambda_n \varepsilon_n) .$$

En développant ce déterminant par multilinéarité, on obtient 2^n termes dont :

$$\det_{\mathcal{B}}(\lambda_1 \varepsilon_1, \ldots, \lambda_n \varepsilon_n) ,$$

et n termes de la forme ($j \in [\![1, n]\!]$) :

$$\det_{\mathcal{B}}(\lambda_1 \varepsilon_1, \ldots, \lambda_{j-1} \varepsilon_{j-1}, V, \lambda_{j+1} \varepsilon_{j+1}, \ldots, \lambda_n \varepsilon_n) =$$
$$= \Big(\prod_{h \neq j} \lambda_h\Big) \det_{\mathcal{B}}(\varepsilon_1, \ldots, \varepsilon_{j-1}, V, \varepsilon_{j+1}, \ldots, \varepsilon_n) = \prod_{h \neq j} \lambda_h ;$$

tous les autres termes sont nuls, car le déterminant est une forme n-linéaire alternée. On retrouve donc l'égalité :

$$\det(M) = \prod_{i=1}^{n} \lambda_i + \sum_{j=1}^{n} \prod_{h \neq j} \lambda_h .$$

c) D'après les formules de Cramer, si $(x_1, \ldots, x_n)$ est la solution du système de Cramer du *a*), pour tout $j \in [\![1, n]\!]$, $x_j = \dfrac{D_j}{D}$. Nous en dé

tout $j \in [\![1, n]\!]$:

$$D_j = x_j\, D = \frac{D}{\lambda_j}\left(A_j - \frac{\sum_{i=1}^{n} \Lambda_i\, A_i}{D}\right) = \frac{1}{\lambda_j}\left(D\, A_j - \sum_{i=1}^{n} \Lambda_i\, A_i\right) .$$

§ XIV.3 *ÉQUATIONS LINÉAIRES SUR UN CORPS : CAS GÉNÉRAL*

Exercice 7 :

Soit $n \in \mathbb{N}^*$. On considère un système linéaire *de Cramer :*

$$\sum_{j=1}^{n} a_{i,j}\, x_j = b_i \quad 1 \leqslant i \leqslant n ,$$

dont on note $(\alpha_1, \ldots, \alpha_n)$ la solution, et Δ le déterminant. Pour $(c_1, \ldots, c_n) \in K^n$, démontrer que :

$$c_1\, \alpha_1 + \ldots + c_n\, \alpha_n = -\frac{1}{\Delta}\, D \text{ , avec } D = \det \left[\begin{array}{c|c} A & B \\ \hline {}^tC & 0 \end{array}\right] ,$$

où $A = [a_{i,j}] \in \mathfrak{M}_n(K)$, ${}^tC = [c_1, \ldots, c_n]$ et ${}^tB = [b_1, \ldots, b_n]$.

■

Soient $C_1, \ldots, C_n$ les colonnes de la matrice A . Par définition :

$$\alpha_1\, C_1 + \ldots + \alpha_n\, C_n = B .$$

Dans le déterminant D , on peut retrancher de la dernière colonne la combinaison linéaire $\alpha_1\, C'_1, \ldots + \alpha_n\, C'_n$ des n colonnes précédentes. On obtient l'égalité :

$$D = \det \left[\begin{array}{c|c} A & 0 \\ \hline {}^tC & d \end{array}\right] ,$$

où $d = -(\alpha_1\, c_1 + \ldots + \alpha_n\, c_n)$. Nous en déduisons :

$$D = -d \det(A) = -(\alpha_1\, c_1 + \ldots + \alpha_n\, c_n)\, \Delta ,$$

ce qu'il fallait démontrer.

Exercice 10 *(méthode de Frobenius)* :

On donne deux entiers n et p : $1 \leqslant p < n$, et une matrice $M = [a_{i,j}] \in \mathfrak{M}_{p,n}(K)$ supposée de *rang* p. On considère le système linéaire *homogène* de matrice M :

$$(\mathcal{SL}) \quad \sum_{j=1}^{n} a_{i,j}\, x_j = 0 \quad 1 \leqslant i \leqslant p\,.$$

a) Montrer qu'on peut choisir des $(a_{i,j})$ dans K ($p+1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n$) tels que la matrice $N = [a_{i,j}]_{(i,j)\in[\![1,n]\!]^2}$ soit inversible.

b) En supposant choisis de tels $(a_{i,j})$, pour chaque $(i,j) \in [\![p+1,n]\!] \times [\![1,n]\!]$, soit $A_{i,j}$ le cofacteur de $a_{i,j}$ dans N. Démontrer que pour chaque $i \in [\![p+1,n]\!]$, la suite des cofacteurs $S_i = (A_{i,1},\ldots,A_{i,n})$ est une solution de $(\mathcal{SL})$. Montrer que les $(S_i)_{p+1\leqslant i\leqslant n}$ sont linéairement indépendantes dans K^n, et en déduire qu'elles forment *une base* du sous-K-ev des solutions de $(\mathcal{SL})$. ■

a) Pour $i \in [\![1,p]\!]$, notons $L_i = [a_{i,1},\ldots,a_{i,n}] \in \mathfrak{M}_{1,n}(K)$ la i-ième ligne de la matrice M. La matrice M étant de rang p, le rang de la famille $(L_1,\ldots,L_p)$ est p. D'après le théorème de la base incomplète, il existe des matrices lignes $L_{p+1},\ldots,L_n \in \mathfrak{M}_{1,n}(K)$, telles que la famille $(L_i)_{i\in[\![1,n]\!]}$ soit une base du K-ev $\mathfrak{M}_{1,n}(K)$. Notons $N \in \mathfrak{M}_n(K)$ la matrice dont les lignes sont $(L_1,\ldots,L_n)$. Pour tout $(i,j) \in [\![1,p]\!] \times [\![1,n]\!]$, le coefficient d'indice (i,j) de la matrice N est $a_{i,j}$, et la matrice N, étant de rang n (rang de ses lignes), est inversible. La matrice N répond donc aux conditions de l'énoncé.

b) Rappelons que si $\widetilde{N}$ désigne la matrice complémentaire de la matrice N (c'est-à-dire la transposée de la comatrice de N), on a l'égalité (Théorème XIII.4.5) :

$$N\,\widetilde{N} = \det(N)\; I_n\,.$$

Cette égalité s'écrit :

$$(\forall (i,j) \in [\![1,n]\!]^2) \quad a_{i,1}\,A_{j,1} + \ldots + a_{i,n}\,A_{j,n} = \delta_{i,j}\det(N)\,.$$

En particulier, pour tout $i \in [\![1,p]\!]$, et pour tout $j \in [\![p+1,n]\!]$,

$$a_{i,1}\,A_{j,1} + \ldots + a_{i,n}\,A_{j,n} = 0\,.$$

La suite S_j est donc, pour tout $j \in [\![p+1, n]\!]$ solution du système $(\mathcal{SL})$.

Les vecteurs ligne associés aux suites S_j, pour $j \in [\![p+1, n]\!]$ sont les vecteurs ligne d'indices $p+1$ à n de la comatrice de N. Cette matrice étant, par construction de N, inversible, ces vecteurs lignes sont linéairement indépendants, et les suites $(S_j)_{j \in [\![p+1,n]\!]}$ sont par conséquent linéairement indépendantes. Comme la matrice M du système homogène $(\mathcal{SL})$ est de rang p, le sous-K-ev des solutions de ce système est de dimension $n-p$. La famille $(S_j)_{j \in [\![p+1,n]\!]}$ en est donc une base.

Exercice 13 :

Soient (a_1, a_2, a_3, a_4), (b_1, b_2, b_3, b_4) et (c_1, c_2, c_3, c_4) dans $\mathbb{R}^4$ tels que $\operatorname{rg}\begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \end{bmatrix} = 2$ et $(c_1, c_2, c_3, c_4) \neq (0,0,0,0)$.

On considère le système linéaire $(\mathcal{S})$:

$$\begin{cases} (a_2b_3 - a_3b_2)\,x_1 + (a_3b_1 - a_1b_3)\,x_1 + (a_1b_2 - a_2b_1)\,x_3 = c_4 \\ (a_2b_4 - a_4b_2)\,x_1 + (a_4b_1 - a_1b_4)\,x_2 + (a_1b_2 - a_2b_1)\,x_4 = -c_3 \\ (a_3b_4 - a_4b_3)\,x_1 + (a_4b_1 - a_1b_4)\,x_3 + (a_1b_3 - a_3b_1)\,x_4 = c_2 \\ (a_3b_4 - a_4b_3)\,x_2 + (a_4b_2 - a_2b_4)\,x_3 + (a_2b_3 - a_3b_2)\,x_4 = -c_1 \end{cases}.$$

Trouver une CNS d'existence de solutions, et dans la cas où cette condition est vérifiée, donner un système de deux équations équivalent à $\mathcal{S}$. ■

On remarque que ces équations s'écrivent :

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ x_1 & x_2 & x_3 \end{vmatrix} = c_4 \quad , \quad \begin{vmatrix} a_1 & a_2 & a_4 \\ b_1 & b_2 & b_4 \\ x_1 & x_2 & x_4 \end{vmatrix} = -c_3 \ ,$$

$$\begin{vmatrix} a_1 & a_3 & a_4 \\ b_1 & b_3 & b_4 \\ x_1 & x_3 & x_4 \end{vmatrix} = c_2 \quad , \quad \begin{vmatrix} a_2 & a_3 & a_4 \\ b_2 & b_3 & b_4 \\ x_2 & x_3 & x_4 \end{vmatrix} = -c_1 \ .$$

On voit donc que ces conditions sont réalisées si, et seulement si, pour tout $(y_1, y_2, y_3, y_4) \in \mathbb{R}^4$:

$$\begin{vmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \end{vmatrix} = c_1\,y_1 + c_2\,y_2 + c_3\,y_3 + c_4\,y_4 \ .$$

Une condition nécessaire d'existence de solutions est donc visiblement :

$$c_1\,a_1 + c_2\,a_2 + c_3\,a_3 + c_4\,a_4 = 0 \quad \text{et} \quad c_1\,b_1 + c_2\,b_2 + c_3\,b_3 + c$$

Le vecteur (c_1, c_2, c_3, c_4) doit donc être orthogonal à (a_1, a_2, a_3, a_4) et à (b_1, b_2, b_3, b_4), pour la structure euclidienne canonique de $\mathbb{R}^4$. Montrons que ces conditions sont suffisantes en résolvant dans ce cas le système $\mathcal{S}$.

Notons (d_1, d_2, d_3, d_4) les réels tels que pour tout (x_1, x_2, x_3, x_4), on ait l'égalité :

$$\begin{vmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ x_1 & x_2 & x_3 & x_4 \\ c_1 & c_2 & c_3 & c_4 \end{vmatrix} = d_1 x_1 + d_2 x_2 + d_3 x_3 + d_4 x_4 \ ;$$

ces réels sont les cofacteurs relatifs à la troisième ligne de la matrice. Les vecteurs (a_1, a_2, a_3, a_4) et (b_1, b_2, b_3, b_4) sont linéairement indépendants par hypothèse, et le vecteur non nul (c_1, c_2, c_3, c_4) leur est orthogonal. Nous en déduisons que ces trois vecteurs sont linéairement indépendants. Les mineurs de la matrice :

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ c_1 & c_2 & c_3 & c_4 \end{pmatrix} ,$$

ne sont donc pas tous nuls, d'où $(d_1, d_2, d_3, d_4) \neq (0, 0, 0, 0)$. Remarquons que le vecteur (d_1, d_2, d_3, d_4) est par définition orthogonal aux vecteurs (a_1, a_2, a_3, a_4), (b_1, b_2, b_3, b_4) et (c_1, c_2, c_3, c_4) ; les vecteurs (a_1, a_2, a_3, a_4), (b_1, b_2, b_3, b_4), (c_1, c_2, c_3, c_4) et (d_1, d_2, d_3, d_4) sont par conséquent linéairement indépendants, et forment une base de l'espace $\mathbb{R}^4$.

Rappelons que $(x_1, x_2, x_3, x_4) \in \mathbb{R}^4$ est solution de $\mathcal{S}$ si, et seulement si, pour tout $(y_1, y_2, y_3, y_4) \in \mathbb{R}^4$:

$$\begin{vmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \end{vmatrix} = c_1 y_1 + c_2 y_2 + c_3 y_3 + c_4 y_4 \ .$$

Cette égalité est vraie pour tout $(y_1, y_2, y_3, y_4) \in \mathbb{R}^4$ si, et seulement si, elle est vraie pour les vecteurs d'une base de $\mathbb{R}^4$. Notons $\mathcal{B}$ la base canonique de $\mathfrak{M}_{1,4}(\mathbb{R})$, et posons $A = [a_1, a_2, a_3, a_4]$, $B = [b_1, b_2, b_3, b_4]$, $C = [c_1, c_2, c_3, c_4]$, $D = [d_1, d_2, d_3, d_4]$ et $X = [x_1, x_2, x_3, x_4]$. D'après ce qui précède, $(x_1, x_2, x_3, x_4) \in \mathbb{R}^4$ est solution de $\mathcal{S}$ si, et seulement si,

$$\det_{\mathcal{B}}(A, B, X, A) = (C \mid A) \quad , \quad \det_{\mathcal{B}}(A, B, X, B) = (C \mid B),$$
$$\det_{\mathcal{B}}(A, B, X, C) = (C \mid C) \quad , \quad \det_{\mathcal{B}}(A, B, X, D) = (C \mid D) \ .$$

Les deux premières conditions sont par hypothèse vérifiées (C orthogonal à A et à B), le système $\mathcal{S}$ est donc équivalent à un système de deux équations linéaires.

Remarquons que par définition de D, pour tout $X \in \mathfrak{M}_{1,4}(\mathbb{R})$, on a l'égalité : $\det_{\mathcal{B}}(A, B, X, C) = (D \mid X)$. De manière analogue soit $E \in \mathfrak{M}_{1,4}(\mathbb{R})$ tel que pour tout $X \in \mathfrak{M}_{1,4}(\mathbb{R})$, on ait l'égalité :

$$\det_{\mathcal{B}}(A, B, X, D) = (E \mid X) .$$

Cette matrice ligne E est orthogonale à A, B, D, elle appartient donc à la droite engendrée par C. Ecrivons $E = \lambda C$; par définition de E et de D :

$$\det_{\mathcal{B}}(A, B, C, D) = (E \mid C) = \lambda (C \mid C) = -\det_{\mathcal{B}}(A, B, D, C) = -(D \mid D) .$$

Nous en déduisons en particulier : $\lambda \neq 0$. Les deux équations équivalentes à $\mathcal{S}$ s'écrivent alors :

$$(X \mid D) = (C \mid C) \quad \text{et} \quad (E \mid X) = (C \mid D) = 0 ,$$

soit :

$$\begin{array}{rcl} d_1 x_1 + d_2 x_2 + d_3 x_3 + d_4 x_4 & = & c_1^2 + c_2^2 + c_3^2 + c_4^2 \\ c_1 x_1 + c_2 x_2 + c_3 x_3 + c_4 x_4 & = & 0 \end{array}$$

Remarquons enfin que l'ensemble des solutions de ce système équivalent à $\mathcal{S}$ n'est pas vide, car c'est l'intersection de deux hyperplans affines orthogonaux (dans un espace euclidien de dimension 4). Les conditions $(A \mid C) = 0$ et $(B \mid C) = 0$, sont donc bien nécessaires et suffisantes pour que le système $\mathcal{S}$ ait des solutions.

Exercice 14 :

Dans un plan euclidien orienté muni d'un repère orthonormé direct $(O, \vec{i}, \vec{j})$, on donne trois droites D, D' et D'' non concourantes et deux à deux non parallèles, d'équations respectives $u\,x + v\,y + w = 0$, $u'\,x + v'\,y + w' = 0$ et $u''\,x + v''\,y + w'' = 0$. On note A, A', A'' les sommets, définis respectivement par (D', D''), (D'', D) et (D, D'). On pose :

$$W = \begin{vmatrix} u' & v' \\ u'' & v'' \end{vmatrix}, \quad W' = \begin{vmatrix} u'' & v'' \\ u & v \end{vmatrix}, \quad W'' = \begin{vmatrix} u & v \\ u' & v' \end{vmatrix} \text{ et}$$

$$\Delta = \begin{vmatrix} u & v & w \\ u' & v' & w' \\ u'' & v'' & w'' \end{vmatrix} .$$

a) Montrer que l'aire algébrique du triangle $(AA'A'')$ est

$$\frac{1}{2\,W\,W'\,W''}\,\Delta^2 ,$$

(l'aire est comptée positivement si les sommets (A, A', A'') sont parcourus dans le sens direct).

b) Généraliser à $n+1$ hyperplans en position générale d'un espace euclidien de dimension n, et au volume du polyèdre borné qu'ils délimitent. ■

a) Soit

$$M = \begin{pmatrix} u & v & w \\ u' & v' & w' \\ u'' & v'' & w'' \end{pmatrix} .$$

Notons (α, β) les coordonnées de A, (α', β') celles de A' et (α'', β'') celles de A''. On observe l'égalité :

$$\begin{vmatrix} u & v & u\alpha + v\beta + w \\ u' & v' & 0 \\ u'' & v'' & 0 \end{vmatrix} = \begin{vmatrix} u & v & u\alpha + v\beta + w \\ u' & v' & u'\alpha + v'\beta + w' \\ u'' & v'' & u''\alpha + v''\beta + w'' \end{vmatrix} = \Delta .$$

Nous en déduisons :

$$u\alpha + v\beta + w = \frac{\Delta}{W} .$$

On détermine de manière analogue "la valeur en les autres sommets de l'équation du côté opposé" ; on trouve :

$$u'\alpha' + v'\beta' + w' = \frac{\Delta}{W'} \quad \text{et} \quad u''\alpha'' + v''\beta'' + w'' = \frac{\Delta}{W''} .$$

On obtient par conséquent l'égalité matricielle :

$$\begin{pmatrix} u & v & w \\ u' & v' & w' \\ u'' & v'' & w'' \end{pmatrix} \times \begin{pmatrix} \alpha & \alpha' & \alpha'' \\ \beta & \beta' & \beta'' \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} \frac{\Delta}{W} & 0 & 0 \\ 0 & \frac{\Delta}{W'} & 0 \\ 0 & 0 & \frac{\Delta}{W''} \end{pmatrix} ,$$

d'où finalement :

$$\begin{vmatrix} \alpha & \alpha' & \alpha'' \\ \beta & \beta' & \beta'' \\ 1 & 1 & 1 \end{vmatrix} = \frac{\Delta^2}{W\,W'\,W''} .$$

Cette expression est le double de l'aire algébrique du triangle (A, A', A''), puisque :

$$\begin{vmatrix} \alpha & \alpha' & \alpha'' \\ \beta & \beta' & \beta'' \\ 1 & 1 & 1 \end{vmatrix} = \begin{vmatrix} \alpha & \alpha' - \alpha & \alpha'' - \alpha \\ \beta & \beta' - \beta & \beta'' - \beta \\ 1 & 0 & 0 \end{vmatrix} =$$

$$= \begin{vmatrix} \alpha' - \alpha & \alpha'' - \alpha \\ \beta' - \beta & \beta'' - \beta \end{vmatrix} = \det_{(\vec{i},\vec{j})}\left(\overrightarrow{AA'}, \overrightarrow{AA''}\right) .$$

On obtient donc l'égalité de l'énoncé.

b) Soit E un espace euclidien orienté de dimension n muni d'un repère orthonormé direct $(O, e_1, \ldots, e_n)$. Soit pour tout $i \in [\![1, n+1]\!]$, un hyperplan affine H_i d'équation $\sum_{j=1}^{n} u_{i,j}\, x_j + w_i = 0$ dans le repère $(O, e_1, \ldots, e_n)$. On notera M la matrice telle que pour tout $(i,j) \in [\![1, n+1]\!] \times [\![1, n]\!]$, $M_{i,j} = u_{i,j}$, et telle que pour tout $i \in [\![1, n+1]\!]$, $M_{i,n+1} = w_i$; soit :

$$M = \begin{pmatrix} u_{1,1} & \cdots & u_{1,n} & w_1 \\ \vdots & \vdots & \vdots & \vdots \\ u_{n+1,1} & \cdots & u_{n+1,n} & w_{n+1} \end{pmatrix}.$$

Pour tout $i \in [\![1, n+1]\!]$, le cofacteur d'indices $(i, n+1)$ dans la matrice M sera noté W_i. On suppose que pour tout $i \in [\![1, n+1]\!]$, les n hyperplans $(H_h)_{h \neq i}$ se coupent en un point unique A_i. Le déterminant de la matrice du système d'équations dont la solution est le n-uplet des coordonnées de A_i étant le mineur d'indices $(i, n+1)$ dans la matrice M, nous en déduisons que le cofacteur W_i n'est pas nul.

Déterminons maintenant, comme dans le cas où $n = 2$, la valeur en A_i de l'équation de la face opposée H_i, pour tout $i \in [\![1, n+1]\!]$. Notons $(\alpha_{1,i}, \ldots, \alpha_{n,i})$ les coordonnées de A_i. On a l'égalité :

$$\begin{vmatrix} u_{1,1} & \cdots & u_{1,n} & 0 \\ \vdots & \vdots & \vdots & \vdots \\ u_{i-1,1} & \cdots & u_{i-1,n} & 0 \\ u_{i,1} & \cdots & u_{i,n} & \sum_{j=1}^{n} u_{i,j}\, \alpha_j + w_i \\ u_{i+1,1} & \cdots & u_{i+1,n} & 0 \\ \vdots & \vdots & \vdots & \vdots \\ u_{n+1,1} & \cdots & u_{n+1,n} & 0 \end{vmatrix} = \left(\sum_{j=1}^{n} u_{i,j}\, \alpha_j + w_i \right) W_i =$$

$$= \begin{vmatrix} u_{1,1} & \cdots & u_{1,n} & \sum_{j=1}^{n} u_{1,j}\, \alpha_j + w_1 \\ \vdots & \vdots & \vdots & \vdots \\ u_{i-1,1} & \cdots & u_{i-1,n} & \sum_{j=1}^{n} u_{i-1,j}\, \alpha_j + w_{i-1} \\ u_{i,1} & \cdots & u_{i,n} & \sum_{j=1}^{n} u_{i,j}\, \alpha_j + w_i \\ u_{i+1,1} & \cdots & u_{i+1,n} & \sum_{j=1}^{n} u_{i+1,j}\, \alpha_j + w_{i+1} \\ \vdots & \vdots & \vdots & \vdots \\ u_{n+1,1} & \cdots & u_{n+1,n} & \sum_{j=1}^{n} u_{n+1,j}\, \alpha_j + w_{n+1} \end{vmatrix}.$$

Notons $C_1, \dots, C_n, W$ les colonnes de la matrice M, et $\mathcal{B}_0$ la base canonique de $\mathfrak{M}_{n+1,1}(\mathbb{R})$. L'égalité ci-dessus s'écrit :

$$\left(\sum_{j=1}^{n} u_{i,j}\,\alpha_j + w_i\right) W_i = \det_{\mathcal{B}_0}\left(C_1, \dots, C_n, \sum_{j=1}^{n} \alpha_j\, C_j + W\right) =$$
$$= \det_{\mathcal{B}_0}(C_1, \dots, C_n, W) = \det(M) = \Delta\ .$$

Nous en déduisons, pour tout $i \in [\![1, n+1]\!]$, l'égalité :

$$\sum_{j=1}^{n} u_{i,j}\,\alpha_j + w_i = \frac{\Delta}{W_i}\ .$$

Nous obtenons par conséquent l'égalité matricielle :

$$\begin{pmatrix} u_{1,1} & \dots & u_{1,n} & w_1 \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ u_{n+1,1} & \dots & u_{n+1,n} & w_{n+1} \end{pmatrix} \times \begin{pmatrix} \alpha_{1,1} & \dots & \dots & \alpha_{1,n+1} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{n,1} & \dots & \dots & \alpha_{n,n+1} \\ 1 & \dots & \dots & 1 \end{pmatrix} =$$
$$= \mathrm{Diag}\left(\frac{\Delta}{W_1}, \dots, \frac{\Delta}{W_{n+1}}\right)\ .$$

Nous en déduisons :

$$\begin{vmatrix} \alpha_{1,1} & \dots & \dots & \alpha_{1,n+1} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{n,1} & \dots & \dots & \alpha_{n,n+1} \\ 1 & \dots & \dots & 1 \end{vmatrix} = \frac{\Delta^n}{W_1 \dots W_{n+1}}\ .$$

En retranchant la dernière colonne des précédentes dans ce déterminant, nous obtenons, en notant $\mathcal{B} = (e_1, \dots, e_n)$ la base orthonormée utilisée :

$$\frac{\Delta^n}{W_1 \dots W_{n+1}} = \det_{\mathcal{B}}\left(\overrightarrow{A_{n+1}A_1}, \dots, \overrightarrow{A_{n+1}A_n}\right)\ .$$

On démontre en analyse que la valeur absolue de ce déterminant est la mesure du parallélotope engendré par les vecteurs $\left(\overrightarrow{A_{n+1}A_1}, \dots, \overrightarrow{A_{n+1}A_n}\right)$, et que c'est la mesure du convexe engendré par les points $(A_1, \dots, A_{n+1})$, multipliée par $n!$ (cf. Tome 3 § VII.6). La mesure "algébrique" de ce convexe compact est donc :

$$\frac{1}{n!}\,\frac{\Delta^n}{W_1 \dots W_{n+1}}\ .$$

Le lecteur remarquera qu'une transposition sur les sommets change le signe de cette mesure algébrique, et donc qu'une permutation σ sur les sommets multiplie cette mesure par la signature de la permutation : $\varepsilon(\sigma)$.

Exercice 16 :

Discuter sur $\mathbb{C}$, et résoudre, le système d'équations ci-après

$$\begin{cases} x^2 - yz = \alpha \\ y^2 - zx = \beta \\ z^2 - xy = \gamma \end{cases}$$

à trois inconnues x , y , z . ■

Les conditions sont réalisées si, et seulement si, pour tout $(u,v,w) \in \mathbb{C}^3$, on a l'égalité :

$$\begin{vmatrix} x & y & z \\ z & x & y \\ u & v & w \end{vmatrix} = \beta u + \gamma v + \alpha w \ .$$

On en déduit que le triplet (x,y,z) vérifie nécessairement les conditions :

$$\begin{cases} \beta x + \gamma y + \alpha z = 0 \\ \beta z + \gamma x + \alpha y = 0 \end{cases} \quad \text{soit} \quad \begin{cases} \beta x + \gamma y + \alpha z = 0 \\ \gamma x + \alpha y + \beta z = 0 \end{cases}$$

1) Supposons d'abord que la matrice de ce système soit de rang 2. Si (x,y,z) est solution, alors il existe $\lambda \in \mathbb{C}$, tel que :

$$x = \lambda \begin{vmatrix} \gamma & \alpha \\ \alpha & \beta \end{vmatrix} \quad y = \lambda \begin{vmatrix} \alpha & \beta \\ \beta & \gamma \end{vmatrix} \quad z = \lambda \begin{vmatrix} \beta & \gamma \\ \gamma & \alpha \end{vmatrix} \ .$$

Un tel triplet est solution si, et seulement si :

$$\begin{aligned} \lambda^2\big((\gamma\beta - \alpha^2)^2 - (\alpha\gamma - \beta^2)(\beta\alpha - \gamma^2)\big) &= \alpha \ , \\ \lambda^2\big((\alpha\gamma - \beta^2)^2 - (\beta\alpha - \gamma^2)(\gamma\beta - \alpha^2)\big) &= \beta \ , \\ \lambda^2\big((\beta\alpha - \gamma^2)^2 - (\gamma\beta - \alpha^2)(\alpha\gamma - \beta^2)\big) &= \gamma \ . \end{aligned}$$

En développant on trouve :

$$\begin{aligned} \lambda^2\,\alpha\,(\alpha^3 + \beta^3 + \gamma^3 - 3\,\alpha\beta\gamma) &= \alpha \ , \\ \lambda^2\,\beta\,(\alpha^3 + \beta^3 + \gamma^3 - 3\,\alpha\beta\gamma) &= \beta \ , \\ \lambda^2\,\gamma\,(\alpha^3 + \beta^3 + \gamma^3 - 3\,\alpha\beta\gamma) &= \gamma \ . \end{aligned}$$

Comme le triplet (α,β,γ) n'est pas nul la condition s'écrit :

$$\lambda^2\big(\alpha^3 + \beta^3 + \gamma^3 - 3\,\alpha\beta\gamma\big) = 1 \ .$$

On peut remarquer que :

$$\alpha^3+\beta^3+\gamma^3-3\,\alpha\,\beta\,\gamma=\begin{vmatrix}\alpha & \beta & \gamma\\ \gamma & \alpha & \beta\\ \beta & \gamma & \alpha\end{vmatrix}=(\alpha+\beta+\gamma)\,(\alpha+\mathrm{j}\,\beta+\mathrm{j}^2\,\gamma)(\alpha+\mathrm{j}^2\,\beta+\mathrm{j}\,\gamma)\,.$$

Si ce déterminant est nul, il n'y a pas de solutions, et s'il est non nul, il y a deux solutions opposées pour le triplet (x,y,z).

2) Supposons maintenant que la matrice $\begin{pmatrix}\beta & \gamma & \alpha\\ \gamma & \alpha & \beta\end{pmatrix}$ soit de rang 1 (d'où $\alpha^3+\beta^3+\gamma^3-3\,\alpha\,\beta\,\gamma=0$). Il existe donc un complexe $\lambda\neq 0$ tel que $\gamma=\lambda\,\beta$, $\alpha=\lambda\,\gamma$ et $\beta=\lambda\,\alpha$. On voit que $\lambda^3=1$, et que le triplet (α,β,γ) est de la forme $\alpha\,(1,\lambda,\lambda^2)$, α étant un complexe non nul. Inversement la matrice est bien de rang 1 dans ce cas.

Les équations s'écrivent alors :

$$x^2-y\,z=\alpha\;;\quad y^2-z\,x=\lambda\,\alpha\;;\quad z^2-x\,y=\lambda^2\,\alpha\,.$$

Posons $y'=\lambda\,y$ et $z'=\lambda^2\,z$, d'où $y=\lambda^2\,y'$ et $z=\lambda\,z'$. Les conditions s'écrivent :

$$x^2-y'\,z'=y'^2-z'\,x=z'^2-x\,y'=\alpha\,.$$

On est donc ramené au cas où $\lambda=1$. Résolvons le système dans ce cas. Un système équivalent est alors le système :

$$\begin{aligned}&x^2-y\,z+y^2-z\,x+z^2-x\,y=3\,\alpha\\ &(x^2-y\,z)-(y^2-z\,x)=(x-y)(x+y+z)=0\\ &(x^2-y\,z)-(z^2-x\,y)=(x-z)(x+y+z)=0\,.\end{aligned}$$

On a donc nécessairement $x+y+z=0$ (sinon $x=y=z$ et $\alpha=0$). Le triplet (x,y,z) est donc solution si, et seulement si, il vérifie les deux conditions :

$$\begin{aligned}&x+y+z=0\\ &x^2-y\,z+y^2-z\,x+z^2-x\,y=(x+\mathrm{j}\,y+\mathrm{j}^2\,z)(x+\mathrm{j}^2\,y+\mathrm{j}\,z)=3\alpha\,.\end{aligned}$$

En notant $\sigma_1=x+y+z$ et $\sigma_2=x\,y+y\,z+z\,x$, ces conditions s'écrivent aussi : $\sigma_1=0$ et $\sigma_2=-\alpha$. Les solutions du système sont donc les listes de zéros des polynômes de la forme $X^3-\alpha\,X+\mu$, où $\mu\in\mathbb{C}$.

Reprenons la discussion générale de ce cas. D'après ce qui précède, λ étant un complexe tel que $\lambda^3=1$, le triplet (x,y,z) est solution du système :

$$x^2-y\,z=\alpha\;;\quad y^2-z\,x=\lambda\,\alpha\;;\quad z^2-x\,y=\lambda^2\,\alpha\,,$$

si, et seulement si,

$$x + \lambda y + \lambda^2 z = 0 \quad \text{et} \quad (x + \mathrm{j}\,\lambda y + \mathrm{j}^2\lambda^2 z)(x + \mathrm{j}^2\lambda y + \mathrm{j}\,\lambda^2 z) = 3\alpha\ .$$

Posons $\mu = \mathrm{j}\,\lambda$ et $\nu = \mathrm{j}^2\,\lambda$, de telle sorte que λ, μ, ν soient les trois racines cubiques de 1 ; avec ces notations, on obtient la condition équivalente :

$$x + \lambda y + \lambda^2 z = 0 \quad \text{et} \quad (x + \mu y + \mu^2 z)(x + \nu y + \nu^2 z) = 3\alpha\ .$$

Posons $x' = x + \lambda y + \lambda^2 z$, $y' = x + \mu y + \mu^2 z$ et $z' = x + \nu y + \nu^2 z$; x', y', z' sont les coordonnées du triplet (x, y, z) dans une certaine base de $\mathbb{C}^3$, et l'ensemble des solutions du système est l'ensemble des triplets (x, y, z) tels que :

$$x' = 0 \quad \text{et} \quad y'\,z' = 3\alpha\ .$$

L'ensemble des solutions est donc, pour chacune des 3 valeurs possibles de λ, une conique.

3) Supposons maintenant $\alpha = \beta = \gamma = 0$. Le triplet $(x, y, z) \in \mathbb{C}^3$ est solution du système si, et seulement si la matrice $\begin{pmatrix} x & y & z \\ z & x & y \end{pmatrix}$ n'est pas de rang 2. On a vu (début de la discussion du cas 2)) que l'ensemble des solutions est la réunion des droites vectorielles engendrées par les vecteurs $(1, 1, 1)$, $(1, \mathrm{j}, \mathrm{j}^2)$, $(1, \mathrm{j}^2, \mathrm{j})$. Ces trois vecteurs sont linéairement indépendants (déterminant de Vandermonde).

Chapitre XV

RÉDUCTION D'ENDOMORPHISMES OU DE MATRICES CARRÉES

§ XV.1 *VALEURS PROPRES ET POLYNÔME CARACTÉRISTIQUE*

Exercice 1 :

Calculer les polynômes caractéristiques des matrices suivantes, le corps de base étant $\mathbb{C}$.

c) $M = \begin{bmatrix} a^2 & a\,b & a\,b & b^2 \\ a\,b & a^2 & b^2 & a\,b \\ a\,b & b^2 & a^2 & a\,b \\ b^2 & a\,b & a\,b & a^2 \end{bmatrix}$

f) $M = \Gamma(a_0, \ldots, a_{n-1}) = \begin{bmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ a_{n-1} & a_0 & \ldots & a_{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ a_1 & a_2 & \ldots & a_0 \end{bmatrix}$.

g) $M = \begin{bmatrix} 0 & \ldots & \ldots & 0 & a_n \\ \vdots & & & \vdots & a_{n-1} \\ \vdots & & & \vdots & \vdots \\ 0 & \ldots & \ldots & 0 & a_2 \\ a_n & a_{n-1} & \ldots & a_2 & a_1^2 \end{bmatrix}$. ■

c) Introduisons la matrice carrée $A = \begin{bmatrix} a & b \\ b & a \end{bmatrix}$. La matrice de l'énoncé s'écrit :

$$M = \left[\begin{array}{c|c} a\,A & b\,A \\ \hline b\,A & a\,A \end{array}\right].$$

On remarque l'égalité matricielle (produits par blocs) :

$$\left[\begin{array}{c|c} a\,A - X\,I_2 & -b\,A \\ \hline 0 & I_2 \end{array}\right] \times \left[\begin{array}{c|c} a\,A - X\,I_2 & b\,A \\ \hline b\,A & a\,A - X\,I_2 \end{array}\right] =$$

$$= \left[\begin{array}{c|c} (a\,A - X\,I_2)^2 - b^2\,A^2 & 0 \\ \hline b\,A & a\,A - X\,I_2 \end{array}\right] .$$

Nous en déduisons :

$$\chi_{a\,A}(X)\ \chi_M(X) = \det\left((a\,A - X\,I_2)^2 - b^2\,A^2\right)\ \chi_{a\,A}(X) ,$$

d'où :

$$\chi_M(X) = \det\left((a\,A - X\,I_2)^2 - b^2\,A^2\right) =$$
$$= \det(a\,A - X\,I_2 - b\,A)\ \det(a\,A - X\,I_2 + b\,A) .$$

De manière générale, si $(u, v) \in \mathbb{C}^2$, on a l'égalité :

$$\det\begin{bmatrix} u - X & v \\ v & u - X \end{bmatrix} = (u - X)^2 - v^2 = (u + v - X)(u - v - X) .$$

On obtient facilement :

$$\chi_M(X) = \left((a + b)^2 - X\right)\left(a^2 - b^2 - X\right)^2\left((b - a)^2 - X\right) .$$

f) On voit que le déterminant de cette matrice circulante est le déterminant de la matrice circulante $\Gamma(a_0 - X, a_1, \ldots, a_{n-1}) \in \mathfrak{M}_n(\mathbb{C}[X])$. D'après l'exemple 4 du § XIII.5, ce déterminant est :

$$\chi_M(X) = \prod_{j=0}^{n-1}\left(a_0 - X + \zeta^j\,a_1 + \zeta^{2\,j}\,a_2 + \ldots + \zeta^{(n-1)\,j}\,a_{n-1}\right) ,$$

où ζ est une racine primitive n-ième de 1.

g) Soient μ et ν deux éléments du corps de base. Introduisons les matrices :

$$M = \begin{bmatrix} 0 & a_n \\ \vdots & \vdots \\ \vdots & \vdots \\ 0 & a_2 \\ 1 & \mu \end{bmatrix} \quad \text{et} \quad N = \begin{bmatrix} a_n & \ldots & \ldots & a_2 & \nu \\ 0 & \ldots & \ldots & 0 & 1 \end{bmatrix} .$$

Nous utiliserons le résultat de l'exercice 3, qui a été démontré sous une forme légèrement différente dans la résolution de l'exercice 25 du §XII.5 ; nous obtenons :

$$\chi_{MN}(X) = (-1)^{n-2}\, X^{n-2}\ \chi_{NM}(X)\ .$$

La matrice MN est :

$$\begin{bmatrix} 0 & a_n \\ \vdots & \vdots \\ \vdots & \vdots \\ 0 & a_2 \\ 1 & \mu \end{bmatrix} \times \begin{bmatrix} a_n & \dots & \dots & a_2 & \nu \\ 0 & \dots & \dots & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & \dots & \dots & 0 & a_n \\ \vdots & & & \vdots & a_{n-1} \\ \vdots & & & \vdots & \vdots \\ 0 & \dots & \dots & 0 & a_2 \\ a_n & a_{n-1} & \dots & a_2 & \nu+\mu \end{bmatrix}\ .$$

La matrice NM s'écrit :

$$\begin{bmatrix} a_n & \dots & \dots & a_2 & \nu \\ 0 & \dots & \dots & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 0 & a_n \\ \vdots & \vdots \\ \vdots & \vdots \\ 0 & a_2 \\ 1 & \mu \end{bmatrix} = \begin{bmatrix} \nu & \sum_{i=2}^{n} a_i^2 + \nu\mu \\ 1 & \mu \end{bmatrix}\ .$$

Nous en déduisons ;

$$\chi_{MN}(X) = (-1)^{n-2}\, X^{n-2}\ \left(X^2 - (\nu+\mu)\, X - (a_2^2 + \dots + a_n^2)\right)\ .$$

Dans le cas particulier de l'énoncé, en prenant par exemple $\nu = a_1^2$ et $\mu = 0$, on obtient le polynôme caractéristique :

$$(-1)^{n-2}\, X^{n-2}\ \left(X^2 - a_1^2\, X - (a_2^2 + \dots + a_n^2)\right)\ .$$

Exercice 2 :

Soit $n \in \mathbb{N}^*$. On donne $(a_1, \dots, a_n)$ et $(b_1, \dots, b_n)$ dans $\mathbb{R}^n$ tels que $a_1 < a_2 < \dots < a_n$ et $(\forall i)\ b_i > 0$. Montrer que le polynôme caractéristique de la matrice

$$M = \begin{bmatrix} a_1+b_1 & b_1 & \dots & b_1 \\ b_2 & a_2+b_2 & \dots & b_2 \\ \vdots & \vdots & \ddots & \vdots \\ b_n & b_n & \dots & a_n+b_n \end{bmatrix}$$

est dissocié et à facteurs simples dans $\mathbb{R}[X]$. ■

Notons $\mathcal{B} = (\varepsilon_1, \ldots, \varepsilon_n)$ la base canonique du $\mathbb{R}$-ev $\mathfrak{M}_{1,n}(\mathbb{R})$, et L la matrice ligne $L = \varepsilon_1 + \ldots + \varepsilon_n$. On voit que pour tout $t \in \mathbb{R}$:

$$\det(M - t\,I_n) = \det_{\mathcal{B}}\big((a_1 - t)\,\varepsilon_1 + b_1\,L, \ldots, (a_n - t)\,\varepsilon_n + b_n\,L\big)\ .$$

En développant ce déterminant par multilinéarité, et en tenant compte du fait que le déterminant est une fonction alternée, on trouve :

$$\det(M - t\,\mathrm{Id}_E) = \det_{\mathcal{B}}\big((a_1 - t)\,\varepsilon_1, \ldots, (a_n - t)\,\varepsilon_n\big) +$$
$$\sum_{i=1}^{n} \det_{\mathcal{B}}\big((a_1 - t)\varepsilon_1, \ldots, (a_{i-1} - t)\varepsilon_{i-1}, b_i\,L, (a_{i+1} - t)\varepsilon_{i+1}, \ldots (a_n - t)\varepsilon_n\big)\ .$$

On obtient facilement l'égalité :

$$\chi_M(t) = \det(M - t\,I_n) = \prod_{i=1}^{n}(a_i - t) + \sum_{j=1}^{n} b_j \prod_{i \neq j}(a_i - t)\ .$$

Remarquons que pour tout $i \in [\![1, n]\!]$,

$$\chi_M(a_j) = b_j(a_1 - a_j)\ldots(a_{j-1} - a_j)\,(a_{j+1} - a_j)\ldots(a_n - a_j)\ ,$$

dont le signe est celui de $(-1)^{j-1}$. D'autre part, le signe de $\chi_M(t)$, si t est plus grand que tous les zéros de ce polynôme, est celui de $(-1)^n$. Le polynôme χ_M a donc un zéro sur l'intervalle $]a_n, +\infty[$, et un zéro sur chaque intervalle $]a_i, a_{i+1}[$, où $i \in [\![1, n-1]\!]$. Le polynôme χ_M a donc au moins n zéros réels distincts, donc exactement n zéros réels simples, puisqu'il est de degré n.

Exercice 7 :

Soit n, p deux entiers $\geqslant 2$. On donne $A_0, A_1, \ldots, A_{p-1}$ dans $\mathfrak{M}_n(\mathbb{C})$ et on considère la matrice *circulante par blocs* $M \in \mathfrak{M}_{np}(\mathbb{C})$:

$$M = \begin{bmatrix} A_0 & A_1 & \ldots & A_{p-1} \\ A_{p-1} & A_0 & \ldots & A_{p-2} \\ \vdots & \vdots & \vdots & \vdots \\ A_1 & A_2 & \ldots & A_0 \end{bmatrix}.$$

a) Calculer $\chi_M(X)$ sous forme d'un produit de p facteurs de degré n (cf. exercice 19 du §XIII.5).

b) Soit $\alpha \in \mathbb{C}$. On suppose $A_k = \alpha^k\,A_0$ pour tout k. Donner une expression de $\chi_M(X)$ sous forme du déterminant d'une matrice carrée d'ordre n. ■

a) Calculons d'abord le déterminant de cette matrice circulante par blocs. Soit ζ un générateur du groupe des racines p-ièmes de 1 dans $\mathbb{C}$. Notons $\Omega \in \mathfrak{M}_{np}(\mathbb{C})$ la matrice composée de p^2 blocs carrés de taille n, dont le bloc d'indice (i,j), pour $(i,j) \in [\![1,p]\!]^2$, est $\zeta^{(i-1)(j-1)} I_n$. La matrice $\Gamma(A_0, A_1, \ldots, A_{p-1}) \times \Omega$ est composée de p^2 blocs carrés de taille n et pour tout $(i,j) \in [\![1,p]\!]^2$, son bloc d'indices (i,j) est :

$$B_{i,j} = \sum_{k=1}^{p} A_{\overline{k-i}} \zeta^{(k-1)(j-1)} I_n .$$

Pour $h \in \mathbb{Z}$, $\overline{h}$ représente ici le reste dans la division euclidienne de h par p. On remarque que pour tout $(i,j) \in [\![1,p]\!]^2$, l'application $k \mapsto \overline{k-i}$ est une bijection $[\![1,p]\!] \to [\![0,p-1]\!]$, et que d'autre part, en notant $q = \overline{k-i}$:

$$\zeta^{(k-1)(j-1)} = \zeta^{(k-i)(j-1)} \zeta^{(i-1)(j-1)} = \zeta^{q(j-1)} \zeta^{(i-1)(j-1)} .$$

Nous en déduisons :

$$B_{i,j} = \sum_{q=0}^{p-1} A_q \zeta^{q(j-1)} \zeta^{(i-1)(j-1)} I_n = \zeta^{(i-1)(j-1)} I_n \sum_{q=0}^{p-1} \zeta^{q(j-1)} A_q .$$

On a donc l'égalité :

$$\Gamma(A_0, A_1, \ldots, A_{p-1}) \times \Omega = \Omega \times \Delta ,$$

où Δ est la matrice diagonale par blocs, dont le bloc diagonal d'indice j est :

$$D_j = \sum_{q=0}^{p-1} \zeta^{q(j-1)} A_q .$$

La matrice Ω est bien inversible : on vérifie facilement que si $\overline{\Omega}$ est sa conjuguée, $\Omega \overline{\Omega} = p I_{np}$.

Nous en déduisons finalement :

$$\det(\Gamma(A_0, A_1, \ldots, A_{p-1})) = \prod_{j=1}^{p} \det\left(\sum_{q=0}^{p-1} \zeta^{q(j-1)} A_q \right) .$$

On voit qu'on obtient le polynôme caractéristique de cette matrice circulante par blocs, en remplaçant le bloc A_0 par le bloc $A_0 - X I_n$ dans cette expression. Le polynôme caractéristique de $M = \Gamma(A_0, A_1, \ldots, A_{p-1})$ est donc :

$$\chi_M(X) = \prod_{j=1}^{p} \det\left(A_0 + \zeta^{j-1} A_1 + \ldots + \zeta^{(p-1)(j-1)} A_{p-1} - X I_n \right) .$$

On a obtenu ainsi une factorisation du polynôme χ_M en p facteurs de degré n, puisque les matrices A_i sont de taille n.

b) Pour tout $j \in [\![1,p]\!]$, posons comme ci-dessus :

$$D_j = A_0 + \zeta^{j-1} A_1 + \ldots + \zeta^{(p-1)(j-1)} A_{p-1} .$$

Dans tous les cas, le polynôme caractéristique de M est le déterminant de la matrice $P \in \mathfrak{M}_n(\mathbb{C}(X))$:

$$P = (D_1 - X I_n)(D_2 - X I_n)\ldots(D_p - X I_n) ,$$

ce qui ne signifie pas que les différents facteurs du produit commutent entre eux. Dans le cas particulier où $A_k = \alpha^k A_0$, les matrices A_k, et les matrices D_j, commutent entre elles. On peut calculer plus précisément P. Soit pour tout $j \in [\![1,p]\!]$, $\lambda_j \in \mathbb{C}$ tel que :

$$D_j = \sum_{q=0}^{p-1} \zeta^{q(j-1)} A_q = \left(\sum_{q=0}^{p-1} \zeta^{q(j-1)} \alpha^q \right) A_0 = \lambda_j A_0 .$$

Supposons d'abord $\alpha^p \neq 1$. Dans ce cas, pour tout $j \in [\![1,p]\!]$, on a l'égalité :

$$\lambda_j = \frac{(\zeta^{j-1}\alpha)^p - 1}{\zeta^{j-1}\alpha - 1} = \frac{\alpha^p - 1}{\zeta^{j-1}\alpha - 1} .$$

Nous en déduisons :

$$P = \prod_{j=1}^{p} \left(\frac{\alpha^p - 1}{\zeta^{j-1}\alpha - 1} A_0 - X I_n \right) =$$

$$= \frac{X^p}{\prod_{j=1}^{p} (\zeta^{j-1}\alpha - 1)} \prod_{j=1}^{p} \left(\frac{\alpha^p - 1}{X} A_0 - (\zeta^{j-1}\alpha - 1) I_n \right) =$$

$$= \frac{(-X)^p}{\prod_{j=1}^{p} (1 - \zeta^{j-1}\alpha)} \prod_{j=1}^{p} \left(\frac{\alpha^p - 1}{X} A_0 + I_n - \zeta^{j-1}\alpha I_n \right) .$$

Nous obtenons donc :

$$P = \frac{(-X)^p}{1 - \alpha^p} \left(\left(\frac{\alpha^p - 1}{X} A_0 + I_n \right)^p - \alpha^p I_n \right) =$$

$$= \frac{(-1)^p}{\alpha^p - 1} \left(\alpha^p X^p I_n - \left((\alpha^p - 1) A_0 + X I_n \right)^p \right.$$

Examinons maintenant le cas où $\alpha^p = 1$, soit $\alpha = \zeta^{-(k-1)}$ où $k \in [\![1,p]\!]$. On voit que pour tout $j \in [\![1,p]\!]$, si $j \neq k$ alors $\lambda_j = 0$, et si $j = k$, $\lambda_j = p$. On a donc ici l'égalité :

$$P = \prod_{j=1}^{p} (\lambda_j A_0 - X I_n) = (-X)^{p-1} (p A_0 - X I_n) .$$

Exercice 9 :

Soit E un K-ev non nul de dimension finie.
a) Soit u et v deux endomorphismes de E *permutables* ($u v = v u$). Montrer que tout sous-espace propre de l'un est stable par l'autre. Si K est algébriquement clos, en déduire que u et v ont au moins un vecteur propre commun.
b) Soit u et $v \in \mathrm{Hom}_K(E)$ et $\beta \in K \setminus \{0\}$ tel que $u v - v u = \beta u$. On suppose K de caractéristique 0. Démontrer que u est nilpotent (*i.e.* $\exists p \in \mathbb{N}^* \mid u^p = 0$).
c) Avec les hypothèses du *b*) mais en supposant K algébriquement clos, démontrer que u et v ont au moins un vecteur propre commun.
d) Sous les hypothèses du *c*), prouver que u et v sont simultanément trigonalisables. ■

a) Soit λ une valeur propre de u, si $x \in E$ est dans l'espace propre de u relatif à la valeur propre λ (noté ici $E_{u,\lambda}$), alors $v(u(x)) = v(\lambda x) = \lambda v(x) = u(v(x))$, donc $v(x) \in E_{u,\lambda}$. L'espace $E_{u,\lambda}$ est par conséquent stable par v. De même les espaces propres de v sont stables par u.

Si K est algébriquement clos, comme E est non nul, u a au moins une valeur propre $\lambda \in K$. Notons $F = E_{u,\lambda}$. L'espace F est un sous-K-ev non nul et stable par v ; l'endomorphisme v', induit par v sur F, admet au moins une valeur propre $\mu \in K$; si $x \neq 0$ est un vecteur propre de v' pour la valeur propre μ, on voit que $v(x) = v'(x) = \mu x$ et $u(x) = \lambda x$. Le vecteur x est donc un vecteur propre commun à u et à v.

b) Vérifions par récurrence sur $p \in \mathbb{N}$, l'égalité $u^p v - v u^p = p \beta u^p$. Elle est vraie pour $p = 0$ et pour $p = 1$ par hypothèse. Si elle est vérifiée pour $p \geqslant 0$, alors :

$$u^{p+1} v = u^p (u v) = u^p (v u + \beta u) = u^p v u + \beta u^{p+1} = (u^p v) u + \beta u^{p+1} =$$
$$= (v u^p + p \beta u^p) u + \beta u^{p+1} = v u^{p+1} + (p +$$

l'égalité est donc vérifiée pour $p+1$. La propriété est donc vraie pour tout $p \in \mathbb{N}$.

Si u n'était pas nilpotent, les scalaires $p\beta$, pour $p \in \mathbb{N}$, seraient tous valeurs propres de l'endomorphisme $w \mapsto wv - vw$ de $\mathrm{Hom}_K(E)$. Ce K-ev étant de dimension finie, et le corps K étant de caractéristique 0, c'est impossible, et par conséquent u est nilpotent.

c) L'endomorphisme u étant nilpotent, il n'est pas injectif. Le noyau de u est donc un sous-K-ev non nul, et il est stable par v : si $u(x) = 0$, alors $u(v(x)) = v(u(x)) + \beta u(x) = 0$. L'endomorphisme v' de $\mathrm{Ker}\,(u)$ induit par v sur $\mathrm{Ker}\,(u)$ a au moins une valeur propre λ (puisque K est supposé algébriquement clos). Si $x \neq 0$ est un vecteur propre de v' pour la valeur propre λ, alors $v(x) = v'(x) = \lambda x$, et $u(x) = 0$, donc x est un vecteur propre commun à u et à v.

d) Démontrons cette propriété par récurrence sur la dimension $n > 0$ du K-ev E (elle est évidemment vérifiée si E est une droite). Supposons cette propriété vraie pour tout K-ev E de dimension $n-1$, où $n > 1$. Soit E de dimension n, $\beta \in K \setminus \{0\}$, et u et v deux endomorphismes de E tels que $uv - vu = \beta u$. En transposant nous obtenons ${}^t u\,{}^t v - {}^t v\,{}^t u = -\beta\,{}^t u$. D'après le *c*), il existe un scalaire λ et une forme linéaire $\varphi \neq 0$, tels que ${}^t u(\varphi) = \varphi \circ u = 0$ et ${}^t v(\varphi) = \varphi \circ v = \lambda\varphi$. Soit $H = \mathrm{Ker}\,(\varphi)$, c'est un hyperplan de E, et il est stable par u et v : si $\varphi(x) = 0$, alors $\varphi(u(x)) = 0$, et $\varphi(v(x)) = \lambda\varphi(x) = 0$. On peut appliquer aux endomorphismes u', resp. v', induits sur H par u, resp. v, l'hypothèse de récurrence. Il existe donc une base $(e_1, \ldots, e_{n-1})$ de H dans laquelle les matrices de u' et de v' soient trigonales supérieures. Il est clair que si e_n est un vecteur quelconque tel que $(e_1, \ldots, e_{n-1}, e_n)$ soit une base de E, les matrices de u et de v dans cette base sont trigonales supérieures. Les endomorphismes u et v sont donc simultanément trigonalisables. La propriété est donc vraie dans tout K-ev de dimension n. Cela achève la démonstration par récurrence.

§ XV.2 *TRIGONALISATION*

Exercice 2 :

a) Soit u et v dans $\mathrm{Hom}_K(E)$ *permutables* et trigonalisables. Montrer qu'il existe une base $\mathcal{B}$ de E telle que $\mathrm{Mat}_{\mathcal{B}}(u)$ et $\mathrm{Mat}_{\mathcal{B}}(v)$ soient toutes deux trigonales supérieures.

b) Soit $\mathcal{H}$ une partie non vide de $\mathrm{Hom}_K(E)$ telle que : pour tous u et v dans $\mathcal{H}$, on ait $uv = vu$, et que ch

soit trigonalisable. Montrer qu'il existe une base $\mathcal{B}$ de E telle que $(\forall u \in \mathcal{H})$ $\mathrm{Mat}_{\mathcal{B}}(u)$ soit trigonale supérieure. ■

Le a) étant une conséquence évidente du b), nous démontrons seulement le b). Les K-ev seront supposés de dimension finie. Nous utiliserons le lemme suivant :

Lemme :

Soit E un K-ev de dimension finie, $f \in \mathrm{Hom}_K(E)$ et F un sous-K-ev f-stable. Si f est trigonalisable, l'endomorphisme induit par f sur F est trigonalisable. ■

Notons g l'endomorphisme induit par f sur F. Comme f est trigonalisable, le polynôme caractéristique de f est dissocié dans $K[X]$. Le polynôme caractéristique de g divise celui de f et est donc dissocié dans $K[X]$. Nous en déduisons, d'après le théorème XV.2.2, que g est trigonalisable. Fin du lemme.

Démontrons par récurrence sur $n = \dim E > 0$, que si $\mathcal{H}$ est une partie non vide de $\mathrm{Hom}_K(E)$ constituée d'endomorphismes trigonalisables et deux à deux permutables, les éléments de $\mathcal{H}$ sont simultanément trigonalisables. Cette propriété est évidemment vraie pour $n = 1$. Supposons cette propriété vraie pour $n-1$, $n > 1$. Soit E un K-ev de dimension n et $\mathcal{H}$ une partie non vide de $\mathrm{Hom}_K(E)$ constituée d'endomorphismes trigonalisables et deux à deux permutables. Si les éléments de $\mathcal{H}$ sont tous des homothéties, alors ils sont évidemment simultanément trigonalisables. Sinon, soit $u \in \mathcal{H}$ qui ne soit pas une homothétie, l'endomorphisme ${}^t u \in \mathrm{Hom}_K(E^*)$ n'est pas une homothétie et il est trigonalisable. Il a donc au moins une valeur propre $\lambda \in K$, et l'espace propre associé, que nous noterons V, n'est pas nul et n'est pas E^*. Les endomorphismes ${}^t v$, où $v \in \mathcal{H}$, commutent avec ${}^t u$ et laissent donc tous le sous-K-ev V stable. Les endomorphismes du K-ev V induits par ces endomorphismes ${}^t v$, où $v \in \mathcal{H}$, sont trigonalisables (Lemme), commutent entre eux, et comme $0 < \dim(V) < n$, d'après l'hypothèse de récurrence ils sont simultanément trigonalisables. Ils ont donc au moins un vecteur propre commun. Il existe donc une forme linéaire non nulle $\varphi \in V \subset E^*$, telle que pour tout $v \in \mathcal{H}$, il existe $\mu \in K$, tel que ${}^t v(\varphi) = \mu\,\varphi$.
Notons $H = \mathrm{Ker}\,(\varphi)$, c'est un hyperplan de E, et il est stable par tous les endomorphismes $v \in \mathcal{H}$: si $\varphi(x) = 0$, $\varphi(v(x)) = \mu\varphi(x) = 0$. Soit $v \in \mathcal{H}$, il induit sur H un endomorphisme v' de H qui est trigonalisable (Lemme). Notons $\mathcal{H}'$ l'ensemble des endomorphismes de H induits sur H par les éléments de $\mathcal{H}$; les éléments de $\mathcal{H}'$ sont deux à deux permutables et trigonalisables, on peut donc appliquer à $\mathcal{H}'$ l'hypothèse de récurrence. Il existe donc une base $(e_1, \ldots, e_{n-1})$ de H dans laquelle les matrices des endomorphismes $v' \in \mathcal{H}'$ sont toutes trigonales supérieures. Il est clair que si $e_n \in E$ est tel que $(e_1, \ldots, e_{n-1}, e_n)$ est une base $\mathcal{B}$ de E

dans $\mathcal{B}$ des éléments de $\mathcal{H}$ sont toutes trigonales supérieures. La propriété est donc vraie pour n. Cela termine la démonstration par récurrence.

Exercice 8 :

Le corps K est supposé de caractéristique $p \geqslant 3$.

Soit $(a_0, a_1, \ldots, a_{p-1}) \in K^p$. On considère la matrice circulante

$$M = \Gamma(a_0, \ldots, a_{p-1}) = \begin{bmatrix} a_0 & a_1 & \ldots & a_{p-1} \\ a_{p-1} & a_0 & \ldots & a_{p-2} \\ \vdots & \vdots & \vdots & \vdots \\ a_1 & a_2 & \ldots & a_0 \end{bmatrix} \in \mathfrak{M}_p(K).$$

Calculer le polynôme caractéristique et le déterminant de M, et retrouver ainsi le résultat de l'exercice 24 du §XIII.5 :

$$\det(M) = \sum_{i=0}^{p-1} a_i^p \,. \blacksquare$$

La caractéristique p du corps K est un nombre premier. Rappelons que pour tout entier $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$ (Corollaire du Théorème IV.4.1). Nous en déduisons que si A est un anneau commutatif dans lequel $p \cdot 1_A = 0$, pour tout $(x, y) \in A^2$, $(x+y)^p = x^p + y^p$. Nous utiliserons cette propriété avec $A = K[X]$.

Soit la matrice circulante particulière $C = \Gamma(0, 1, 0, \ldots, 0) \in \mathfrak{M}_p(K)$. Son polynôme caractéristique est :

$$\det(\Gamma(-X, 1, 0, \ldots, 0)) = \det \begin{bmatrix} -X & 1 & 0 & \ldots & 0 \\ 0 & -X & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \ldots & -X & 1 \\ 1 & 0 & \ldots & \ldots & -X \end{bmatrix}.$$

En développant ce déterminant par rapport à la première colonne on trouve :

$$\det(\Gamma(-X, 1, 0, \ldots, 0)) = (-1)^p (X^p - 1) \,.$$

En tenant compte de la remarque préliminaire, et du fait que p est impair, on obtient :

$$\chi_C(X) = (-1)^p (X^p + (-1)^p) = (-1)^p (X-1)^p = (1-X)^p \,.$$

Le polynôme caractéristique de C étant dissocié sur K, la matrice C est trigonalisable ; elle est semblable à une matrice trigonale dont tous les coefficients diagonaux sont 1.

On remarque l'égalité :

$$M = \Gamma(a_0, a_1, \ldots, a_{p-1}) = a_0\, I_p + a_1\, C + \ldots + a_{p-1}\, C^{p-1} = Q(C)\ ,$$

où $Q = a_0 + a_1\, X + \ldots + a_{p-1}\, X^{p-1} \in K_{p-1}[X]$. La matrice $M = Q(C)$ est donc semblable à une matrice trigonale dont les coefficients diagonaux sont tous $Q(1)$. Nous en déduisons, en utilisant le préliminaire :

$$\det(M) = Q(1)^p = (a_0 + a_1 + \ldots + a_{p-1})^p = a_0^p + a_1^p + \ldots + a_{p-1}^p\ .$$

D'autre part, le polynôme caractéristique de M est le polynôme :

$$(Q(1) - X)^p = (a_0 + \ldots + a_p - X)^p = a_0^p + \ldots + a_{p-1}^p - X^p\ .$$

Exercice 9 :

Soit F un ensemble d'endomorphismes de E. On dit que F est trigonalisable (ou que la *réduction simultanée* à la forme trigonale est possible pour F) s'il existe une base de E dans laquelle la matrice de *tout* $u \in F$ soit trigonale supérieure. Soit E' un sous-K-ev de E, *F-stable* (*i.e.* tel que $u(E') \subset E'$ pour tout $u \in F$). Tout u induit donc un endomorphisme u' de E' et un endomorphisme $\bar{u}$ de $E/_{E'}$. Soit F' l'ensemble des u' et $\overline{F}$ l'ensemble des $\bar{u}$.
On suppose F' trigonalisable dans E' et $\overline{F}$ trigonalisable dans $E/_{E'}$. Montrer que F est trigonalisable dans E. En déduire une autre démonstration du théorème XV.2.2. ■

Soit p la dimension de E' ; nous pouvons supposer $1 \leqslant p < n = \dim(E)$, sinon la propriété est évidente. Soit $\mathcal{B}' = (e_1, \ldots, e_p)$ une base de E' et $\overline{\mathcal{B}} = (a_1, a_2, \ldots, a_{n-p})$ une base de $E/_{E'}$. Soient $(e_{p+1}, \ldots, e_n)$ des éléments de E tels que pour tout $j \in [\![1, n-p]\!]$, la classe modulo E' de e_{p+j} soit a_j. Montrons que $\mathcal{B} = (e_1, \ldots, e_p, e_{p+1}, \ldots, e_n)$ est une famille libre, donc une base de E. Si $(\lambda_1, \ldots, \lambda_n) \in K^n$ est tel que :

$$\lambda_1\, e_1 + \ldots + \lambda_n\, e_n = 0\ , \tag{1}$$

en prenant les classes modulo E', on trouve :

$$\lambda_{p+1}\, a_1 + \ldots + \lambda_n\, a_{n-p} = 0\ .$$

Comme la famille $(a_1, a_2, \ldots, a_{n-p})$ est libre dans $E/_{E'}$, nous en déduisons :

$$\lambda_{p+1} = \ldots = \lambda_n = 0\ .$$

En reprenant l'égalité initiale (1), on obtient :

$$\lambda_1 e_1 + \ldots + \lambda_p e_p = 0 .$$

Comme la famille $(e_1, \ldots, e_p)$ est libre dans E', nous en déduisons $\lambda_1 = \ldots = \lambda_p = 0$, et finalement $(\forall i \in [\![1, n]\!])\ \lambda_i = 0$. La famille $\mathcal{B} = (e_1, \ldots, e_n)$ est donc une base de E.

Soit $u \in \mathrm{Hom}_K(E)$ tel que E' soit stable par u. Notons, pour tout $(i, j) \in [\![1, n]\!]^2$, $\mu_{i,j}$ le coefficient d'indice (i, j) de la matrice de u dans la base $\mathcal{B}$; on a donc pour tout $j \in [\![1, n]\!]$:

$$u(e_j) = \sum_{i=1}^{n} \mu_{i,j}\, e_i .$$

Notons $\pi : E \to E/_{E'}$ l'application canonique. Pour tout $j \in [\![p+1, n]\!]$:

$$\pi(u(e_j)) = \bar{u}(\pi(e_j)) = \bar{u}(a_{j-p}) = \sum_{i=p+1}^{n} \mu_{i,j}\pi(e_i) = \sum_{i=p+1}^{n} \mu_{i,j}\, a_{i-p} .$$

Pour tout $(i, j) \in [\![p+1, n]\!]^2$ le coefficient $\mu_{i,j}$ est donc le coefficient d'indice $(i-p, j-p)$ de la matrice de $\bar{u}$ dans la base $(a_1, \ldots, a_{n-p})$ de $E/_{E'}$. La matrice de u dans la base $\mathcal{B}$ est donc de la forme :

$$\left[\begin{array}{c|c} A & B \\ \hline 0 & C \end{array}\right] ,$$

où $A = \mathrm{mat}_{\mathcal{B}'}(u')$, $C = \mathrm{mat}_{\overline{\mathcal{B}}}(\bar{u})$. Remarquons qu'on peut en déduire l'égalité :

$$\chi_u(X) = \chi_{u'}(X)\ \chi_{\bar{u}}(X)$$

Si on prend dans E' une base $\mathcal{B}'$ dans laquelle la matrice de tout $u' \in F'$ soit trigonale supérieure, et dans $E/_{E'}$ une base $\overline{\mathcal{B}}$ dans laquelle la matrice de tout $\bar{u} \in \overline{F}$ soit trigonale supérieure, on voit qu'on obtient par le procédé décrit ci-dessus des bases de E dans lesquelles la matrice de tout $u \in F$ est trigonale supérieure. L'ensemble F est donc trigonalisable.

Reprenons la démonstration du théorème XV.2.2. Démontrons par récurrence sur $n = \dim E > 0$, que si le polynôme caractéristique de $u \in \mathrm{Hom}_K(E)$ est dissocié dans K, alors u est trigonalisable (la réciproque est évidente). C'est vrai pour $n = 1$. Supposons la propriété vraie pour $n-1$ ($n > 1$). Soit E un K-ev de dimension n et $u \in \mathrm{Hom}_K(E)$ dont le polynôme caractéristique est dissocié sur K. Si u est une homothétie, alors u est évidemment trigonalisable. Dans le cas contraire, comme

caractéristique de u est dissocié sur K, u a au moins une valeur propre λ. Notons $E' = \mathrm{Ker}\,(u - \lambda\,\mathrm{Id}_E)$; ce sous-K-ev est u-stable et il n'est ni nul, ni égal à E. Notons comme ci-dessus u' l'endomorphisme induit par u sur E' et $\bar{u}$ l'endomorphisme de $E/_{E'}$ associé. Nous avons démontré l'égalité :

$$\chi_u(X) = \chi_{u'}(X)\ \chi_{\bar{u}}(X)\ .$$

Le polynôme caractéristique de $\bar{u}$ est donc dissocié dans K ; nous déduisons de l'hypothèse de récurrence que $\bar{u}$ est trigonalisable. Les endomorphismes u' et $\bar{u}$ étant trigonalisables, l'endomorphisme u est trigonalisable. La propriété est donc vraie pour n. Cela achève la démonstration par récurrence.

Exercice 11 :

> Soit $n \in \mathbb{N}^*$; on donne A et B dans $\mathfrak{M}_n(\mathbb{C})$. Montrer que A et B ont une valeur propre commune si, et seulement si, il existe $P \in \mathfrak{M}_n(\mathbb{C})$, $P \neq 0$, telle que $AP = PB$. ■

Soit E un $\mathbb{C}$-ev de dimension n, nous allons démontrer que si f et g sont deux endomorphismes de E, f et g ont une valeur propre commune si, et seulement si, il existe un endomorphisme $h \in \mathrm{Hom}_K(E)$, $h \neq 0$, tel que $f \circ h = h \circ g$. Il est clair que cette propriété est équivalente à celle de l'énoncé.

Supposons que f et g aient une valeur propre commune $\lambda \in \mathbb{C}$. Il existe un vecteur $v \in E$, $v \neq 0$, tel que $f(v) = \lambda v$, et puisque λ est une valeur propre de ${}^t g$, il existe une forme linéaire φ sur E, non nulle, telle que ${}^t g(\varphi) = \varphi \circ g = \lambda\varphi$. Considérons l'endomorphisme h défini par $h(x) = \varphi(x)\,v$, pour tout $x \in E$. L'endomorphisme h n'est pas nul, et pour tout $x \in E$:

$$f(h(x)) = \varphi(x)\,f(v) = \varphi(x)\,\lambda\,v \quad \text{et} \quad h(g(x)) = \varphi(g(x))\,v = \lambda\,\varphi(x)\,v\ .$$

On a donc $f \circ h = h \circ g$ (nous n'utilisons pas ici le fait que $\mathbb{C}$ soit algébriquement clos).

Réciproquement, supposons qu'il existe un endomorphisme $h \in \mathrm{Hom}_K(E)$, $h \neq 0$, tel que $f \circ h = h \circ g$. Il est clair que le sous-K-ev non nul $F = \mathrm{Im}\,(h)$ est stable par f. Comme le corps $\mathbb{C}$ est algébriquement clos, l'endomorphisme induit sur F par f a au moins une valeur propre λ. Il existe donc un vecteur $v \in \mathrm{Im}\,(h)$, $v \neq 0$, tel que $f(v) = \lambda v$. Il existe donc un vecteur $u \in E$, $u \notin \mathrm{Ker}\,(h)$, tel que $f(h(u)) = \lambda\,h(u) = h(g(u))$. L'endomorphisme $f \circ h - \lambda h$ est nul en u et sur $\mathrm{Ker}\,(h)$, il est donc nul sur $\mathbb{C}\,u \oplus \mathrm{Ker}\,(h)$. On a donc pour tout $x \in \mathrm{Ker}\,(h)$, et pour tout $\mu \in \mathbb{C}$ l'égalité :

$$h(g(\mu\,u + x)) = f(h(\mu\,u + x)) = \lambda\,h(\mu\,u + x)\ .$$

Nous en déduisons :

$$\mathbb{C}\,u \oplus \mathrm{Ker}\,(h) \subset \mathrm{Ker}\,(h \circ (g - \lambda\,\mathrm{Id}_E)) \ .$$

Si l'endomorphisme $g - \lambda\,\mathrm{Id}_E$ était injectif, le noyau de $h \circ (g - \lambda\,\mathrm{Id}_E)$ serait de même dimension que celui de h. On voit donc que $g - \lambda\,\mathrm{Id}_E$ n'est pas injectif, c'est-à-dire que λ est valeur propre de g. Nous avons donc démontré que f et g ont une valeur propre commune.

Les deux propriétés sont donc équivalentes.

§ XV.3 *SOUS-ESPACES PROPRES*

Exercice 1 :

Trouver les $(a, b, c, d, e, f) \in \mathbb{C}^6$ tels que la matrice $M \in \mathfrak{M}_4(\mathbb{C})$ suivante soit diagonalisable :

$$M = \begin{bmatrix} 1 & a & b & c \\ 0 & 1 & d & e \\ 0 & 0 & -1 & f \\ 0 & 0 & 0 & -1 \end{bmatrix} . \blacksquare$$

Il est clair que le polynôme caractéristique de cette matrice est le polynôme $(1 - X)^2\,(-1 - X)^2$. Elle est donc diagonalisable si, et seulement si, l'espace propre relatif à la valeur propre 1 est de dimension 2 et l'espace propre relatif à la valeur propre -1 est aussi de dimension 2. La matrice M est donc diagonalisable si, et seulement si, $\mathrm{rg}\,(M - I_4) = 4 - 2 = 2$ et si $\mathrm{rg}\,(M + I_4) = 4 - 2 = 2$. Or on voit que :

$$M - I_4 = \begin{bmatrix} 0 & a & b & c \\ 0 & 0 & d & e \\ 0 & 0 & -2 & f \\ 0 & 0 & 0 & -2 \end{bmatrix} \quad \text{et} \quad M + I_4 = \begin{bmatrix} 2 & a & b & c \\ 0 & 2 & d & e \\ 0 & 0 & 0 & f \\ 0 & 0 & 0 & 0 \end{bmatrix} .$$

Il est clair que la matrice $M - I_4$ est de rang 2 si, et seulement si, $a = 0$, et que la matrice $M + I_4$ est de rang 2 si, et seulement si, $f = 0$. La matrice M est donc diagonalisable si, et seulement si, $a = f = 0$.

Exercice 2 :

Le corps de base est $\mathbb{C}$. Montrer que la matrice suivante est diagonalisable et calculer ses puissances k-ièmes pour $k \in \mathbb{N}^*$:

$$M = \begin{bmatrix} d & a & b & c \\ a & d & c & b \\ b & c & d & a \\ c & b & a & d \end{bmatrix} , \ (a, b, c, d) \in \mathbb{C}^4 . \blacksquare$$

Soit f l'endomorphisme de $\mathbb{C}^4$ dont la matrice dans la base canonique $\mathcal{B} = (e_1, e_2, e_3, e_4)$ de $\mathbb{C}^4$ est la matrice M. On remarque en faisant la somme des colonnes de M que

$$f(e_1 + e_2 + e_3 + e_4) = (a + b + c + d)\,(e_1 + e_2 + e_3 + e_4)\ .$$

On observe aussi les égalités :

$$\begin{aligned} f(e_1 + e_2 - e_3 - e_4) &= (a + d - b - c)(e_1 + e_2 - e_3 - e_4)\ ; \\ f(e_1 - e_2 + e_3 - e_4) &= (b + d - a - c)(e_1 - e_2 + e_3 - e_4)\ ; \\ f(e_1 - e_2 - e_3 + e_4) &= (c + d - a - b)(e_1 - e_2 - e_3 + e_4)\ . \end{aligned}$$

Notons $e'_1 = e_1 + e_2 + e_3 + e_4$, $e'_2 = e_1 + e_2 - e_3 - e_4$, $e'_3 = e_1 - e_2 + e_3 - e_4$ et $e'_4 = e_1 - e_2 - e_3 + e_4$. On voit que $e'_1 + e'_2 + e'_3 + e'_4 = 4\,e_1$, $e'_1 + e'_2 - e'_3 - e'_4 = 4\,e_2$, $e'_1 - e'_2 + e'_3 - e'_4 = 4\,e_3$, et $e'_1 - e'_2 - e'_3 + e'_4 = 4\,e_4$. La famille $\mathcal{B}' = (e'_1, e'_2, e'_3, e'_4)$ est donc une famille génératrice, et par conséquent une base, de $\mathbb{C}^4$. La matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$ est la matrice :

$$P = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}\ .$$

Les calculs précédents prouvent l'égalité $P^{-1} = \frac{1}{4}\,P$. Indépendamment du fait que les valeurs propres soient distinctes ou non, la famille $\mathcal{B}' = (e'_1, e'_2, e'_3, e'_4)$ est une base diagonale pour f. La matrice M est donc toujours diagonalisable et semblable à la matrice diagonale dont les coefficients diagonaux sont :

$$(\alpha, \beta, \gamma, \delta) = (a + b + c + d, a + d - b - c, b + d - a - c, c + d - a - b)\ .$$

Comme :

$$M = P\,\mathrm{Diag}\,(\alpha, \beta, \gamma, \delta)\ P^{-1}\ ,$$

nous en déduisons que pour tout $k \in \mathbb{N}^*$:

$$M^k = P\,\mathrm{Diag}\left(\alpha^k, \beta^k, \gamma^k, \delta^k\right) P^{-1}\ .$$

Exercice 3 :

> Le corps de base est $\mathbb{C}$. Pour chacune des matrices suivantes, dire si elle est ou non diagonalisable, et lorsqu'elle est diagonalisable, en donner une base de vecteurs propres :

d) $M = \begin{bmatrix} a_1 & a_2 & \dots & a_n \\ a_2 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ a_n & 0 & \dots & 0 \end{bmatrix}$, avec $n \geqslant 2$.

e) $M = \begin{bmatrix} c & a & \dots & a & b \\ a & c & & \dots & \dots \\ \vdots & & \ddots & a & \vdots \\ a & \dots & a & c & b \\ b & \dots & \dots & b & c \end{bmatrix}$.

f) $M = \begin{bmatrix} 1 & x+\frac{1}{x} & x^2+\frac{1}{x^2} \\ x+\frac{1}{x} & 1 & x+\frac{1}{x} \\ x^2+\frac{1}{x^2} & x+\frac{1}{x} & 1 \end{bmatrix}$, avec $x \in \mathbb{C}^*$. ■

d) Si pour tout $i \in [\![2,n]\!]$, $a_i = 0$, la matrice M est diagonale. Nous supposerons dans la suite $\exists i \in [\![2,n]\!] \mid a_i \neq 0$.

Notons $\mathcal{B} = (e_1, \dots, e_n)$ la base canonique de $\mathbb{C}^n$, et f l'endomorphisme de $\mathbb{C}^n$ dont la matrice dans la base $\mathcal{B}$ est M. On voit que l'image de f est engendrée par les vecteurs e_1 et $v = \sum_{i=1}^{n} a_i e_i$, qui sont linéairement indépendants. L'endomorphisme f et sa matrice M sont de rang 2.

Montrons de manière générale qu'un endomorphisme f d'un K-ev E est diagonalisable si, et seulement si, l'endomorphisme induit par f sur $\mathrm{Im}\,(f)$ est diagonalisable et $\mathrm{Im}\,(f) \cap \mathrm{Ker}\,(f) = \{0\}$. Cette condition est évidemment suffisante car alors $\mathrm{Im}\,(f)$ a une base de vecteurs propres et $E = \mathrm{Ker}\,(f) \oplus \mathrm{Im}\,(f)$. Inversement, supposons que f soit diagonalisable. Si v est un vecteur propre correspondant à une valeur propre λ non nulle, comme $\frac{1}{\lambda} f(v) = v$, on en déduit $v \in \mathrm{Im}\,(f)$. On a donc, en notant $E_\lambda = \mathrm{Ker}\,(f - \lambda \mathrm{Id}_E)$, l'inclusion :

$$\mathrm{Im}\,(f) \supset \bigoplus_{\lambda \neq 0} E_\lambda \quad (\lambda \text{ valeur propre}) .$$

Comme d'autre part $\mathrm{Ker}\,(f)$ est, s'il n'est pas nul, l'espace propre associé à la valeur propre 0, on a :

$$E = \mathrm{Ker}\,(f) \oplus \bigoplus_{\lambda \neq 0} E_\lambda \quad (\lambda \text{ valeur propre}) .$$

La somme directe $\bigoplus_{\lambda \neq 0} E_\lambda$ a donc même dimension que $\mathrm{Im}\,(f)$ et lui est donc égale. Nous en déduisons que l'endomorphisme induit par f

est diagonalisable, et que $E = \mathrm{Ker}\,(f) \oplus \mathrm{Im}\,(f)$. Nous aurions pu aussi utiliser le fait que l'endomorphisme induit sur un sous espace stable par un endomorphisme diagonalisable est diagonalisable, cf. Théorème XV.5.2, Exemple 2.

Dans le cas de l'exercice, on vérifie que

$$f(e_1) = v \quad \text{et} \quad f(v) = a_1\, v + \left(\sum_{i=2}^{n} a_i^2\right) e_1 \ .$$

Posons $s = \sum_{i=2}^{n} a_i^2$, la matrice de l'endomorphisme induit par f sur $\mathrm{Im}\,(f)$ dans la base (e_1, v) est :

$$M' = \begin{bmatrix} 0 & s \\ 1 & a_1 \end{bmatrix} \ .$$

Le polynôme caractéristique de cette matrice est :

$$X^2 - a_1\, X - s = X^2 - a_1\, X - \sum_{i=2}^{n} a_i^2 \ .$$

D'après ce qui précède, f est diagonalisable si, et seulement si la matrice M' est régulière ($f_{\|\mathrm{Im}(f)}$ injective) et diagonalisable. Or une matrice carrée élément de $\mathfrak{M}_2(\mathbb{C})$ est diagonalisable si, et seulement si, soit elle a deux valeurs propres distinctes, soit elle a une seule valeur propre λ et elle est la matrice $\mathrm{Diag}\,(\lambda, \lambda)$. Le deuxième cas étant ici exclu, nous en déduisons que M est diagonalisable si, et seulement si, $\sum_{i=2}^{n} a_i^2 \neq 0$ et $a_1^2 + 4 \sum_{i=2}^{n} a_i^2 \neq 0$.

On obtient une base de vecteurs propres pour f en prenant une base du noyau, de dimension $n-2$, et une base de vecteurs propres dans $\mathrm{Im}\,(f)$, espace engendré par e_1 et v.

e) Notons $M(a, b, c)$ cette matrice. On voit que si $P \in \mathrm{GL}_n(\mathbb{C})$ est telle qu'il existe $c \in \mathbb{C}$ pour lequel la matrice $P^{-1}\, M(a, b, c)\, P$ est diagonale, alors cette propriété est vraie pour tout $c \in \mathbb{C}$. Nous pouvons donc supposer $c = a$. Soit f l'endomorphisme dont la matrice est $M(a, b, a)$ dans la base canonique de $\mathbb{C}^n$, notée ici $\mathcal{B} = (e_1, \ldots, e_n)$. On voit que pour tout $i \in [\![1, n-1]\!]$:

$$f(e_i) = a\,(e_1 + \ldots + e_{n-1}) + b\, e_n \ ,$$

et :

$$f(e_n) = b\,(e_1 + \ldots + e_{n-1}) + a\, e_n \ .$$

Les vecteurs $u = e_1 + \ldots + e_{n-1}$ et e_n engendrent un sous-espace vectoriel E', stable par f, qui contient $\mathrm{Im}\,(f)$. La famille $(e_1 - e_2, ..$

est libre, et engendre un sous-espace vectoriel E'', stable par f et inclus dans le noyau de f. Démontrons que la famille $(e_1 - e_2, \ldots, e_1 - e_{n-1}, u, e_n)$ est libre. Si $\lambda_2, \ldots, \lambda_{n-1}, \alpha, \beta$ sont des complexes tels que :

$$\lambda_2 (e_1 - e_2) + \ldots + \lambda_{n-1} (e_1 - e_{n-1}) + \alpha (e_1 + \ldots + e_{n-1}) + \beta e_n = 0 ,$$

alors évidemment $\beta = 0$ et :

$$\lambda_2 + \ldots + \lambda_{n-1} + \alpha = 0 \quad \text{et} \quad \alpha = \lambda_2 = \ldots = \lambda_{n-1} .$$

Nous en déduisons $(n-1)\alpha = 0$, d'où $\alpha = 0$; tous les coefficients de la combinaison linéaire sont donc nuls. La famille $(e_1 - e_2, \ldots, e_1 - e_{n-1}, u, e_n)$ est par conséquent libre. On a donc $E = E' \oplus E''$, les espaces E' et E'' étant stables par f. L'endomorphisme f est diagonalisable si, et seulement si, l'endomorphisme f' induit par f sur E', et l'endomorphisme f'' induit par f sur E'' sont diagonalisables. La condition est évidemment suffisante, et elle est nécessaire d'après le Théorème XV.5.2, Exemple 2. L'endomorphisme f'' étant nul, f est diagonalisable si, et seulement si f' l'est. On voit que $f(u) = (n-1)(a u + b e_n)$ et $f(e_n) = b u + a e_n$. La matrice de f' dans la base (u, e_n) de E' est donc la matrice :

$$M' = \begin{bmatrix} (n-1)a & b \\ (n-1)b & a \end{bmatrix} .$$

Le polynôme caractéristique de M' est $X^2 - n a X + (n-1)(a^2 - b^2)$. La matrice M' est diagonalisable, si elle est diagonale, i.e. si $b = 0$, ou si ses valeurs propres sont distinctes, i.e. si $n^2 a^2 - 4(n-1)(a^2 - b^2) \neq 0$. Si ces conditions sont réalisées, et que (v, w) est une base diagonale pour f', une base diagonale pour f est $(e_1 - e_2, \ldots, e_1 - e_{n-1}, v, w)$.

f) Posons $u = x + \dfrac{1}{x}$. Nous noterons $\mathcal{B} = (e_1, e_2, e_3)$ la base canonique de $\mathbb{C}^3$, et f l'endomorphisme de $\mathbb{C}^3$ dont la matrice dans $\mathcal{B}$ est la matrice M, c'est-à-dire :

$$M = \begin{bmatrix} 1 & u & u^2 - 2 \\ u & 1 & u \\ u^2 - 2 & u & 1 \end{bmatrix} .$$

On observe que $f(e_1 + e_3) = (u^2 - 1)(e_1 + e_3) + 2 u e_2$, $f(e_2) = u(e_1 + e_3) + e_2$ et $f(e_1 - e_3) = (3 - u^2)(e_1 - e_3)$. Dans la nouvelle base $(e'_1, e'_2, e'_3) = (e_1 + e_3, e_2, e_1 - e_3)$, la matrice de f est donc :

$$M' = \begin{bmatrix} u^2 - 1 & u & 0 \\ 2u & 1 & 0 \\ 0 & 0 & 3 - u^2 \end{bmatrix} .$$

Notons f' l'endomorphisme induit par f sur le sous espace stable E' engendré par (e'_1, e'_2). On voit que le polynôme caractéristique de f' est le polynôme $P = X^2 - u^2 X - (1+u^2) = (X+1)(X-1-u^2)$. On démontre comme dans les deux exemples précédents, que f est diagonalisable si, et seulement si, f' l'est. Déterminons l'espace propre de f' relatif à la valeur propre -1. Si $v \in E'$ a pour coordonnées $(x, y) \in \mathbb{C}^2$ dans la base (e'_1, e'_2), il est dans ce sous espace propre si, et seulement si ;

$$\begin{cases} (u^2-1)\,x + u\,y &= -x \\ 2\,u\,x + y &= -y \end{cases} \quad \text{soit} \quad u\,x + y = 0\,.$$

L'espace E'_{-1} est donc toujours de dimension 1. Nous en déduisons que f' est diagonalisable si, et seulement si ses valeurs propres sont distinctes, soit $u^2 \neq -2$, c'est-à-dire $x^2 + \dfrac{1}{x^2} + 4 \neq 0$ (on obtient facilement $x^2 \neq -2 \pm \sqrt{3}$). Supposons cette condition réalisée et déterminons l'espace propre relatif à la valeur propre $1+u^2$ de f'. Si $v \in E'$ a pour coordonnées $(x, y) \in \mathbb{C}^2$ dans la base (e'_1, e'_2), il est dans ce sous espace propre si, et seulement si ;

$$\begin{cases} (u^2-1)\,x + u\,y &= (1+u^2)\,x \\ 2\,u\,x + y &= (1+u^2)\,y \end{cases} \quad \text{soit} \quad -2\,x + u\,y = 0\,.$$

Une base de vecteurs propres pour f' est donc par exemple la base (e''_1, e''_2), où $e''_1 = e'_1 - u\,e'_2 = (e_1 + e_3) - u\,e_2$, et $e''_2 = u\,e'_1 + 2\,e'_2 = u\,(e_1 + e_3) + 2\,e_2$.

En conclusion, f est diagonalisable si, et seulement si, $u^2 \neq -2$, et dans ce cas, une base diagonale pour f est $\mathcal{B}'' = (e''_1, e''_2, e''_3)$, où :

$$\begin{aligned} e''_1 &= (e_1 + e_3) - u\,e_2 && \text{valeur propre} \quad -1 \\ e''_2 &= u\,(e_1 + e_3) + 2\,e_2 && \text{valeur propre} \quad 1+u^2 \\ e''_3 &= e_1 - e_3 && \text{valeur propre} \quad 3-u^2\,. \end{aligned}$$

Exercice 4 :

Soit $n \in \mathbb{N}^*$ $(n \geqslant 2)$ et $(a_0, a_1, \ldots, a_{n-1}) \in \mathbb{C}^n$. On considère la matrice circulante :

$$M = \Gamma(a_0, \ldots, a_{n-1}) = \left[a_{\overline{j-i}}\right] \qquad (i,j) \in [\![1, n]\!]^2\,,$$

où $\bar{k}$ désigne le reste de k mod (n) pour $k \in \mathbb{Z}$. Montrer que M est diagonalisable, et la diagonaliser en calculant $\Omega_n M \Omega_n^{-1}$, où $\Omega_n = \left[\omega^{(i-1)(j-1)}\right]$, $((i,j) \in [\![1, n]\!]^2)$ est la matrice *alternante* d'ordre n $(\omega = \mathrm{e}^{2\mathrm{i}\pi/n})$ (cf. §XIII.5, exemple 4). ■

Soit $\mathcal{B} = (e_1, \ldots, e_n)$ la base canonique de $\mathbb{C}^n$ et f l'endomorphisme de $\mathbb{C}^n$ tel que pour tout $i \in [\![1, n]\!]$, $f(e_i) = e_{\sigma(i)}$, où σ est la

$\begin{pmatrix} 1 & 2 & \dots & n \\ n & 1 & \dots & (n-1) \end{pmatrix}$. Nous noterons C la matrice de f dans la base $\mathcal{B}$. Pour tout $\zeta \in \mu_n$, posons $v_\zeta = e_1 + \zeta e_2 + \ldots + \zeta^{n-1} e_n$. On voit que :

$$f(v_\zeta) = e_n + \zeta e_1 + \ldots + \zeta^{n-1} e_{n-1} = \zeta v_\zeta \ .$$

Pour tout $\zeta \in \mu_n$, v_ζ est donc vecteur propre de f pour la valeur propre ζ. L'endomorphisme f est donc diagonalisable, et si ω est un générateur du groupe μ_n, la famille $\mathcal{V} = (v_1, v_\omega, \ldots, v_{\omega^{n-1}})$ est une base dans laquelle la matrice de f est la matrice $\Delta = \mathrm{Diag}\left(1, \omega, \ldots, \omega^{n-1}\right)$. Pour tout $(i,j) \in [\![1,n]\!]^2$, le coefficient d'indice (i,j) de la matrice matrice de passage de la base canonique $\mathcal{B}$ à la base $\mathcal{V}$ est $\omega^{(i-1)(j-1)}$; cette matrice de passage est donc la matrice alternante Ω_n. Son inverse est la matrice $\frac{1}{n}\overline{\Omega}_n$. On a donc les relations :

$$C = \frac{1}{n}\Omega_n \Delta \overline{\Omega}_n \quad \text{où} \quad \Delta = \mathrm{Diag}\left(1, \omega, \ldots, \omega^{n-1}\right) \ , \quad \text{et} \quad C^n = I_n \ .$$

On remarque d'autre part que :

$$M = a_0 I_n + a_1 C + \ldots a_{n-1} C^{n-1} = Q(C) \ ,$$

où Q est le polynôme $a_0 + a_1 X + \ldots + a_{n-1} X^{n-1}$. Toutes ces matrices sont donc simultanément diagonalisables. On a l'égalité :

$$M = Q(C) = \frac{1}{n}\Omega_n Q(\Delta) \overline{\Omega}_n \ ,$$

et :

$$Q(\Delta) = \mathrm{Diag}\left(Q(1), Q(\omega), \ldots, Q(\omega^{n-1})\right) \ .$$

Exercice 5 :

Soit b et c dans $\mathbb{C}^*$. On considère la matrice $M \in \mathfrak{M}_n(\mathbb{C})$ suivante, où $n \geqslant 2$:

$$M = \begin{bmatrix} 0 & c & 0 & \dots & 0 \\ b & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & c \\ 0 & \dots & 0 & b & 0 \end{bmatrix}$$

Montrer que M est diagonalisable, et en calculer une base de vecteurs propres. ■

Montrons d'abord qu'on peut se ramener au cas où $b = c = 1$. Soit $\mathcal{B} = (e_1, \ldots, e_n)$ la base canonique de $\mathbb{C}^n$ et f l'endomorphisme do

dans la base $\mathcal{B}$ est M. Il existe $\rho \in \mathbb{C}$ tel que $\rho^2 = \dfrac{b}{c}$, posons $\mu = c\rho = \dfrac{b}{\rho}$. Pour tout $i \in [\![1, n]\!]$, posons $e'_i = \rho^{i-1} e_i$. On vérifie les égalités :

$$f(e'_1) = b e_2 = \mu \rho e_2 = \mu e'_2 ,$$

pour tout $i \in [\![2, n-1]\!]$:

$$f(e'_i) = \rho^{i-1}(c e_{i-1} + b e_{i+1}) = c\rho e'_{i-1} + \frac{b}{\rho} e'_{i+1} = \mu (e'_{i-1} + e'_{i+1}) ,$$

et :

$$f(e'_n) = \rho^{n-1} c e_{n-1} = \rho c e'_{n-1} = \mu e'_{n-1} .$$

La matrice de f dans la nouvelle base $\mathcal{B}' = (e'_1, \dots, e'_n)$ est :

$$M' = \mu \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 1 & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \dots & 0 & 1 & 0 \end{bmatrix} .$$

Un complexe λ est valeur propre de M' si, et seulement si, il existe un n-uplet $(x_1, \dots, x_n) \in \mathbb{C}^n$, non nul, vérifiant les équations :

$$\begin{aligned} & x_2 = \lambda x_1 \\ (\forall i \in [\![2, n-1]\!]) \quad & x_{i-1} + x_{i+1} = \lambda x_i \\ & x_{n-1} = \lambda x_n . \end{aligned}$$

Le complexe λ est donc valeur propre de M' si, et seulement si, il existe des complexes $(x_0, x_1, \dots, x_n, x_{n+1})$, non tous nuls, tels que :

$$(1) \qquad (\forall i \in [\![1, n]\!]) \quad x_{i-1} - \lambda x_i + x_{i+1} = 0 ,$$

et $x_0 = x_{n+1} = 0$. Le polynôme du second degré associé à cette relation de récurrence est le polynôme $X^2 - \lambda X + 1$. Cherchons des solutions pour λ sous la forme $2\cos\theta$, où $\theta \in]0, \pi[$. Les zéros du polynôme sont alors $e^{i\theta}$ et $e^{-i\theta}$, et ils sont distincts. Une suite $(x_k)_{k\in\mathbb{N}}$ vérifie la relation de récurrence :

$$(\forall k \in \mathbb{N}^*) \quad x_{k-1} - 2\cos\theta\, x_k + x_{k+1} = 0 ,$$

si, et seulement si, il existe deux complexes u et v tels que :

$$(\forall k \in \mathbb{N}) \quad x_k = u e^{i k\theta} + v e^{-i k\theta} .$$

Puisqu'ici on doit avoir $x_0 = x_{n+1} = 0$, on doit avoir les égalités :

$$u + v = 0 \quad \text{et} \quad u\,\mathrm{e}^{\mathrm{i}\,(n+1)\,\theta} + v\,\mathrm{e}^{-\mathrm{i}\,(n+1)\,\theta} = 0\ ,$$

d'où $v = -u$, et comme u ne peut pas être nul, nécessairement :

$$\mathrm{e}^{\mathrm{i}\,(n+1)\,\theta} - \mathrm{e}^{-\mathrm{i}\,(n+1)\,\theta} = 0 \quad \text{soit} \quad \sin(n+1)\theta = 0\ .$$

Le réel θ est donc nécessairement de la forme $\dfrac{j\,\pi}{n+1}$, où $j \in [\![1, n]\!]$.

Inversement, supposons que λ soit l'un des n réels $z_j = 2\cos\left(\frac{j\,\pi}{n+1}\right)$, où $j \in [\![1, n]\!]$; la suite $(x_k)_{k \in [\![0, n+1]\!]}$ définie par :

$$(\forall k \in [\![0, n+1]\!]) \quad x_k = \sin\left(\frac{k\,j\,\pi}{n+1}\right)\ ,$$

n'est pas identiquement nulle, elle vérifie la relation de récurrence (1), et les conditions $x_0 = x_{n+1} = 0$. Les n complexes $\lambda_j = 2\cos\left(\frac{j\,\pi}{n+1}\right)$, où $j \in [\![1, n]\!]$ sont donc les valeurs propres de la matrice M'. Les matrices M' et M sont donc diagonalisables. Le calcul ci-dessus montre que pour tout $j \in [\![1, n]\!]$, le vecteur :

$$v_j = \sum_{k=1}^{n} \sin\left(\frac{k\,j\,\pi}{n+1}\right) e'_k = \sum_{k=1}^{n} \sin\left(\frac{k\,j\,\pi}{n+1}\right) \rho^{k-1}\, e_k\ ,$$

est un vecteur propre pour la valeur propre $\lambda_j = 2\cos\left(\frac{j\,\pi}{n+1}\right)$ de l'endomorphisme f.

Exercice 11 :

On suppose $K = \mathbb{C}$ et on donne $n \in \mathbb{N}^*$. On considère le *discriminant général* d'ordre n défini au § X.6 : $D(X_1, \ldots, X_n) = \prod_{1 \leqslant i < j \leqslant n} (X_i - X_j)^2$, où $(X_1, \ldots, X_n)$ est un système d'indéterminées sur $\mathbb{C}$.

On notera Φ le polynôme à n lettres à coefficients dans $\mathbb{C}$ tel que $D(X_1, \ldots, X_n) = \Phi(\sigma_1, \ldots, \sigma_n)$, où :

$$\sigma_k = \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} X_{i_1} \ldots X_{i_k} \quad \text{(cf.§ X.4)}\ .$$

Pour toute matrice $M \in \mathfrak{M}_n(\mathbb{C})$, on note son polynôme caractéristique $\chi_M(X) =$

$= (-1)^n\big(X^n - \tau_1(M)\,X^{n-1} + \tau_2(M)\,X^{n-2} + \ldots + (-1)^n\,\tau_n(M)\big)$.

a) Montrer que $f(M) = \Phi(\tau_1(M), \ldots, \tau_n(M))$ est une fonction polynomiale non nulle sur $\mathfrak{M}_n(\mathbb{C})$, et que $\chi_M(X)$ a toutes ses racines distinctes ssi $f(M) \neq 0$.

b) Soit S l'ensemble des matrices diagonalisables dans $\mathfrak{M}_n(\mathbb{C})$. Montrer que si une fonction polynomiale $g : \mathfrak{M}_n(\mathbb{C}) \to \mathbb{C}$ est nulle sur S, alors $g = 0$ (cf. théorème X.1.4). ■

a) La fonction f est polynomiale, puisque les fonctions $M \mapsto \tau_k(M)$, pour $k \in [\![1, n]\!]$, sont polynomiales, et que la fonction Φ l'est aussi.
Supposons qu'une numérotation des zéros du polynôme caractéristique de la matrice M soit $(\lambda_1, \ldots, \lambda_n)$. Pour tout $k \in [\![1, n]\!]$, on a alors par identification $\tau_k(M) = \sigma_k(\lambda_1, \ldots, \lambda_n)$; on en déduit l'égalité :

$$f(M) = D(\lambda_1, \ldots, \lambda_n) = \prod_{1 \leqslant i < j \leqslant n} (\lambda_i - \lambda_j)^2 .$$

On voit donc que $f(M) \neq 0$ si, et seulement si, le polynôme caractéristique de M a n zéros simples. Cela implique évidemment que f n'est pas la fonction polynomiale nulle, par exemple $f(M) \neq 0$ si $M = \mathrm{Diag}\,(1, 2, \ldots, n)$.

b) D'après le théorème XV.3.3, et le *a*), si $f(M) \neq 0$, alors M est diagonalisable. On a donc l'inclusion :

$$\{M \mid f(M) \neq 0\} \subset S .$$

Si g est une fonction polynomiale nulle sur S, alors elle est nulle sur l'ensemble $\{M \mid f(M) \neq 0\}$; comme f n'est pas la fonction polynomiale identiquement nulle, d'après le principe de prolongement des identités algébriques nous en déduisons $g = 0$ (cf. Théorème X.1.4).

Exercice 13 :

On reprend les notations de l'exercice 11 ci-dessus. Une fonction polynomiale $I : \mathfrak{M}_n(\mathbb{C}) \to \mathbb{C}$ est dite *invariante* ssi :

$$(\forall P \in \mathrm{GL}\,(n, \mathbb{C}),\ \ \forall M \in \mathfrak{M}_n(\mathbb{C}))\quad I(P\,M\,P^{-1}) = I(M) .$$

a) Vérifier, en revenant à l'étude du § XV.1, que chacune des fonctions $\tau_k : \mathfrak{M}_n(\mathbb{C}) \to \mathbb{C}$ est invariante ($1 \leqslant k \leqslant n$).

b) Les fonctions polynomiales invariantes sur $\mathfrak{M}_n(\mathbb{C})$ forment une sous-$\mathbb{C}$-algèbre $\mathcal{I}$ de l'algèbre des fonctions

sur $\mathfrak{M}_n(\mathbb{C})$.

c) La suite $(\tau_1, \tau_2, \ldots, \tau_n)$ est *algébriquement libre* sur $\mathbb{C}$.

d) Soit $I : \mathfrak{M}_n(\mathbb{C}) \to \mathbb{C}$ une fonction polynomiale invariante. Pour $(\lambda_1, \ldots, \lambda_n) \in \mathbb{C}^n$, on pose

$$\Psi(\lambda_1, \ldots, \lambda_n) = I(\mathrm{Diag}\,(\lambda_1, \ldots, \lambda_n))\,.$$

Montrer que Ψ est polynomiale *symétrique* sur $\mathbb{C}^n$; en déduire qu'on a un polynôme unique Θ à n lettres sur $\mathbb{C}$ tel que $\Psi(\lambda_1, \ldots, \lambda_n) = \Theta(s_1, \ldots, s_n)$, en notant

$$s_k = \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} \lambda_{i_1} \ldots \lambda_{i_k} \quad \text{pour } 1 \leqslant k \leqslant n\,.$$

On définit alors $J : \mathfrak{M}_n(\mathbb{C}) \to \mathbb{C}$, $M \mapsto \Theta(\tau_1(M), \ldots, \tau_n(M))$. En utilisant le résultat de l'exercice 11 *b*) ci-dessus, montrer que $I = J$. Conclure : quelle est l'algèbre $\mathcal{J}$? ■

a) On sait que deux matrices semblables ont même polynôme caractéristique. Nous en déduisons que si $M \in \mathfrak{M}_n(\mathbb{C})$ et $P \in \mathrm{GL}\,(n, \mathbb{C})$, alors

$$\begin{aligned}(-1)^n\ \chi_M(X) &= (-1)^n\ \chi_{PMP^{-1}}(X) = \\ &= X^n - \tau_1(M)\,X^{n-1} + \tau_2(M)\,X^{n-2} - \ldots + (-1)^n\,\tau_n(M) = \\ &= X^n - \tau_1(PMP^{-1})\,X^{n-1} + \ldots + (-1)^n\,\tau_n(PMP^{-1})\,.\end{aligned}$$

Ces deux polynômes ont mêmes coefficients, et par conséquent, pour tout $k \in [\![1, n]\!]$, $\tau_k(M) = \tau_k(PMP^{-1})$. Les fonctions polynomiales τ_k, pour $k \in [\![1, n]\!]$, sont donc bien invariantes.

b) On constate que la fonction nulle sur $\mathfrak{M}_n(\mathbb{C})$ est polynomiale invariante. Soient I et J des fonctions polynomiales invariantes sur $\mathfrak{M}_n(\mathbb{C})$, et $\lambda \in \mathbb{C}$. Pour tout $P \in \mathrm{GL}\,(n, \mathbb{C})$ et $M \in \mathfrak{M}_n(\mathbb{C})$, on a l'égalité :

$$\begin{aligned}(I + \lambda\,J)(P\,M\,P^{-1}) &= I(P\,M\,P^{-1}) + \lambda\,J(P\,M\,P^{-1}) = \\ &= I(M) + \lambda\,J(M) = (I + \lambda\,J)(M)\,.\end{aligned}$$

L'application polynomiale $I + \lambda\,J$ est invariante.
L'ensemble des applications polynomiales invariantes est donc un sous-$\mathbb{C}$-espace vectoriel de $\mathfrak{M}_n(\mathbb{C})$.

La fonction constante égale à 1 sur $\mathfrak{M}_n(\mathbb{C})$, est bien polynomiale invariante. Soient I et J des fonctions polynomiales invariantes sur $\mathfrak{M}_n(\mathbb{C})$. Pour tout $P \in \mathrm{GL}\,(n, \mathbb{C})$ et $M \in \mathfrak{M}_n(\mathbb{C})$, on a l'égalité :

$$(I\,J)(P\,M\,P^{-1}) = I(P\,M\,P^{-1})\,J(P\,M\,P^{-1}) = I(M)\,J(M) =$$

Donc $I\,J$ est polynomiale invariante.

L'ensemble des applications polynomiales invariantes est donc une sous-$\mathbb{C}$-algèbre de l'algèbre des fonctions polynomiales sur $\mathfrak{M}_n(\mathbb{C})$.

c) Soit $P \in \mathbb{C}(X_1, \ldots, X_n)$ tel que pour toute matrice $M \in \mathfrak{M}_n(X)$, on ait $P(\tau_1(M), \ldots, \tau_n(M)) = 0$; cette égalité est vraie en particulier pour toute matrice diagonale $M = \mathrm{Diag}\,(\lambda_1, \ldots, \lambda_n)$. Dans ce cas, on a :

$$\chi_M(X) = \prod_{i=1}^{n}(\lambda_i - X) = (-1)^n \left(X^n - s_1\, X^{n-1} + \ldots + (-1)^n\, s_n\right) ,$$

où pour tout $k \in [\![1, n]\!]$, $s_k = \sigma_k(\lambda_1, \ldots, \lambda_n)$. On voit donc que pour tout $k \in [\![1, n]\!]$, $\tau_k(M) = s_k = \sigma_k(\lambda_1, \ldots, \lambda_n)$. La fonction polynomiale sur $\mathbb{C}^n$:

$$(\lambda_1, \ldots, \lambda_n) \mapsto P(\sigma_1(\lambda_1, \ldots, \lambda_n), \ldots, \sigma_n(\lambda_1, \ldots, \lambda_n)) ,$$

est donc identiquement nulle. Le polynôme

$$P(\sigma_1(X_1, \ldots, X_n), \ldots, \sigma_n(X_1, \ldots, X_n)) ,$$

est donc nul. Comme les polynômes $\sigma_1, \ldots, \sigma_n$ sont algébriquement indépendants, nous en déduisons $P = 0$. Les fonctions polynomiales $\tau_1, \ldots, \tau_n$ sont donc algébriquement indépendantes.

d) Soit $(\lambda_1, \ldots, \lambda_n) \in \mathbb{C}^n$, montrons que pour toute permutation $\sigma \in \mathfrak{S}_n$ les matrices $\mathrm{Diag}\,(\lambda_1, \ldots, \lambda_n)$ et $\mathrm{Diag}\left(\lambda_{\sigma(1)}, \ldots, \lambda_{\sigma(n)}\right)$ sont semblables. Soit f l'endomorphisme de $\mathbb{C}^n$ dont la matrice dans la base canonique $\mathcal{B} = (e_1, \ldots, e_n)$ de $\mathbb{C}^n$ est la matrice $\mathrm{Diag}\,(\lambda_1, \ldots, \lambda_n)$. La matrice de f dans la base $(e_{\sigma(1)}, \ldots, e_{\sigma(n)})$ est visiblement la matrice $\mathrm{Diag}\left(\lambda_{\sigma(1)}, \ldots, \lambda_{\sigma(n)}\right)$. Ces deux matrices diagonales sont donc bien semblables.

La fonction Ψ est évidemment polynomiale ; pour tout $(\lambda_1, \ldots, \lambda_n) \in \mathbb{C}^n$, et pour toute permutation $\sigma \in \mathfrak{S}_n$, puisque les matrices $\mathrm{Diag}\,(\lambda_1, \ldots, \lambda_n)$ et $\mathrm{Diag}\left(\lambda_{\sigma(1)}, \ldots, \lambda_{\sigma(n)}\right)$ sont semblables, et que la fonction polynomiale I est invariante, on a l'égalité :

$$\begin{aligned}\Psi(\lambda_{\sigma(1)}, \ldots, \lambda_{\sigma(n)}) &= I\left(\mathrm{Diag}\left(\lambda_{\sigma(1)}, \ldots, \lambda_{\sigma(n)}\right)\right) = \\ &= I\left(\mathrm{Diag}\,(\lambda_1, \ldots, \lambda_n)\right) = \Psi(\lambda_1, \ldots, \lambda_n) .\end{aligned}$$

La fonction Ψ est donc polynomiale symétrique sur $\mathbb{C}^n$. Il existe par conséquent un unique polynôme Θ à n lettres sur $\mathbb{C}$ tel que pour tout $(\lambda_1, \ldots, \lambda_n) \in \mathbb{C}^n$, on ait l'égalité :

$$\Psi(\lambda_1, \ldots, \lambda_n) = \Theta(s_1, \ldots, s_n) ,$$

où pour tout $k \in [\![1, n]\!]$,

$$s_k = \sigma_k(\lambda_1, \ldots, \lambda_n) = \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} \lambda_{i_1} \ldots \lambda_{i_k} .$$

Soit M une matrice diagonalisable, i.e. $M \in S$ (cf. exercice 11), semblable à la matrice diagonale $\Delta = \mathrm{Diag}\,(\lambda_1, \ldots, \lambda_n)$. Pour tout $k \in [\![1, n]\!]$, puisque la fonction polynomiale τ_k est invariante (cf. *a*)), on a l'égalité $\tau_k(M) = \tau_k(\Delta) = \sigma_k(\lambda_1, \ldots, \lambda_n) = s_k$. Nous en déduisons :

$$J(M) = \Theta(\tau_1(M), \ldots, \tau_n(M)) = \Theta(\tau_1(\Delta), \ldots, \tau_n(\Delta)) =$$
$$= \Theta(s_1, \ldots, s_n) = \Psi(\lambda_1, \ldots, \lambda_n) = I(\Delta) = I(M) .$$

Les fonctions polynomiales invariantes I et J coïncident donc sur l'ensemble S des matrices diagonalisables. La fonction polynomiale $I - J$, qui est nulle sur S, est identiquement nulle (exercice 11 *b*)).

Nous en déduisons que pour toute fonction polynomiale I, invariante sur $\mathfrak{M}_n(\mathbb{C})$, il existe un unique (cf. *c*)) polynôme Θ tel que pour toute matrice $M \in \mathfrak{M}_n(\mathbb{C})$, on ait l'égalité :

$$I(M) = \Theta(\tau_1(M), \ldots, \tau_n(M)) .$$

Puisque pour tout $k \in [\![1, n]\!]$, la fonction polynomiale τ_k est invariante, on voit que l'algèbre $\mathcal{I}$ est l'algèbre $\mathbb{C}[\tau_1, \ldots, \tau_n]$, isomorphe à $\mathbb{C}[X_1, \ldots, X_n]$, puisque $(\tau_1, \ldots, \tau_n)$ est algébriquement libre.

§ XV.4 *POLYNÔMES D'ENDOMORPHISMES OU DE MATRICES*

Exercice 3 :

Soit $n \in \mathbb{N}^*$. On note $\mathcal{C}$ l'ensemble des $M \in \mathfrak{M}_n(K)$ telles que $Q_M(X) = (-1)^n \chi_M(X)$ (*i.e.* $\deg(Q_M(X)) = n$).

a) Montrer qu'il existe des fonctions polynomiales $f_1, \ldots, f_k$ sur $\mathfrak{M}_n(K)$ (avec k convenable) telles que :

$$M \notin \mathcal{C} \Leftrightarrow (\forall i \in [\![1, k]\!]\ f_i(M) = 0) .$$

b) Si $K = \mathbb{R}$ ou $\mathbb{C}$, en déduire que $\mathcal{C}$ est un *ouvert dense* de $\mathfrak{M}_n(K)$. ■

a) Soit $M \in \mathfrak{M}_n(K)$, on voit que le degré du polynôme minimal de M est n si, et seulement si, la famille $(I_n, M, \ldots, M^{n-1})$ es

$(m_1, \ldots, m_{n^2})$ une base du K-ev $\mathfrak{M}_n(K)$. Pour toute partie I de $[\![1, n^2]\!]$ de cardinal n, notons f_I l'application qui à $M \in \mathfrak{M}_n(K)$ fait correspondre le mineur $\Delta_{I,[\![1,n]\!]}$ de la matrice $\mu(M) \in \mathfrak{M}_{n^2,n}(K)$ dont les colonnes sont les vecteurs colonnes des coordonnées des matrices $(I_n, M, \ldots, M^{n-1})$ dans la base $(m_1, \ldots, m_{n^2})$. Les applications f_I sont polynomiales sur $\mathfrak{M}_n(K)$, puisque les différentes coordonnées des matrices $I_n, M, \ldots, M^{n-1}$ dans la base $(m_1, \ldots, m_{n^2})$ sont des fonctions polynomiales de M. La famille $(I_n, M, \ldots, M^{n-1})$ est libre si, et seulement si, l'un des ces mineurs n'est pas nul, i.e. si, et seulement si :

$$(\exists I \in \mathcal{P}_n([\![1, n^2]\!])) \quad f_I(M) \neq 0 \ .$$

En numérotant ces fonctions polynomiales de 1 à $k = \binom{n^2}{n}$, on trouve une famille de fonctions polynomiales vérifiant les conditions de l'énoncé.

b) Posons pour tout $i \in [\![1, k]\!]$

$$O_i = \{M \in \mathfrak{M}_n(K) \mid f_i(M) \neq 0\} \ .$$

L'ensemble O_i, image réciproque par l'application continue (car polynomiale) f_i, de l'ouvert $\mathbb{R}^*$ de $\mathbb{R}$ (resp. $\mathbb{C}^*$ de $\mathbb{C}$), est un ouvert de $\mathfrak{M}_n(\mathbb{R})$ (resp. de $\mathfrak{M}_n(\mathbb{C})$).

D'après le *a*), on a l'égalité :

$$\mathcal{C} = \bigcup_{i=1}^{k} O_i \ .$$

Nous en déduisons que $\mathcal{C}$ est un ouvert de $\mathfrak{M}_n(\mathbb{R})$ (resp. de $\mathfrak{M}_n(\mathbb{C})$). Supposons que $\mathcal{C}$ ne soit pas partout dense, alors pour tout $i \in [\![1, k]\!]$, l'ouvert O_i n'est pas partout dense. Dans ce cas, pour $i \in [\![1, k]\!]$ donné, il existe une matrice $M_0 \in \mathfrak{M}_n(K)$, et un voisinage V de M_0 dans $\mathfrak{M}_n(K)$, tel que $V \cap O_i = \emptyset$; la fonction polynomiale f_i est donc nulle sur V, donc identiquement nulle (voir exercice 1 du § X.1). On voit donc que si $\mathcal{C}$ n'était pas partout dense, toutes les fonctions polynomiales f_i, pour $i \in [\![1, k]\!]$, seraient identiquement nulles, et l'ensemble $\mathcal{C}$ serait vide.

Or l'exercice 2 montre qu'il existe des matrices dont le polynôme minimal est égal au polynôme caractéristique. Il suffit d'ailleurs de le vérifier dans un seul cas, par exemple pour la matrice :

$$M = \begin{bmatrix} 0 & \ldots & \ldots & \ldots & 0 \\ 1 & \ddots & & & \vdots \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & 1 & 0 \end{bmatrix}$$

dont le polynôme caractéristique est $(-1)^n X^n$, et dont le polynôme minimal est X^n. En effet si g est l'endomorphisme de K^n dont la matrice dans la base canonique $\mathcal{B} = (e_1, \ldots, e_n)$ est M, $g^{n-1}(e_1) = e_n \neq 0$. Le polynôme minimal de M divise X^n, s'écrit donc X^p où $p \in [\![1, n]\!]$, et $p > n-1$, donc $p = n$.

L'ensemble $\mathcal{C}$ n'est donc pas vide, et est, d'après ce qui précède, partout dense.

Exercice 4 :

Soit $n \in \mathbb{N}^*$. On donne A et B éléments de $\mathfrak{M}_n(\mathbb{C})$. Montrer l'équivalence entre les 3 conditions suivantes :

(I) $(\forall C \in \mathfrak{M}_n(\mathbb{C}))$, l'équation $AX - XB = C$, $X \in \mathfrak{M}_n(\mathbb{C})$, a une solution unique.

(II) $(\forall X \in \mathfrak{M}_n(\mathbb{C}))\quad AX - XB = 0 \Rightarrow X = 0$.

(III) A et B n'ont pas de valeur propre commune. ■

Soit $f : \mathfrak{M}_n(\mathbb{C}) \to \mathfrak{M}_n(\mathbb{C})$, $X \mapsto AX - XB$. L'application f est évidemment un endomorphisme du $\mathbb{C}$-ev $\mathfrak{M}_n(\mathbb{C})$. La propriété (I) exprime que f est bijective. La propriété (II) exprime que f est injective. Les propriétés (I) et (II) sont donc équivalentes. La contraposée de l'équivalence (II $\Leftrightarrow$ III) a été démontrée dans l'exercice 11 du § XV.2. Les propriétés (II) et (III) sont donc équivalentes.

Exercice 6 :

Soit $n \in \mathbb{N}$, $n \geqslant 2$, et $M \in \mathfrak{M}_n(K)$. On pose $N = M - XI_n$ (X est une indéterminée sur K) et $\widetilde{N} = [S_{i,j}(X)]_{(i,j)\in[\![1,n]\!]^2}$. (On sait que $\forall (i,j)\ S_{i,j}(X) \in K_{n-1}[X]$). Soit Δ le pgcd normalisé des $(S_{i,j}(X))$ dans $K[X]$, dont on vérifiera qu'il est $\neq 0$. Enfin soit $T = \dfrac{1}{\Delta}\widetilde{N}$.

a) Prouver que Δ divise $\chi_M(X)$ (utiliser $\widetilde{N}N = \chi_M(X) I_n$).

b) Si $G(X) = \dfrac{1}{\Delta}\chi_M(X)$, montrer que $TN = G(X) I_n$, et en déduire que Q_M divise G.

c) Soit $D(X) = \dfrac{\chi_M(X)}{Q_M(X)}$. Montrer qu'on a $B \in \mathfrak{M}_n(K[X])$ telle que $BN = NB = Q_M(X) I_n$.

d) Démontrer $DBN = \widetilde{N}N$. En déduire que $DB = \widetilde{N}$, puis, que D divise Δ. En déduire enfin l'expression du polynôme minimal :

$$Q_M(X) = \frac{(-1)^n\ \chi_M(X)}{\Delta}\ .\ \blacksquare$$

Si le pgcd des polynômes $(S_{i,j}(X))$, où $(i,j) \in [\![1,n]\!]^2$, était nul, ces polynômes seraient tous nuls, d'où $\widetilde{N} = 0$; cela impliquerait $0 = N\widetilde{N} = \chi_M(X)\, I_n$, d'où $\chi_M(X) = 0$, ce qui est exclu, puisque ce polynôme est de degré n.

a) On a l'égalité :

$$\Delta \cdot T\,N = \widetilde{N}\,N = \chi_M(X) \cdot I_n\ .$$

Les coefficients d'indice $(1,1)$ des deux matrices étant égaux, on voit que Δ divise $\chi_M(X)$. On pose $\chi_M(X) = \Delta\, G(X)$.

b) Nous en déduisons $\Delta \cdot T\,N = \Delta\, G(X) \cdot I_n$, d'où, puisque $\Delta \neq 0$, $T\,N = G(X) \cdot I_n$.

Posons

$$G(X) = \sum_{k=0}^{n} a_k\, X^k\ .$$

On constate l'égalité :

$$G(X\,I_n) - G(M) = \sum_{k=1}^{n} a_k \left((X\,I_n)^k - M^k\right) = (M - X\,I_n)\,B = B\,(M - X\,I_n)\ ,$$

où la matrice $B \in \mathfrak{M}_n(K[X])$ est :

$$B = -\sum_{k=1}^{n} a_k \sum_{i=0}^{k-1} X^i\, M^{k-i-1} \quad (M^0 = I_n)\ .$$

Nous en déduisons :

$$G(M) = G(M) - G(X\,I_n) + G(X)\,I_n = -B\,N + T\,N = (T - B)\,(M - X\,I_n)\ .$$

Une telle égalité n'est possible que si $T - B = 0$ et $G(M) = 0$, en effet si $T - B \neq 0$, on peut écrire $T - B = A_0 + X\,A_1 + \ldots + X^k\,A_k$, où $(A_0, \ldots, A_k) \in \mathfrak{M}_n(K)^{k+1}$, $A_k \neq 0$. On aurait alors l'égalité :

$$\begin{aligned} 0 &= (A_0 + \ldots + X^k\,A_k)\,(M - X\,I_n) - G(M) = \\ &= A_0 M - G(M) + X(A_1 M - A_0) + \ldots + X^k(A_k M - A_{k-1}) \end{aligned}$$

ce qui est contradictoire puisque $A_k \neq 0$ (lemme 1 du théorème de Hamilton-Cayley).

Nous en déduisons finalement $G(M) = 0$, et par conséquent Q_M divise G dans $K[X]$.

c) En remplaçant dans le début de la question précédente G par Q_M, on démontre l'existence d'une matrice $B \in \mathfrak{M}_n(K[X])$ telle que :

$$Q_M(X\,I_n) - Q_M(M) = (M - X\,I_n)\,B = B\,(M - X\,I_n)\ .$$

Comme ici $Q_M(M) = 0$, on en déduit :

$$Q_M(X)\,I_n = Q_M(X\,I_n) = B\,N = N\,B\ .$$

d) Nous en déduisons l'égalité :

$$D \cdot B\,N = D\,Q_M(X) \cdot I_n = \chi_M(X) \cdot I_n = \widetilde{N}\,N\ ,$$

d'où $D \cdot B = \widetilde{N}$, puisque la matrice N est régulière dans l'anneau $\mathfrak{M}_n(K[X])$ (son déterminant est le polynôme caractéristique de M). Le polynôme D divise donc tous les coefficients de la matrice $\widetilde{N}$, et divise par conséquent leur pgcd, le polynôme Δ.

Rappelons que $D\,Q_M = \chi_M = \Delta\,G$. Comme Q_M divise G (cf. *b*)), nous en déduisons Δ divise D. Les polynômes D et Δ sont par conséquent associés. Le coefficient dominant de Δ est 1 car c'est un pgcd normalisé, et le coefficient dominant de D est $(-1)^n$, car D est le quotient exact de χ_M, de coefficient dominant $(-1)^n$, par le polynôme Q_M, unitaire. Nous en déduisons $D = (-1)^n\,\Delta$, et par conséquent :

$$Q_M = \frac{(-1)^n\ \chi_M}{\Delta}\ .$$

Exercice 8 :

On donne $n \in \mathbb{N}^*$, $m \in \mathbb{N}^*$. Soit $A_0, A_1, \ldots, A_m$ dans $\mathfrak{M}_n(\mathbb{C})$, et $f(X) = \det\left(A_0\,(X^m\,I_n) + A_1\,(X^{m-1}\,I_n) + \ldots + A_m\right)$, ($X$: indéterminée sur $\mathbb{C}$). Montrer que si $M \in \mathfrak{M}_n(\mathbb{C})$ vérifie

$$A_0\,M^m + A_1\,M^{m-1} + \ldots + A_m = 0\,,$$

alors $f(M) = 0$ (généralisation du théorème XV.4.

Comme $A_0 M^m + A_1 M^{m-1} + \ldots + A_m = 0$, on a l'égalité :

$$A_0 (X^m I_n) + A_1 (X^{m-1} I_n) + \ldots + A_m =$$
$$= A_0 (X^m I_n - M^m) + A_1 (X^{m-1} I_n - M^{m-1}) + \ldots + A_{m-1}(X I_n - M) .$$

Posons pour $k \in \mathbb{N}^*$:

$$B_k = M^{k-1} + X M^{k-2} + \ldots + X^{k-2} M + X^{k-1} I_n .$$

On voit que pour tout $k \in \mathbb{N}^*$:

$$B_k (X I_n - M) = (X I_n - M) B_k = X^k I_n - M^k .$$

Nous en déduisons :

$$A_0 (X^m I_n) + A_1 (X^{m-1} I_n) + \ldots + A_m =$$
$$= (A_0 B_m + A_1 B_{m-1} + \ldots + A_{m-1} B_1)(X I_n - M) .$$

En prenant les déterminants, on voit que $f(X)$ est divisible par le polynôme caractéristique de M, et par conséquent que $f(M) = 0$ (théorème de Hamilton-Cayley).

Exercice 9 :

Le corps de base est $\mathbb{C}$. Pour $n \in \mathbb{N}^*$ on pose $\zeta_n = \mathrm{e}^{2\mathrm{i}\pi/n}$ et on se propose de calculer la somme de Gauss $G_n = \sum_{k=0}^{n-1} \zeta_n^{k^2}$.

a) Calculer G_1, G_2, G_3, G_4 et G_5. Calculer $\sum_{k=0}^{n-1} \zeta_n^{kr}$ pour $r \in \mathbb{Z}$.

b) On considère la matrice $A_n = [a_{r,s}]_{(r,s)\in[\![1,n]\!]^2}$ telle que $a_{r,s} = \zeta_n^{(r-1)(s-1)}$. Montrer que $G_n = \mathrm{Tr}\,(A_n)$. Calculer A_n^2 et A_n^4. En déduire que A_n a, au plus, 4 valeurs propres.

c) Montrer que toute matrice $U \in \mathfrak{M}_n(\mathbb{C})$ telle que $U^2 = I_n$ est diagonalisable. Pour n impair ($n = 2p+1$) expliciter une base dans laquelle A_n^2 est diagonale.

d) Montrer que $G_n \overline{G}_n = \sum_{0\leqslant r\leqslant n-1} \left(\sum_{0\leqslant s\leqslant n-1} \zeta_n^{(r+s)^2 - r^2} \right)$ et en déduire que, pour $n = 2p+1$, $|G_n| = \sqrt{n}$.

e) Montrer que la matrice A_n est semblable à une matrice diagonale $\mathrm{Diag}\,(\lambda_1, \ldots, \lambda_n)$, où les coefficients (λ_i) prennent leurs valeurs dans $\{\sqrt{n}, -\sqrt{n}, \mathrm{i}\sqrt{n}, -\mathrm{i}\sqrt{n}\}$.

Soit a, b, c, d le nombre de fois que ces valeurs respectives sont prises. Montrer que si $n = 2p+1$ $(p \in \mathbb{N})$, on a $a+b = p+1$, $c+d = p$, $(a-b)^2 + (c-d)^2 = 1$. Calculer $\det(A_n) = \prod_{k=1}^{n} \lambda_k$ et en déduire que $(b+d)$ a la même parité que p. Achever la détermination de G_n lorsque n est impair. ■

a) On trouve $G_1 = 1$, $G_2 = 1-1 = 0$, $G_3 = 1+\mathrm{j}+\mathrm{j}^4 = 1+2\,\mathrm{j} = \mathrm{i}\sqrt{3}$, $G_4 = 1+\mathrm{i}+\mathrm{i}^4+\mathrm{i}^9 = 2(1+\mathrm{i})$; enfin, en notant $u = \mathrm{e}^{2\,\mathrm{i}\,\pi/5}$, on trouve $G_5 = 1+u+u^4+u^9+u^{16} = 1+2(u+\bar{u}) = 1+4\cos(2\,\pi/5) = \sqrt{5}$.

Si $\zeta_n^r \neq 1$, on a l'égalité :

$$\sum_{k=0}^{n-1} \zeta_n^{k\,r} = \frac{1-\zeta_n^{n\,r}}{1-\zeta_n^r} = 0\,,$$

et si $\zeta_n^r = 1$, ce qui est vrai si, et seulement si, n divise r, nous obtenons :

$$\sum_{k=0}^{n-1} \zeta_n^{k\,r} = n\,.$$

b) On constate l'égalité :

$$\mathrm{Tr}\,(A_n) = \sum_{h=1}^{n} \zeta_n^{(h-1)(h-1)} = \sum_{k=0}^{n-1} \zeta_n^{k^2} = G_n\,.$$

Calcul de A_n^2 ; pour tout $(r,s) \in [\![1,n]\!]^2$, le coefficient d'indice (r,s) de la matrice A_n^2 est :

$$\sum_{h=1}^{n} \zeta_n^{(r-1)(h-1)}\,\zeta_n^{(h-1)(s-1)} = \sum_{h=1}^{n} \zeta_n^{(h-1)(r+s-2)}\,.$$

D'après ce qui précède, cette somme est nulle sauf si $n \,|\, r+s-2$, auquel cas elle est égale à n. On en déduit facilement l'égalité :

$$A_n^2 = n \begin{bmatrix} 1 & 0 & \dots & \dots & 0 \\ 0 & & & \ddots & 1 \\ \vdots & 0 & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 1 & 0 & \dots & 0 \end{bmatrix}$$

On voit que $A_n^2 = n M_\sigma$, où M_σ est la matrice associée à la permutation $\begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix}$ qui est visiblement involutive. Nous en déduisons l'égalité $A_n^4 = n^2 I_n$. Les valeurs propres de la matrice A_n sont donc dans l'ensemble des zéros du polynôme $X^4 - n^2$, soit l'ensemble $\{\sqrt{n}, -\sqrt{n}, \mathrm{i}\sqrt{n}, -\mathrm{i}\sqrt{n}\}$.

c) Le polynôme $X^2 - n^2$ étant dissocié à facteurs simples dans $\mathbb{C}[X]$, la matrice A_n^2 est diagonalisable (théorème XV.5.2). Si $\mathcal{B} = (e_1, e_2, \dots, e_n)$ est la base canonique de $\mathbb{C}^n$, et si f est l'endomorphisme de $\mathbb{C}^n$ dont la matrice dans $\mathcal{B}$ est $\frac{1}{n} A_n^2$, f est la symétrie par rapport au sous-espace $\mathrm{Ker}\,(f - \mathrm{Id}_E)$ parallèlement au sous-espace $\mathrm{Ker}\,(f + \mathrm{Id}_E)$. On a $f(e_1) = e_1$, et pour tout $k \in [\![2, n]\!]$, $f(e_k) = e_{n+2-k}$. Si $n = 2p + 1$, on voit que la base

$$\mathcal{B}' = (e_1, e_2+e_n, e_3+e_{n-1}, \dots, e_{p+1}+e_{p+2}, e_2-e_n, e_3-e_{n-1}, \dots, e_{p+1}-e_{p+2}),$$

est une base diagonale pour l'endomorphisme f. On a $f(e_1) = e_1$, pour tout $k \in [\![2, p+1]\!]$ $f(e_k + e_{n+2-k}) = e_{n+2-k} + e_k$, et pour tout $k \in [\![2, p+1]\!]$ $f(e_k - e_{n+2-k}) = e_{n+2-k} - e_k = -(e_k - e_{n+2-k})$. L'espace propre E_1 est engendré par $(e_1, e_2+e_n, \dots, e_{p+1}+e_{p+2})$, il est de dimension $p+1$. L'espace propre E_{-1} est engendré par $(e_2 - e_n, \dots, e_{p+1} - e_{p+2})$, il est de dimension p.

d) On a l'égalité :

$$G_n \overline{G}_n = \left(\sum_{k=0}^{n-1} \zeta_n^{k^2}\right)\left(\sum_{r=0}^{n-1} \zeta_n^{-r^2}\right) = \sum_{r=0}^{n-1}\sum_{k=0}^{n-1} \zeta_n^{k^2-r^2}.$$

Notons $m \mapsto \overline{m}$ l'application $\mathbb{Z} \to [\![0, n-1]\!]$ qui à un entier m fait correspondre le reste dans la division euclidienne de m par n. Pour $r \in \mathbb{Z}$ fixé, l'application $s \mapsto \overline{r+s}$ est une bijection $[\![0, n-1]\!] \to [\![0, n-1]\!]$, et comme pour tout $s \in [\![0, n-1]\!]$ on a l'égalité :

$$\zeta_n^{\left(\overline{r+s}\right)^2} = \zeta_n^{(r+s)^2},$$

nous en déduisons :

$$G_n \overline{G}_n = \sum_{r=0}^{n-1}\sum_{s=0}^{n-1} \zeta_n^{\left(\overline{r+s}\right)^2 - r^2} = \sum_{r=0}^{n-1}\sum_{s=0}^{n-1} \zeta_n^{(r+s)^2-r^2} = \sum_{s=0}^{n-1} \zeta^{s^2} \sum_{r=0}^{n-1} \zeta_n^{2rs}.$$

Pour $s \in [\![0, n-1]\!]$ fixé, la somme

$$S_s = \sum_{r=0}^{n-1} \zeta_n^{2rs},$$

est $\neq 0$ si, et seulement si, $n \mid 2s$; si n est impair cette condition équivaut à la condition $n \mid s$, soit, puisque $s \in [\![0, n-1]\!]$, $s = 0$. Comme $S_0 = n$, on en déduit l'égalité :

$$G_n \overline{G}_n = S_0 = n ,$$

d'où $|G_n| = \sqrt{n}$.

e) Le polynôme $P = X^4 - n^2$, qui est dissocié à zéros simples dans $\mathbb{C}[X]$, est annulé par la matrice A_n. Nous en déduisons que cette matrice est diagonalisable (Théorème XV.5.2). Les valeurs propres de A_n sont dans l'ensemble $\{\sqrt{n}, -\sqrt{n}, \mathrm{i}\sqrt{n}, -\mathrm{i}\sqrt{n}\}$, ensemble des zéros du polynôme P. Soit g l'endomorphisme de $\mathbb{C}^n$ dont la matrice dans la base canonique $\mathcal{B}$ de $\mathbb{C}^n$ est $\frac{1}{\sqrt{n}} A_n$. On a l'égalité $g^2 = f$ (cf. *c*)). Notons de manière générale $E_{f,\lambda} = \mathrm{Ker}\,(f - \lambda \mathrm{Id}_E)$, pour $\lambda \in \mathbb{C}$, et de même avec g, indépendamment du fait que $\lambda \in \mathbb{C}$ soit ou non valeur propre de f (resp. de g). Les nombres a, b, c, d sont respectivement les dimensions des espaces $E_{g,1}, E_{g,-1}, E_{g,\mathrm{i}}, E_{g,-\mathrm{i}}$. On a aussi $\dim E_{f,1} = p+1$ et $\dim E_{f,-1} = p$ (cf. *c*)). Les inclusions :

$$E_{g,1} \oplus E_{g,-1} \subset E_{f,1} \quad \text{et} \quad E_{g,\mathrm{i}} \oplus E_{g,-\mathrm{i}} \subset E_{f,-1} ,$$

sont évidentes, et il y a égalité puisque :

$$\mathbb{C}^n = E_{g,1} \oplus E_{g,-1} \oplus E_{g,\mathrm{i}} \oplus E_{g,-\mathrm{i}} = E_{f,1} \oplus E_{f,-1} .$$

Nous en déduisons $a + b = p + 1$ et $c + d = p$.

Nous pouvons aussi utiliser l'égalité

$$G_n = \mathrm{Tr}\,(A_n) = \sqrt{n}\,\mathrm{Tr}\,(g) = \sqrt{n}\,(a - b + \mathrm{i}\,(c - d)) ,$$

d'où, puisque $|G_n| = \sqrt{n}$, $(a-b)^2 + (c-d)^2 = 1$.

Calcul du déterminant de A_n :

$$\det(A_n) = (\sqrt{n})^n (-1)^b\, \mathrm{i}^{\,c}\, (-\mathrm{i})^d = (\sqrt{n})^n\, (-1)^{b+d}\, \mathrm{i}^{\,c+d} = (\sqrt{n})^n\, \mathrm{i}^{\,2(b+d)+p} .$$

Ce déterminant est un déterminant de Vandermonde :

$$D_n = \det(A_n) = V_n(1, \zeta_n^1, \ldots, \zeta_n^{n-1}) = \prod_{0 \leqslant i < j \leqslant n-1} (\zeta_n^j - \zeta_n^i) .$$

Posons $\xi = \mathrm{e}^{\mathrm{i}\pi/n}$ ($\xi^2 = \zeta_n$). On remarque l'égalité :

$$D_n = \prod_{0 \leqslant i < j \leqslant n-1} (\xi^{2j} - \xi^{2i}) = \prod_{0 \leqslant i < j \leqslant n-1} \xi^{i+j} \prod_{0 \leqslant i < j \leqslant n-1} \left(\xi^{j-i} - \xi^{-(j-i)}\right) .$$

On trouve :

$$\sum_{i<j} i+j = \frac{1}{2}\sum_{i\neq j} i+j = \sum_{i\neq j} i = (n-1)\sum_{i=0}^{n-1} i = \frac{1}{2}(n-1)^2 n = 2p^2 n\ ,$$

et par conséquent :

$$\prod_{0\leqslant i<j\leqslant n-1} \xi^{i+j} = \xi^{2p^2 n} = \zeta_n^{n\,p^2} = 1\ .$$

Nous en déduisons :

$$D_n = \prod_{0\leqslant i<j\leqslant n-1} \left(\xi^{j-i} - \xi^{-(j-i)}\right) = (2\,\mathrm{i}\,)^{\frac{n(n-1)}{2}} \prod_{1\leqslant i<j\leqslant n} \sin\left(\frac{(j-i)\,\pi}{n}\right)\ .$$

On remarque que pour tout (i,j) tel que $1 \leqslant i < j \leqslant n$, $0 < \frac{(j-i)\,\pi}{n} < \pi$. Le produit des sinus est donc un nombre réel > 0. On peut donc écrire :

$$D_n = \rho_n\,\mathrm{i}^{\,\frac{n(n-1)}{2}} = \rho_n\,\mathrm{i}^{\,(2p+1)\,p} \quad \text{avec} \quad \rho_n > 0\ .$$

Remarquons que c'est seulement ici qu'intervient le fait que ζ_n n'est pas une quelconque racine primitive n-ième de 1. Nous obtenons finalement l'égalité :

$$D_n = \rho_n\,\mathrm{i}^{\,(2p+1)\,p} = (\sqrt{n})^n\,\mathrm{i}^{\,2\,(b+d)+p}\ ,$$

d'où :

$$(2p+1)\,p \equiv 2\,(b+d) + p \bmod 4 \quad \text{soit} \quad p^2 \equiv b+d \bmod 2\ .$$

L'entier $b+d$, et l'entier $b-d$ ont donc même parité que p.

Supposons $p = 2q$, alors $a+b = 2q+1$ est impair, donc $a-b$ est impair, et $c+d = 2q$ est pair, donc $c-d$ est pair. Comme $(a-b)^2 + (c-d)^2 = 1$, on voit que $a-b = \varepsilon \in \{-1,1\}$, et $c = d = q$. On a l'égalité $2b = 2q+1-\varepsilon$, donc $2\,(b-d) = 1-\varepsilon$ est un multiple de 4. Nous en déduisons $\varepsilon = 1$, et $b = c = d = q$, $a = q+1$. Nous obtenons dans ce cas l'égalité :

$$G_n = \sqrt{n}\,\big(a - b + \mathrm{i}\,(c-d)\big) = \sqrt{n}\ .$$

Ce résultat est cohérent avec ce que nous avions déjà trouvé : $G_5 = \sqrt{5}$.

Supposons $p = 2q+1$, alors $a+b = 2\,(q+1)$ est pair, donc $a-b$ est pair, et $c+d = 2q+1$ est impair, donc $c-d$ est impair. Comme $(a-b)^2+(c-d)^2 = 1$, on voit que $a = b = q+1$ et $c-d = \varepsilon \in \{-1,1\}$. On a l'égalité $2d = 2q+1-\varepsilon$, donc $2\,(b-d) = 1+\varepsilon$ est congru à 2 modulo 4.

que $\varepsilon = 1$, d'où $a = b = c = q + 1$ et $d = q$. Nous obtenons donc dans ce cas l'égalité :

$$G_n = \sqrt{n}\,(a - b + \mathrm{i}\,(c - d)) = \mathrm{i}\,\sqrt{n}\,.$$

Ce résultat est cohérent avec ce que nous avions déjà trouvé : $G_3 = \mathrm{i}\sqrt{3}$.

Le lecteur pourra se reporter à la résolution de l'exercice 37 du chapitre VIII.3 du recueil d'exercices résolus d'analyse du cours de mathématiques - 2, pour une détermination des sommes de Gauss G_n, pour tout $n \in \mathbb{N}^*$, n pair ou impair.

§ XV.5 *SOUS-ESPACES CARACTÉRISTIQUES*

Exercice 1 :

Soit $n \in \mathbb{N}^*$ et $M \in \mathfrak{M}_n(\mathbb{R})$ telle que le polynôme $\chi_M(X)$ soit *dissocié sur* $\mathbb{R}$. Montrer que, pour que M soit diagonalisable dans $\mathfrak{M}_n(\mathbb{R})$, il faut et il suffit qu'elle le soit dans $\mathfrak{M}_n(\mathbb{C})$. Généraliser en remplaçant $\mathbb{R}$ et $\mathbb{C}$ par un corps commutatif K et une extension L de K. ■

Résolvons le cas général. On voit que si M est diagonalisable dans $\mathfrak{M}_n(K)$, alors elle est diagonalisable dans $\mathfrak{M}_n(L)$. Etudions l'implication réciproque.

Il semble intuitivement clair que la matrice M a même polynôme minimal, qu'elle soit considérée comme élément de $\mathfrak{M}_n(K)$ ou qu'elle soit considérée comme élément de $\mathfrak{M}_n(L)$. En admettant cette propriété, si M est diagonalisable dans $\mathfrak{M}_n(L)$, son polynôme minimal est dissocié et à facteurs simples dans $L[X]$ (corollaire du théorème XV.5.2), mais comme par hypothèse il est dissocié dans $K[X]$, il est dissocié et à facteurs simples dans $K[X]$. Nous en déduisons (corollaire du théorème XV.5.2) que M est diagonalisable dans $\mathfrak{M}_n(K)$.

Démontrons maintenant que pour toute matrice $M \in \mathfrak{M}_n(K)$, le polynôme minimal de M dans $\mathfrak{M}_n(K)$ est le même que le polynôme minimal dans $\mathfrak{M}_n(L)$. Montrons pour cela le lemme suivant :

Lemme :

Soit E un K-ev de dimension $p \in \mathbb{N}^*$, F un L-ev de dimension p (F peut être muni aussi d'une structure de K-ev) et f une application K-linéaire $E \to F$. On suppose qu'il existe une base $(e_1, \ldots, e_p)$ du K-ev E telle que $(f(e_1), \ldots, f(e_p))$ soit une base du L-ev F. Avec ces hypothèses, si $(v_1, \ldots, v_k)$ es

libre dans le K-ev E, $(f(v_1),\dots,f(v_k))$ est une famille libre dans le L-ev F. ■

Dans le K-ev E, on peut compléter la famille libre $(v_1,\dots,v_k)$ pour former une base $(v_1,\dots,v_p)$. Soit P la matrice de passage de la base $(e_1,\dots,e_p)$ vers la base $(v_1,\dots,v_p)$. Notons $a_{i,j}$, pour $(i,j)\in[\![1,p]\!]^2$, le coefficient d'indice (i,j) de P ; on a, pour tout $j\in[\![1,p]\!]$:

$$v_j=\sum_{i=1}^{p}a_{i,j}\,e_i\ .$$

D'où, pour tout $j\in[\![1,p]\!]$:

$$f(v_j)=\sum_{i=1}^{p}a_{i,j}\,f(e_i)\ .$$

La matrice de la famille de vecteurs $(f(v_1),\dots,f(v_p))\in F^p$ dans la base $(f(e_1),\dots,f(e_p))$ est donc la matrice P. Cette matrice est inversible dans $\mathfrak{M}_p(K)$ et par conséquent inversible dans $\mathfrak{M}_p(L)$. Nous en déduisons que $(f(v_1),\dots,f(v_p))$ est une base du L-ev F, et par conséquent que la famille $(f(v_1),\dots,f(v_k))$ est libre dans le L-ev F. Fin du Lemme.

Les espaces considérés ici sont $E=\mathfrak{M}_n(K)$ et $F=\mathfrak{M}_n(L)$; l'application f est l'injection canonique $\mathfrak{M}_n(K)\to\mathfrak{M}_n(L)$; elle transforme la base canonique du K-ev $\mathfrak{M}_n(K)$ en la base canonique du L-ev $\mathfrak{M}_n(L)$. Soit $M\in\mathfrak{M}_n(K)$, $P\in K[X]$ son polynôme minimal dans $\mathfrak{M}_n(K)$, et d le degré de ce polynôme. On sait que la famille $(I_n,\dots,M^{d-1})$ est libre dans $\mathfrak{M}_n(K)$. D'après le lemme, elle est libre dans le L-ev $\mathfrak{M}_n(L)$. Soit $P'\in L[X]$ le polynôme minimal de M dans $\mathfrak{M}_n(L)$, et d' le degré de ce polynôme. On voit que $d'\geqslant d$. Or $P(M)=0$, donc P' divise P dans $L[X]$. Nous en déduisons $d=d'$ et, puisque P et P' sont normalisés, $P=P'$, ce qu'il fallait démontrer. Cela achève la résolution de cet exercice.

Exercice 2 :

Soit E un K-ev de dimension finie $n\geqslant 1$ et $u\in\mathrm{Hom}_K(E)$ dont le polynôme caractéristique est *dissocié* dans $K[X]$. Montrer que u est diagonalisable ssi $(\forall\lambda\in K)\ \mathrm{rg}\,(u-\lambda\,\mathrm{Id}_E)=\mathrm{rg}\,(u-\lambda\,\mathrm{Id}_E)^2$. ■

Soit $\lambda\in K$, comme $\mathrm{Ker}\,(u-\lambda\,\mathrm{Id}_E)\subset\mathrm{Ker}\,(u-\lambda\,\mathrm{Id}_E)^2$, ces deux sous-$K$-ev sont égaux si, et seulement si, ils ont même dimension, soit si, et seulement si, $\mathrm{rg}\,(u-\lambda\,\mathrm{Id}_E)=\mathrm{rg}\,(u-\lambda\,\mathrm{Id}_E)^2$. Remarquons

$\mathrm{Ker}\,(u-\lambda\,\mathrm{Id}_E) = \mathrm{Ker}\,(u-\lambda\,\mathrm{Id}_E)^2$ est vraie si λ n'est pas valeur propre de u, puisqu'alors $u-\lambda\,\mathrm{Id}_E$ et $(u-\lambda\,\mathrm{Id}_E)^2$ sont injectifs. Nous voyons donc que la condition : $(\forall\lambda\in K)\ \ \mathrm{rg}\,(u-\lambda\,\mathrm{Id}_E) = \mathrm{rg}\,(u-\lambda\,\mathrm{Id}_E)^2$, est vraie si, et seulement si, pour toute valeur propre λ de u, $\mathrm{Ker}\,(u-\lambda\,\mathrm{Id}_E) = \mathrm{Ker}\,(u-\lambda\,\mathrm{Id}_E)^2$.

Supposons u diagonalisable, et notons $(\lambda_1,\ldots,\lambda_k)$ ses valeurs propres (distinctes). Pour tout $i\in[\![1,k]\!]$ on note E_{λ_i} l'espace propre relatif à la valeur propre λ_i de u. On a :

$$E = \bigoplus_{j=1}^{k} E_{\lambda_j}\ .$$

Soit $x = x_1+\ldots+x_k$, où pour tout $j\in[\![1,k]\!]$, $x_j\in E_{\lambda_j}$. Pour $i\in[\![1,k]\!]$, on a

$$(u-\lambda_i\,\mathrm{Id}_E)(x) = \sum_{j=1}^{k}(\lambda_j-\lambda_i)\,x_j\ ,$$

et

$$(u-\lambda_i\,\mathrm{Id}_E)^2(x) = \sum_{j=1}^{k}(\lambda_j-\lambda_i)^2\,x_j\ .$$

Les valeurs propres $(\lambda_1,\ldots,\lambda_k)$ étant distinctes, $(u-\lambda_i\,\mathrm{Id}_E)^2(x)=0$ si, et seulement si, $(\forall j\neq i)\ \ x_j=0$, soit si, et seulement si, $x\in E_{\lambda_i}$. Nous en déduisons, pour tout $i\in[\![1,k]\!]$, l'égalité :

$$E_{\lambda_i} = \mathrm{Ker}\,(u-\lambda_i\,\mathrm{Id}_E) = \mathrm{Ker}\,(u-\lambda_i\,\mathrm{Id}_E)^2\ ,$$

ce qu'il fallait démontrer.

Supposons maintenant que le polynôme minimal P de u soit dissocié ; nous pouvons poser :

$$P = \prod_{i=1}^{k}(X-\lambda_i)^{n_i}\ ,$$

où pour tout $i\in[\![1,k]\!]$, $n_i\in\mathbb{N}^*$, et $\lambda_1,\ldots,\lambda_k$ sont les valeurs propres de u (distinctes). On suppose de plus que pour tout $i\in[\![1,k]\!]$:

$$\mathrm{Ker}\,(u-\lambda_i\,\mathrm{Id}_E) = \mathrm{Ker}\,(u-\lambda_i\,\mathrm{Id}_E)^2\ .$$

Supposons qu'il existe $i\in[\![1,k]\!]$ tel que $n_i\geqslant 2$. On a alors l'égalité :

$$(u-\lambda_i\,\mathrm{Id}_E)^2\,(u-\lambda_i\,\mathrm{Id}_E)^{n_i-2}\prod_{j\neq i}(u-\lambda_j\,\mathrm{Id}_E)^{n_j} = 0\ .$$

ce qui s'écrit aussi :

$$\mathrm{Im}\left((u-\lambda_i \mathrm{Id}_E)^{n_i-2}\prod_{j\neq i}(u-\lambda_j \mathrm{Id}_E)^{n_j}\right) \subset \mathrm{Ker}\,(u-\lambda_i \mathrm{Id}_E)^2 \ .$$

Comme $\mathrm{Ker}\,(u-\lambda_i \mathrm{Id}_E) = \mathrm{Ker}\,(u-\lambda_i \mathrm{Id}_E)^2$, nous en déduisons :

$$\mathrm{Im}\left((u-\lambda_i \mathrm{Id}_E)^{n_i-2}\prod_{j\neq i}(u-\lambda_j \mathrm{Id}_E)^{n_j}\right) \subset \mathrm{Ker}(u-\lambda_i \mathrm{Id}_E) \ ,$$

soit :

$$(u-\lambda_i \mathrm{Id}_E)\,(u-\lambda_i \mathrm{Id}_E)^{n_i-2}\prod_{j\neq i}(u-\lambda_j \mathrm{Id}_E)^{n_j} = 0 \ .$$

Cela contredirait la minimalité du polynôme P.
Nous en déduisons que le polynôme P est dissocié et à facteurs simples, et par conséquent que u est diagonalisable (Théorème XV.5.2).

Exercice 3 :

> Soit E un K-ev de dimension finie $n \geqslant 1$ et $u \in \mathrm{Hom}_K(E)$, supposé *diagonalisable*. On donne un sous-K-ev F de E qui est u-stable. Montrer que F admet dans E un supplémentaire u-stable. ■

Soient $\lambda_1, \ldots, \lambda_k$ les valeurs propres de u (distinctes). Pour $i \in [\![1,k]\!]$, nous noterons E_{λ_i} l'espace propre relatif à la valeur propre λ_i de u. Par définition :

$$E = \bigoplus_{i=1}^{k} E_{\lambda_i} \ .$$

Le sous-K-ev F étant u-stable, on sait qu'il est somme (directe) de sous-K-ev des espaces propres (Remarque 2, Théorème XV.5.1 ("lemme des noyaux")). On a donc une décomposition :

$$F = \bigoplus_{i=1}^{k} F_i \ .$$

où, pour tout $i \in [\![1,k]\!]$, F_i est un sous-K-ev de E_{λ_i}. Pour tout $i \in [\![1,k]\!]$, F_i a, dans E_{λ_i}, un supplémentaire G_i, et ce supplémentaire est bien stable par u puisque l'endomorphisme de E_{λ_i} induit par u est l'homothétie de rapport λ_i. On voit facilement que le sous-K-ev :

$$G = \bigoplus_{i=1}^{k} G_i \ ,$$

est un supplémentaire u-stable de F.

Exercice 4 :

> Soit E un K-ev de dimension finie $n \geqslant 1$. On donne une partie non vide $\mathcal{H}$ de $\mathrm{Hom}_K(E)$ telle que $(\forall (u,v) \in \mathcal{H}^2) \quad uv = vu$, et $(\forall u \in \mathcal{H}) \quad u$ est diagonalisable. Montrer qu'il existe une base $\mathcal{B}$ de E telle que, pour tout $u \in \mathcal{H}$, $\mathcal{B}$ est une base de vecteurs propres de u (raisonner par récurrence sur n). ■

Démontrons cette propriété par récurrence sur la dimension n de E. Elle est évidemment vraie pour $n = 1$. Supposons que cette propriété soit vraie pour tout K-ev de dimension $\leqslant n$, où $n \in \mathbb{N}^*$. Soit E un K-ev de dimension $(n+1)$, et $\mathcal{H}$ une partie de $\mathrm{Hom}_K(E)$ vérifiant les hypothèses de l'énoncé.

Si les éléments de $\mathcal{H}$ sont tous des homothéties, alors toute base de E est pour tout $u \in \mathcal{H}$ une base de vecteurs propres de u. Sinon, il existe $u \in \mathcal{H}$ qui ne soit pas une homothétie. Soient $\lambda_1, \ldots, \lambda_k$ les valeurs propres de u (distinctes) ; par hypothèse $k \geqslant 2$. Notons, pour $i \in [\![1,k]\!]$, E_{λ_i} l'espace propre relatif à la valeur propre λ_i de u. On a par hypothèse :

$$E = \bigoplus_{i=1}^{k} E_{\lambda_i} .$$

Soit $i \in [\![1,k]\!]$, pour tout $v \in \mathcal{H}$, comme v et u commutent, E_{λ_i} est stable par v, et l'endomorphisme v' de E_{λ_i}, induit par v sur E_{λ_i}, est diagonalisable (Théorème XV.5.2 Exemple 2). Soit $\mathcal{H}'$ l'ensemble des endomorphismes de E_{λ_i} induits sur E_{λ_i} par les $v \in \mathcal{H}$. L'ensemble $\mathcal{H}'$ est un ensemble d'endomorphismes diagonalisables et deux à deux permutables de E_{λ_i}. Comme $\dim E_{\lambda_i} < (n+1)$, on peut appliquer à $\mathcal{H}'$ l'hypothèse de récurrence. Il existe donc une base $\mathcal{B}'_i$ de E_{λ_i} qui est, pour tout $v \in \mathcal{H}$, composée de vecteurs propres de v.

En concaténant les bases $\mathcal{B}'_i$, pour $i \in [\![1,k]\!]$, on obtient une base $\mathcal{B}$ de E telle que pour tout $v \in \mathcal{H}$, $\mathcal{B}$ est constituée de vecteurs propres de v. La propriété est donc vraie pour $n+1$, ce qui termine la démonstration par récurrence.

Exercice 6 :

> Soit E un $\mathbb{C}$-ev de dimension finie $n \geqslant 1$ et $f \in \mathrm{Hom}_{\mathbb{C}}(E)$. On note T_f l'endomorphisme de $\mathrm{Hom}_{\mathbb{C}}(E)$ tel que
>
> $$T_f(u) = f \circ u - u \circ f , \quad \text{pour } u \in \mathrm{Hom}_{\mathbb{C}}(E) .$$
>
> Montrer que T_f est diagonalisable si, et seuleme

‖ diagonalisable. ■

Montrons que si f est diagonalisable, alors $1'_f$ est diagonalisable, le corps de base étant quelconque, noté K.

Soit $(e_1, \ldots, e_n)$ une base de E composée de vecteurs propres de f, et $(u_{i,j})_{(i,j)\in[\![1,n]\!]^2}$ la base de $\mathrm{Hom}_K(E)$ associée, c'est-à-dire par définition, pour tout $(i,j) \in [\![1,n]\!]^2$, et pour tout $h \in [\![1,n]\!]$ (δ symbole de Kronecker) :

$$u_{i,j}(e_h) = \delta_{j,h}\, e_i \ .$$

Rappelons que pour tout $(i,j,h,k) \in [\![1,n]\!]^4$, on a l'égalité :

$$u_{i,j} \circ u_{h,k} = \delta_{j,h}\, u_{i,k} \ .$$

Posons, pour $i \in [\![1,n]\!]$, $f(e_i) = \lambda_i\, e_i$, on a donc :

$$f = \sum_{i=1}^{n} \lambda_i\, u_{i,i} \ .$$

Pour tout $(h,k) \in [\![1,n]\!]^2$ on a l'égalité :

$$T_f(u_{h,k}) = \sum_{i=1}^{n} \lambda_i\, u_{i,i}\, u_{h,k} - \sum_{j=1}^{n} \lambda_j\, u_{h,k}\, u_{j,j} = (\lambda_h - \lambda_k)\, u_{h,k} \ .$$

La base $(u_{h,k})_{(h,k)\in[\![1,n]\!]^2}$ est donc une base de $\mathrm{Hom}_K(E)$ constituée de vecteurs propres de T_f. Nous en déduisons que l'endomorphisme T_f de $\mathrm{Hom}_K(E)$ est diagonalisable, ce qu'il fallait démontrer.

Réciproque : nous supposerons que T_f est diagonalisable et que le polynôme caractéristique de f est dissocié sur K, ce qui est vrai si $K = \mathbb{C}$. D'après le Théorème XV.5.5, on peut écrire f sous la forme $f = D + \nu$, où D est diagonalisable, ν nilpotent, et $D\nu = \nu D$. On a bien sûr l'égalité $T_f = T_D + T_\nu$. Les endomorphismes T_D et T_ν commutent, en effet, pour tout $u \in \mathrm{Hom}_K(E)$:

$$\begin{aligned} T_D(T_\nu(u)) &= D\,(\nu\, u - u\,\nu) - (\nu\, u - u\,\nu)\, D = \\ &= D\nu u - D u \nu - \nu u D - u \nu D = \\ &= \nu\, D u - \nu u D - D u \nu - u D \nu = T_\nu(T_D(u)) \ . \end{aligned}$$

L'endomorphisme T_D est, d'après ce qui précède, diagonalisable. Montrons enfin que l'endomorphisme T_ν est nilpotent. Montrons pour cela par récurrence sur $m \in \mathbb{N}^*$, que pour tout $u \in \mathrm{Hom}_K(E)$, on a l'égalité :

$$(T_\nu)^m(u) = \sum_{i=0}^{m} (-1)^i \binom{m}{i} \nu^{m-i}\, u\, \nu^i \ .$$

Cette égalité est vraie par définition pour $m = 1$; supposons la vraie pour m ($m \geqslant 1$). On obtient pour tout $u \in \mathrm{Hom}_K(E)$:

$$\begin{aligned}
(T_\nu)^{m+1}(u) &= \sum_{i=0}^{m}(-1)^i\binom{m}{i}\nu^{m+1-i}\,u\,\nu^i - \sum_{i=0}^{m}(-1)^i\binom{m}{i}\nu^{m-i}\,u\,\nu^{i+1} \\
&= \sum_{i=0}^{m}(-1)^i\binom{m}{i}\nu^{m+1-i}\,u\,\nu^i + \sum_{j=1}^{m+1}(-1)^j\binom{m}{j-1}\nu^{m+1-j}\,u\,\nu^j = \\
&= \nu^{m+1}u + \sum_{i=1}^{m}(-1)^i\left(\binom{m}{i} + \binom{m}{i-1}\right)\nu^{m+1-i}\,u\,\nu^i + u\,\nu^{m+1} = \\
&= \sum_{i=0}^{m+1}(-1)^i\binom{m+1}{i}\nu^{m+1-i}\,u\,\nu^i\ .
\end{aligned}$$

L'égalité est donc vraie pour $m+1$. Cette égalité est donc vraie pour tout $m \in \mathbb{N}^*$.
Supposons $\nu^k = 0$, où $k \in \mathbb{N}^*$, pour tout $u \in \mathrm{Hom}_K(E)$ on a l'égalité :

$$(T_\nu)^{2k-1}(u) = \sum_{i=0}^{2k-1}(-1)^i\binom{2k-1}{i}\nu^{2k-1-i}\,u\,\nu^i\ .$$

Or si $i \in [\![0, k-1]\!]$, $2k-1-i \geqslant k$, donc $\nu^{2k-1-i} = 0$, et si $i \in [\![k, 2k-1]\!]$, $\nu^i = 0$. Nous en déduisons $(T_\nu)^{2k-1} = 0$. L'endomorphisme T_ν est donc bien nilpotent.
On voit donc que l'égalité : $T_f = T_D + T_\nu$, est la décomposition de Jordan de l'endomorphisme T_f (Théorème XV.5.5). Comme T_f est supposé diagonalisable, nous en déduisons $T_\nu = 0$, soit ν central, et par conséquent de la forme $\lambda\,\mathrm{Id}_E$, où $\lambda \in K$. Mais comme ν est nilpotent, ce n'est possible que si $\lambda = 0$, soit $\nu = 0$. L'endomorphisme f est donc diagonalisable, ce qu'il fallait démontrer.

Exercice 8 :

Soit p et n deux entiers $\geqslant 2$ et $A_0, A_1, \ldots, A_{p-1} \in \mathfrak{M}_n(\mathbb{C})$ des matrices *deux à deux permutables* et *diagonalisables*. On considère la matrice circulante par blocs $M \in \mathfrak{M}_{np}(\mathbb{C})$:

$$M = \begin{bmatrix} A_0 & A_1 & \ldots & A_{p-1} \\ A_{p-1} & A_0 & \ldots & \vdots \\ \vdots & & \ddots & \vdots \\ A_1 & \ldots & \ldots & A_0 \end{bmatrix}.$$

Montrer que M est diagonalisable. ■

Nous reprenons les notations et résultats de l'exercice 7 du § XV.1. Nous avions noté alors $M = \Gamma(A_0, \ldots, A_{p-1})$.

Soit ζ un générateur du groupe des racines p-ièmes de 1 dans $\mathbb{C}$. Notons $\Omega \in \mathfrak{M}_{np}(\mathbb{C})$ la matrice composée de p^2 blocs carrés de taille n, dont le bloc d'indice (i,j), pour $(i,j) \in [\![1,p]\!]^2$, est $\zeta^{(i-1)(j-1)} I_n$. La matrice $\Gamma(A_0, A_1, \ldots, A_{p-1}) \times \Omega$ est composée de p^2 blocs carrés de taille n et pour tout $(i,j) \in [\![1,p]\!]^2$, son bloc d'indice (i,j) est :

$$B_{i,j} = \sum_{k=1}^{p} A_{\overline{k-i}} \zeta^{(k-1)(j-1)} I_n .$$

Pour $h \in \mathbb{Z}$, $\overline{h}$ représente ici le reste dans la division euclidienne de h par p. On remarque que pour tout $(i,j) \in [\![1,p]\!]^2$, l'application $k \mapsto \overline{k-i}$ est une bijection entre $[\![1,p]\!]$ et $[\![0,p-1]\!]$, et que d'autre part, en notant $q = \overline{k-i}$:

$$\zeta^{(k-1)(j-1)} = \zeta^{(k-i)(j-1)} \zeta^{(i-1)(j-1)} = \zeta^{q(j-1)} \zeta^{(i-1)(j-1)} .$$

Nous en déduisons :

$$B_{i,j} = \sum_{q=0}^{p-1} A_q \zeta^{q(j-1)} \zeta^{(i-1)(j-1)} I_n = \zeta^{(i-1)(j-1)} I_n \sum_{q=0}^{p-1} \zeta^{q(j-1)} A_q .$$

On a donc l'égalité :

$$\Gamma(A_0, A_1, \ldots, A_{p-1}) \times \Omega = \Omega \times \Delta ,$$

où Δ est la matrice diagonale par blocs, dont le bloc diagonal d'indice j est :

$$D_j = \sum_{q=0}^{p-1} \zeta^{q(j-1)} A_q .$$

La matrice Ω est bien inversible : on vérifie facilement que si $\overline{\Omega}$ est sa conjuguée, $\Omega \overline{\Omega} = p I_{np}$. On voit donc que la matrice $M = \Gamma(A_0, \ldots, A_{p-1})$ est semblable à la matrice Δ, et par conséquent qu'elle est diagonalisable si, et seulement si, Δ est diagonalisable.

Les matrices A_q, pour $q \in [\![0,p-1]\!]$, sont diagonalisables et deux à deux permutables. D'après l'exercice 4, elles sont simultanément diagonalisables. Il est alors clair que les matrices D_j, pour $j \in [\![1,p]\!]$, sont diagonalisables (simultanément d'ailleurs), et par conséquent que Δ est diagonalisable. La matrice M est donc diagonalisable.

Exercice 9 :

> Soit $n \in \mathbb{N}^*$ $(n \geqslant 2)$ et E un $\mathbb{C}$-ev de dimension n. Montrer qu'il existe un voisinage V de Id_E dans $\mathrm{Hom}_{\mathbb{C}}(E)$ tel que $\{\mathrm{Id}_E\}$ soit le seul sous-groupe de $\mathrm{GL}_{\mathbb{C}}(E)$ inclus dans V. ■

Soit $\varphi : E \to \mathbb{C}^n$ un isomorphisme $\mathbb{C}$-linéaire. L'application : $\mathrm{Hom}_{\mathbb{C}}(E) \to \mathrm{Hom}_{\mathbb{C}}(\mathbb{C}^n)$, $f \mapsto \varphi f \varphi^{-1}$, est un isomorphisme d'algèbres et un homéomorphisme pour les topologies des normes. On voit donc que la proposition de l'énoncé est vraie si, et seulement si, elle est vraie dans le cas particulier où $E = \mathbb{C}^n$, ce que nous supposerons dans ce qui suit.

Munissons l'espace $\mathbb{C}^n$ de la norme hermitienne canonique, et le $\mathbb{C}$-espace $\mathrm{Hom}_{\mathbb{C}}(\mathbb{C}^n)$ de la norme associée :

$$|||f||| = \sup_{x \neq 0} \left\{ \frac{\|f(x)\|}{\|x\|} \right\} .$$

Soit H un sous-groupe de $\mathrm{GL}_{\mathbb{C}}(\mathbb{C}^n)$, $H \neq \{\mathrm{Id}_E\}$, montrons qu'il existe dans H des éléments g tels que $|||g - \mathrm{Id}_E||| \geqslant c$, où c est la longueur du côté d'un triangle équilatéral inscrit dans un cercle de rayon 1, soit $c = \sqrt{3}$. Nous pourrons en déduire que la boule ouverte de centre Id_E et de rayon $\sqrt{3}$ dans $\mathrm{Hom}_{\mathbb{C}}(\mathbb{C}^n)$ ne contient qu'un seul sous-groupe de $\mathrm{GL}_{\mathbb{C}}(\mathbb{C}^n)$, le sous-groupe $\{\mathrm{Id}_E\}$.

Supposons que H contienne un élément f qui ait une valeur propre $\lambda \in \mathbb{C}$, de module $\neq 1$. Soit $x \in \mathbb{C}^n$, $x \neq 0$, tel que $f(x) = \lambda x$. Pour tout $k \in \mathbb{Z}$, $f^k \in H$ et $(f^k - \mathrm{Id}_E)(x) = (\lambda^k - 1)x$. Nous en déduisons, pour tout $k \in \mathbb{Z}$:

$$|||f^k - \mathrm{Id}_E||| \geqslant |\lambda^k - 1| .$$

L'ensemble $\{|\lambda^k - 1| \ , \ k \in \mathbb{Z}\}$ n'étant pas majoré, il existe $k \in \mathbb{Z}$ tel que $|\lambda^k - 1| \geqslant \sqrt{3}$. Il existe donc $g \in H$ tel que $|||g - \mathrm{Id}_E||| \geqslant \sqrt{3}$.

Supposons maintenant que pour tout $f \in H$, les valeurs propres de f soient toutes de module 1. On suppose d'abord qu'il y a au moins un élément f de H, qui ait une valeur propre $\lambda \neq 1$. Comme λ^{-1} est valeur propre de $f^{-1} \in H$, on peut supposer que la partie imaginaire de λ est $\geqslant 0$. Posons $\lambda = e^{i\theta}$, où $\theta \in]0, \pi]$. Comme précédemment, pour tout $k \in \mathbb{Z}$,

$$|||f^k - \mathrm{Id}_E||| \geqslant |\lambda^k - 1| = 2\,|\sin(k\theta/2)| .$$

Si $\pi/3 \leqslant \theta/2 \leqslant \pi/2$, on choisit $k = 1$; sinon, on prend le plus petit entier k tel que $\pi/3 \leqslant k\theta/2$. On a alors $(k-1)\theta/2 < \pi/3$, et comme

on a $\pi/3 \leqslant k\theta/2 < 2\pi/3$. On trouve donc toujours un entier k tel que $|\sin(k\theta/2)| \geqslant \sqrt{3}/2$. Il existe donc $g \in H$ tel que

$$|||g - \mathrm{Id}_E||| \geqslant \sqrt{3} .$$

Supposons enfin que pour tout $f \in H$, toutes les valeurs propres de f soient 1. Soit $f \in H$, $f \neq \mathrm{Id}_E$. On peut écrire $f = \mathrm{Id}_E + h$, où h est nilpotent non nul (Théorème XV.5.5). Soit $x \in \mathrm{Ker}\,(h^2) \setminus \mathrm{Ker}\,(h)$. Pour tout $k \in \mathbb{N}^*$, en utilisant la formule du binôme, et le fait que pour tout $p > 1$, $h^p(x) = 0$, on voit que :

$$(f^k - \mathrm{Id}_E)(x) = k\,h(x) .$$

Nous en déduisons que pour tout $k \in \mathbb{N}^*$:

$$|||f^k - \mathrm{Id}_E||| \geqslant k\frac{\|h(x)\|}{\|x\|} .$$

On peut donc trouver $k \in \mathbb{N}^*$ tel que $|||f^k - \mathrm{Id}_E||| \geqslant \sqrt{3}$. On peut donc trouver $g \in H$ tel que :

$$|||g - \mathrm{Id}_E||| \geqslant \sqrt{3} .$$

Cela termine la démonstration.

Exercice 12 :

Soit $n \in \mathbb{N}^*$. Une matrice $S = [p_{i,j}]_{(i,j)\in[\![1,n]\!]^2} \in \mathfrak{M}_n(\mathbb{R})$ est dite *stochastique* ssi

$$(\forall (i,j) \in [\![1,n]\!]^2)\ p_{i,j} \in \mathbb{R}_+ \quad \text{et} \quad (\forall i \in [\![1,n]\!])\ \sum_{j=1}^{n} p_{i,j} = 1 .$$

Elle est dite *stochastique stricte* ssi, de plus, on a : $\forall (i,j)\ p_{i,j} > 0$. On notera $\mathcal{S}$ (resp. $\mathcal{S}^*$) l'ensemble des matrices stochastiques (resp. stochastiques strictes) de $\mathfrak{M}_n(\mathbb{R})$. Ces ensembles sont stables par le produit.

a) Soit $S = [p_{i,j}] \in \mathcal{S}^*$ fixée. L'élément de $\mathrm{Hom}_{\mathbb{C}}(\mathbb{C}^n)$ dont la matrice dans la base canonique $\mathcal{B} = (e_1, \ldots, e_n)$ de $E = \mathbb{C}^n$, est S, sera noté U.

1) On munit E de la norme

$$x = (x_1, \ldots, x_n) \mapsto \operatorname*{Max}_{i\in[\![1,n]\!]}(|x_i|) = \|x\| .$$

Montrer que pour tout $x \in E$, $\|U(x)\| \leqslant \|x\|$, et en déduire que si $\lambda \in \mathbb{C}$ est valeur propre de U, alors $|\lambda| \leqslant$

2) Montrer que 1 est valeur propre de U, que le $\mathbb{C}$-sous-espace propre correspondant est de dimension 1, et que 1 est la seule valeur propre de U qui soit de module 1.

3) Soit α_1 la multiplicité de la valeur propre 1 de U, montrer que $\alpha_1 = 1$.

4) Soit P la somme vectorielle des espaces caractéristiques de U *autres que* N_1, et soit $\varphi : E \to N_1$ la projection de E sur N_1 parallèlement à P.

- Si $x \in E$, on a $\lim\limits_{m\to\infty} U^m(x) = \varphi(x)$.
- En déduire qu'il existe $c_1, c_2, \ldots, c_n \in \mathbb{R}_+$ tels que $\sum\limits_{i=1}^{n} c_i = 1$

et que

$$\lim_{m\to\infty} S^m = \begin{bmatrix} c_1 & c_2 & \ldots & c_n \\ c_1 & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ c_1 & c_2 & \ldots & c_n \end{bmatrix}.$$

b) Etudier de même le cas où S fixée est une matrice de $\mathcal{S}$. Montrer que les valeurs propres d'une telle S dont le module est égal à 1 sont en réalité des racines N-ièmes de 1 pour N convenable.

c) *Application numérique* :

$$S = \begin{pmatrix} 1/2 & 1/4 & 1/4 \\ 1/4 & 1/2 & 1/4 \\ 1/4 & 1/4 & 1/2 \end{pmatrix} \quad \text{et} \quad S = \begin{pmatrix} 1/2 & 1/2 & 0 \\ 0 & 1/2 & 1/2 \\ 0 & 0 & 1 \end{pmatrix}. \blacksquare$$

a) 1) Soit $x = (x_1, \ldots, x_n) \in \mathbb{C}^n$, les composantes de $U(x)$ sont les complexes :

$$y_i = \sum_{j=1}^{n} p_{i,j}\, x_j \quad (i \in [\![1, n]\!]).$$

Comme pour tout $(i, j) \in [\![1, n]\!]^2$, $p_{i,j} \in \mathbb{R}_+$, on voit que pour tout $i \in [\![1, n]\!]$:

$$|y_i| \leqslant \sum_{j=1}^{n} p_{i,j}\, |x_j| \leqslant \sum_{j=1}^{n} p_{i,j}\, \|x\| = \|x\|.$$

Nous en déduisons $\|U(x)\| \leqslant \|x\|$. Il est alors clair que les valeurs propres de U sont toutes de module $\leqslant 1$.

2) On vérifie facilement que $U(1, 1, \ldots, 1) = (1, 1, \ldots, 1)$ et par conséquent que 1 est valeur propre de U.

Soit $\lambda \in \mathbb{C}$ valeur propre de U, $|\lambda| = 1$, et $x = (x_1, \ldots, x_n)$ vecteur propre pour la valeur propre λ de U. On a pour tout $i \in [\![1, n]\!]$ l'égalité :

$$(1) \qquad \sum_{j=1}^{n} p_{i,j}\, x_j = \lambda\, x_i \ ,$$

d'où, pour $i \in [\![1, n]\!]$ tel que $|x_i| = \|x\|$ (> 0) :

$$(2) \qquad g = \sum_{j=1}^{n} p_{i,j}\, \frac{x_j}{\lambda\, x_i} = 1 \ .$$

Les complexes $\dfrac{x_j}{\lambda\, x_i}$ sont tous de module $\leqslant 1$. Le complexe g est un barycentre à coefficients > 0 de cette famille et il est géométriquement clair que l'égalité (2) n'est possible que si $(\forall j)\ \dfrac{x_j}{\lambda\, x_i} = 1$. Plus précisément, posons pour tout $j \in [\![1, n]\!]$ $\dfrac{x_j}{\lambda\, x_i} = a_j + \mathrm{i}\, b_j$, où $(a_j, b_j) \in \mathbb{R}^2$. On a pour tout $j \in [\![1, n]\!]$ $a_j^2 + b_j^2 \leqslant 1$, d'où $a_j \leqslant 1$. D'autre part :

$$\sum_{j=1}^{n} p_{i,j}\, a_j = 1 = \sum_{j=1}^{n} p_{i,j} \quad \text{d'où} \quad \sum_{j=1}^{n} p_{i,j}\, (1 - a_j) = 0 \ .$$

Nous en déduisons, puisque les coefficients $p_{i,j}$ sont tous > 0 et que les réels $1 - a_j$ sont $\geqslant 0$, que pour tout $j \in [\![1, n]\!]$, $a_j = 1$. Mais alors, pour tout $j \in [\![1, n]\!]$, $b_j = 0$ et $\dfrac{x_j}{\lambda\, x_i} = a_j + \mathrm{i}\, b_j = 1$, ce que nous voulions démontrer. En particulier pour $j = i$ cela implique $\lambda = 1$; d'où $(\forall j \in [\![1, n]\!])$ $x_j = x_i$. On voit donc que la seule valeur propre de U de module 1 est 1, et que l'espace propre associé est de dimension 1, engendré par le n-uplet $(1, 1, \ldots, 1)$.

3) L'espace caractéristique N_1 relatif à la valeur propre 1 de U est de dimension α_1, il est stable par U et $U_1 = U\|_{N_1}$ s'écrit $U_1 = \mathrm{Id}_{E_1} + v$, où v est nilpotent. Si $v \neq 0$ alors $\mathrm{Ker}\,(v^2) \neq \mathrm{Ker}\,(v)$ (sinon $(\forall k \in \mathbb{N}^*)$ $\mathrm{Ker}\,(v) = \mathrm{Ker}\,(v^k) = N_1$ et $v = 0$). On peut donc trouver $y \in N_1$, tel que $v^2(y) = 0$ et $v(y) \neq 0$. On a alors, pour tout $m \in \mathbb{N}^*$:

$$U^m(y) = U_1^m(y) = (\mathrm{Id}_{N_1} + v)^m(y) = y + \binom{m}{1} v(y) = y + m\, v(y) \ ,$$

d'où :

$$m\, \|v(y)\| \leqslant \|U^m(y)\| + \|y\| \leqslant 2\, \|y\| \ .$$

Cela est évidemment contradictoire, donc $v = 0$, soit $U_1 = \mathrm{Id}_{N_1}$. On voit alors que N_1 est aussi l'espace propre de U relatif à la valeur propre 1 de U, et qu'il est de dimension 1. Nous en déduisons $\alpha_1 = \dim N$

4) Soit $\lambda \in \mathbb{C}$ une valeur propre de U, $\lambda \neq 1$, donc $|\lambda| < 1$, et N l'espace caractéristique associé, de dimension α. Le sous-espace N est stable par U et on peut écrire $U\|_N = \lambda \mathrm{Id}_N + w$, où w est un endomorphisme nilpotent de N. Pour tout $y \in N$, pour tout $m \in \mathbb{N}$, $m \geqslant \alpha$, en utilisant l'égalité du binôme de Newton nous obtenons :

$$U^m(y) = (\lambda \mathrm{Id}_N + w)^m(y) = \sum_{k=0}^{\alpha-1} \binom{m}{k} \lambda^{m-k} w^k(y) .$$

Posons $P_0(X) = 1$ et pour tout $k \in [\![1, \alpha - 1]\!]$:

$$P_k(X) = \frac{X(X-1)\dots(X-k+1)}{k(k-1)\dots 1} .$$

Pour tout $k \in [\![0, \alpha - 1]\!]$, comme P_k est un polynôme, on sait que

$$\lambda^{m-k} \binom{m}{k} = \lambda^{m-k} P_k(m) \underset{m\to\infty}{\longrightarrow} 0 .$$

Nous en déduisons $U^m(y) \underset{m\to\infty}{\longrightarrow} 0$.

Soit $x \in E$, écrivons $x = \varphi(x) + y_1 + \dots + y_k$, où $y_1, \dots, y_k$ sont les projections de x sur les espaces caractéristiques de U, relatifs aux valeurs propres autres que 1. D'après ce qui précède, pour tout $i \in [\![1, k]\!]$, $U^m(y_i) \underset{m\to\infty}{\longrightarrow} 0$, donc $U^m(x) \underset{m\to\infty}{\longrightarrow} \varphi(x)$ ($\varphi(x)$ est invariant par U).

Nous en déduisons $U^m \underset{m\to\infty}{\longrightarrow} \varphi$, et par conséquent que $S^m \underset{m\to\infty}{\longrightarrow} \mathrm{Mat}_{\mathscr{B}}(\varphi)$. Les vecteurs colonnes de cette matrice sont les vecteurs colonnes des coordonnées des vecteurs $(\varphi(e_1), \dots, \varphi(e_n))$ dans la base canonique de $\mathbb{C}^n$. Comme $\varphi(e_1), \dots, \varphi(e_n)$ sont dans l'espace propre de U relatif à la valeur propre 1, il sont colinéaires à $(1, 1, \dots, 1)$, et de plus $\varphi(e_1) + \dots + \varphi(e_n) = \varphi(e_1 + \dots + e_n) = e_1 + \dots + e_n$. On voit donc qu'il existe des *complexes* $(c_1, \dots, c_n)$ tels que : $\sum_{i=1}^{n} c_i = 1$ et :

$$\mathrm{Mat}_{\mathscr{B}}(\varphi) = \lim_{m\to\infty} S^m = \begin{bmatrix} c_1 & c_2 & \dots & c_n \\ c_1 & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ c_1 & c_2 & \dots & c_n \end{bmatrix} .$$

Remarquons enfin que puisque $\mathscr{S}$ est stable par le produit, pour tout $m \in \mathbb{N}^*$, $S^m \in \mathscr{S}$. Les coefficients de la matrice $\mathrm{Mat}_{\mathscr{B}}(\varphi)$, limites de suites de réels $\geqslant 0$, sont tous *réels* $\geqslant 0$. On a donc pour tout $i \in [\![1, n$

Remarquons enfin que nous avons obtenu ce résultat en utilisant uniquement le fait que 1 est la seule valeur propre de module 1, et que l'espace propre relatif à la valeur propre 1 est de dimension 1. L'hypothèse que S est stochastique sticte n'a été utilisée que pour démontrer que dans ce cas, ces conditions sont réunies.

b) On démontre avec les mêmes arguments que dans le *a*), que pour tout $x \in \mathbb{C}^n$, $\|U(x)\| \leqslant \|x\|$, et par conséquent que les valeurs propres de U sont de module $\leqslant 1$. Mais ici 1 n'est pas nécessairement la seule valeur propre de module 1. On peut remarquer que pour tout $\sigma \in \mathfrak{S}_n$, la matrice associée $M_\sigma \in \mathfrak{M}_n(\mathbb{C})$ est stochastique (diagonalisable car $M_\sigma^{n!} = I_n$). Les valeurs propres de ces matrices sont des racines m-ièmes de 1, avec $m \in \mathbb{N}^*$.

Montrons que si $\lambda \in \mathbb{C}$, $|\lambda| = 1$, est valeur propre de U, il existe $m \in [\![1, n]\!]$ tel que $\lambda^m = 1$. Soit $x = (x_1, \ldots, x_n) \in \mathbb{C}^n$ non nul tel que $U(x) = \lambda x$. Soit $I = \{i \in [\![1, n]\!] \mid |x_i| = \|x\|\}$, et $Z = \{x_i\ , i \in I\}$. Soit $i \in I$ on peut écrire comme dans la question précédente :

$$g = \sum_{j=1}^{n} p_{i,j} \frac{x_j}{\lambda x_i} = 1 \ .$$

En reprenant la même méthode, on voit qu'ici, si $j \in [\![1, n]\!]$ est tel que $p_{i,j} > 0$, alors $x_j = \lambda x_i$. Comme il existe un tel j, sinon la somme de la ligne i serait 0, et non pas 1, on voit que $\lambda x_i = x_j \in Z$. L'application $\mu_\lambda : \mathbb{C} \to \mathbb{C}$, $z \mapsto \lambda z$, laisse donc stable l'ensemble fini Z. On voit donc que λ est de période non nulle dans le groupe multiplicatif $\mathbb{U}$ des complexes de module 1 ; cette période m vérifie bien sûr $m \leqslant \mathrm{card}\,(Z) \leqslant \mathrm{card}\,(I) \leqslant n$.

Montrons maintenant que si $\lambda \in \mathbb{C}$, $|\lambda| = 1$, est une valeur propre de U, alors l'espace caractéristique N relatif à cette valeur propre est identique à l'espace propre. Posons $U\|_N = \lambda \mathrm{Id}_N + v$ où v est nilpotent. Si $v \neq 0$, il existe $y \in N$ tel que $v^2(y) = 0$ et $v(y) \neq 0$. On a alors pour tout $m \in \mathbb{N}^*$ l'égalité :

$$U^m(y) = \lambda^m y + m \lambda^{m-1} v(y) \ ,$$

d'où :

$$m \ \|v(y)\| \leqslant \|U(y)\| + \|y\| \leqslant 2 \ \|y\| \ .$$

Ce qui est évidemment contradictoire. Donc $v = 0$, et $U\|_N = \lambda \mathrm{Id}_N$, ce qui prouve que N est aussi le sous-espace propre associé à la valeur propre λ.

On pourrait enfin démontrer comme dans la question précédente, que si y est dans la somme P des espaces caractéristiques relatifs aux valeurs propres de module < 1, alors $U^m(y) \underset{m \to \infty}{\longrightarrow} 0$. Soient $\lambda_1, \ldots, \lambda_k$ les valeurs propres de U de module 1 (il y a au moins 1). Pour $x \in E$, posons $x = y$

où $y \in P$ et pour tout $i \in [\![1,k]\!]$, $y_i \in N_i = E_{\lambda_i}$. Pour tout $m \in \mathbb{N}$ on a l'égalité :

$$U^m(x) = U^m(y) + \lambda_1^m y_1 + \ldots + \lambda_k^m y_k \ ,$$

donc, si d est un multiple commun des ordres de $(\lambda_1, \ldots, \lambda_k)$ (on peut prendre $n!$), on a :

$$U^{m\,d}(x) \underset{m\to\infty}{\longrightarrow} y_1 + \ldots + y_k \ .$$

Nous en déduisons $U^{m\,d} \underset{m\to\infty}{\longrightarrow} \varphi$, où φ est le projecteur sur la somme des espaces propres de U relatifs à ses valeurs propres de module 1. La matrice de φ dans la base canonique est donc une matrice stochastique. Cette matrice est singulière si, et seulement si, U a des valeurs propres de module < 1. On peut donc d'une certaine manière étendre les résultats obtenus dans le a).

c) 1) Le polynôme caractéristique χ_S de la matrice :

$$S = \begin{pmatrix} 1/2 & 1/4 & 1/4 \\ 1/4 & 1/2 & 1/4 \\ 1/4 & 1/4 & 1/2 \end{pmatrix}$$

se calcule facilement, et on obtient la factorisation $\chi_S = (1-X)\,(1/4-X)^2$ (le zéro 1 est prévu). L'espace propre relatif à la valeur propre 1 est de dimension 1 engendré par $(1,1,1)$, puisque la matrice S est stochastique stricte. On trouve facilement qu'un triplet $(x_1,x_2,x_3) \in \mathbb{C}^3$ est vecteur propre pour la valeur propre $1/4$ si, et seulement si :

$$x_1 + x_2 + x_3 = 0 \ .$$

L'espace propre correspondant est donc de dimension 2, et la matrice S est diagonalisable. La famille $\mathcal{B}' = (e'_1, e'_2, e'_3)$, où $e'_1 = e_1 - e_2$, $e'_2 = e_2 - e_3$ et $e'_3 = e_1 + e_2 + e_3$ est une base constituée de vecteurs propres pour l'endomorphisme U de matrice S. Soit P la matrice de passage de $\mathcal{B}$, base canonique, vers $\mathcal{B}'$. On obtient :

$$P = \begin{pmatrix} 1 & 0 & 1 \\ -1 & 1 & 1 \\ 0 & -1 & 1 \end{pmatrix} \quad \text{et} \quad P^{-1} = \frac{1}{3}\begin{pmatrix} 2 & -1 & -1 \\ 1 & 1 & -2 \\ 1 & 1 & 1 \end{pmatrix} \ .$$

On a donc l'égalité :

$$S = \frac{1}{3}\begin{pmatrix} 1 & 0 & 1 \\ -1 & 1 & 1 \\ 0 & -1 & 1 \end{pmatrix} \times \begin{pmatrix} 1/4 & 0 & 0 \\ 0 & 1/4 & 0 \\ 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 2 & -1 & -1 \\ 1 & 1 & -2 \\ 1 & 1 & \end{pmatrix} \ .$$

La limite de la matrice S^m, quand m tend vers l'infini, est :

$$\lim_{m\to\infty} S^m = \frac{1}{3}\begin{pmatrix} 1 & 0 & 1 \\ -1 & 1 & 1 \\ 0 & -1 & 1 \end{pmatrix} \times \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 2 & -1 & -1 \\ 1 & 1 & -2 \\ 1 & 1 & 1 \end{pmatrix},$$

soit :

$$\lim_{m\to\infty} S^m = \frac{1}{3}\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

2) On a ici :

$$S = \begin{pmatrix} 1/2 & 1/2 & 0 \\ 0 & 1/2 & 1/2 \\ 0 & 0 & 1 \end{pmatrix}$$

Cette matrice étant trigonale, on trouve $\chi_S(X) = (1/2 - X)^2(1 - X)$. On détermine l'espace propre relatif à la valeur propre 1 de U : c'est le sous-espace engendré par $(1,1,1)$, et l'espace propre relatif à la valeur propre $1/2$: on trouve le sous-espace engendré par e_1. La matrice S n'est donc pas diagonalisable. Prenons comme nouvelle base $\mathcal{B}' = (e'_1, e'_2, e'_3)$ où $e'_1 = e_1$, $e'_2 = 2\,e_2$, et $e'_3 = e_1 + e_2 + e_3$. Dans cette base, la matrice de U est :

$$S' = \begin{pmatrix} 1/2 & 1 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1/2 & 0 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

On exprime ainsi la matrice S' sous la forme d'une somme d'une matrice diagonale et d'une matrice nilpotente (de période 2), qui commutent. Pour tout $m \in \mathbb{N}^*$, on a :

$$S'^m = \begin{pmatrix} 1/2^m & m\,1/2^{m-1} & 0 \\ 0 & 1/2^m & 0 \\ 0 & 0 & 1 \end{pmatrix} \underset{m\to\infty}{\longrightarrow} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

On trouve aussi :

$$S^m \underset{m\to\infty}{\longrightarrow} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

§ XV.6 *SUITES DÉFINIES PAR UNE RELATION DE RÉCURRENCE LINÉAIRE*

Exercice 2 :

‖ Soit $p \in \mathbb{N}$ $(p \geqslant 2)$ et (u_n) une suite de $\mathbb{R}_+^*$

$u_0, u_1, \ldots, u_{p-1}$ donnés > 0 et

$$(\forall n \geqslant p) \quad u_n = (u_{n-1}\, u_{n-2} \ldots u_{n-p})^{1/p} .$$

Etudier la suite (u_n) pour $n \to \infty$. ■

Considérons la suite réelle définie pour tout $n \in \mathbb{N}$ par $v_n = \mathrm{Log}\,(u_n)$. La suite v_n vérifie la récurrence linéaire :

$$(1) \qquad (\forall n \geqslant p) \quad v_n = \frac{v_{n-1} + \ldots + v_{n-p}}{p} .$$

Le polynôme associé à cette récurrence linéaire est :

$$P(X) = p\,X^p - (X^{p-1} + X^{p-2} + \ldots + X + 1) .$$

Montrons que P a p zéros simples dans $\mathbb{C}$, tous de module $\leqslant 1$, et que 1 est son seul zéro de module 1 . Posons $Q(X) = (X-1)\,P$, on a l'égalité :

$$Q(X) = P(X)\,(X-1) = p\,X^p\,(X-1) - (X^p - 1) = p\,X^{p+1} - (p+1)\,X^p + 1 .$$

En dérivant on obtient :

$$Q'(X) = p\,(p+1)\,X^{p-1}\,(X-1) .$$

On voit donc que les zéros de Q sont tous simples, sauf 1 qui est d'ordre 2 . Les zéros de P sont donc tous simples. Soit $z \in \mathbb{C}$ un zéro de P , on voit que :

$$p\,|z|^p = \left|z^{p-1} + \ldots + z + 1\right| \leqslant |z|^{p-1} + \ldots + |z| + 1 .$$

Si $|z| > 1$, alors $p\,|z|^p > |z|^{p-1} + \ldots + |z| + 1$, donc $|z| \leqslant 1$.
Si $|z| = 1$, alors

$$p = \left|z^{p-1} + \ldots + z + 1\right| = |z|^{p-1} + \ldots + |z| + 1 ;$$

comme il y a égalité dans l'inégalité triangulaire, on en déduit que les nombres complexes $1, z, \ldots, z^{p-1}$ sont alignés et de même sens (pour la structure de $\mathbb{R}$-ev de $\mathbb{C}$), et donc que $z = 1$.

Notons $z_1, z_2, \ldots, z_{p-1}$ les zéros complexes différents de 1 de P . Comme la suite $(v_n)_{n\in\mathbb{N}}$ vérifie la relation de récurrence (1) , il existe des scalaires $(\lambda_1, \ldots, \lambda_{p-1}, \lambda_p) \in \mathbb{C}^p$, tels que :

$$(\forall n \in \mathbb{N}) \quad v_n = \lambda_1\, z_1^n + \ldots + \lambda_{p-1}\, z_{p-1}^n + \lambda_p .$$

Nous en déduisons que la suite $(v_n)_{n\in\mathbb{N}}$ est convergente de lim

Le coefficient λ_p est déterminé par les valeurs initiales $(v_0, \ldots, v_{p-1})$ de la suite. On a pour tout $i \in [\![0, p-1]\!]$ l'égalité :

$$v_i = \sum_{k=1}^{p-1} \lambda_k \, z_k^i + \lambda_p \ .$$

Soit D le polynôme tel que $P = (X-1)\,D$, dont les zéros sont $z_1, \ldots, z_{p-1}$. Posons $D = \alpha_0 + \ldots + \alpha_{p-1}\,X^{p-1}$. On a l'égalité :

$$\sum_{i=0}^{p-1} \alpha_i \, v_i = \sum_{i=0}^{p-1} \alpha_i \left(\sum_{k=1}^{p-1} \lambda_k \, z_k^i + \lambda_p \right) = \sum_{k=1}^{p-1} \lambda_k \left(\sum_{i=0}^{p-1} \alpha_i \, z_k^i \right) + \lambda_p \sum_{k=1}^{p-1} \alpha_k =$$

$$= \sum_{k=1}^{p-1} \lambda_k \, D(z_k) + \lambda_p \, D(1) = \lambda_p \, D(1) \ .$$

On peut donc ainsi calculer la limite λ_p, en fonction des valeurs initiales de la suite.

On obtient précisément :

$$D(X) = \frac{(X^p - X^{p-1}) + (X^p - X^{p-2}) + \ldots + (X^p - 1)}{X - 1} =$$

$$= X^{p-1} + (X^{p-1} + X^{p-2}) + \ldots + (X^{p-1} + \ldots + X + 1) =$$

$$= p\,X^{p-1} + (p-1)\,X^{p-2} + \ldots + 2\,X + 1 \ .$$

Donc $D(1) = \dfrac{p(p+1)}{2}$, et :

$$v_m \underset{m \to \infty}{\longrightarrow} \frac{2}{p(p+1)} (v_0 + 2\,v_1 + \ldots + p\,v_{p-1}) = \lambda_p \ .$$

Nous en déduisons finalement :

$$u_m \underset{m \to \infty}{\longrightarrow} \sqrt[\frac{p(p+1)}{2}]{u_0 \, u_1^2 \ldots u_{p-1}^p} \ .$$

Exercice 9 :

On désigne par D_n le nombre de *dérangements* de $\mathfrak{S}_n$ (*i.e.* le nombre de permutations σ de $[\![1, n]\!]$ telles que $(\forall i)\ \sigma(i) \neq i$). Montrer que $D_1 = 0$, $D_2 = 1$, et que $D_{n+1} = n\,(D_n + D_{n-1})$ pour tout $n \geqslant 2$. Si on pose $u_n = \dfrac{D_n}{n!}$ montrer que la suite (u_n) vérifie la relation de récurrence $n\,u_n = (n-1)\,u_{n-}$

En calculant $v_n = u_n - u_{n-1}$, en déduire l'expression exacte de u_n puis de D_n. ■

Le seul élément de $\mathfrak{S}_1$ est l'identité, qui n'est pas un dérangement, donc $D_1 = 0$. Les éléments de $\mathfrak{S}_2$ sont l'identité et la transposition $\tau_{1,2}$ qui est un dérangement, donc $D_2 = 1$.
Remarquons que pour tout $n \in \mathbb{N}^*$, D_n est le nombre de dérangements d'un ensemble fini quelconque de cardinal n. Soit E de cardinal $n+1$ ($n \geqslant 2$), et $x_0 \in E$. Pour x_1 fixé dans $E \setminus \{x_0\}$, dénombrons les dérangements σ de E tels que $\sigma(x_0) = x_1$. Il y a deux possibilités, soit $\sigma(x_1) = x_0$, soit $\sigma(x_1) \neq x_0$. Le nombre des dérangements σ de E tels que $\sigma(x_0) = x_1$ et $\sigma(x_1) = x_0$ est visiblement le nombre de dérangements de $E \setminus \{x_0, x_1\}$, soit D_{n-1}. Soit maintenant σ dérangement de E tel que $\sigma(x_0) = x_1$ et $\sigma(x_1) \neq x_0$. On remarque que $\sigma' = \tau_{x_0,x_1} \circ \sigma$ a pour seul point fixe x_0 ($\tau_{x_0,x_1} \circ \sigma(x) = x \Leftrightarrow \sigma(x) = \tau_{x_0,x_1}(x)$) ; inversement, si σ' est une permutation de E qui a pour seul point fixe x_0, la permutation $\sigma = \tau_{x_0,x_1} \circ \sigma'$ est un dérangement de E tel que $\sigma(x_0) = x_1$ et $\sigma(x_1) \neq x_0$. Le nombre de permutations de E qui ont comme seul point fixe x_0 est bien sûr D_n. Le nombre de possibilités pour x_1 étant n, nous en déduisons :

$$D_{n+1} = n\,(D_n + D_{n-1})\ .$$

Pour tout $n \geqslant 2$, on a donc l'égalité :

$$(n+1)!\,u_{n+1} = n\,n!\,u_n + n\,(n-1)!\,u_{n-1}\ ,$$

d'où :

$$(n+1)\,u_{n+1} = n\,u_n + u_{n-1} \quad \text{soit encore} \quad (n+1)\,(u_{n+1} - u_n) = -(u_n - u_{n-1})\ .$$

Comme $u_2 - u_1 = \dfrac{1}{2}$, on voit que $u_3 - u_2 = -\dfrac{1}{2.3}$ etc., $u_n - u_{n-1} = \dfrac{(-1)^n}{n!}$.
On en déduit $u_2 = \dfrac{1}{2!}$, $u_3 = \dfrac{1}{2!} - \dfrac{1}{3!}$ etc., et finalement, pour tout $n \geqslant 2$:

$$u_n = \frac{1}{2!} - \frac{1}{3!} + \ldots + \frac{(-1)^n}{n!}\ .$$

Nous en déduisons, pour tout $n \geqslant 2$ l'égalité :

$$D_n = n! \sum_{k=2}^{n} \frac{(-1)^k}{k!}\ .$$

Chapitre XVI

COMPLÉMENT : RÉDUCTION DE JORDAN

§ XVI.1 *ÉTUDE DES ENDOMORPHISMES NILPOTENTS*

Exercice 2 :

Dans un K-ev E de dimension $n \geqslant 1$, soit u un endomorphisme nilpotent de période n. Montrer que les seuls sous-K-ev u-stables de E sont $\{0\}, \mathrm{Ker}(u), \ldots, \mathrm{Ker}\left(u^{n-1}\right), E$. ■

On sait que la suite croissante des noyaux :

$$\{0\} \subset \mathrm{Ker}(u) \subset \ldots \subset \mathrm{Ker}\left(u^{n-1}\right) \subset \mathrm{Ker}\left(u^{n}\right) = E ,$$

est strictement croissante, et que par conséquent, pour tout $i \in [\![0, n]\!]$, $\dim \mathrm{Ker}\left(u^{i}\right) = i$.

Soit F un sous-K-ev u-stable, notons k le plus grand entier dans $[\![0, n]\!]$ tel que $\mathrm{Ker}\left(u^{k}\right) \subset F$. Si $k = n$, alors $E = F$; supposons $k < n$. On a alors les inclusions :

$$\mathrm{Ker}\left(u^{k}\right) \subset \mathrm{Ker}\left(u^{k+1}\right) \cap F \subset \mathrm{Ker}\left(u^{k+1}\right) .$$

La deuxième inclusion est stricte, sinon $\mathrm{Ker}\left(u^{k+1}\right) \subset F$. Comme

$$\dim \mathrm{Ker}\left(u^{k+1}\right) = 1 + \dim \mathrm{Ker}\left(u^{k}\right) ,$$

la première inclusion est nécessairement une égalité.

Soit u_1 l'endomorphisme de F induit par u sur F. On a :

$$\mathrm{Ker}\left(u_1^{k}\right) = \mathrm{Ker}\left(u^{k}\right) \cap F = \mathrm{Ker}\left(u^{k}\right) = \mathrm{Ker}\left(u^{k+1}\right) \cap F = \mathrm{Ker}\left(u_1^{k+1}\right) .$$

La suite des noyaux itérés de u_1 est donc stationnaire au moins à partir du rang k, donc :

$$\mathrm{Ker}\left(u^{k}\right) \cap F = \mathrm{Ker}\left(u_1^{k}\right) = \mathrm{Ker}\left(u_1^{n}\right) = F .$$

Nous en déduisons $F \subset \mathrm{Ker}\,(u^k)$, et finalement $F = \mathrm{Ker}\,(u^k)$.

Les sous-K-ev u-stables sont donc les noyaux itérés de u.

Exercice 6 :

On prend pour K le corps $\mathbb{Z}/p\mathbb{Z}$ (p premier impair).

Dans $\mathfrak{M}_p(K)$ on considère la matrice

$$M = \begin{bmatrix} -1 & 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & & \ddots & \ddots & 1 \\ 1 & 0\dots & \dots & 0 & -1 \end{bmatrix}.$$

Montrer que M est nilpotente et préciser sa période. ■

Soit la permutation $\sigma = \begin{pmatrix} 1 & 2 & \dots & p \\ p & 1 & \dots & p-1 \end{pmatrix}$, et f l'endomorphisme de K^p associé, c'est-à-dire tel que pour tout $i \in [\![1,p]\!]$, $f(e_i) = e_{\sigma(i)}$, où $(e_1,\dots,e_p)$ est la base canonique de K^p. On voit que M est la matrice dans la base canonique de $f - \mathrm{Id}_{K^p}$. Comme $\sigma^p = \mathrm{Id}_{[\![1,p]\!]}$, et que p est la caractéristique du corps de base, on voit que :

$$(f - \mathrm{Id}_{K^p})^p = f^p - \mathrm{Id}_{K^p} = 0\,.$$

La matrice M est donc nilpotente.

On vérifie que pour tout $i \in [\![0,p-1]\!]$, $f^i(e_p) = e_{p-i}$. Nous en déduisons :

$$(f - \mathrm{Id}_{K^p})^{p-1}(e_p) = \sum_{j=0}^{p-1} \binom{p-1}{j} (-1)^j\, f^{p-1-j}(e_p) = \sum_{j=0}^{p-1} \binom{p-1}{j} (-1)^j\, e_{j+1}\,.$$

Ce vecteur n'est pas nul, par exemple sa première coordonnée est 1. On voit donc que $(f - \mathrm{Id}_{K^p})^{p-1} \neq 0$. La matrice M est par conséquent nilpotente de période p.

§ XVI.2 *RÉDUCTION DE JORDAN QUAND $\chi_u(X)$ EST DISSOCIÉ*

Exercice 1 :

Si le corps de base K est *algébriquement clos*, et

prouver que toute matrice $M \in \mathfrak{M}_n(K)$ est semblable à sa transposée, en utilisant une réduction de Jordan, ce qui permet de se ramener au cas où M est une matrice de Jordan.
Etendre ce résultat au cas où K n'est pas algébriquement clos en utilisant le théorème VII.7.3 et l'exercice 11 du § XIV.3. ■

Soient p et q des entiers > 0, A et A' matrices semblables dans $\mathfrak{M}_p(K)$, B et B' matrices semblables dans $\mathfrak{M}_q(K)$. Montrons que la matrice $M \in \mathfrak{M}_{p+q}(K)$ constituée par les blocs diagonaux A et B, est semblable à la matrice $M' \in \mathfrak{M}_{p+q}(K)$, constituée par les blocs diagonaux A' et B'.
Il existe $P \in \mathrm{GL}(p, K)$ et $Q \in \mathrm{GL}(q, K)$ telles que $AP = PA'$ et $BQ = QB'$. On a alors l'égalité (produits par blocs) :

$$\left[\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right] \times \left[\begin{array}{c|c} P & 0 \\ \hline 0 & Q \end{array}\right] = \left[\begin{array}{c|c} AP & 0 \\ \hline 0 & BQ \end{array}\right] =$$

$$= \left[\begin{array}{c|c} PA' & 0 \\ \hline 0 & QB' \end{array}\right] = \left[\begin{array}{c|c} P & 0 \\ \hline 0 & Q \end{array}\right] \times \left[\begin{array}{c|c} A' & 0 \\ \hline 0 & B' \end{array}\right] .$$

La matrice composée des blocs diagonaux P et Q étant inversible, les matrices M et M' sont semblables. Cette propriété s'étend par récurrence aux matrices diagonales par blocs.

Soit $M \in \mathfrak{M}_n(K)$, dont le polynôme caractéristique est dissocié dans $K[X]$, M est semblable à une matrice diagonale par blocs, les blocs diagonaux étant des matrices de Jordan. Il existe donc une matrice $P \in \mathrm{GL}(n, K)$ et des matrices de Jordan $J_1, \ldots, J_k$, telles que :

$$MP = P\,\mathrm{Diag}(J_1, \ldots, J_k) .$$

Supposons avoir démontré qu'une matrice de Jordan est semblable à sa transposée, alors les matrices $\mathrm{Diag}(J_1, \ldots, J_k)$ et

$$\mathrm{Diag}\left({}^tJ_1, \ldots, {}^tJ_k\right) = {}^t\mathrm{Diag}(J_1, \ldots, J_k) ,$$

sont semblables entre elles. Comme d'autre part :

$${}^tP\,{}^tM = {}^t\mathrm{Diag}(J_1, \ldots, J_k)\,{}^tP ,$$

on voit que les matrices ${}^tM$, ${}^t\mathrm{Diag}(J_1, \ldots, J_k)$, $\mathrm{Diag}(J_1, \ldots, J_k)$ et M sont semblables entre elles. Cela démontre la proposition de l'énoncé.

Il reste à prouver qu'une matrice de Jordan est semblable à sa transposée. Soit $p \in \mathbb{N}^*$, $\lambda \in K$, et f l'endomorphisme de K^p dont la

la base canonique $\mathcal{B} = (e_1, \ldots, e_p)$ de K^p est la matrice de Jordan $J_\lambda(p)$. On a $f(e_1) = \lambda e_1$, et pour tout $i \in [\![2, p]\!]$ (si $p \geqslant 2$), $f(e_i) = \lambda e_i + e_{i-1}$. Posons pour tout $i \in [\![1, p]\!]$, $e'_i = e_{p+1-i}$. On a $f(e'_p) = f(e_1) = \lambda e'_p$, et pour tout $i \in [\![1, p-1]\!]$ (si $p \geqslant 2$), $f(e'_i) = \lambda e'_i + e'_{i+1}$. La matrice de f dans la base $\mathcal{B}' = (e'_1, \ldots, e'_p)$ est donc :

$$\mathrm{Mat}_{\mathcal{B}'}(f) = \begin{bmatrix} \lambda & 0 & \ldots & \ldots & 0 \\ 1 & \ddots & \ddots & & \vdots \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & 1 & \lambda \end{bmatrix} = {}^t\mathrm{Mat}_{\mathcal{B}}(f) = {}^t J_\lambda(p) \, .$$

Les matrices $J_\lambda(p)$ et ${}^t J_\lambda(p)$ sont donc semblables, ce qu'il fallait démontrer.

Nous pouvons en déduire que si le polynôme caractéristique de M est dissocié dans $K[X]$, alors M est semblable à sa transposée. Soit maintenant $M \in \mathfrak{M}_n(K)$, quelconque. D'après le théorème VII.7.3, il existe une extension L du corps K telle que $\chi_M(X)$ soit dissocié dans $L[X]$. D'après ce qui précède, la matrice M est semblable dans $\mathfrak{M}_n(L)$ à sa transposée. L'exercice 11 du § XIV.3, nous permet de conclure, dans le cas où K est infini, que M et sa transposée sont semblables dans $\mathfrak{M}_n(K)$.

Exercice 2 :

Le corps de base est $\mathbb{C}$. Trouver la forme réduite de Jordan de la matrice :

b) $$M = \begin{bmatrix} 3 & -5 & 2 & -6 \\ 0 & 5 & 0 & 4 \\ -2 & 7 & -1 & 11 \\ 0 & -4 & 0 & -3 \end{bmatrix} .$$

Préciser le changement de base à effectuer pour cette réduction, calculer également M^k pour $k \in \mathbb{N}$ ainsi que $\exp(M)$. ■

b) Soit u l'endomorphisme de $\mathbb{C}^4$ dont la matrice dans la base canonique $\mathcal{B} = (e_1, e_2, e_3, e_4)$ est M. On remarque que le sous-$\mathbb{C}$-espace engendré par les vecteurs e_1 et e_3 est u-stable. Soit $\mathcal{B}' = (e_1, e_3, e_2, e_4)$, la matrice de u dans $\mathcal{B}'$ est :

$$M' = \begin{bmatrix} 3 & 2 & -5 & -6 \\ -2 & -1 & 7 & 11 \\ 0 & 0 & 5 & 4 \\ 0 & 0 & -4 & -3 \end{bmatrix} .$$

On trouve alors facilement que le polynôme caractéristique des matrices M et M' est :

$$\chi_M(X) = (X^2 - 2X + 1)(X^2 - 2X + 1) = (X - 1)$$

La matrice $N' = M' - I_4$ est nilpotente. On trouve :

$$N' = \begin{bmatrix} 2 & 2 & -5 & -6 \\ -2 & -2 & 7 & 11 \\ 0 & 0 & 4 & 4 \\ 0 & 0 & -4 & -4 \end{bmatrix} .$$

Posons :

$$A = 2\begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix} \quad B = \begin{bmatrix} -5 & -6 \\ 7 & 11 \end{bmatrix} \quad C = 4\begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix} .$$

On a $A^2 = 0$ et $C^2 = 0$, donc (produits par blocs) :

$$N'^2 = \left[\begin{array}{c|c} 0 & AB + BC \\ \hline 0 & 0 \end{array}\right] \quad N'^3 = \left[\begin{array}{c|c} 0 & ABC \\ \hline 0 & 0 \end{array}\right] \quad \text{et} \quad N'^4 = 0 .$$

On obtient :

$$AB + BC = \begin{bmatrix} 8 & 14 \\ -20 & -26 \end{bmatrix} \quad \text{et} \quad ABC = 24\begin{bmatrix} -1 & -1 \\ 1 & 1 \end{bmatrix} .$$

La matrice N' est donc nilpotente de période 4. La réduite de Jordan de M est donc $J_1(4)$. Soit N la matrice de $u - \mathrm{Id}_{\mathbb{C}^4}$ dans la base canonique, le changement de base étant évident, on obtient :

$$N^2 = \begin{bmatrix} 0 & 8 & 0 & 14 \\ 0 & 0 & 0 & 0 \\ 0 & -20 & 0 & -26 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{et} \quad N^3 = 24\begin{bmatrix} 0 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} .$$

Le noyau de $v^3 = \left(u - \mathrm{Id}_{\mathbb{C}^4}\right)^3$ est donc l'hyperplan H d'équation $x_2 + x_4 = 0$ dans la base canonique. Si $a \in \mathbb{C}^4$, $a \notin H$, alors $(v^3(a), v^2(a), v(a), a)$ est une base dans laquelle la matrice de u est $J_1(4)$.

Comme $M = I_4 + N$, pour tout $m \in \mathbb{N}$, si $m \geqslant 2$ alors :

$$M^m = I_4 + mN + \frac{m(m-1)}{2} N^2 + \frac{m(m-1)(m-2)}{6} N^3 .$$

Cette égalité est encore vraie si $m = 0$, $m = 1$ ou $m = 2$.

On trouve aussi :

$$\exp M = \exp I_4 \exp N = \mathrm{e}\left(I_4 + N + \frac{1}{2} N^2 + \frac{1}{6} N^3\right) = \mathrm{e}\left(M + \frac{1}{2}\right.$$

d'où après calcul :

$$\exp M = \mathrm{e}\begin{bmatrix} 3 & -5 & 2 & -3 \\ 0 & 5 & 0 & 4 \\ -2 & 1 & -1 & 2 \\ 0 & -4 & 0 & -3 \end{bmatrix}.$$

Exercice 3 :

On donne $P(X) = \prod_{i=1}^{p} (\lambda_i - X)^{\alpha_i} \in K[X]$, avec des λ_i distincts, des $\alpha_i \geqslant 1$ et $p \geqslant 1$ et $\alpha_1 + \alpha_2 + \ldots + \alpha_p = n \geqslant 1$ et on donne des entiers $\beta_i \in [\![1, \alpha_i]\!]$ pour $i \in [\![1, p]\!]$. Trouver une matrice $M \in \mathfrak{M}_n(K)$ telle que $\chi_M(X) = P(X)$ et $Q_M(X) = \prod_{i=1}^{p} (X - \lambda_i)^{\beta_i}$. ■

Soit M une matrice diagonale par blocs. Il est clair que son polynôme caractéristique est le produit des polynômes caractéristiques de ses blocs diagonaux, et que son polynôme minimal est le ppcm des polynômes minimaux de ses blocs diagonaux. Il nous suffit donc de prouver que pour tout $\lambda \in K$, pour tout $\alpha \in \mathbb{N}^*$ et pour tout $\beta \in [\![1, \alpha]\!]$, il existe une matrice $A \in \mathfrak{M}_\alpha(K)$ dont le polynôme caractéristique soit $(\lambda - X)^\alpha$, et dont le polynôme minimal soit $(X - \lambda)^\beta$. Si $M \in \mathfrak{M}_\alpha(K)$ est nilpotente de période β, on voit que le polynôme caractéristique de la matrice $M + \lambda I_\alpha$ est $(\lambda - X)^\alpha$, et que son polynôme minimal est $(X - \lambda)^\beta$. On obtient une telle matrice M en prenant dans $\mathfrak{M}_\alpha(K)$ la matrice diagonale par blocs, constituée du bloc diagonal $J(\beta)$ (matrice nilpotente de Jordan d'ordre β) et, si $\beta < \alpha$, du bloc diagonal nul.

§ XVI.3 *SOUS-ESPACES MONOGÈNES*

Exercice 1 :

On suppose le K-ev E de dimension $n \geqslant 1$, et u-monogène, pour $u \in \mathrm{Hom}_K(E)$. Trouver l'ensemble $\mathscr{C}_u$ (dont on vérifiera que c'est une sous-K-algèbre de $\mathrm{Hom}_K(E)$) :

$$\mathscr{C}_u = \{v \in \mathrm{Hom}_K(E) \mid v \circ u = u \circ v\}$$

($\mathscr{C}_u$ est appelé le *commutant* de u). Préciser $\dim_K(\mathscr{C}_u)$. ■

Pour tout $u \in \mathrm{Hom}_K(E)$ fixé, l'application $T_u : \mathrm{Hom}_K(E) \to \mathrm{Hom}_K(E)$, $v \mapsto v \circ u - u \circ v$, est une application K-linéaire. Comme $\mathscr{C}_u =$

voit que $\mathscr{C}_u$ est un sous-K-ev de $\mathrm{Hom}_K(E)$. On vérifie aussi que $\mathrm{Id}_E \in \mathscr{C}_u$, et que si v_1 et v_2 sont des éléments de $\mathscr{C}_u$, alors :

$$v_1 \circ v_2 \circ u = v_1 \circ u \circ v_2 = u \circ v_1 \circ v_2 \ .$$

Nous en déduisons que $\mathscr{C}_u$ est une sous-K-algèbre de $\mathrm{Hom}_K(E)$.

Comme $\mathscr{C}_u$ est une sous-K-algèbre de $\mathrm{Hom}_K(E)$ qui contient u, elle contient $K[u] = \{P(u) \mid P \in K[X]\}$. Montrons que si E est u-monogène, alors $\mathscr{C}_u = K[u]$. La dimension de $\mathscr{C}_u$ sera alors $n = \dim E$, puisque dans ce cas $(\mathrm{Id}_E, u, \ldots, u^{n-1})$ est une base de $K[u]$.

Soit $x_0 \in E$ tel que $(x_0, u(x_0), \ldots, u^{n-1}(x_0))$ soit une base de E, et $g \in \mathscr{C}_u$. Il existe une famille $(\lambda_0, \ldots, \lambda_{n-1}) \in K^n$ telle que $g(x_0) = \lambda_0 x_0 + \ldots + \lambda_{n-1} u^{n-1}(x_0)$. Il existe donc un polynôme $Q \in K[X]$ tel que $g(x_0) = [Q(u)](x_0)$. Pour tout $x \in E$, il existe un polynôme $P \in K[X]$ tel que $x = [P(u)](x_0)$. Comme $u \in \mathscr{C}_g$, on en déduit $P(u) \in \mathscr{C}_g$, c'est-à-dire g commute avec $P(u)$. Nous en déduisons :

$$\begin{aligned} g(x) &= g\big(P(u)(x_0)\big) = [P(u)]\big(g(x_0)\big) = \\ &= [P(u)]\big([Q(u)](x_0)\big) = [Q(u)]\big([P(u)](x_0)\big) = [Q(u)](x) \ . \end{aligned}$$

Cette égalité étant vraie pour tout $x \in E$, on en déduit $g = Q(u)$. Cela démontre l'inclusion $\mathscr{C}_u \subset K[u]$ et finalement l'égalité $\mathscr{C}_u = K[u]$, ce qu'il fallait démontrer.

BIBLIOGRAPHIE

BOREVITCH Z. I., CHAFAREVITCH J. R., *Théorie des nombres,* Gauthier-Villars, 1967.
BOURBAKI N., *Algèbre,* chap. I à III ; Hermann, 1982.
BOURBAKI N., *Groupes et Algèbres de Lie,* Hermann, 1982.
BOUTELOUP, *L'algèbre linéaire,* P.U.F., coll. « Que Sais-je ? »
CALAIS J., *Eléments de Théorie des groupes,* P.U.F., coll. « Mathématiques ».
CARREGA J. C., *Théorie des corps, la règle et le compas,* Hermann, 1981.
CHAMBADAL L., OVAERT J.-L., *Algèbre linéaire et tensorielle,* Dunod, 1968.
COHEN Paul, *Set Theory and the continuum hypothesis,* Benjamin, 1966.
COMTET L., *Analyse combinatoire,* T 1 et 2, P.U.F.
DELLACHERIE C., *Nombres au hasard,* Public. Univ. Louis Pasteur, Strasbourg, 1978.
DICKSON L. E., *Introduction to the theory of numbers,* Dover.
DUBREIL P., *Leçons d'Algèbre moderne,* Dunod, 1964.
GAAL L., *Classical Galois Theory, with examples,* Chelsea, 3ème éd., 1979.
GALOIS E., *Œuvres,* Gauthier-Villars, 1962.
GAUSS C. F., *Recherches Arithmétiques,* Blanchard, Paris.
GODEMENT R., *Cours d'Algèbre,* Hermann, 1969.
HARDY G. H., WRIGHT E. M., *An Introduction to the theory of numbers,* Oxford Uni, Press, 1959.
ITARD J., *Les nombres premiers,* P.U.F., coll. « Que sais-je ? ».
ITARD J., *Arithmétique et théorie des nombres,* P.U.F., coll. « Que sais-je ? ».
JACOBSON N., *Lectures in abstract algebra,* Tome 3, Springer.
JORDAN C., *Traité des Substitutions,* Gauthier-Villars, 1927, Blanchard, 1957.
KREISEL G., KRIVINE J. L., *Eléments de Logique Mathématique,* Dunod, 1967.
KRIVINE J. L., *Théorie axiomatique des ensembles,* P.U.F., coll. « Sup ».
LEDERMANN W., *Introduction to the theory of finite groups,* Wiley, 1961.
MOISOTTE L., *Exercices de Mathématiques,* Dunod, 1982.
RYSER H. J., *Mathématiques combinatoires,* Dunod, 1969.
SAMUEL P., ZARISKY O., *Commutative Algebra,* Tome 1, Van Nostrand.
SAMUEL P., *Théorie algébrique des nombres,* Hermann, 1967.
SCHWERDTFEGER, *Geometry of complex numbers,* Toronto.
SIERPINSKY W., *250 Problèmes de théorie des nombres,* Hachette.
SIERPINSKY W., *Elementary theory of numbers,* Watszawa, 1964.
WARUSFEL A., *Structures algébriques finies,* Hachette.
WEBER H., *Lehrbuch der Algebra,* T. 1 à 3, Chelsca.

J.M. Arnaudiès P. Delezoide
H. Fraysse

Exercices résolus d'algèbre du cours de mathématiques - 1

Ce recueil contient 355 exercices résolus choisis parmi les énoncés les plus représentatifs du cours d'algèbre.

Très détaillées et de niveau varié, les solutions ont été rédigées avec le souci constant d'approfondir les notions abordées et d'élargir la portée des exercices.

Dans la lignée du cours avec lequel il forme un ensemble sans égal (J.M. Arnaudiès et H. Fraysse, *cours de mathématiques*, tome 1, *algèbre*), ce recueil est un outil de travail complet et vivant qui ouvre la voie aux résultats concrets et pratiques.

L'ensemble comportera 4 volumes :

- *Exercices résolus d'analyse*, 1993 ;
- *Exercices résolus d'algèbre*, 1994 ;
- *Exercices résolus d'analyse* (compléments), 1995 ;
- *Exercices résolus d'algèbre bilinéaire et géométrie*, 1996, à paraître.

9 782100 014705

Code 041470
ISBN 2 10 001470 6

DUNOD