Préparation à l'agrégation interne

Gaetan Bisson

https://gaati.org/bisson/

Préambule

Toutes les informations relatives aux modalités du concours se trouvent sur le site Web du jury ; il est crucial que les candidats le lisent de fond en comble !

`http://agrint.agreg.org/`

On y trouvera notamment le programme officiel. Le présent document n'en reprend toutefois pas la structure, car il est parfaitement stupide de parler des anneaux avant les groupes ; heureusement qu'il ne s'agit pas là d'un programme d'enseignement...

Pour se préparer concrètement aux épreuves, il est en outre indispensable de s'entraîner ; nous recommandons pour cela les sujets d'annales que l'on pourra notamment trouver rassemblés sur le site :

`http://megamaths.perso.neuf.fr/ann.html`

Table des matières

Chapitre 1

Ensembles et logique

L'objectif de ce chapitre n'est pas d'étudier les ensembles pour eux-mêmes, mais de formaliser deux notions clefs : celle de relation d'équivalence et celle d'ordre. On les retrouvera au cœur des constructions algébriques et analytiques, respectivement.

Prérequis. Logique du premier ordre. Vocabulaire ensembliste. Produit cartésien.

1.1 Relations d'équivalence

On souhaite souvent identifier les objets partageant une propriété mathématique donnée, afin de n'étudier qu'elle et pas les objets dans toute leur complexité. Pensons notamment à l'étude des entiers *modulo un nombre donné* ou encore des variétés différentielles *à homéomorphisme près*.

Définition. *Une relation d'équivalence sur un ensemble X est une application*

$$\equiv : \begin{cases} X \times X \longrightarrow \{vrai, faux\} \\ (a,b) \longmapsto a \equiv b \end{cases}$$

qui vérifie les propriétés :

- $\forall a \in X, \forall b \in X, \forall c \in X, a \equiv b \wedge b \equiv c \Rightarrow a \equiv c$ (transitivité)
- $\forall a \in X, \forall b \in X, a \equiv b \Rightarrow b \equiv a$ (symétrie)
- $\forall a \in X, a \equiv a$ (réflexivité)

Définition. *La classe d'un élément $a \in X$ est l'ensemble $\overline{a} = \{b \in X : b \equiv a\}$.*
L'ensemble des classes s'appelle l'ensemble quotient $X / \equiv$.

Proposition. *Les classes partitionnent X, c'est-à-dire que :*

- $\bigcup_{a \in X} \overline{a} = X$
- $\overline{a} \cap \overline{b} \neq \emptyset \Rightarrow \overline{a} = \overline{b}$

On considérera souvent des classes comme les images réciproques d'une fonction.

Exemple. *Soit $f : X \to Y$ une application. La relation d'équivalence $x \equiv y \Leftrightarrow f(x) = f(y)$ partitionne X en classes appelées les fibres de f. Inversement, si $\equiv$ est une relation d'équivalence sur X, la fonction $x \in X \mapsto \overline{x} \in X / \equiv$ permet de retrouver les classes voulues.*

1.2 Ordre

Définition. *Un ordre sur un ensemble X est une application*

$$\leqslant : \begin{cases} X \times X \longrightarrow \{vrai, faux\} \\ (a,b) \longmapsto a \leqslant b \end{cases}$$

qui vérifie les propriétés :

— $\forall a \in X, \forall b \in X, \forall c \in X, a \leqslant b \wedge b \leqslant c \Rightarrow a \leqslant c$ (transitivité)
— $\forall a \in X, \forall b \in X, a \leqslant b \wedge b \leqslant a \Rightarrow a = b$ (antisymétrie)
— $\forall a \in X, \forall b \in X, a \leqslant b \vee b \leqslant a$ (totalité)

Exemple. *L'ordre naturel sur les réels, l'ordre lexicographique, etc.*

Définition. *On dit qu'un ensemble est bien ordonné si chacune de ses parties non-vides admet un plus petit élément.*

Exemple. *L'ensemble $\mathbb{N}$ muni de son ordre naturel est bien ordonné.*
L'ensemble $[0;1] \subset \mathbb{R}$ n'est pas bien ordonné.

Théorème (Zermelo)**.** *Sous l'axiome du choix, tout ensemble peut être bien ordonné.*

L'ensemble $\mathbb{R}$ peut donc être bien ordonné mais, évidemment, tout bon ordre qu'il admet n'a pas grand chose à voir avec son ordre naturel et est donc d'utilité douteuse.

1.3 Cardinaux

La définition suivante devrait déjà être connue de tous. On l'utilise partout en algèbre !

Définition. *On dit qu'une fonction $f : X \to Y$ est :*
— *une surjection si $\forall y \in Y, \exists x \in X, f(x) = y$;*
— *une injection si $\forall x \in X, \forall b \in X, f(a) = f(b) \Rightarrow a = b$;*
— *une bijection si c'est à la fois une surjection et une injection.*

Théorème (Cantor–Bernstein)**.** *Si $f : X \to Y$ et $g : Y \to X$ sont deux injections, alors X et Y sont en bijection.*

L'existence d'injections permet donc d'ordonner les ensembles à bijection près.

Définition. *On dit que deux ensembles ont le même cardinal s'ils sont en bijection.*
On dit qu'un ensemble est fini s'il est en bijection avec $\{1, \dots, k\}$.
On dit qu'un ensemble est dénombrable s'il est en bijection avec $\mathbb{N}$.

Proposition. *Sous l'axiome du choix, l'existence d'injection est un bon ordre sur les cardinaux ; on a :*

$$0 < 1 < 2 < \cdots < \aleph_0 < \aleph_1 < \aleph_2 < \cdots$$

On notera $|X|$ ou encore $\#X$ le cardinal d'un ensemble ; si l'ensemble est fini c'est son nombre d'éléments ; s'il est infini, c'est $\aleph_i$ pour un certain i. On sait que $\aleph_0 = |\mathbb{N}|$ mais que vaut $\aleph_1$?

Proposition. *L'ensemble $\mathbb{Q}$ des nombres rationnels est dénombrable.*
Toute union dénombrable d'ensembles dénombrables est dénombrable.

Corollaire. *L'ensemble des nombres algébriques est dénombrable.*

Théorème (Cantor). *L'ensemble* $\mathbb{R}$ *des nombres réels n'est pas dénombrable.*

Plus généralement, on peut montrer que X n'est jamais en bijection avec l'ensemble de ses parties $\mathfrak{P}(X)$. Comme $\mathbb{R}$ est en bijection avec $\mathfrak{P}(\mathbb{N})$, le résultat ci-dessus s'ensuit.

Remarque. *L'hypothèse du continu affirme qu'il n'existe aucun cardinal entre celui de* $\mathbb{N}$ *et celui de* $\mathbb{R}$. *On aurait donc* $\aleph_1 = |\mathbb{R}|$.

Le résultat ci-dessous sera souvent utile pour des questions de dénombrement.

Proposition (formule du crible). *Soit* $X_1, \dots, X_k$ *des parties d'un ensemble* E *; on a*

$$\left| \bigcup_{i \in \{1,\dots,k\}} X_k \right| = \sum_{S \subset \{1,\dots,k\}} (-1)^{|S|+1} \left| \bigcap_{i \in S} X_i \right|.$$

Exercice. *Montrer qu'un ensemble est infini si et seulement si, pour toute application de lui-même dans lui-même, il admet une partie stable autre que l'ensemble vide et lui-même.*

Chapitre 4

Groupes et géométrie

Les groupes sont la base de l'algèbre. En tant qu'enseignants du secondaire, vous les manipulez régulièrement, même si c'est sans les formaliser. Prenez garde toutefois de vous défaire des automatismes acquis dans $\mathbb{C}$ et ses sous-structures.

4.1 Groupes

Définition. *Un groupe est un ensemble G muni d'une loi de composition*

$$+ : \begin{cases} G \times G \longrightarrow G \\ (x, y) \longmapsto x + y \end{cases}$$

qui vérifie les propriétés :

— $\forall x \in G, \forall y \in G, \forall z \in G, x + (y + z) = (x + y) + z$ (associativité)
— $\exists 0 \in G, \forall x \in G, x + 0 = x$ (élément neutre)
— $\forall x \in G, \exists y \in G, x + y = 0$ (inverse)

De surcroit, on dit qu'il est abélien ou commutatif si :

— $\forall x \in G, \forall y \in G, x + y = y + x$ (commutativité)

Le programme mentionne explicitement les groupes arithmétiques classiques :

— $\mathbb{Z}$, les entiers relatifs munis de l'addition ;
— $\mathbb{Q}$, les nombres rationnels munis de l'addition ;
— $\mathbb{R}$, les nombres réels munis de l'addition ;
— $\mathbb{C}$, les nombres complexes munis de l'addition ;
— $\mathbb{Q}^\times$, les nombres rationnels non nuls munis de la multiplication ;
— $\mathbb{R}^\times$, les nombres réels non nuls muni de la multiplication ;
— $\mathbb{C}^\times$, les nombres complexes non nuls munis de la multiplication ;
— $\mathbb{U}_n = \{x \in \mathbb{C} : x^n = 1\}$, les racines n^{e} de l'unité munis de la multiplication ;
— $\mathbb{Z}/n\mathbb{Z}$, les entiers modulo n munis de l'addition modulaire ;
— $(\mathbb{Z}/n\mathbb{Z})^\times$, les entiers inversibles modulo n munis de la multiplication modulaire ;

ainsi que les groupes géométriques classiques :

— les automorphismes d'un espace affine, munis de la composition ;
— les homothéties et translations d'un espace affine, munis de la composition ;
— les isométries et des déplacements d'un espace affine euclidien, munis de la composition ;
— les isométries laissant stable une partie de l'espace, munis de la composition ;
— les isométries laissant stable un polygone régulier de degré n (groupe diédral) ;
— les similitudes directes et indirectes d'un plan affine euclidien, munis de la composition.

Notation. Lorsque la loi de composition est évidente, il pourra être opportun de la noter comme l'addition ou la multiplication des entiers ; on dira que le groupe est noté additivement ou multiplicativement. **Attention, les symboles « + » et « × » ne vérifient alors pas nécessairement toutes les propriétés de l'addition et de la multiplication usuelles.**

Définition. *L'ordre d'un groupe est son cardinal.*

On a par exemple $|\mathbb{U}_n| = n$ et $|\mathbb{U}| = \infty$.

Définition. *On appelle sous-groupe d'un groupe $(G, \cdot)$ tout groupe de la forme $(H, \cdot)$ avec $H \subset G$.*

Proposition. *Pour que $H \subset G$ soit un sous-groupe, il faut et il suffit qu'il contienne l'élément neutre et soit stable par la loi de composition et son inverse.*

Théorème (Lagrange)**.** *L'ordre de tout sous-groupe divise celui du groupe.*

Démonstration. Le sous-groupe $H \subset G$ induit une relation d'équivalence $x \sim y \iff x y^{-1} \in H$ dont les classes comprennent chacune $|H|$ éléments et partitionnent G. □

Exercice. *Démontrer que $\mathbb{U}_n \subset \mathbb{U}_m$ si et seulement si $n \mid m$.*

Il est naturel (et fort utile) de se demander quel sous-groupe on obtient en « combinant » certains éléments donnés d'un groupe.

Définition. *Soit $(g_1, \dots, g_k)$ une famille d'éléments d'un groupe G. On appelle sous-groupe engendré et on note $\langle g_1, \dots, g_k \rangle$ le plus petit sous-groupe de G contenant chacun des g_i.*

On dit qu'un groupe G est monogène s'il est engendré par un seul élément ; s'il est de surcroit fini on dit qu'il est cyclique.

Si G est commutatif, alors on peut écrire ces sous-groupes explicitement :

$$\langle g_1, \dots, g_k \rangle = \left\{ g_1^{\alpha_1} \cdot \vdots \cdot g_k^{\alpha_k} : \alpha \in \mathbb{Z}^k \right\}.$$

Exemple. *Le groupe $\mathbb{Z}$ est monogène, mais le groupe $\mathbb{Z}^\times$ ne l'est pas. Le groupe $\mathbb{U}_n$ est cyclique, mais le groupe $\mathbb{U}$ ne l'est pas.*

Définition. *L'ordre d'un élément g d'un groupe G est l'ordre du sous-groupe $< g >$ qu'il engendre.*

Par le théorème de Lagrange, l'ordre de tout élément divise celui du groupe.

Proposition. *Si x et y sont deux éléments d'un groupe commutatif, alors*

$$\operatorname{pgcd}(\operatorname{ord}(x), \operatorname{ord}(y)) = 1 \Longrightarrow \operatorname{ord}(x y) = \operatorname{ord}(x) \operatorname{ord}(y)$$

Rappelons qu'un sous-groupe H induit une relation d'équivalence sur G ; l'ensemble quotient G/H admet lui aussi une structure de groupe lorsque la propriété ci-dessous est vérifiée.

Définition. *Un sous-groupe H d'un groupe G est dit distingué lorsque*

$$\forall g \in G, \left\{ g h g^{-1} : h \in H \right\} = H.$$

Évidemment, dans un groupe abélien, tous les sous-groupes sont distingués.

Définition. *On appelle groupe quotient de G par un sous-groupe distingué H le groupe $\{gH : g \in G\}$ muni de la loi de composition induite, à savoir, $gH \cdot g'H = (gg')H$.*

Exemple. *Pour tout entier $n \in \mathbb{N}$ le groupe $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}, +)$. Le quotient correspondant se note $\mathbb{Z}/n\mathbb{Z}$, c'est le groupe des entiers modulo n. Cas particuliers :*

- *Pour $n = 0$, on a $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\{0\} = \mathbb{Z}$.*
- *Pour $n = 1$, on a $\mathbb{Z}/1\mathbb{Z} = \mathbb{Z}/\mathbb{Z} = \{0\}$.*
- *Pour $n = 2$, on a $\mathbb{Z}/2\mathbb{Z} = \{0 + 2\mathbb{Z}, 1 + 2\mathbb{Z}\}$.*

4.2 Morphismes

En algèbre, la notion de structure (que ce soit de groupes, d'anneaux, de modules, etc.) est étroitement liée à la notion duale de morphismes, c'est-à-dire d'applications préservant la structure. Dans le cas des groupes, il n'y a que la loi de composition à préserver :

Définition. *On appelle morphisme de groupe toute application $f : G \to H$ d'un groupe G vers un groupe H vérifiant*

$$\forall x \in G, \forall y \in G, f(x \cdot y) = f(x) \cdot f(y).$$

Le noyau de f est le sous-groupe distingué $\ker(f) = \{x \in G : f(x) = 1\} \subset G$ *; son image est le sous-groupe* $\mathrm{im}(f) = \{f(x) : x \in G\} \subset H$.

L'injectivité équivaut à $\ker(f) = \{1\}$ *et la surjectivité à* $\mathrm{im}(f) = H$. *On qualifie d'isomorphisme tout morphisme bijectif; on dit alors que G et H sont isomorphes et on note $G \simeq H$.*

On qualifie d'endomorphisme tout morphisme de G dans lui-même.

Théorème. *Si $f : G \to H$ est un morphisme de groupe, on a*

$$G/\ker(f) \simeq \mathrm{im}(f).$$

On aurait déjà pu écrire ce résultat pour les quotients des ensembles par les relations d'équivalences issues de fonctions. Il trouve cependant toute sa puissance en ce qu'il préserve la structure de groupe. Nous le généraliserons par la suite aux morphismes d'anneaux, de modules, etc. C'est notamment le fameux théorème du rang !

Exercice. *Montrer que $\mathbb{Q}/\mathbb{Z}$ est isomorphe à son quotient par tout sous-groupe fini.*

Exercice. *Soit p un nombre premier. Montrer que $\left\{z \in \mathbb{C} : \exists n \in \mathbb{N}, z^{p^n} = 1\right\}$ est un sous-groupe de $\mathbb{C}^\times$ qui n'est pas isomorphe au produit de deux groupes non triviaux.*

Exercice. *Soit G un groupe abélien fini dont l'ordre n admet la factorisation $n = \prod_{p \in \mathscr{P}} p^{\alpha_p}$. Montrer que G est isomorphe au produit des sous-groupes $G_p = \left\{x^{n/p^{\alpha_p}} : x \in G\right\}$ et que ces derniers vérifient $|G_p| = p^{\alpha_p}$.*

Le résultat de cet exercice peut se généraliser en le théorème de structure des groupes abéliens finis (hors programme, mais tellement éclairant) que voici.

Théorème. *Soit G un groupe abélien fini. Il existe une famille d'entiers $(d_1, \dots, d_k)$ vérifiant $d_i \mid d_{i+1}$ pour tout $i \in \{1, \dots, k-1\}$ tel que*

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}.$$

4.3 Action de groupe

La notion de groupe a été développée en grande partie pour étudier la structure abstraite des transformations géométriques ; il est ainsi naturel de vouloir la voir agir sur des ensembles, par exemple celui des points du plan.

Définition. *Une application $f : G \times S \to S$ avec G un groupe et S un ensemble est qualifiée d'action de groupe lorsqu'elle vérifie :*

- $\forall g \in G, \forall h \in G, \forall x \in S, f(g, f(h, x)) = f(gh, x)$;
- $\forall x \in S, f(1, x) = x$.

De manière équivalente mais plus savante, une action d'un groupe G sur un ensemble S n'est d'autre qu'un morphisme de groupe de G dans $\mathrm{Aut}(S)$, le groupe des bijections de S dans S. Par la suite, on notera l'action implicitement, c'est-à-dire, en posant $f(g,x) = gx$.

Définition. *Soit $G \to \mathrm{Aut}(S)$ une action de groupe. On définit :*
— *L'orbite d'un point $x \in S$ est la partie* $\mathrm{orb}(x) = Gx = \{gx : g \in G\} \subset S$.
— *Le stabilisateur d'un point $x \in S$ est le sous-groupe* $\mathrm{stab}(x) = \{g \in G : gx = x\} \subset G$.

Proposition. *Pour tout $x \in S$, on a* $|G/\mathrm{stab}(x)| = |\mathrm{orb}(x)|$.

Tout groupe G opère bien évidemment sur lui-même directement par $(g,x) \mapsto gx$. Mais on peut aussi définir d'autres actions.

Définition. *On appelle action de conjugaison d'un groupe G sur lui-même l'action $(g,x) \mapsto gxg^{-1}$. Les orbites de cette action sont appelées les classes de conjugaison du groupe. Les automorphismes du type $x \mapsto gxg^{-1}$ sont dits intérieurs.*

Les automorphismes intérieurs et les classes de conjugaisons jouent un rôle clef dans de nombreux résultats importants malheureusement hors programme. On peut toutefois voir la pertinence de ces notions en les spécialisant au cas classique $G = \mathrm{Mat}_n(\mathbb{K})$: les classes de conjugaison sont alors celles des matrices semblables et réduire une matrice revient à chercher des éléments distingués de sa classe.

4.4 Groupe symétrique

Définition. *Le groupe symétrique, noté $\mathfrak{S}_n$, est celui des bijections de l'ensemble $\{1,\dots,n\}$ dans lui-même. Ses éléments sont appelés les permutations.*

On a vu en cours de dénombrement que $|\mathfrak{S}_n| = n!$.

Définition. *On appelle cycle d'ordre k toute permutation de la forme*

$$\tau_{y_1,y_2,\dots,y_k} = \begin{cases} y_1 & \mapsto y_2 \\ y_2 & \mapsto y_3 \\ & \vdots \\ y_{k-1} & \mapsto y_k \\ y_k & \mapsto y_1 \\ x & \mapsto x \quad \text{si } x \notin \{y_1, y_2, \dots, y_k\} \end{cases}$$

où $(y_1, y_2, \dots, y_k)$ est une famille de k éléments distincts de $\{1,\dots,n\}$.
Les cycles d'ordre deux s'appellent les transpositions.

Les permutations engendrent les cycles par l'identité

$$\tau_{y_1,y_2,\dots,y_k} = \tau_{y_1,y_2} \circ \tau_{y_2,y_3} \circ \cdots \circ \tau_{y_{k-1},y_k}$$

et cela leur permet d'engendrer le groupe symétrique :

Proposition. *Toute permutation se décompose en produit de cycles à supports disjoints. Cette décomposition est unique à l'ordre près.*

Démonstration. Les orbites de g partitionnent $\{1,\dots,n\}$. □

Définition. *La signature, notée ε, est l'unique morphisme non trivial de $\mathfrak{S}_n$ dans $\mathbb{C}^\times$. Elle vérifie*

$$\varepsilon(\tau_{y_1,\dots,y_k}) = (-1)^{k-1}.$$

Son noyau est un sous-groupe distingué de $\mathfrak{S}_n$ appelé groupe alterné $\mathfrak{A}_n$.

Exercice. *Déterminer le centre du groupe alterné $\mathfrak{A}_n$. On distinguera les cas $n \leqslant 3$ et $n \geqslant 4$.*

4.5 Groupes linéaires

Rappelons que dans tout ce document $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

L'ensemble $\mathrm{Mat}_n(\mathbb{K})$ des matrices de taille $n \times n$ sur $\mathbb{K}$ est évidemment un groupe pour l'addition mais c'est sa structure multiplicative qui est réellement intéressante :

Définition. *Les groupes de matrices classiques sont :*

- $\mathrm{GL}_n(\mathbb{K})$*, le groupe linéaire, formé des matrices inversibles ;*
- $\mathrm{SL}_n(\mathbb{K})$*, le groupe spécial linéaire, formé des matrices de déterminant unité ;*
- $\mathrm{O}_n(\mathbb{K})$*, le groupe orthogonal, formé des matrices* M *vérifiant* ${}^tMM = \mathrm{id}$*;*
- $\mathrm{U}_n(\mathbb{K})$*, le groupe unitaire, formé des matrices* M *vérifiant* ${}^t\overline{M}M = \mathrm{id}$*;*
- $\mathrm{SO}_n(\mathbb{K})$*, le groupe spécial orthogonal, égal à* $\mathrm{O}_n(\mathbb{K}) \cap \mathrm{SL}_n(\mathbb{K})$*;*
- $\mathrm{SU}_n(\mathbb{K})$*, le groupe spécial unitaire, égal à* $\mathrm{U}_n(\mathbb{K}) \cap \mathrm{SL}_n(\mathbb{K})$.

Annales. En application de ce chapitre, faire les deux premières parties de la première composition de la session 2000 du concours de l'agrégation interne.

Chapitre 3

Algèbre générale

3.1 Anneaux

Définition. *Un anneau est un groupe commutatif* $(A,+)$ *muni d'une loi de composition*

$$\cdot : \begin{cases} A \times A \longrightarrow A \\ (x,y) \longmapsto x \cdot y \end{cases}$$

qui vérifie les propriétés :

- $\forall x \in A, \forall y \in A, \forall z \in A, x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (associativité)
- $\exists 1 \in A, \forall x \in A, x \cdot 1 = x$ (élément neutre)
- $\forall x \in A, \forall y \in A, \forall z \in A, x \cdot (y+z) = x \cdot y + x \cdot z$ (distributivité)

De surcroit, on dit que :

- *il est commutatif si* $\forall x \in A, \forall y \in A, x \cdot y = y \cdot x$
- *il est intègre si* $\forall x \in A, \forall y \in A, x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$
- *c'est un corps si* $\forall x \in A^*, \exists y \in A, x \cdot y = 1$

où $A^* = A \setminus \{0\}$ *désigne l'ensemble A privé du neutre pour « + ».*

Vous connaissez de nombreux tels objets :

- le corps $\mathbb{C}$ des nombres complexes ;
- le corps $\mathbb{R}$ des nombres réels ;
- le corps $\mathbb{Q}$ des nombres rationnels ;
- l'anneau $\mathbb{Z}$ des nombres entiers ;
- l'anneau $\mathbb{Z}[i]$ des entiers de Gauss ;
- l'anneau $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$ formé des nombres $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ avec $(a,b,c,d) \in \mathbb{Z}^4$;
- l'anneau $\mathbb{Z}/n\mathbb{Z}$ des entiers modulo un nombre n ;
- le corps $\mathbb{Z}/p\mathbb{Z}$ des entiers modulo un nombre premier p ;
- l'anneau $\mathbb{Z}[x]$ des polynômes à coefficients entiers ;
- l'anneau $\mathbb{Q}[x]$ des polynômes à coefficients rationnels ;
- le corps $\mathbb{Q}(x)$ des fractions rationnelles à coefficients rationnels ;
- l'anneau $\mathbb{R}^{\mathbb{R}}$ des fonctions réelles, munies de l'addition et du produit point par point ;
- l'anneau $\mathscr{C}^\infty(\mathbb{R},\mathbb{R})$ des fonctions infiniment dérivables, munies des mêmes lois ;
- l'anneau $\mathscr{C}^0_{2\pi}(\mathbb{R},\mathbb{R})$ des fonctions 2π-périodiques munies de l'addition point par point et de la convolution

$$f \star g : t \mapsto \int_t^{t+2\pi} f(u) g(t-u) d\,u ;$$

— l'anneau $\mathrm{Mat}_n(k)$ des matrices carrées à coefficients dans un corps k quelconque ;

Proposition. *Tout corps est intègre. Tout anneau intègre fini est un corps.*

Dans un anneau, les identités remarquables qui découlent directement des propriétés élémentaires des lois de composition sont vérifiées. Attention toutefois à ce qu'un anneau n'est pas nécessairement commutatif ! On a par exemple :

Proposition. *Si x et y sont deux éléments d'un anneau vérifiant $xy = yx$, alors pour tout $n \in \mathbb{N}$ on a :*

$$x^n - y^n = (x-y)\sum_{k=0}^{n-1} x^k y^{n-1-k}$$
$$(x+y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k}$$

Dans un corps, on peut de surcroit diviser par tout élément non nul ; si $x \neq 1$ la première identité implique alors :

$$\sum_{k=0}^{n-1} x^k = \frac{x^n - 1}{x - 1}$$

Pour simplifier, nous travaillerons désormais exclusivement avec des anneaux commutatifs. On pourra toutefois considérer le cas de $\mathrm{Mat}_n(k)$ en exercice.

Définition. *Un élément x d'un anneau $(A, +, \times)$ est dit :*
— *inversible (ou que c'est une unité) s'il admet un inverse pour la multiplication.*
— *irréductible s'il ne peut pas s'écrire comme produit de deux éléments non inversibles.*
— *premier si $\forall y \in A, \forall z \in A, x \mid yz \Rightarrow x \mid y \vee x \mid z$.*

L'ensemble des unités forme un groupe pour la multiplication, appelé groupe multiplicatif et noté $A^\times$. Il peut être réduit à $\{\pm 1\}$ ou être infini ; nous en verrons des exemples plus tard.

Si A est intègre, tout premier est irréductible. La réciproque est vraie lorsque élément x admet une décomposition en produit de facteurs premiers $x = u\,p_1 \dots p_r$ unique à l'ordre des facteurs premiers p_i et à l'unité u près. Mais une telle décomposition n'existe pas toujours et il est plus fructueux de considérer les morphismes plutôt que les éléments.

Définition. *On appelle morphisme d'anneau toute application $f : A \to B$ d'un anneau A vers un anneau B vérifiant*
— $\forall x \in A, \forall y \in B, f(x+y) = f(x) + f(y)$
— $\forall x \in A, \forall y \in B, f(x \cdot y) = f(x) \cdot f(y)$
— $f(1_A) = 1_B$
La même terminologie (noyau, image, isomorphisme, etc.) que précédemment s'applique.

L'image d'un morphisme d'anneau est un anneau. Cependant, le noyau d'un morphisme d'anneau n'en est pas un (car il ne contient pas l'unité) ; c'est ce qu'on appelle un idéal :

Définition. *On appelle idéal I d'un anneau A tout sous-ensemble de A vérifiant :*
— $\forall x \in I, -x \in I$
— $\forall x \in I, \forall y \in I, x + y \in I$
— $\forall x \in I, \forall y \in A, xy \in I$

Les deux premières propriétés signifient que c'est un sous-groupe pour l'addition.

Définition. *Étant donné un idéal I d'un anneau A, l'anneau quotient A/I est formé des classes $\{a+I : a \in A\}$ muni des lois induites :*

$$(a+I)+(b+I)=(a+b)+I$$
$$(a+I)\cdot(b+I)=(a\cdot b)+I$$

Théorème. *Si $f : A \to B$ est un morphisme d'anneau, on a*

$$A/\ker(f) \simeq \mathrm{im}(f).$$

Certains idéaux donnent des quotients plus riches que d'autres :

Définition. *On dit qu'un idéal I est :*
- *premier si $\forall x \in A, \forall y \in A, xy \in I \Rightarrow x \in I \vee y \in I$;*
- *maximal s'il n'est contenu dans aucun idéal autre que A entier.*

Théorème. *Tout quotient d'un anneau par un idéal premier est intègre. Tout quotient d'un anneau par un idéal maximal est un corps.*

Certains idéaux sont en outre plus facile à écrire que d'autres.

Définition. *Pour tout $x \in A$ l'idéal $xA = \{xy : y \in A\}$ est dit principal et noté (x).*

Définition. *On dit qu'un anneau A est :*
- *euclidien, s'il admet une division euclidienne ;*
- *principal, si tous ses idéaux sont principaux ;*
- *factoriel, si chaque élément se décompose uniquement en produit de facteurs premiers.*

Chaque propriété ci-dessus implique les suivantes.

Exemple. *L'anneau $\mathbb{Z}$ est principal. L'anneau $\mathbb{Z}[i]$ l'est mais $\mathbb{Z}[\sqrt{-23}]$ ne l'est pas. L'anneau $\mathbb{Z}[x]$ ne l'est pas mais $\mathbb{Q}[x]$ l'est.*

Historiquement, la notion d'idéal a été introduite lorsqu'on a remarqué que dans certains anneaux l'unicité de la décomposition en produit de facteurs premiers était violée. Par exemple, dans $\mathbb{Q}(\sqrt{-5})$ on a $6 = 2\cdot 3 = (1+\sqrt{-5})\cdot(1-\sqrt{-5})$. Or, dans les anneaux considérés, l'unicité de cette factorisation *pour les idéaux* est vérifiée. Dans l'exemple ci-dessus, les idéaux correspondants aux facteurs ne sont pas premiers et peuvent encore être réduits :

$$(6) = (2, 1+\sqrt{-5})\cdot(2, 1+\sqrt{-5})\cdot(3, 1+\sqrt{-5})\cdot(3, 1-\sqrt{-5})$$

Définition. *Soient a et b deux éléments d'un anneau principal.*

On appelle plus grand commun diviseur et on note $\mathrm{pgcd}(a,b)$ *tout générateur de l'idéal $(a)+(b)$. On appelle plus petit commun multiple et on note* $\mathrm{ppcm}(a,b)$ *tout générateur de l'idéal $(a)\cap(b)$.*

Le théorème de Bézout est alors une trivialité. Et lorsqu'on a une division euclidienne l'algorithme d'Euclide étendu s'applique. On peut ainsi l'appliquer à $\mathbb{Z}$, $\mathbb{Q}[X]$, etc.

3.2 Entiers relatifs

Le vocabulaire de la théorie des anneaux commutatifs présenté plus haut coïncide exactement avec celui de l'arithmétique que vous connaissez déjà. Ce n'est pas un hasard !

Proposition. *Tout idéal de $\mathbb{Z}$ est de la forme $n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}$ pour un certain $n \in \mathbb{N}$.*
L'idéal $n\mathbb{Z}$ est premier (ou irréductible) si et seulement si l'entier n l'est.

L'anneau $\mathbb{Z}$ est ainsi principal, donc factoriel. Il est courant d'en interpréter les notions usuelles de pgcd et de ppcm en termes d'idéaux :

Proposition. *Le* pgcd *de deux entiers x et y est le générateur positif de l'idéal $(x)+(y)$.*
Le ppcm *de deux entiers x et y est le générateur positif de l'idéal $(x)\cap(y)$.*

En quotientant $\mathbb{Z}$ par ses idéaux on obtient les anneaux $\mathbb{Z}/n\mathbb{Z}$. La structure de ces anneaux est fortement liée à celle des idéaux dont ils sont issus ; c'est un fait général mais pour notre usage il suffira d'en connaître la spécialisation suivante :

Théorème (dit « des restes Chinois »). *Deux entiers m et n sont premiers entre eux si et seulement si le morphisme d'anneaux*

$$\begin{cases} \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \qquad x \longmapsto (x \bmod m, x \bmod n) \end{cases}$$

est un isomorphisme.

Le groupe multiplicatif de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est aussi l'objet de résultats classiques ; son ordre se note $\varphi(n)$ et la fonction φ porte le nom de « fonction indicatrice d'Euler ».

Théorème. *La classe d'un entier x est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si* $\operatorname{pgcd}(x,n) = 1$.
On a ainsi

$$\varphi(p^\ell) = (p-1)p^{\ell-1}$$
$$\varphi(\ell m) = \varphi(\ell)\varphi(m)$$

pour tout nombre premier p et tout couple (ℓ, m) d'entiers premiers entre eux.

Exercice. *On note σ la fonction associant à tout entier la somme de ses diviseurs. Par exemple, $\sigma(14) = 1+2+7+14 = 24$. Montrer que si m et n sont premiers entre eux alors on a $\sigma(mn) = \sigma(m)\sigma(n)$. Montrer que si p est premier alors $\sigma(p^\alpha) = \frac{p^{\alpha+1}-1}{p-1}$.*

Exercice. *On munit l'ensemble des fonctions de $\mathbb{N}^*$ dans $\mathbb{C}$ de l'addition usuelle ainsi que du produit définit par $f \star g : n \mapsto \sum_{d|n} f(d)g(\frac{n}{d})$; montrer que cela en fait un anneau commutatif. En caractériser les éléments inversibles. Calculer $\mu \star (n \mapsto 1)$ où μ dénote la fonction associant $(-1)^r$ à tout produit de r premiers distincts et 0 à tout multiple de carré non trivial. En déduire que si $f(n) = \sum_{d|n} g(d)$ alors $g(n) = \sum_{d|n} \mu(\frac{n}{d}) f(d)$.*

3.3 Polynômes sur un corps

Théorème. *Si $\mathbb{K}$ est un corps, l'anneau $\mathbb{K}[X]$ des polynômes univariés à coefficients dans $\mathbb{K}$ est euclidien, donc principal, donc factoriel.*

La division euclidienne implique l'équivalence $P(\alpha) = 0 \Leftrightarrow (X-\alpha) \mid P$ quelques soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Un polynôme de degré k admet donc au plus k racines.

Remarque. *Si $\mathbb{K}$ n'est lui-même qu'un anneau alors $\mathbb{K}[X]$ admet des propriétés plus subtiles dont nous ne discuterons pas ici. Par exemple, $\mathbb{Z}[X]$ admet des idéaux non principaux comme $(X-2, X^2)$.*

On peut appliquer à $\mathbb{K}[X]$ les mêmes méthodes qu'à $\mathbb{Z}$ pour calculer une division euclidienne, un pgcd voire encore une factorisation.

Théorème (d'Alembert–Gauss). *Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement ceux de degré un.*

Ainsi, dans $\mathbb{R}[X]$, ce sont ceux de degré un ainsi que les trinômes du second degré avec $\Delta < 0$. Dans $\mathbb{Q}[X]$ ou encore $(\mathbb{Z}/p\mathbb{Z})[X]$, toutefois, il existe des polynômes irréductibles de degré arbitraire. On a par exemple :

Proposition (dit « critère d'Eisenstein »). *Si p est un nombre premier et si $(a_0, a_1, \dots, a_n)$ est une famille d'entiers vérifiant :*
- *$p \mid a_i$ pour tout $i \in \{0, \dots, n-1\}$*
- *$p \nmid a_n$*
- *$p^2 \nmid a_0$*

Alors le polynôme $a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ est irréductible dans $\mathbb{Q}[X]$.

3.4 Corps

Définition. *On appelle sous-corps premier d'un corps K celui engendré par son unité pour la multiplication.*
S'il est fini alors il est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ et on dit que K est de caractéristique p.
S'il est infini alors il est isomorphe à $\mathbb{Q}$ et on dit que K est de caractéristique 0.

Définition. *On appelle corps des fractions d'un anneau intègre A le plus petit corps dont c'est un sous-anneau.*

En tant qu'anneau, le corps des fractions est engendré par A et les inverses de ses éléments non-nuls ; il consiste ainsi des fractions de la forme $\frac{x}{y}$ pour $x \in A$ et $y \in A^*$ avec toutes les propriétés qui s'imposent.

Définition. *Si K est un sous-corps de L on dit aussi que L est une extension de K.*
Un élément $x \in L$ est dit algébrique sur K s'il est racine d'un polynôme non-nul à coefficients dans K ; il est dit transcendent sinon.

Exemple. *Le nombre $j = e^{\frac{2\pi i}{3}} = \frac{-1+i\sqrt{3}}{2}$ est algébrique sur $\mathbb{Q}$; le nombre π ne l'est pas.*

Exercice. *Soient α et β deux entiers. Montrer que $\mathbb{Q}(\sqrt{\alpha})$ et $\mathbb{Q}(\sqrt{\beta})$ sont isomorphes si et seulement si $\sqrt{\alpha\beta}$ est un nombre entier.*

Exercice. *Soit $R \in \mathbb{C}(X)$ une fonction rationnelle non constante. Montrer que tous les nombres complexes, sauf peut-être un, sont dans son image. À quelle condition R est-elle bijective ?*

Exercice. *Montrer que la fonction indicatrice d'Euler vérifie $n = \sum_{k \mid n} \varphi(k)$ pour tout $n \in \mathbb{N}$. En déduire que tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique. Pour cela on pourra exploiter le fait que le polynôme $X^k - 1$ admet au plus k racines.*

Annales. En application de ce chapitre et du précédent, faire la première composition de la session 2015 du concours de l'agrégation interne. Faire aussi la première composition de la session 1996 du même concours, à l'exception de sa dernière partie.

Chapitre 5

Algèbre linéaire sur un corps commutatif

Les espaces vectoriels peuvent être définis sur un corps arbitraire $\mathbb{K}$; le contexte habituel est celui de $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ mais attention : on pourra parfois rencontrer $\mathbb{K} = \mathbb{Q}$ ou encore $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$.

5.1 Espaces vectoriels et algèbres

Définition. *Un espace vectoriel sur $\mathbb{K}$ est un ensemble E muni de deux applications, $+ : E \times E \to E$ (appellée « addition ») et $\cdot : \mathbb{K} \times E \to E$ (appelée « multiplication scalaire »), qui vérifient :*

1. $\forall (x, y, z) \in E^3, (x + y) + z = x + (y + z)$ *(associativité)*
2. $\exists \overrightarrow{0} \in E, \forall x \in E, \overrightarrow{0} + x = x$ *(élément neutre)*
3. $\forall x \in E, \exists y \in E, x + y = \overrightarrow{0}$ *(élément inverse)*
4. $\forall (x, y) \in E^2, x + y = y + x$ *(commutativité)*
5. $\forall x \in E, 1 \cdot x = x$
6. $\forall (\lambda, x, y) \in \mathbb{K} \times E^2, \lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$
7. $\forall (\lambda, \mu, x) \in \mathbb{K}^2 \times E, (\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$
8. $\forall (\lambda, \mu, x) \in \mathbb{K}^2 \times E, \lambda \cdot (\mu \cdot x) = (\lambda\mu) \cdot x$

Exemple. *On a notamment les espaces vectoriels suivants :*

- *l'espace $\mathbb{K}^n$ des vecteurs de longueur n à coefficients dans $\mathbb{K}$ (pour $\mathbb{K} = \mathbb{R}$ c'est le plan usuel lorsque $n = 2$ et l'espace usuel lorsque $n = 3$) ;*
- *l'espace $\mathbb{K}^{\mathbb{N}}$ des suites à coefficients dans $\mathbb{K}$;*
- *l'espace $\mathbb{K}^{(\mathbb{N})}$ des suites à coefficients dans $\mathbb{K}$ s'annulant à partir d'un certain rang ;*
- *l'espace $\mathscr{C}^0([0; 1], \mathbb{K})$ des fonctions continues de $[0, 1]$ dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.*

Définition. *Une algèbre est un espace vectoriel $(A, +, \cdot)$ muni d'une application supplémentaire $\times : A \times A \to A$ vérifiant :*

1. $\forall (x, y, z) \in A^3, x \times (y + z) = x \times y + x \times z$
2. $\forall (x, y, z) \in A^3, (x + y) \times z = x \times z + y \times z$
3. $\forall (\lambda, \mu, x, y) \in \mathbb{K}^2 \times A^2, (\lambda \cdot x) \times (\mu \cdot y) = (\lambda\mu) \cdot (x \times y)$

Elle est dite :

— *associative si* $\forall (x,y,z) \in A^3, (x \times y) \times z = x \times (y \times z)$
— *unifère si* $\exists 1 \in A, \forall x \in A, x \times 1 = 1 \times x = x$
— *commutative si* $\forall (x,y) \in A^2, x \times y = y \times x$

Exemple. *On a notamment les algèbres suivantes :*
— *l'algèbre* $\mathbb{K}[x]$ *des polynômes en une indéterminée à coefficients dans* $\mathbb{K}$*;*
— *plus généralement, toute extension de corps est une algèbre ;*
— *l'algèbre des transformations affines du plan pour* $\mathbb{K} = \mathbb{R}$*;*
— *l'algèbre* $\mathrm{End}(E)$ *des endomorphismes d'un espace vectoriel ;*
— *l'algèbre* $\mathrm{Mat}_n(\mathbb{K})$ *des matrices de taille* $n \times n$ *à coefficients dans* $\mathbb{K}$*;*

On ne verra que très peu de résultats concernant les algèbres elles-mêmes ; introduire cette terminologie nous servira quasi exclusivement à remarquer que tel ou tel ensemble d'opérateurs forme une algèbre.

Définition. *On appelle combinaison linéaire d'une famille* $(x_i)_{i\in I}$ *de vecteurs de* E *tout vecteur de la forme* $\sum_{i\in I} \lambda_i x_i$ *où les coefficients* $\lambda_i \in \mathbb{K}$ *sont nuls sauf pour un nombre fini d'indices* $i \in I$*.*
Leur ensemble forme le sous espace vectoriel engendré par les x_i *que l'on note* $\langle x_i \rangle_{i\in I}$*.*
On dit que cette famille est :
— *génératrice si* $\langle x_i \rangle_{i\in I} = E$*.*
— *libre si la seule combinaison linéaire nulle est celle de coefficients nuls.*
— *une base si elle est à la fois libre et génératrice.*

Théorème (dit « de la base incomplète »)**.** *Si* L *est une famille libre et* G *une famille génératrice d'un espace* E*, il existe une base de* E *contenant* L *et contenue dans* $L \cup G$*.*

Théorème (dit « de la dimension »)**.** *Toutes les bases d'un même espace vectoriel ont le même cardinal, que l'on appelle dimension de l'espace vectoriel.*

Ce résultat est particulièrement explicite dans le cas où la dimension est finie, mais n'oublions pas (encore) le cas de la dimension infinie et ses subtilités !

Exemple. *Notamment :*
— *La dimension de* $\mathbb{R}^n$ *comme espace vectoriel sur* $\mathbb{R}$ *est* n*.*
— *La dimension de* $\mathbb{C}^n$ *comme espace vectoriel sur* $\mathbb{R}$ *est* $2n$*.*
— *L'espace* $\mathbb{R}^{(\mathbb{N})}$ *n'admet pas de famille génératrice finie.*
— *L'espace* $\mathbb{R}^{\mathbb{N}}$ *n'admet pas de famille génératrice dénombrable.*
— *L'espace vectoriel* $\mathbb{R}$ *sur* $\mathbb{Q}$ *n'admet pas de famille génératrice dénombrable.*

Afin d'étudier confortablement un espace vectoriel, l'idéal est certainement de trouver une base présentant des propriétés adaptées à cette étude. Cela ne sera toutefois pas toujours possible et dans ce cas nous chercherons alors à décomposer l'espace vectoriel en sous espaces.

Définition. *On appelle somme d'une famille* $(F_i)_{i\in I}$ *de sous espaces le sous espace des vecteurs de la forme* $\sum_{i\in I} x_i$ *où les termes* $x_i \in F_i$ *sont nuls sauf pour un nombre fini d'indices* $i \in I$*.*
Cette somme est dite directe si on a $\sum_{i\in I} x_i = \overrightarrow{0}$ *uniquement lorsque* $\forall i \in I, x_i = \overrightarrow{0}$*.*
Les espaces F_i *sont dits supplémentaires si leur somme est directe et vaut* E*.*

Proposition. *Si* F *et* G *sont deux sous espaces vectoriels d'un même espace vectoriel, alors on a :*

$$\dim(F+G) = \dim(F) + \dim(G) - \dim(F \cap G).$$

Remarquons que, d'après le théorème de la base incomplète, tout sous espace vectoriel admet des supplémentaires. C'est évident en dimension finie mais repose sur l'axiome du choix en dimension infinie.

5.2 Applications linéaires

Évidemment, on souhaite maintenant étudier les applications qui préservent les structures introduites plus haut.

Définition. *Une application $\phi : E \to F$ entre deux espaces vectoriels est dite linéaire si elle vérifie $\phi(\lambda x + \mu y) = \lambda\phi(x) + \mu\phi(y)$ quels que soient $(\lambda, \mu) \in \mathbb{K}^2$ et $(x, y) \in E^2$.*
Son noyau $\ker(\phi)$ *est le sous espace formé des vecteurs $x \in E$ vérifiant $\phi(x) = 0$.*
Son image $\mathrm{im}(\phi)$ *est le sous espace formé des vecteurs $\phi(x) \in F$.*
Son rang $\mathrm{rg}(\phi)$ *est la dimension de son image.*

Définition. *Une application $\phi : E \to F$ entre deux algèbres est un morphisme d'algèbre si elle vérifie de surcroit $\phi(x \times y) = \phi(x) \times \phi(y)$ quels que soient $(x, y) \in E^2$.*

On note $\mathrm{Hom}(E, F)$ ou parfois $\mathscr{L}(E, F)$ l'ensemble de toutes les applications linéaires de E dans F ; c'est lui-même un espace vectoriel pour les lois de composition induites :

$$\phi + \psi : x \longmapsto \phi(x) + \psi(x)$$
$$\lambda \cdot \phi : x \longmapsto \lambda \cdot \phi(x)$$

Le noyau et l'image sont des paramètres cruciaux :
— L'application $\phi : E \to F$ est injective si et seulement si $\ker(\phi) = \{\overrightarrow{0}\}$.
— L'application $\phi : E \to F$ est surjective si et seulement si $\mathrm{im}(\phi) = F$.
On appelle isomorphisme d'espaces vectoriels toute application linéaire bijective ; sa réciproque est aussi linéaire et cette notion coïncide donc avec celle d'applications linéaires inversibles.

Théorème. *Pour tout application linéaire $\phi : E \to F$ on a $E / \ker(\phi) \simeq \mathrm{im}(\phi)$.*

Par les dimensions, on obtient l'égalité que beaucoup appellent le théorème du rang :

$$\dim(E) = \dim(\ker(\phi)) + \mathrm{rg}(\phi)$$

Certaines classes d'applications linéaires méritent des notations spécifiques.
— $\mathrm{Hom}(E, \mathbb{K}) = E^*$ l'espace des formes linéaires de E.
— $\mathrm{Hom}(E, E) = \mathrm{End}(E)$ l'algèbre des endomorphismes de E ;
L'ensemble des endomorphismes inversibles (appelés automorphismes) forme un groupe pour la composition noté $\mathrm{Aut}(E)$ ou encore $\mathscr{GL}(E)$, pour « groupe linéaire ».

Dans un espace vectoriel de dimension finie n, d'après le théorème du rang, tout endomorphisme injectif est surjectif et vice-versa. Les automorphismes sont donc caractérisés par l'égalité $\ker(\phi) = \{\overrightarrow{0}\}$ ou, de manière équivalente, l'égalité $\mathrm{rg}(\phi) = n$. Attention, ceci est faux en dimension infinie.

Mentionnons enfin des classes plus anecdotiques d'applications linéaires.

Définition. *Une application linéaire π vérifiant $\pi^2 = \pi$ est appelée projecteur.*
Une application linéaire σ vérifiant $\sigma^2 = \mathrm{id}$ est appelée symétrie (ou involution).

Exemple. *Soit $(E_i)_{i \in I}$ une famille finie de sous espaces vectoriels de E supplémentaires. Les applications $\pi_j : \begin{cases} E \longrightarrow E_j \\ \sum_{i \in I} x_i \longmapsto x_j \end{cases}$ pour $j \in I$ sont des projecteurs dont la somme est l'identité.*

Exercice. *Montrer que, pour tout endomorphisme ϕ, la suite $\left(\ker(\phi^k)\right)_{k \in \mathbb{N}}$ est croissante alors que $\left(\mathrm{im}(\phi^k)\right)_{k \in \mathbb{N}}$ est décroissante.*

Exercice. *Montrer qu'il n'existe pas d'application linéaire injective (resp. surjective) de $\mathbb{R}^p$ dans $\mathbb{R}^q$ lorsque $p > q$ (resp. $p < q$).*

Exercice. *Soit E un espace vectoriel. Montrer la linéarité de l'application*

$$\mathrm{ad} : \begin{cases} \mathscr{L}(E) \longrightarrow \mathscr{L}(\mathscr{L}(E)) \\ f \longmapsto (g \mapsto fg - gf) \end{cases}.$$

À quelle condition sur f l'application $\mathrm{ad}(f)$ est-elle injective ou surjective ?
Supposant que $f^n = 0$, montrer que $\mathrm{ad}(f)^{2n-1} = 0$ mais que $f^{n-1} \in \mathrm{im}(\mathrm{ad}(f)^{2n-2})$.

5.3 Représentation matricielle

Restreignons nous à présent au cas de la dimension finie. Afin de représenter efficacement une application linéaire, il suffit de décrire la transformation qu'elle fait subir à des bases des espaces vectoriels concernés.

Définition. *La matrice d'une application linéaire $\phi : E \to F$ dans des bases $(e_i)_{i\in\{1,\dots,n\}}$ de E et $(f_j)_{j\in\{1,\dots,m\}}$ de F est le tableau de scalaires $(\lambda_{j,i})_{(j,i)\in\{1,\dots,m\}\times\{1,\dots,n\}}$ vérifiant $\phi(e_i) = \sum_{j\in\{1,\dots,m\}} \lambda_{j,i} f_j$ pour tout $i \in \{1,\dots,n\}$; on note :*

$$\mathrm{mat}_{(e_i,f_j)}(\phi) = \begin{pmatrix} \lambda_{1,1} & \lambda_{1,2} & \cdots & \lambda_{1,n} \\ \lambda_{2,1} & \lambda_{2,2} & \cdots & \lambda_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{m,1} & \lambda_{m,2} & \cdots & \lambda_{m,n} \end{pmatrix}$$

Si $E = F$ et $\phi = \mathrm{id}$, on l'appelle matrice de passage de la base (e_i) vers (f_j).

On appelle matrice de taille $m \times n$ tout tel tableau de scalaires et on note leur ensemble $\mathrm{Mat}_{m,n}(\mathbb{K})$. Les opérations sur les applications linéaires se traduisent directement en termes de matrices. Soient en effet E, F et G trois espaces vectoriels dont des bases de chacun ont été fixées. La multiplication par un scalaire $\mu \in \mathbb{K}$ s'écrit :

$$\begin{array}{ccccc} \mu & \cdot & \begin{cases} E \longrightarrow F \\ x \longmapsto \phi(x) \end{cases} & = & \begin{cases} E \longrightarrow F \\ x \longmapsto \mu\phi(x) \end{cases} \\ \mu & \cdot & (\lambda_{j,i}) & = & (\mu\lambda_{j,i}) \end{array}$$

L'addition s'écrit :

$$\begin{array}{ccccc} \begin{cases} E \longrightarrow F \\ x \longmapsto \phi(x) \end{cases} & + & \begin{cases} E \longrightarrow F \\ x \longmapsto \psi(x) \end{cases} & = & \begin{cases} E \longrightarrow F \\ x \longmapsto \phi(x) + \psi(x) \end{cases} \\ (\lambda_{j,i}) & + & (\mu_{j,i}) & = & (\lambda_{j,i} + \mu_{j,i}) \end{array}$$

Et la composition des applications correspond à :

$$\begin{array}{ccccc} \begin{cases} F \longrightarrow G \\ x \longmapsto \psi(x) \end{cases} & \circ & \begin{cases} E \longrightarrow F \\ x \longmapsto \phi(x) \end{cases} & = & \begin{cases} E \longrightarrow G \\ x \longmapsto \psi(\phi(x)) \end{cases} \\ (\mu_{k,j}) & \cdot & (\lambda_{j,i}) & = & \left(\sum_j \mu_{k,j}\lambda_{j,i}\right) \end{array}$$

On parle ainsi de l'espace vectoriel $\mathrm{Mat}_{m,n}(\mathbb{K})$, de l'algèbre $\mathrm{Mat}_n(\mathbb{K})$ des matrices carrées de taille $n \times n$ ainsi que du groupe $\mathrm{GL}_n(\mathbb{K})$ des matrices carrées inversibles de taille $n \times n$.

Attention ! Tout comme la composition des applications linéaires, la multiplication des matrices n'est pas commutative : le produit MN n'est défini que si M a autant de colonnes que N a de lignes. Dans $\mathrm{Mat}_{n,n}(\mathbb{K})$ cette multiplication admet un élément neutre qui correspond à l'application identité ; sa matrice s'écrit

$$\mathrm{id} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}.$$

Remarquons que la matrice identité de taille $n \times n$ est aussi un élément neutre à droite dans $\mathrm{Mat}_{m,n}(\mathbb{K})$ et à gauche dans $\mathrm{Mat}_{n,m}(\mathbb{K})$.

Définition. *Le rang de toute matrice* $\mathrm{mat}(\phi)$ *est celui de l'application linéaire* ϕ *; il ne dépend pas des deux bases choisies. La trace d'un endomorphisme* ϕ *est celle de la matrice* $\mathrm{mat}(\phi) = (\lambda_{j,i})$*, à savoir* $\sum_i \lambda_{i,i}$ *; elle ne dépend pas de la base choisie.*

On retiendra :
— $\mathrm{rg}(PMQ) = \mathrm{rg}(M)$ si tant est que P et Q soient inversibles.
— $\mathrm{tr}(MN) = \mathrm{tr}(NM)$.

5.4 Systèmes d'équations

Tout système d'équations linéaire avec second membre (une expression désuète signifiant « affine ») en les indéterminées $(x_i)_{i\in\{1,\dots,n\}}$ s'écrit

$$\begin{cases} y_1 &= \lambda_{1,1}x_1 &+ \lambda_{1,2}x_2 &+ \cdots &+ \lambda_{1,n}x_n \\ y_2 &= \lambda_{2,1}x_1 &+ \lambda_{2,2}x_2 &+ \cdots &+ \lambda_{2,n}x_n \\ & \vdots & & & \\ y_m &= \lambda_{m,1}x_1 &+ \lambda_{m,2}x_2 &+ \cdots &+ \lambda_{m,n}x_n \end{cases}$$

ce se traduit en écriture matricielle par

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix} = \begin{pmatrix} \lambda_{1,1} & \lambda_{1,2} & \cdots & \lambda_{1,n} \\ \lambda_{2,1} & \lambda_{2,2} & \cdots & \lambda_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{m,1} & \lambda_{m,2} & \cdots & \lambda_{m,n} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

et inverser cette matrice est donc parfaitement équivalent à résoudre ce système en gardant les variables $(y_i)_{i\in\{1,\dots,m\}}$ formelles.

Pour déterminer si une matrice carrée donnée est inversible, on peut calculer son noyau, son rang ou encore son déterminant ; pour l'inverser, on dispose de formules plus élaborées encore. En pratique, toutefois, tous les calculs se mènent par la méthode dite « du pivot de Gauss » : elle consiste à appliquer à la matrice une suite d'opérations élémentaires afin de la ramener sous forme triangulaire, où les taches ci-dessus sont alors triviales.

Définition. *La méthode dite « du pivot de Gauss » consiste à appliquer les opérations suivantes à une matrice* $M \in \mathrm{Mat}_{m,n}(\mathbb{K})$*.*

1. *Si la première colonne est nulle, aller en 5.*
2. *Si* $m_{1,1} = 0$*, trouver* i *tel que* $m_{i,1} \neq 0$ *et intervertir les lignes* 1 *et* i*.*

3. *Pour j de 2 à m :*
4. *Ajouter à la ligne j le produit de la première ligne par $-m_{j,1}/m_{1,1}$.*
5. *Retourner en 1 en se restreignant à la sous matrice d'indices $\{2,\dots,m\}\times\{2,\dots,n\}$.*

Si elle est carrée, la matrice triangulaire obtenue peut de surcroit être mise sous forme diagonale en lui appliquant à nouveau la méthode dite « du pivot de Gauss » mais cette fois ci sur les colonnes. On pourrait enfin se ramener à une matrice du type

$$J_r = \begin{pmatrix} \mathrm{id}_r & 0 \\ 0 & 0_{n-r} \end{pmatrix}$$

en multipliant chaque ligne (ou colonne) par l'inverse de son coefficient diagonal.

Les opérations effectuées par la méthode dite « du pivot de Gauss » sur les lignes (comme décrit ci-dessus) correspondent à la multiplication de M à gauche par :

— $\mathrm{id} - E_{1,1} - E_{i,i} + E_{1,i} + E_{i,1}$, matrice de permutation, pour l'étape 2 ;
— $\mathrm{id} - m_{j,1}/m_{1,1}E_{1,j}$, matrice de transvection, pour l'étape 4.
— $\mathrm{id} + (m_{i,i}^{-1} - 1)E_{i,i}$, matrice de dilatation, pour obtenir J_r.

où $E_{i,j}$ dénote la matrice de $\mathrm{Mat}_m(\mathbb{K})$ dont les coefficients sont nuls à l'exception d'un unique « 1 » placé à l'intersection de la i^{e} ligne et de la j^{e} colonne.

Cela ramène notamment l'inversion de M à celle de ces matrices élémentaires. D'un point de vue plus théorique, cela montre :

Théorème. *Le groupe $\mathrm{GL}_n(\mathbb{K})$ est engendré par les matrices de permutation, de transvection et de dilatation. Le groupe $\mathrm{SL}_n(\mathbb{K})$ est engendré par les matrices de permutation et de transvection.*

5.5 Déterminants

Nous allons à présent développer un outil puissant lié à l'inversibilité des matrices. Géométriquement il mesure le volume du parallélépipède décrit par les vecteurs colonnes (ou lignes) d'une matrice.

Définition. *On appelle forme n-linéaire alternée d'un espace vectoriel E toute application $\varphi : E^n \to \mathbb{K}$ linéaire en chacune de ses n variables et s'annulant sur tous les n-uplets liés.*

En particulier, si $n > \dim(E)$, alors seule la forme nulle convient.

Théorème. *Si $n = \dim(E)$ alors l'espace vectoriel de ses formes n-linéaires alternées est de dimension un.*

Démonstration. Soit $(e_i)_{i\in\{1,\dots,n\}}$ une base de E. Évaluons une forme n-linéaire alternée φ en les vecteurs arbitraires $x_i = \sum_{j=1}^{n} \lambda_{i,j} e_j$ pour $i \in \{1,\dots,n\}$:

$$\begin{aligned}
\varphi(x_1,\dots,x_n) &= \varphi\left(\sum_{j=1}^{n}\lambda_{1,j}e_j,\dots,\sum_{j=1}^{n}\lambda_{n,j}e_j\right)\\
&= \sum_{s\in\{1,\dots,n\}^n} \varphi\left(\lambda_{1,s_1}e_{s_1},\dots,\lambda_{n,s_n}e_{s_n}\right)\\
&= \sum_{s\in\{1,\dots,n\}^n} \varphi\left(e_{s_1},\dots,e_{s_n}\right)\prod_{i=1}^{n}\lambda_{i,s_i}\\
&= \sum_{\sigma\in\mathfrak{S}_n} \varphi\left(e_{\sigma(1)},\dots,e_{\sigma(n)}\right)\prod_{i=1}^{n}\lambda_{i,\sigma(i)}\\
&= \varphi(e_1,\dots,e_n)\sum_{\sigma\in\mathfrak{S}_n}(-1)^{\varepsilon(\sigma)}\prod_{i=1}^{n}\lambda_{i,\sigma(i)}
\end{aligned}$$

□

Fort de cette observation, introduisons enfin le déterminant.

Définition. *On appelle déterminant d'une matrice* $M \in \mathrm{Mat}_n(\mathbb{K})$ *la quantité*

$$\det(M) = \sum_{\sigma \in \mathfrak{S}_n} (-1)^{\varepsilon(\sigma)} \prod_{i=1}^{n} m_{i,\sigma(i)}.$$

On appelle déterminant d'un endomorphisme la quantité par laquelle celui-ci multiplie les déterminants des familles de vecteurs ; c'est aussi le déterminant de toute matrice le représentant.

Corollaire. *Une matrice* M *est inversible si et seulement si* $\det(M) \neq 0$.
On a $\det(MN) = \det(M)\det(N)$ *et ainsi* $\det(M^{-1}) = \det(M)^{-1}$.

Il s'ensuit notamment que l'ensemble des matrices de déterminant unité forme un groupe pour la multiplication noté $\mathrm{SL}_n(\mathbb{K})$.

Finissions en considérant le calcul pratique de déterminant qui se fera principalement en exploitant la proposition suivante. Elle peut facilement être déduite de la définition ci-dessus.

Proposition (développement suivant les colonnes)**.** *Pour toute matrice* $M \in \mathrm{Mat}_n(\mathbb{K})$ *et tout indice* $j \in \{1, \dots, n\}$ *on a*

$$\det(M) = \sum_{i=1}^{n} (-1)^{i+j} m_{ij} \det\big(\mathrm{mineur}_{i,j}(M)\big)$$

où $\mathrm{mineur}_{i,j}(M)$ *dénote la matrice de taille* $(n-1) \times (n-1)$ *déduite de* M *en supprimant sa* i^e *ligne et sa* j^e *colonne.*

Corollaire. *Lorsque* M *est inversible on a*

$$M^{-1} = \frac{1}{\det(M)}\, {}^t \underbrace{\big((-1)^{i+j} \det(\mathrm{mineur}_{i,j}(M))\big)_{i,j}}_{\text{matrice des cofacteurs}}$$

Démonstration. En multipliant M par le membre de droite on obtient la matrice dont le coefficient d'indice (i, j) vaut

$$\frac{1}{\det(M)} \sum_k m_{i,k} (-1)^{j+k} \det(\mathrm{mineur}_{j,k}(M))$$

Or cette somme n'est autre que le développement suivant la k^{e} ligne d'une certaine matrice :

- Pour $i = j$ c'est M ; le coefficient d'indice (i, i) vaut donc $\frac{1}{\det(A)} \det(A) = 1$.
- Pour $i \neq j$ c'est M avec la k^{e} ligne remplacée par la i^{e} ; son déterminant s'annule et il en va de même du coefficient d'indice (i, j).

□

5.6 Dualité

Définition. *On appelle dual d'un espace vectoriel* E *l'espace vectoriel de ses formes linéaires* E^*.

Proposition. *À toute base* (e_i) *de* E *correspond la base duale* $(x \mapsto \lambda_i(x))$ *de* E^* *définie par la décomposition* $x = \sum_i \lambda_i(x) e_i$. *On a en particulier* $\dim(E^*) = \dim(E)$.

On peut remarquer que le noyau de toute forme linéaire $\varphi : E \to \mathbb{K}$ non nulle est un hyperplan de E, c'est-à-dire un sous espace vectoriel de dimension $\dim(E) - 1$. C'est en réalité une facette d'un fait bien plus général.

Proposition. *L'application associant à tout sous espace vectoriel $F \subset E$ l'espace vectoriel $F^\perp \subset E^*$ des formes linéaires s'annulant dessus est une bijection. On a* $\dim(F) + \dim(F^\perp) = \dim(E)$.

Pour le calcul, on pourra utiliser les identités $(F+G)^\perp = F^\perp \cap G^\perp$ et $(F \cap G)^\perp = F^\perp + G^\perp$.

Définition. *On appelle duale d'une application linéaire $\phi : E \to F$ l'application linéaire $\phi^* : \psi \in F^* \to \psi \circ \phi \in E^*$.*

Dans les bases duales la matrice de ϕ^* s'écrit :

$$\mathrm{mat}(\phi^*) = (\lambda_{j,i}) = {}^t(\lambda_{i,j}) = {}^t\,\mathrm{mat}(\phi)$$

Proposition. *Pour toute matrice carrée M on a* $\mathrm{rg}({}^tM) = \mathrm{rg}(M)$ *et* $\det({}^tM) = \det(M)$

5.7 Réduction

L'objectif de cette section est, étant donné un endomorphisme ϕ d'un espace vectoriel de dimension finie, de trouver une base sur laquelle il agit de manière relativement simple, typiquement, par dilatation. Si $M = \mathrm{mat}(\phi)$ dans une base arbitraire, cela revient à trouver une matrice P inversible (de passage dans la nouvelle base) pour laquelle PMP^{-1} est une matrice « simple », typiquement, diagonale. Nous exploiterons indifféremment ces deux points de vues, linéaire et matriciel.

Définition. *On dit que M est diagonalisable s'il existe P inversible telle que PMP^{-1} est diagonale. On dit que M est trigonalisable s'il existe P inversible telle que PMP^{-1} est triangulaire.*

Si x est un vecteur d'une base sur laquelle l'endomorphisme agit par dilatation, alors on a $\phi(x) = \lambda x$ pour un certain $\lambda \in \mathbb{K}$, soit encore $x \in \ker(\phi - \lambda\,\mathrm{id})$. Ce critère nous permet de chercher de tels vecteurs, espérant en trouver suffisamment pour former une base.

Définition. *Si $\phi - \lambda\,\mathrm{id}$ n'est pas injectif, on dit que :*
- *le scalaire λ est une valeur propre de ϕ ;*
- *l'espace propre associé à λ est* $\ker(\phi - \lambda\,\mathrm{id})$*;*
- *les vecteurs non triviaux de ce noyau sont des vecteurs propres ;*

L'ensemble des valeurs propres s'appelle le spectre et se note $\mathrm{sp}(\phi)$.

Lemme. *Toute famille $(x_1, \dots, x_k)$ de vecteurs propres associés à des valeurs propres distinctes $(\lambda_1, \dots, \lambda_k)$ est libre.*

Tout endomorphisme admet donc au plus $n = \dim(E)$ valeurs propres distinctes ; lorsque cette quantité est atteinte, tout n-uplet de vecteurs propres associés forme une base et l'endomorphisme est diagonalisable. La trace et le déterminant étant invariants par $M \mapsto PMP^{-1}$, on peut alors les lire directement sur la matrice diagonale : la trace est la somme des valeurs propres et le déterminant leur produit.

En toute généralité, on a :

Théorème. *Un endomorphisme ϕ est diagonalisable si et seulement si on a* $E = \bigoplus_\lambda \ker(\phi - \lambda\,\mathrm{id})$.

Afin de mettre ce critère sous forme effective, il nous faut à présent introduire les polynômes d'endomorphismes.

Définition. *On appelle polynôme caractéristique d'un endomorphisme ϕ le polynôme $\chi_\phi(X) = \det(\phi - X\,\mathrm{id}) \in \mathbb{K}[X]$.*

À ϕ fixé, l'application

$$\begin{cases} \mathbb{K}[X] \longrightarrow \mathrm{End}(E) \\ P \longmapsto P(\phi) \end{cases}$$

est un morphisme d'algèbre commutative. (L'algèbre $\mathrm{End}(E)$ n'est évidemment pas commutative, mais l'image de ce morphisme, à savoir la sous algèbre $\mathbb{K}[\phi]$, l'est.)

Théorème (Cayley–Hamilton). *Le polynôme caractéristique χ_ϕ annule l'endomorphisme ϕ.*

Définition. *On appelle polynôme annulateur de ϕ tout polynôme $P \in \mathbb{K}[X]$ tel que $P(\phi) = 0$.*

L'ensemble de ces polynômes forme un idéal de $\mathbb{K}[X]$; il est monogène car l'anneau est principal. On note μ_ϕ son polynôme unitaire de plus petit degré, appelé polynôme minimal. On a donc $\mu_\phi \mid \chi_\phi$ et, inversement, il n'est pas difficile de montrer que chaque facteur irréductible de χ_ϕ divise μ_ϕ.

Lemme. *Les exposants k_λ du polynôme minimal $\mu_\phi(X) = \prod_\lambda (X-\lambda)^{k_\lambda}$ sont les plus petits entiers tels que $E = \bigoplus_\lambda \ker(\phi - \lambda)^{k_\lambda}$.*

Théorème. *Un endomorphisme est diagonalisable si et seulement si son polynôme minimal est scindé à racines simples.*

Un endomorphisme est trigonalisable si et seulement s'il admet un polynôme annulateur scindé.

Corollaire. *Sur le corps des complexes $\mathbb{C}$, tous les endomorphismes sont trigonalisables.*

Parfois, une seule matrice ne suffit pas...

Théorème. *Si ϕ et ψ sont diagonalisables et commutent, alors ils sont co-diagonalisables.*

Si ϕ et ψ sont trigonalisables et commutent, alors ils sont co-trigonalisables.

Exercice. *La suite de Fibonacci est définie par $F_0 = 0$, $F_1 = 1$ et $F_{n+1} = F_n + F_{n-1}$.*

Trouver une matrice $M \in \mathrm{Mat}_2(\mathbb{R})$ telle que $M \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix}$.

Diagonaliser M et en déduire une formule explicite pour le terme général F_n.

Exercice. *Soit une matrice $x \in \mathrm{Mat}_n(\mathbb{C})$ de polynôme minimal $\prod_{i=1}^m (X-\lambda_i)^{r_i}$.*

Soit une fonction $f \in \mathscr{C}^\infty(\mathbb{C},\mathbb{C})$ et un polynôme $P \in \mathbb{C}[X]$ qui interpole f sur le spectre de x, c'est-à-dire qui vérifie $P^{(j)}(\lambda_i) = f^{(j)}(\lambda_i)$ pour tout $j \in \{0,\dots,r_i-1\}$ et tout $i \in \{1,\dots,m\}$. Montrer que la matrice $P(x)$ ne dépend pas du polynôme P choisi ; on la note $f(x)$.

Montrer que $\exp(x)$ *correspond à l'exponentielle matricielle classique.*

Montrer que $(f+g)(x) = f(x) + g(x)$ et que $(f \cdot g)(x) = f(x)g(x)$.

Si x est nilpotente montrer que, pour tout entier i, il existe une matrice y telle que $(\mathrm{id}+y)^i = \mathrm{id}+x$.

5.8 Topologie

Soient n un entier fixé et $\mathbb{K}$ le corps des réels ou des complexes. L'espace vectoriel $\mathrm{Mat}_n(\mathbb{K})$ étant de dimension finie, toutes ses normes sont équivalentes et induisent donc la même topologie. On pourra notamment utiliser indistinctement les normes suivantes :

$$\|A\|_\infty = \max\left\{ \left| a_{ij} \right| : (i,j) \in \{1,\dots,n\}^2 \right\}$$

$$|||A||| = \sup_{x \in \mathbb{K}^n \setminus \{\vec{0}\}} \frac{\|Ax\|}{\|x\|}$$

(La seconde pouvant être définie pour toute norme $\|\cdot\|$ de $\mathbb{K}^n$.)

Théorème. *La partie* $\mathrm{GL}_n(\mathbb{K})$ *est un ouvert dense de* $\mathrm{Mat}_n(\mathbb{K})$.

Sa structure topologique nous permet de considérer des fonctions continues sur $\mathrm{Mat}_n(\mathbb{K})$.

Définition. *Soit A une matrice carrée. La série*

$$\sum_{k=0}^{\infty} \frac{1}{k!} A^k$$

converge coefficient par coefficient vers une matrice que l'on note e^A.

En pratique, lorsqu'il s'agira de calculer l'exponentielle d'une matrice donnée, il sera souvent opportun de commencer par la diagonaliser.

Lemme. *Si les matrices A et B commutent alors on a $e^{A+B} = e^A e^B$.*

Corollaire. *L'exponentielle est une application continue de* $\mathrm{Mat}_n(\mathbb{K})$ *dans* $\mathrm{GL}_n(\mathbb{K})$.

Démonstration. Appliquer le lemme à $B = -A$ puis $|||B||| < \varepsilon$. □

Proposition. *Soit A une matrice de* $\mathrm{Mat}_n(\mathbb{K})$. *La fonction $Z : t \mapsto \exp(tA)$ est l'unique fonction de $\mathscr{C}^1(\mathbb{R}, \mathrm{Mat}_n(\mathbb{K}))$ vérifiant*

$$Z' = AZ \qquad \text{et} \qquad Z(0) = \mathrm{id}_n$$

Démonstration. Dériver la série pour voir que cette fonction est bien solution ; appliquer le théorème de Cauchy–Lipschitz pour voir qu'elle est unique. □

Chapitre 9

Analyse réelle et complexe

9.1 Nombres réels et complexes

Le corps $\mathbb{Q}$ des nombres rationnels se construit de manière explicite à partir des entiers naturels et donne ainsi rarement matière à confusion. En revanche, savoir si les réels 1 et $0,999\ldots$ sont égaux est une question qui égare encore bien des mathématiciens amateurs.

Définition. *Soit $(E,<)$ un ensemble ordonné. La borne supérieure d'une partie $F \subset E$ est, si elle existe, le plus petit majorant de F. On dit que $(E,<)$ vérifie la propriété de la borne supérieure si toute partie non-vide majorée admet une borne supérieure.*

Soit $(E,|\cdot|)$ un espace métrique. Une suite $(x_n) \in E^{\mathbb{N}}$ est dite de Cauchy si elle satisfait

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall m,n > N, |x_n - x_m| < \varepsilon.$$

On dit que $(E,|\cdot|)$ est complet lorsque toute suite de Cauchy est convergente.

Le corps des nombres rationnels ne vérifie pas ces propriétés :
— L'ensemble $\{x \in \mathbb{Q} : x^2 < 2\}$ n'admet pas de borne supérieure.
— La suite définie par $x_0 = 1$ et $x_{k+1} = \frac{1}{2+x_k}$ n'admet pas de limite dans $\mathbb{Q}$.

C'est pour y remédier que l'on construit les réels, soit en rajoutant les bornes supérieures des ensembles non-vides majorés (coupures de Dedekind), soit en rajoutant les limites des suites de Cauchy (complétion métrique), ces deux approches donnant au final un résultat équivalent. Ces constructions étant techniques, on se contente souvent de retenir les propriétés fondamentales :

Théorème. *Le corps $\mathbb{R}$ des nombres réels est complet et vérifie la propriété de la borne supérieure.*

Comme vous le savez, cet ensemble de nombres est parfaitement adapté pour représenter les grandeurs physiques. Toutefois il présente l'inconvénient algébrique que certains polynômes non constants n'y admettent aucune racine.

Définition. *On dit qu'un corps $\mathbb{K}$ est algébriquement clos si tout polynôme non constant de $\mathbb{K}[X]$ admet une racine.*

Le polynôme x^2+1 n'admettant aucune racine réelle, on construit le corps des complexes en rajoutant une racine à ce polynôme (clôture algébrique). Cela suffit pour obtenir toutes les racines voulues :

Théorème (d'Alembert–Gauss). *Le corps $\mathbb{C} = \mathbb{R}[X]/(X^2+1) = \mathbb{R}[i]$ est algébriquement clos.*

9.2 Suites numériques

Nous passerons brièvement sur ces notions qui devraient déjà être maîtrisées. Remarquer que seules les propriétés faisaient intervenir l'ordre sont spécifiques aux suites réelles.

Définition. *On dit qu'une suite $(x_n) \in \mathbb{C}^{\mathbb{N}}$ converge s'il existe un nombre $\ell \in \mathbb{C}$ vérifiant*

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n > N, |x_n - \ell| < \varepsilon.$$

On dit alors que ℓ est la limite de x_n et on note $\ell = \lim x_n$.

Exercice (moyenne de Cesàro). *Si (x_n) est une suite de limite ℓ, montrer que la suite $(\frac{1}{n}\sum_{k=1}^{n} x_k)$ converge vers ℓ.*

On peut montrer que l'application $x \in \mathbb{C}^{\mathbb{N}} \mapsto \lim(x) \in \mathbb{C}$ est un morphisme d'algèbre ; cela permet de manipuler la définition ci-dessus mais ne présente pas d'intérêt au delà.

Théorème. *Toute suite réelle croissante majorée admet une limite.*

Prouver ce théorème est très instructif : poser $\ell = \sup\{x_n\}$ puis vérifier la définition de la limite en exploitant les propriétés de la borne supérieure. S'il pourra aussi être bénéfique de démontrer d'autres théorèmes de convergence (gendarmes, suites adjacentes) leur intérêt théorique ne justifie pas que nous nous attardions dessus.

Définition. *On appelle sous-suite ou suite extraite d'une suite $(x_n)_{n\in\mathbb{N}}$ toute suite de la forme $(x_{\varphi(n)})_{n\in\mathbb{N}}$ où $\varphi : \mathbb{N} \to \mathbb{N}$ est une fonction strictement croissante.*

Définition. *On appelle valeur d'adhérence d'une suite x_n toute limite d'une sous-suite. De manière équivalente, ℓ est une valeur d'adhérence si*

$$\forall \varepsilon > 0, \forall N > 0, \exists n > N, |x_n - \ell| < \varepsilon.$$

Théorème (Bolzano–Weierstrass). *Toute suite bornée admet une valeur d'adhérence. Autrement dit, de toute suite bornée on peut extraire une sous-suite convergente.*

Le programme nous demande d'expliciter le cas classique que voici.

Définition. *Une suite x est dite récurrente linéaire si elle vérifie*

$$\forall n \in \mathbb{N}, a_k x_{n+k} + a_{k-1} x_{n+k-1} + \cdots + a_1 x_{n+1} + a_0 x_n = 0.$$

pour un certain vecteur $(a_0, \ldots, a_k) \in \mathbb{R}^{k+1}$ avec $a_k \neq 0$. On dit que cette relation de récurrence est d'ordre k et de polynôme caractéristique $P(X) = a_k X^k + a_{k-1} X^{k-1} + \cdots + a_1 X + a_0$.

Proposition. *Toute suite récurrente linéaire dont le polynôme caractéristique se factorise en*

$$\prod_{i\in\{1,\ldots,k\}} (X - \alpha_i)^{\beta_i}$$

est une combinaison linéaire des suites $(n^\gamma \alpha_i^n)_{n\in\mathbb{N}}$ avec $\gamma \in \{0, 1, \ldots, \beta_i - 1\}$ et $i \in \{1, \ldots, k\}$.

Démonstration. La relation de récurrence s'écrit

$$\begin{pmatrix} a_{n+k+1} \\ a_{n+k} \\ \vdots \\ a_{n+1} \end{pmatrix} = \begin{pmatrix} a_k & a_{k-1} & \cdots & a_0 \\ 1 & 0 & \cdots & 0 \\ & \ddots & \ddots & \vdots \\ & & 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n+k} \\ a_{n+k-1} \\ \vdots \\ a_n \end{pmatrix}$$

et il s'agit alors de diagonaliser la matrice compagnon. □

Exercice. *Écrire une formule close pour le n^e terme de la suite de Fibonacci.*

9.3 Séries numériques

Définition. *On appelle série de terme général x_n la suite $\left(\sum_{k=0}^{n} x_k\right)_{n\in\mathbb{N}}$. On dit qu'elle converge absolument lorsque $\left(\sum_{k=0}^{n} |x_k|\right)_{n\in\mathbb{N}}$ est bornée. Si ce n'est pas le cas mais que la série converge au sens classique, on dit qu'elle est semi-convergente.*

Exemple. *On a les convergences suivantes :*
- *La série de terme général 1 diverge grossièrement.*
- *La série de terme général $1/n$ diverge.*
- *La série de terme général $(-1)^n/n$ est semi-convergente.*
- *La série de terme général $(-1)^n/n^2$ converge absolument.*

Pour étudier la convergence d'une série on pourra plus généralement se ramener aux cas classiques par le critère de comparaison que voici.

Proposition. *Soit deux séries de terme général positif x_n et y_n.*
Si $y_n = O(x_n)$ et la série de terme général x_n converge, alors l'autre aussi.
Si $y_n \sim x_n$ alors les deux séries sont de même nature ; si elles convergent, leurs restes sont équivalents ; si elles divergent, leurs sommes partielles sont équivalentes.

Les cas les plus classiques sont les suivants.

Proposition (critère de Riemann). *La série de terme général n^α converge absolument si et seulement si $\Re(\alpha) < -1$.*

Démonstration. Comparer cette série avec une intégrale. □

Lorsque $\Re(\alpha) = -1$ et $\alpha \neq -1$, la suite $\sum_{k=0}^{n} k^\alpha$ est semi-convergente. Dans le cas $\alpha = 1$ on a la série harmonique :

$$\sum_{k=1}^{n} \frac{1}{k} = \log(n) + \gamma + \frac{1}{2n} + o\left(\frac{1}{n}\right)$$

Deux critères de convergence par comparaison avec des suites géométriques sont pertinents.

Théorème (règle de Cauchy). *Soit x_n une suite vérifiant $\limsup \sqrt[n]{|x_n|} = \ell$; alors si $\ell > 1$ la série associée diverge et si $\ell < 1$ elle converge.*

Corollaire (règle de d'Alembert). *Soit x_n une suite vérifiant $\lim \left|\frac{x_{n+1}}{x_n}\right| = \ell$; alors si $\ell > 1$ la série associée diverge et si $\ell < 1$ elle converge.*

9.4 Notations de Landau

Ces notations sont associées à la notion de limite ; on peut les utiliser tant pour les suites que pour les fonctions. Nous allons ici les introduire dans le cadre des fonctions car c'est pour leur étude qu'elles seront le plus utiles.

Définition. *Soient f et g deux fonctions réelles, et soit $\alpha \in \mathbb{R} \cup \{\pm\infty\}$. On note :*
- *$f = O_\alpha(g)$ « f est dominée par g en α » lorsque f/g est bornée sur un voisinage d'α.*
- *$f \sim_\alpha g$ « f et g sont équivalentes en α » lorsque f/g a pour limite 1 en α.*
- *$f = o_\alpha(g)$ « f est négligeable devant g en α » lorsque f/g a pour limite 0 en α.*

Attention ! Les équivalents sont très difficile à manipuler sans erreur. Par exemple, en l'infini, on a $x + 1/x \sim x$ et $-x \sim -x$, mais on n'a pas pour autant l'équivalence « somme » $1/x \sim 0$. Lorsque c'est possible, utiliser de préférence les notations o et O. Quelqu'un qui aurait écrit $x + 1/x - x = o(x)$ n'aurait pas commit d'erreur.

Proposition. *Pour tout $n \in \mathbb{N}$, on a les égalités classiques suivantes en zéro :*

$$\begin{aligned}
\frac{1}{1-x} &= \sum_{k=0}^{n} x^k + O(x^{n+1}) && = 1 + x + x^2 + O(x^3) \\
\exp(x) &= \sum_{k=0}^{n} \frac{1}{k!} x^k + O(x^{n+1}) && = 1 + x + \frac{1}{2}x^2 + O(x^3) \\
\log(1-x) &= \sum_{k=1}^{n} \frac{-1}{k} x^k + O(x^{n+1}) && = -x - \frac{1}{2}x^2 - \frac{1}{3}x^3 + O(x^4) \\
(1+x)^\alpha &= \sum_{k=0}^{n} \frac{(\alpha-0)\cdots(\alpha-(k-1))}{k!} x^k + O(x^{n+1}) && = 1 + \alpha x + \frac{\alpha(\alpha-1)}{2!}x^2 + O(x^3) \\
\sqrt{1-x} &= \sum_{k=0}^{n} \frac{(2k)!}{(1-2k)4^k (k!)^2} x^k + O(x^{n+1}) && = 1 - \frac{1}{2}x - \frac{1}{8}x^2 + O(x^3) \\
\sin(x) &= \sum_{k=0}^{n} \frac{(-1)^k}{(2k+1)!} x^{2k+1} + O(x^{2n+3}) && = x - \frac{1}{6}x^3 + \frac{1}{120}x^5 + O(x^7) \\
\cos(x) &= \sum_{k=0}^{n} \frac{(-1)^k}{(2k)!} x^{2k} + O(x^{2n+2}) && = 1 - \frac{1}{2}x^2 + \frac{1}{24}x^4 + O(x^6)
\end{aligned}$$

9.5 Continuité

Définition. *On dit qu'une fonction $f : I \subset \mathbb{R} \to \mathbb{C}$ est continue en $\alpha \in \overline{I}$ lorsqu'il existe un nombre $\ell \in \mathbb{C}$ vérifiant*

$$\forall \varepsilon > 0, \exists \eta > 0, \forall x \in I \cap]\alpha - \eta, \alpha + \eta[, |f(x) - \ell| < \varepsilon;$$

on dit alors que ℓ est la limite de f en α et on note $\ell = \lim_\alpha f$

Si $\alpha \notin I$ on appelle alors prolongement par continuité de f en α la fonction :

$$\begin{cases} I \cup \{\alpha\} \longrightarrow \mathbb{C} \\ \qquad x \longmapsto \begin{cases} f(x) & \text{si } x \in I \\ \lim_\alpha f & \text{si } x = \alpha \end{cases} \end{cases}$$

En notation de Landau la continuité s'écrit $f(x) = f(\alpha) + o(1)$.

Exercice. *Est-il possible de prolonger par continuité les fonctions suivantes ?*

— $x \mapsto \sin(\frac{1}{x})$
— $x \mapsto x \sin(\frac{1}{x})$
— $x \mapsto e^{-\frac{1}{x^2}}$

Théorème (valeurs intermédiaires)**.** *L'image d'un intervalle par une fonction continue est un intervalle.*

Théorème (compacité)**.** *L'image d'un intervalle fermé borné par une fonction continue est un intervalle fermé borné.*

On pourra prouver ces théorèmes pour s'entraîner à utiliser la propriété de la borne supérieure ou celle de Bolzano–Weierstrass.

Exercice. *Soit f une fonction réelle continue sur $[0;1]$ vérifiant $f(0) = f(1)$. Montrer que, quel que soit $n \in \mathbb{N}^\times$, l'équation $f(x + \frac{1}{n}) = f(x)$ admet une solution. Appliquer ce résultat à la fonction $x \mapsto x - \frac{\sin(n\pi x)^2}{\sin(n\pi)^2}$. Et si n est un réel ?*

Il existe des notions de continuité « plus fortes » :

Définition. *On dit que $f : I \subset \mathbb{R} \to \mathbb{C}$ est uniformément continue si*

$$\forall \varepsilon > 0, \exists \eta > 0, \forall \alpha \in I, \forall x \in I, |x - \alpha| < \eta \Longrightarrow |f(x) - f(\alpha)| < \varepsilon$$

(remarquer l'emplacement du quantificateur sur α).

Théorème (Heine). *Toute fonction réelle continue sur un compact est uniformément continue.*

Définition. *On dit que $f : I \subset \mathbb{R} \to \mathbb{C}$ est lipschitzienne s'il existe $\gamma \in \mathbb{R}$ tel que*

$$\forall \alpha \in I, \forall x \in I, |f(x) - f(\alpha)| \leqslant \gamma |x - \alpha|;$$

on dit qu'elle est contractante lorsque $\gamma < 1$.

Évidemment, toute fonction lipschitzienne est uniformément continue, et toute fonction uniformément continue est continue.

Exemple. *La fonction* sin *est lipschitzienne. La fonction $\sqrt{\cdot}$ est uniformément continue mais pas lipschitzienne. La fonction* log *est continue mais pas uniformément continue.*

9.6 Dérivabilité

Définition. *Une fonction $f : I \subset \mathbb{R} \to \mathbb{C}$ est dite dérivable en $\alpha \in \overline{I}$ lorsque la quantité*

$$\lim_{x \to \alpha} \frac{f(x) - f(\alpha)}{x - \alpha}$$

existe ; elle s'appelle alors la dérivée de f en α et se note $f'(\alpha)$.

En notation de Landau cela s'écrit $f(x) = f(\alpha) + f'(\alpha)(x - \alpha) + o(x - \alpha)$.

Comme les limites, on peut calculer les dérivées de fonctions s'exprimant comme combinaisons de fonctions classiques en appliquant quelques règles de calcul.

Proposition. *On a les dérivées classiques :*

$$\sin(x)' = \cos(x) \qquad \exp(x)' = \exp(x) \qquad (x^\alpha)' = \alpha x^{\alpha - 1}$$
$$\cos(x)' = -\sin(x) \qquad \log(x)' = x^{-1}$$

Proposition. *Soient f et g deux fonctions réelles. On a les égalités suivantes :*

$$(f + g)' = f' + g' \qquad (f \cdot g)' = f'g + fg' \qquad \left(\frac{f}{g}\right)' = \frac{f'g - g'f}{g^2}$$
$$(f \circ g)' = g' \cdot (f' \circ g) \qquad \left(f^{-1}\right)' = \frac{1}{f' \circ f^{-1}}$$

Exemple. *Comme* $\tan(x) = \frac{\sin(x)}{\cos(x)}$ *sa dérivée vaut* $\frac{\cos(x)^2+\sin(x)^2}{\cos(x)^2} = \frac{1}{\cos(x)^2}$ *; celle de sa fonction inverse est donc* $\arctan(x)' = \cos(\arctan(x))^2$. *La quantité* $\arctan(x)$ *est l'angle d'un triangle rectangle de côté adjacent* 1 *et côté opposé* x *; l'hypoténuse associé étant* $\sqrt{1+x^2}$*, on trouve*

$$\arctan(x)' = \frac{1}{1+x^2}.$$

La dérivabilité a des conséquences fortes, en premier lieu :

Théorème (accroissements finis). *Soit* $f : \mathbb{R} \to \mathbb{C}$ *une fonction dérivable sur* $[a, b]$ *avec* $a < b$. *Il existe un réel* $c \in]a, b[$ *tel que*

$$f'(c) = \frac{f(b)-f(a)}{b-a}.$$

Corollaire (forme intégrale). *Si* f *est dérivable sur* $[a, b]$ *alors on a l'encadrement*

$$f(a)-(b-a)\inf_{[a,b]} f' \leqslant f(b) \leqslant f(a)+(b-a)\sup_{[a,b]} f'$$

On peut évidemment itérer le processus de dérivation.

Définition. *On note :*

— $\mathscr{D}^n(I, \mathbb{C})$*, l'ensemble des fonctions n fois dérivables de* I *dans* $\mathbb{C}$

— $\mathscr{C}^n(I, \mathbb{C})$*, l'ensemble des fonctions n fois continument dérivables de* I *dans* $\mathbb{C}$

où l'expression « continument dérivable » dénote que la dérivée existe et est continue.

Exemple. *La fonction* $x \mapsto x^2 \sin(\frac{1}{x})$ *est infiniment dérivable sur* $\mathbb{R}^*$*, dérivable sur* $\mathbb{R}$*, mais pas continument dérivable.*

Proposition (fonctions convexes). *Une fonction de classe* $\mathscr{C}^1(I, \mathbb{R})$ *vérifit la propriété*

$$\forall x \in I, \forall y \in I, f\left(\frac{x+y}{2}\right) \leqslant \frac{f(x)+f(y)}{2}$$

si et seulement si sa dérivée est croissante. Remarquons aussi que cela équivaut à la convexité de la partie $\{(x, y) \in I \times \mathbb{R} : y \geqslant f(x)\}$.

9.7 Intégration

Définition. *On dit que* $f : [a, b] \to \mathbb{R}$ *est intégrable au sens de Riemann si*

$$\sup_{x_0<\cdots<x_n} \sum_{k=0}^{n-1}(x_{k+1}-x_k)\inf_{[x_k,x_{k+1}]}(f) = \inf_{x_0<\cdots<x_n} \sum_{k=0}^{n-1}(x_{k+1}-x_k)\sup_{[x_k,x_{k+1}]}(f)$$

où les extremums sont pris sur l'ensemble des subdivisions $a = x_0 < x_1 < \cdots < x_{n-1} < x_n = b$. *On note alors cette quantité* $\int_a^b f$.

Cette notion d'intégrabilité a probablement été retenue par le programme officiel pour son caractère ludique. Elle est peu robuste mais « fera l'affaire » pour des fonctions simples.

Proposition. *Toute fonction continue sauf sur un ensemble dénombrable est intégrable.*

Proposition. *L'intégrale de Riemann est une forme linéaire positive.*

Rappelons les identités classiques :

Théorème. *Lorsque ces quantités sont définies, on a :*

$$\left(\int |f\cdot g|\right)^2 \leqslant \left(\int |f|^2\right)\cdot\left(\int |g|^2\right) \qquad \textit{(Cauchy–Schwartz)}$$

$$\int_a^b f\,g' = f\,g\,]_a^b - \int_a^b f'g \qquad \textit{(intégration par partie)}$$

$$\int_{\phi(a)}^{\phi(b)} f = \int_a^b (f\circ\phi)\cdot\phi' \qquad \textit{(changement de variable)}$$

Définition. *Si f est une fonction positive sur $]a,b[$ on définit :*

$$\int_a^b f = \sup\left\{\int_c^d f : [c,d]\subset]a,b[\right\}$$

Exemple. *La fonction $x\mapsto x^\alpha$ est intégrable sur $[1,+\infty[$ si $\alpha<-1$ et sur $]0,1]$ si $\alpha>-1$. La fonction $x\mapsto e^{-x^2}$ est intégrable sur $\mathbb{R}$ de somme $\sqrt{\pi}$.*

9.8 Suites et séries de fonctions

Commençons par quelques rappels.

Définition. *On dit qu'une suite de fonctions (f_n) converge vers f sur I :*
- *simplement si $\forall x\in I, f_n(x)\to f(x)$.*
- *uniformément si $\|f_n-f\|_\infty\to 0$.*

Et si $f_n=\sum_{k=1}^n g_k$ on dit que la série converge :
- *normalement si $\sum\|g_k\|_\infty$ converge.*

Proposition. *Toute limite uniforme de fonctions continues est continue. De plus, sur un compact :*
- *Toute limite uniforme de fonctions intégrables est intégrable et $\int\lim f_n=\lim\int f_n$.*
- *Toute somme normale de fonctions intégrables est intégrable et $\int\sum f_n=\sum\int f_n$.*

Lorsque la convergence n'est que simple, c'est encore vrai lorsque, au choix :
- *La suite de fonctions est dominée par une fonction intégrable.*
- *La suite de fonctions est croissante.*

On a encore :

Proposition. *Toute limite simple de fonctions $\mathscr{C}^1$ dont les dérivées convergent uniformément est $\mathscr{C}^1$ et vérifie $(\lim f_n)'=\lim f_n'$.*

Théorème. *Si $f:I\times J\subset\mathbb{R}^2\to\mathbb{C}$ vérifie $(x\mapsto f(x,t))\in\mathscr{C}^0$ et que $|f(x,t)|\leqslant g(t)$ avec g intégrable alors $(x\mapsto\int_J f(x,t)dt)\in\mathscr{C}^0$.*

Si $f:I\times J\subset\mathbb{R}^2\to\mathbb{C}$ vérifie $(x\mapsto f(x,t))\in\mathscr{C}^1$ et que $|\partial_x f(x,t)|\leqslant g(t)$ avec g intégrable alors $\partial_x\int_J f(x,t)dt=\int_J\partial_x f(x,t)dt$.

Penchons nous maintenant sur une classe de fonctions bien particulières.

Définition. *On appelle série formelle toute série de la forme $\sum_{n\in\mathbb{N}}a_nx^n$ en une variable $x\in\mathbb{C}$.*

Les séries formelles sont en quelque sorte des polynômes de degré infini ; elles forment une algèbre notée $\mathbb{C}[[x]]$. Lorsque l'on se préoccupe de leur convergence, on a l'algèbre des séries entières que l'on note $\mathbb{C}((x))$.

Proposition (lemme d'Abel). *Toute série formelle $\sum_{n\in\mathbb{N}} a_n x^n$ admet un réel ρ appelé rayon de convergence tel que la série converge absolument dès que $|x| < \rho$ et diverge grossièrement lorsque $|x| > \rho$. Si $\rho > 0$ on dit que la série est entière.*

Théorème (Cauchy–Hadamard). $1/\rho = \limsup \sqrt[n]{a_n}$.

Proposition. *Pour $x < \rho$ la fonction $x \mapsto \sum_{n\in\mathbb{N}} a_n x^n$ est dérivable de dérivée $x \mapsto \sum_{n\in\mathbb{N}^*} n a_n x^{n-1}$.*

L'étude locale de nombreuses fonctions peut se ramener à celle des séries entières.

Théorème (formule de Taylor). *Soit f une fonction réelle dérivable n fois en α. On a :*

$$\begin{aligned} f(x) &= \sum_{k=0}^{n} \frac{f^{(k)}(\alpha)}{k!}(x-\alpha)^k + o_\alpha((x-\alpha)^n) \\ &= f(\alpha) + f'(\alpha)(x-\alpha) + \frac{f''(\alpha)}{2}(x-\alpha)^2 + \cdots + \frac{f^{(n)}(\alpha)}{n!}(x-\alpha)^n + o_\alpha((x-\alpha)^n). \end{aligned}$$

De plus, si f est dérivable $n+1$ fois, alors pour tout x il existe $\beta \in]\alpha, x[$ tel que l'on puisse remplacer $o_\alpha((x-\alpha)^n)$ par $\frac{f^{(n+1)}(\beta)}{(n+1)!}(x-\alpha)^{n+1}$ dans l'expression ci-dessus.

Cela donne un développement limité à l'ordre n pour les fonctions $\mathscr{D}^n$. Mais la réciproque n'est pas vraie : la fonction $x \mapsto x^3 \sin\left(\frac{1}{x}\right)$ admet un développement limité à l'ordre deux en zéro mais n'y est pas dérivable deux fois.

Définition. *Si f est $\mathscr{C}^\infty$ en α et que sa série de Taylor $\sum_{n\in\mathbb{N}} \frac{f^{(n)}(\alpha)}{n!} x^n$ a un rayon de convergence strictement positif, alors on dit que f est entière en α.*

Exercice. *Montrer que la fonction $x \mapsto \exp(-\frac{1}{x^2})$ n'est pas entière en zéro.*

Chapitre 10

Topologie et analyse fonctionnelle

On va étendre l'analyse des fonctions réelles d'une variable réelle dans deux directions : d'abord en étudiant les espaces $\mathbb{R}^n$ et ensuite en étudiant les espaces de fonctions eux-mêmes. Essentiellement toutes les propriétés vues plus haut admettent des généralisations dans les espaces où cela semble raisonnable.

10.1 Espaces métriques

Définition. *On appelle espace métrique tout ensemble E muni d'une fonction $d : E \times E \to \mathbb{R}_+$ appelée distance qui vérifie, pour tout $(x, y, z) \in E^3$:*

- $d(x, y) = d(x, y)$ (symétrie)
- $d(x, y) = 0 \iff x = y$ (discernabilité)
- $d(x, z) \leqslant d(x, y) + d(y, z)$ (inégalité triangulaire)

Exemple. *Voici quelques espaces métriques :*

- *Les réels $\mathbb{R}$ muni de la distance usuelle $d : (x, y) \mapsto |y - x|$.*
- *Le plan $\mathbb{R}^2$ muni de la distance usuelle $d : ((x_0, x_1), (y_0, y_1)) \mapsto \sqrt{(y_0 - x_0)^2 + (y_1 - x_1)^2}$.*
- *Le plan $\mathbb{R}^2$ muni de la distance infinie $d : ((x_0, x_1), (y_0, y_1)) \mapsto \max\{|y_0 - x_0|, |y_1 - x_1|\}$.*
- *Les suites convergentes $c(\mathbb{R})$ muni de la distance $d : ((x_k), (y_k)) \mapsto \max_k |y_k - x_k|$*
- *Les suites convergentes $c(\mathbb{R})$ muni de la distance $d : ((x_k), (y_k)) \mapsto \sum_k \frac{|y_k - x_k|}{k!}$.*
- *Les entiers naturels $\mathbb{N}^*$ muni de la distance p-adique $d(x, y) = p^{-v_p(y-x)}$.*
- *Tout ensemble E muni de la distance discrète $d : (x, y) \mapsto \begin{cases} 0 & \text{si } x = y \\ 1 & \text{si } x \neq y \end{cases}$.*

Définition. *On appelle boule ouverte de centre $x \in E$ et de rayon $\rho > 0$ la partie*

$$\mathscr{B}(x, \rho) = \{y \in E : d(x, y) < r\}.$$

La boule fermée aurait la même définition mais avec une inégalité large ; cependant, elle ne sert jamais et peut même créer des confusions : en pratique, c'est la boule ouverte qui compte.

Définition. *On dit qu'une partie $X \subset E$ est ouverte si chaque point de X admet un voisinage ouvert, c'est-à-dire si*

$$\forall x \in X, \exists \rho > 0, \mathscr{B}(x, \rho) \subset X.$$

On dit qu'une partie $X \subset E$ est fermée si son complémentaire est ouvert.

Ces notions correspondent évidemment à celle dont on a l'habitude dans les ensembles familiers.

Exemple. — *Dans $\mathbb{R}$, les intervalles de la forme $]-\infty, a[$, $]a, b[$, $]b, +\infty[$ sont ouverts.*
— *Dans $\mathbb{R}$, les intervalles de la forme $]-\infty, a]$, $[a, b]$, $[b, +\infty[$ sont fermés.*
— *Dans $\mathbb{R}^2$, la partie $\left\{(x, y) \in \mathbb{R}^2 : y > \sin(x)\right\}$ est ouverte.*
— *Dans tout espace E, les parties E et $\emptyset$ sont à la fois ouvertes et fermées.*
— *Dans $\{x, y\}$ muni de la distance discrète, toute partie est à la fois ouverte et fermée.*

Proposition. *Toute union d'ouverts est ouverte. Toute intersection finie d'ouverts est ouverte. Toute union finie de fermés est fermée. Toute intersection de fermés est fermée.*

On peut encadrer une partie arbitraire par des ensembles ouverts et fermés.

Définition. *Soit X une partie de E. Son intérieur noté $\overset{\circ}{X}$ est le plus grand ouvert contenu dans X. Son adhérence notée $\overline{X}$ est le plus petit fermé contenant X. Sa frontière notée ∂X est $\overline{X} \setminus \overset{\circ}{X}$.*

Toutes les propriétés naturelles concernant l'intérieur et l'adhérence sont vraies.

Définition. *On dit qu'une partie X de E est dense si $\overline{X} = E$.*

Une fois habitué à raisonner en ces termes, toutes les démonstrations vous sembleront évidentes. Pour vous entraîner, montrer que X est dense si et seulement si chaque ouvert de E rencontre X.

Définition. *Relativement à une partie $X \subset E$, on dit que $x \in E$ est :*
— *un point d'accumulation, lorsque $x \in \overline{X \setminus \{x\}}$.*
— *un point isolé, lorsque $x \notin \overline{X \setminus \{x\}}$.*

Par exemple, dans $\mathbb{R}$, l'ensemble des points d'accumulation de $\mathbb{Q}$ est $\mathbb{R}$ lui-même, alors que chaque point de $\mathbb{Z}$ est isolé.

On peut généraliser aux espaces métriques les notions relatives à la convergence des suites et à la continuité des fonctions.

Définition. *Les valeurs d'adhérences d'une suite (x_k) sont les points d'accumulation de $\{x_k\}$.*
Lorsqu'une suite admet une unique valeur d'adhérence, on dit que c'est sa limite.
On dit qu'une suite (x_k) est de Cauchy si $\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n, m > N, d(x_n, x_m) < \varepsilon$.
Un espace métrique dans lequel toute suite de Cauchy converge est dit complet.

Et inversement on a :

Proposition. *L'adhérence de $X \subset E$ est l'ensemble des limites des suites à valeurs dans X.*

Définition. *Si E et F sont deux espaces métriques, on dit qu'une application $f : E \to F$ est continue en $x \in E$ si*

$$\forall \varepsilon > 0, \exists \eta > 0, \forall y \in E, d(x, y) < \eta \Rightarrow d(f(x), f(y)) < \varepsilon$$

ou, de manière équivalente avec les boules,

$$\forall \varepsilon > 0, \exists \eta > 0, f(\mathcal{B}(x, \eta)) \subset \mathcal{B}(f(x), \varepsilon).$$

Théorème. *Une application $f : E \to F$ est continue si et seulement si l'image réciproque de tout ouvert est un ouvert.*

Évidemment, en passant au complémentaire, la même assertion est vérifiée pour les fermés.

10.2 Compacité, connexité, complétude

La compacité signifie que « il n'y a pas de moyen de s'échapper » :

Définition (compacité). *Un espace X est compact si de toute suite à valeurs dans X on peut extraire une sous-suite convergente.*

Les compacts sont toujours fermés et, réciproquement, on a :

Proposition. *Si X est compact, alors toute intersection de X avec un fermé est compact.*

Évidemment, comme toute suite à valeurs dans $X \cap F$ est à valeurs dans X, elle converge, et la limite est nécessairement dans F puisqu'il est fermé.

Théorème. *L'image d'un compact par une application continue est un compact.*

Dans le cas d'une fonction réelle $f : \mathbb{R} \to \mathbb{R}$ on retrouve que l'image d'un intervalle fermé est un intervalle dont les bornes sont atteintes.

La notion de connexité signifie quant à elle qu'on est « en un seul morceau » :

Définition (connexité). *Un espace X est dit connexe s'il ne peut pas s'écrire comme l'union disjointe de deux ouverts non-vides.*

Par exemple, $\mathbb{R}$ est connexe, mais $\mathrm{GL}_2(\mathbb{R})$ ne l'est pas. Les parties connexes de $\mathbb{R}$ sont exactement les intervalles.

Exercice. *Si deux parties connexes ont un élément en commun, leur union est connexe.*

Théorème (valeurs intermédiaires). *L'image d'un connexe par une application continue est un connexe.*

Définition (connexité par arc). *On dit qu'un espace X est connexe par arc si deux points de X peuvent toujours être reliés par un arc continu, c'est-à-dire,*

$$\forall (x, y) \in X^2, \exists f \in \mathscr{C}^0([0,1], X), f(0) = x \wedge f(1) = y$$

Évidemment, la connexité par arc implique la connexité. Elle lui est même équivalente pour tout ouvert d'un espace vectoriel normé.

Définition (complétude). *On dit qu'un espace X est complet si toute suite de Cauchy à valeurs dans X converge.*

Proposition. *Si X est complet, alors toute intersection de X avec un fermé est complet.*

10.3 Espaces vectoriels normés

Soit $\mathbb{K}$ le corps de base que l'on suppose égal à $\mathbb{R}$ ou $\mathbb{C}$.

Définition. *On appelle espace normé tout espace vectoriel E muni d'une fonction $\|\cdot\| : E \to \mathbb{R}_+$ appelée norme qui vérifie, pour tout $\lambda \in \mathbb{K}$ et tout $(x, y) \in E^2$:*

— $\|\lambda x\| = |\lambda| \cdot \|x\|$
— $\|x\| = 0 \iff x = 0$
— $\|x + y\| \leqslant \|x\| + \|y\|$

Toute norme induit une distance $d(x, y) = \|x - y\|$ et toutes les notions définies ci-dessus s'appliquent, notamment la continuité. Pour les applications linéaires, cette dernière est particulièrement facile à tester.

Théorème. *Soit $f : E \to F$ une application linéaire d'espaces vectoriels normés. On définit sa norme comme la quantité*

$$\|f\| = \sup_{x \neq 0} \frac{\|f(x)\|}{\|x\|}.$$

Alors f est continue si et seulement si $\|f\| < \infty$.

En particulier, les opérations d'espace vectoriel (addition de deux vecteurs et multiplication d'un vecteur par un scalaire) sont continues.

En dimension finie, toutes les applications linéaires sont continues. Cela ne dépend pas de la norme choisie sur $\mathbb{K}^n$, pour laquelle on a notamment les possibilités suivantes :

$$\|x\|_1 = \sum_{k=1}^{n} |x_k|$$

$$\|x\|_2 = \sqrt{\sum_{k=1}^{n} |x_k|^2}$$

$$\|x\|_\alpha = \left(\sum_{k=1}^{n} |x_k|^\alpha \right)^{\frac{1}{\alpha}} \quad \text{pour tout } \alpha \in [1, \infty[$$

$$\|x\|_\infty = \max_{k=1}^{n} |x_k|$$

Définition. *On dit que deux normes $\|\cdot\|_a$ et $\|\cdot\|_b$ d'un même espace E sont équivalentes lorsqu'il existe deux réels positifs non nuls a et b tels que*

$$\forall x \in E, a\|x\|_a \leqslant \|x\|_b \leqslant b\|x\|_a.$$

Deux normes équivalentes induisent des distances équivalentes et donc des topologies équivalentes. C'est-à-dire que les ouverts pour l'une sont exactement les ouverts pour l'autre. Toutes les notions vues ci-dessus, notamment la convergence, compacité, connexité, complétude sont donc parfaitement équivalentes pour ces deux normes.

Théorème. *Toutes les normes de $\mathbb{K}^n$ sont équivalentes.*

On pourra donc omettre de préciser la norme lorsque l'on considère de tels espaces d'un point de vue purement topologique.

Proposition. *Dans $\mathbb{K}^n$, les compacts sont exactement les parties fermées et bornées.*

Encore une fois, il peut être instructif de prouver ce résultat en utilisant les ingrédients de Bolzano-Weierstrass.

Corollaire. *De toute suite bornée à valeurs dans $\mathbb{K}^n$ on peut extraire une sous-suite convergente.*

Corollaire. *L'espace $\mathbb{K}^n$ est complet.*

L'équivalence des normes nous incite aussi à faire des produits plus généraux :

Définition. *Soit (E, d_E) et (F, d_F) deux espaces métriques. Alors l'espace $E \times F$ est métrique pour la distance $d((x_E, x_F), (y_E, y_F)) = d(x_E, y_E) + d(x_F, y_F)$.*

On aurait naturellement pu remplacer la somme par le max, la somme des carrés, etc. En exercice on pourra démontrer que de nombreuses propriétés sont préservées par le produit cartésien : le produit de deux compacts est compact, le produit de deux connexes est connexe, le produit de deux complets est complet, etc.

10.4 Espaces de Banach

Définition. *On appelle espace de Banach tout espace vectoriel normé complet.*

C'est évidemment le cas de tout espace vectoriel normé de dimension fini mais l'objectif de cette section est justement de développer des outils qui s'appliquent aussi en dimension infinie.

Énonçons à nouveau la propriété de Cauchy pour les séries.

Proposition. *Soit (x_k) une suite à valeurs dans un espace de Banach.*
La série $\sum x_k$ converge si et seulement si $\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n, m > N, \| \sum_{k=n}^{m} x_k \| < \varepsilon$.
C'est en particulier le cas lorsque la série $\|x_k\|$ converge.

Définition. *On dit qu'une suite d'applications $f_k : X \to E$ d'un ensemble X dans un espace de Banach E converge vers $f : X \to E$*
— *simplement lorsque $\forall x \in X, \forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall k > N, d(f_k(x), f(x)) < \varepsilon$.*
— *uniformément lorsque $\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall k > N, \forall x \in X, d(f_k(x), f(x)) < \varepsilon$.*

La convergence uniforme peut se réécrire simplement $\|f_k - g\|_\infty \to 0$ en utilisant la norme infinie $\|f\|_\infty = \sup\{\|f(x)\| : x \in X\}$.

Comme dans le cas des fonctions réelles, on a un critère de Cauchy uniforme :

Proposition (critère de Cauchy uniforme)**.** *Si E est complet alors $f_k : X \to E$ converge uniformément si et seulement si*

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall k, \ell > N, \|f_k, f_\ell\|_\infty < \varepsilon.$$

Et comme dans le cas des fonctions réelles, on a les résultats suivants.

Proposition. *Soient E et F deux espaces métriques. Toute suite $f_k : E \to F$ de fonctions continues qui converge uniformément est de limite continue.*

Proposition. *Soit E un espace de Banach E. Toute limite simple de fonctions $\mathscr{C}^1([a,b],E)$ dont les dérivées convergent uniformément est $\mathscr{C}^1$ et vérifie $(\lim f_n)' = \lim f_n'$.*

Le cas des séries est similaire. On se contentera ici de discuter d'un exemple important.

Définition. *Soit ϕ un endomorphisme d'un espace vectoriel normé de dimension finie. La série de terme général $\frac{1}{k!}\phi^{(k)}$ converge absolument vers un endomorphisme noté*

$$\exp(\phi) = \sum_{k=0}^{\infty} \frac{1}{k!}\phi^{(k)}.$$

Cela généralise l'application exponentielle classique que l'on retrouve pour $\phi \in \mathrm{End}(\mathbb{C})$. Les propriétés suivantes sont notamment préservées :

— $\exp(0) = \mathrm{id}$
— $\exp(\psi \circ \phi \circ \psi^{-1}) = \psi \circ \exp(\phi) \circ \psi^{-1}$
— $\exp(\phi + \psi) = \exp(\phi)\exp(\psi)$ lorsque ϕ et ψ commutent

En particulier, on a $\exp(\phi)\exp(-\phi) = \mathrm{id}$.

10.5 Espaces préhilbertiens

Définition. *On appelle espace préhilbertien tout espace vectoriel E muni d'une application appelée produit scalaire $(x,y) \in E^2 \mapsto \langle x,y\rangle \in \mathbb{K}$ qui vérifie, pour tout $\lambda \in \mathbb{K}$ et tout $(x,y,z) \in E^3$:*

— $\langle x,y\rangle = \overline{\langle y,x\rangle}$ (symétrie)
— $\langle \lambda x + y, z\rangle = \lambda\langle x,z\rangle + \langle y,z\rangle$ (linéarité)
— $x \neq 0 \Longrightarrow \langle x,x\rangle > 0$ (définie positivité)

On dit que les vecteurs x et y sont orthogonaux si $\langle x,y\rangle = 0$.

Tout produit scalaire induit une norme $\|x\| = \sqrt{\langle x,x\rangle}$; un espace préhilbertien est donc en particulier un espace vectoriel normé. En dimension finie il est donc complet.

Exemple. *Le produit scalaire usuel sur $\mathbb{K}^n$ est $\langle (x_k),(y_k)\rangle = \sum x_k\overline{y_k}$.*
Il s'étend sur $\mathrm{Mat}_{m\times n}(\mathbb{K})$ en le produit scalaire classique $\langle M,N\rangle = {}^tM\overline{N}$.
Un produit scalaire sur $\mathscr{C}^0([a,b],\mathbb{K})$ est $\langle f,g\rangle = \int_a^b f\overline{g}$; cet espace n'est pas complet.

De nombreux résultats classiques de géométrie s'étendent à ce cadre, notamment :

Remarque (Pythagore). *Si x et y sont orthogonaux alors on a $\|x\|^2 + \|y\|^2 = \|x+y\|^2$.*

Théorème (Cauchy–Schwarz). *Pour tout $(x,y) \in E^2$ on a $|\langle x,y\rangle| \leqslant \|x\| \cdot \|y\|$ avec égalité si et seulement si x et y sont colinéaires.*

Évidemment, toute famille de vecteurs deux-à-deux orthogonaux est libre. Pour utiliser pleinement une base d'un espace préhilberten, mieux vaut qu'elle soit de surcroit orthonormée.

Définition. *On dit qu'une famille (x_k) est orthonormée lorsqu'elle vérifie*

$$\langle x_k, x_\ell\rangle = \begin{cases} 1 & \text{si } k = \ell \\ 0 & \text{si } k \neq \ell \end{cases}.$$

La décomposition de tout vecteur z dans une base orthonormée (x_k) est transparente :

$$z = \sum_k \langle z, x_k\rangle x_k$$

On peut construire de telles familles efficacement :

Algorithme (orthonormalisation de Gram–Schmidt).
Entrée : *Une famille libre (x_k) indicée par $k \in \{1, \dots, n\}$.*
Sortie : *Une base orthonormée de l'espace qu'elle engendre.*

1. *Pour k de 1 à n :*
2. *Poser $y_k \leftarrow x_k$.*
3. *Pour ℓ de 1 à $k-1$:*
4. *Poser $y_k \leftarrow y_k - \langle y_k, x_k \rangle x_k$.*
5. *Poser $y_k \leftarrow \frac{1}{\sqrt{\langle y_k, y_k \rangle}} y_k$.*
6. *Renvoyer (y_k).*

Dans l'espace $\mathbb{C}[x]$ on peut notamment appliquer ce procédé à la base canonique $(x^k) = (1, x, x^2, x^3, \dots)$ pour divers produits scalaires afin d'obtenir les classiques polynômes orthogonaux, notamment :

— pour $\langle f, g \rangle = \int_{-1}^{1} f(x)g(x)dx$, les polynômes de Legendre
— pour $\langle f, g \rangle = \int_{-1}^{1} f(x)g(x)\frac{dx}{\sqrt{1-x^2}}$, les polynômes de Tchebychev
— pour $\langle f, g \rangle = \int_{0}^{\infty} f(x)g(x)e^{-x}dx$, les polynômes de Laguerre
— pour $\langle f, g \rangle = \int_{-\infty}^{\infty} f(x)g(x)e^{-x^2}dx$, les polynômes de Hermite

10.6 Séries et approximation

Soit f une fonction réelle. Pour toute famille $(x_k) \in \mathbb{R}^n$ le polynôme

$$\sum_{k=1}^{n} f(x_k) \prod_{\ell \neq k} \frac{x - x_\ell}{x_k - x_\ell}$$

interpole f en les points x_k. Cette construction ne permet toutefois pas d'approcher de manière satisfaisante la fonction f. On a néanmoins :

Théorème (Weierstrass). *Toute fonction continue sur un segment est limite uniforme de polynômes.*

Démonstration. La fonction $f \in \mathscr{C}^0([0,1], \mathbb{R})$ est limite uniforme des polynômes

$$\mathscr{B}_n(f) = \sum_{k=0}^{n} f\left(\frac{k}{n}\right) B_n^k(x) \qquad \text{avec} \qquad B_n^k(x) = C_n^k x^k (1-x)^{n-k}.$$

En effet, l'identité

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

se montre par calcul direct et implique, pour tout $\eta > 0$, l'inégalité

$$\sum_{\left|\frac{k}{n} - x\right| \geqslant \eta} B_n^k(x) \leqslant \frac{1}{n\eta^2}.$$

Comme f est continue sur un compact, elle est uniformément continue ; il existe donc η tel que

$$\left|\frac{k}{n} - x\right| < \eta \Longrightarrow \left|f\left(\frac{k}{n}\right) - f(x)\right| > \varepsilon$$

et ainsi

$$\|f - \mathscr{B}_n(f)\|_\infty \leqslant \varepsilon + \frac{2+\varepsilon}{n\eta^2} \sup|f|.$$

□

L'espace $\mathscr{C}\mathscr{M}^0_{2\pi}(\mathbb{R},\mathbb{C})$ des fonctions continues par morceaux de période 2π muni du produit scalaire $\langle f, g\rangle = \int_0^{2\pi} f\overline{g}$ admet comme famille orthonormale celle des fonctions $x \mapsto e^{inx}$ pour $n \in \mathbb{Z}$. Le sous espace vectoriel qu'elles engendrent est celui des polynômes trigonométriques, c'est-à-dire des fonctions de la forme $x \mapsto \sum_{n=-N}^{N} c_n e^{inx}$. Cet espace étant dense dans $\mathscr{C}\mathscr{M}^0_{2\pi}(\mathbb{R},\mathbb{C})$, on peut l'exploiter afin d'approcher des fonctions arbitraires.

Définition. *Soit $f \in \mathscr{C}\mathscr{M}^0_{2\pi}(\mathbb{R},\mathbb{C})$ une fonction continue par morceaux de période 2π. Pour tout entier relatif n on pose*

$$c_n = \frac{1}{2\pi}\int_0^{2\pi} f(x)e^{-inx}\,dx$$
$$s_N = x \mapsto \sum_{n=-N}^{N} c_n e^{inx}$$

On appelle c_n la suite des coefficients de Fourier et s_N la série de Fourier de f.

Proposition (égalité de Parseval)**.** *Le polynôme trigonométrique s_N est celui de degré N le plus proche de f en moyenne quadratique :*

$$\inf_{p\in P_N} \|p - f\|_2 = \|s_N - f\|_2 = \sqrt{\frac{1}{2\pi}\int_0^{2\pi} |f|^2 - \sum_{n=-N}^{N} |c_n|^2}$$

Cette quantité tend vers zéro lorsque N tend vers l'infini.

On peut parler de convergence si tant est que les points de discontinuité vérifient l'égalité $f(x) = \frac{f(x^+)+f(x^-)}{2}$.

Théorème (Dirichlet)**.** *Si f est $\mathscr{C}^1$ par morceaux alors sa série de Fourier converge simplement vers f.*

Théorème (Fejér)**.** *Si f est continue et $\mathscr{C}^1$ par morceaux alors sa série de Fourier converge normalement vers f.*

Tout ce qui précède s'appliquer à l'espace $\mathscr{C}^0_{2\pi}(\mathbb{R},\mathbb{R})$ en prenant les parties réelles de chaque quantité donnée.

Chapitre 12

Calcul différentiel

Chapitre 2

Algorithmique et informatique

Bibliographie

[1] Vladimir Arnold. *Équations Différentielles Ordinaires*.
Traduit du russe par Djilali Embarek. Collection MIR. Ellipses, 2012.
isbn : 2729873600.

[2] Xavier Gourdon. *Les maths en tête. Analyse*. Ellipses, 2008. isbn : 2729837590.

[3] Xavier Gourdon. *Les maths en tête. Algèbre*. Ellipses, 2009. isbn : 2729850147.

[4] Daniel Perrin. *Cours d'algèbre*. Ellipses, 1998. isbn : 2729855521.

[5] Walter Rudin. *Analyse réelle et complexe*.
Traduit de l'anglais par Nicole Dhombres et François Hoffman. Masson, 1975.
isbn : 2225484007.