

Résumés de cours 2019–2020

D'après Monsieur MERLE, compilé par Quentin DE MUYNCK



Table des matières

Semaine 1 – Fonctions de \mathbb{R} dans \mathbb{R} , trigonométrie	1
Semaine 2 – Dérivation et intégration	7
Semaine 3 – Transformations du graphe, trigonométrie hyperboliques et réciproques, intégration par parties et changement de variables	12
Semaine 4 – Ensembles, quantificateurs, opérations ensemblistes, logique.	15
Semaine 5 – Relations binaires, d'ordre, ordre naturel, minimum et max dans \mathbb{N} , relations d'équivalence	20
Semaine 6 – Axiome du choix, construction de \mathbb{Z} , ordre, anneau et sous-groupes de \mathbb{Z} , arithmétique	23
Semaine 7 – Les rationnels \mathbb{Q} , les réels \mathbb{R} , intervalles, bornes supérieurs, $\overline{\mathbb{R}}$, valeur absolue et développement décimal	31
Semaine 8 – Développement d'un réel en base quelconque, applications, images directes et réciproques, injectivité et surjectivité, lois internes, cardinaux	36
Semaine 9 – Cardinaux, sommes et produits finis, listes, arrangements et combinaisons	42
Semaine 10 – Sommes finies (téléscopage, fonctions génératrices), intégration par parties itérée, début des complexes	46
Semaine 11 – Module, fonctions à valeurs dans \mathbb{C} , exponentielle complexe, argument, linéarisation et antilinéarisation	50
Semaine 12 – Équations polynomiales, géométrie dans le plan complexe, similitudes directes et indirectes	56
Semaine 13 – Groupes, sous-groupes, monogènes, cycliques, morphismes, groupe symétrique, anneaux	60
Semaine 14 – Idéaux, groupes et anneaux quotients	68
Semaine 15 – $\mathbb{Z}/n\mathbb{Z}$, théorème chinois, indicatrice d'EULER, complément HP, caractéristique d'un anneau, équations différentielles d'ordre 1	70
Semaine 16 – Équations différentielles linéaires d'ordre 2, équations à variable sépara- rables, espaces vectoriels	73
Semaine 17 – Applications linéaires, espaces affines, structure d'algèbre, espaces vec- toriels normés, distance et espaces métriques	78
Semaine 18 – Applications lipschitziennes, normes équivalentes, limite dans un espace métrique, sommes et produits de limites, suites de complexes et de réels	84

Semaine 19 – Suites de vecteurs, adjacentes, extraites, suites de CAUCHY, séries de vecteurs, séries de réels positifs	89
Semaine 20 – Croissances comparées, séries de RIEMANN, TCSI, critère de D’ALEMBERT, séries alternées, non-commutativité des séries semi-convergentes, transformation d’ABEL	95
Semaine 21 – Topologie dans un espace métrique, ouverts, fermés, adhérence, intérieur, compacts, continuité ponctuelle	98
Semaine 22 – Théorèmes de composition, opérations algébriques sur les limites, continuité globale, TVI, continuité des applications linéaires et continuité uniforme	104
Semaine 23 – Comparaison au voisinage d’un point, domination, prépondérance, relation d’équivalence, développements limités, applications aux séries	109
Semaine 24 – Dérivabilité, opérations, dérivées d’ordre supérieurs, égalité des accroissements finis, formules de TAYLOR, monotonie et dérivabilité, suites récurrentes d’ordre 1, fonctions convexes	114
Semaine 25 – Polynômes, arithmétique sur un anneau principal	123
Semaine 26 – Arithmétique, PGCD, PPCM, racines d’un polynôme	127
Semaine 27 – Racines d’un polynôme, fractions rationnelles	131
Semaine 28 – DES, calculs d’intégrales, matrices	136
Semaine 29 – Matrices, blocs, familles de vecteurs, dimension d’un espace vectoriel, rang d’une famille, matrice d’une application linéaire, systèmes linéaires et pivot de GAUSS	142
Semaine 30 – Somme de sous-espaces vectoriels, supplémentaires, sommes directes, projecteurs et symétries, sous-espaces propres, changement de bases	153
Semaine 31 – Diagonalisation et trigonalisation, trace d’un endomorphisme, matrices équivalentes et semblables, hyperplans, déterminants (formes multilinéaires)	158
Semaine 32 – Déterminants (calculs), produits scalaires, espaces préhilbertiens, espaces vectoriels normés de dimensions finies, orthogonalité	165
Semaine 33 – Orthogonalité en dimension finie, distance à un espace vectoriel, GRAM-SCHMIDT, endomorphismes (symétriques, orthogonaux) d’un espace euclidien, groupe orthogonal, rotations, orientation d’un espace vectoriel réel, géométrie plane, isométries vectorielles	170
Semaine 34 – Angles, droites affines, géométrie dans l’espace, produit vectoriel, ensembles dénombrables et familles sommables, théorèmes de FUBINI	177
Semaine 35 – Probabilités, conditionnelles et indépendance, variables aléatoires discrètes	185
Semaine 36 – Convergence en loi, variables aléatoires indépendantes, espérance et variance, propriétés de convergence, théorie de l’intégration, sommes de RIEMANN, applications réglées	189

Semaine 1 : Résumé de cours

1 Fonctions de \mathbb{R} dans \mathbb{R} .

Notations : Nous emploierons dans les énoncés ci-dessous l'une des deux notations suivantes :

Notation a) : Soit D et E deux parties de \mathbb{R} . On considère une application f , de D dans E , ce qui signifie que, pour tout $x \in D$, on se donne un unique $f(x) \in E$.

Notation b) : On considère une fonction f de \mathbb{R} dans \mathbb{R} , ce qui signifie que, pour tout $x \in \mathbb{R}$, on associe ou bien aucun réel, ou bien un unique réel qui est alors noté $f(x)$.

Remarque. En pratique, les deux mots *application* et *fonction* sont souvent considérés comme synonymes et c'est le contexte qui permet de savoir laquelle des notations précédentes est employée.

1.1 Graphe d'une fonction

Définition. (Notation b)) Le domaine de définition de f , noté \mathcal{D}_f est l'ensemble des réels $x \in \mathbb{R}$ pour lesquels la quantité $f(x)$ est calculable.

Remarque. On peut ainsi passer d'une notation à l'autre :

Si f est une application de D dans E (notation a)), alors on peut voir f comme une fonction de \mathbb{R} dans \mathbb{R} (notation b)) telle que $D \subset \mathcal{D}_f$.

Réciproquement, si f est une fonction de \mathbb{R} dans \mathbb{R} (notation b)), on peut voir f comme une application de D dans E , pour toute partie D incluse dans \mathcal{D}_f et pour toute partie E contenant

$$f(D) \triangleq \{f(x) / x \in D\}.$$

Notation. Soit f une application de D dans E (notation a)).

Soit D' une partie de D et E' une partie de E .

- On note $f|_{D'}$ l'application de D' dans E qui à x associe $f(x)$. On dit que $f|_{D'}$ est la restriction de f à D' .
- Lorsque, pour tout $x \in D$, $f(x) \in E'$, on note $f|^{E'}$ l'application de D dans E' qui à x associe $f(x)$. On dit que $f|^{E'}$ est la corestriction de f à E' .
- Lorsque, pour tout $x \in D'$, $f(x) \in E'$, on note $f|_{D'}^{E'}$ l'application de D' dans E' qui à x associe $f(x)$.

Définition.

On se place dans le plan usuel, muni d'un repère orthonormé direct (O, \vec{i}, \vec{j}) .

La représentation graphique de f , aussi appelée le graphe de f , est l'ensemble des points du plan de coordonnées $(x, f(x))$, lorsque x décrit \mathcal{D}_f (notation b)), ou bien lorsque x décrit D (notation a)).

Définition. Lorsque $y = f(x)$, où $x \in \mathcal{D}_f$ et $y \in \mathbb{R}$,

- on dit que y est **l'image** de x par f et
- que x est **un antécédent** de y par f .

Tout élément x de \mathcal{D}_f possède une unique image $f(x)$ par f ,

mais si $y \in \mathbb{R}$, y peut ne posséder aucun antécédent par f , il peut aussi en posséder plusieurs.

Les définitions et propriétés qui terminent ce paragraphe sont à connaître même si on ne les démontrera effectivement que plus tard.

Définition : Soit f une application d'un ensemble quelconque E dans un ensemble quelconque F (ainsi E et F ne sont pas forcément des parties de \mathbb{R}).

- On dit que f est surjective si et seulement si $\forall y \in F, \exists x \in E, y = f(x)$. Ainsi, f est surjective si et seulement si tout élément de F possède au moins un antécédent.
- On dit que f est injective si et seulement si $\forall x, y \in E, [f(x) = f(y) \implies x = y]$. Ainsi, f est injective si et seulement si, pour tout couple d'éléments distincts de E , leurs images sont différentes. f est injective si et seulement si tout élément de F possède au plus un antécédent.

Définition. Un polynôme P (à coefficients réels) est une application de \mathbb{R} dans \mathbb{R} (notation a)) de la forme $x \mapsto a_0 + a_1x + \dots + a_nx^n$, où $n \in \mathbb{N}$ et $a_0, \dots, a_n \in \mathbb{R}$.

Si $a_n \neq 0$, on dit que n est le degré de ce polynôme. On note $n = \deg(P)$.

Par convention, l'application identiquement nulle est un polynôme de degré égal à $-\infty$.

Définition. Soit P un polynôme et $\alpha \in \mathbb{R}$.

On dit que α est une racine de P si et seulement si $P(\alpha) = 0$.

Propriété. Soit P un polynôme et $\alpha \in \mathbb{R}$. Alors α est une racine de P si et seulement si il existe un polynôme Q tel que, pour tout $x \in \mathbb{R}$, $P(x) = (x - \alpha)Q(x)$.

Propriété. Soit P un polynôme et $\alpha_1, \dots, \alpha_k$ k réels deux à deux distincts. Alors $\alpha_1, \dots, \alpha_k$ sont des racines de P si et seulement si il existe un polynôme Q tel que, pour tout $x \in \mathbb{R}$, $P(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_k)Q(x)$.

Propriété. Soit P et Q deux polynômes. Alors l'application $x \mapsto P(x)Q(x)$ de \mathbb{R} dans \mathbb{R} est aussi un polynôme, que l'on note PQ . De plus, $\deg(PQ) = \deg(P) + \deg(Q)$.

Théorème. Soit P un polynôme non nul à coefficients réels de degré $n \in \mathbb{N}$. Alors le nombre de racines de P est inférieur ou égal à n .

1.2 Premières caractéristiques d'une fonction

Définition. (Notation b))

- f est paire si et seulement si : $\forall x \in \mathcal{D}_f, [-x \in \mathcal{D}_f] \wedge [f(x) = f(-x)]$.
- f est impaire si et seulement si : $\forall x \in \mathcal{D}_f, [-x \in \mathcal{D}_f] \wedge [f(-x) = -f(x)]$.
- Soit $T > 0$. f est T -périodique si et seulement si $\forall x \in \mathcal{D}_f, [x + T \in \mathcal{D}_f] \wedge f(x + T) = f(x)$.

Propriété.

- Le graphe d'une fonction paire est symétrique par rapport à l'axe des ordonnées.
- Le graphe d'une fonction impaire est symétrique par rapport à l'origine des axes.
- Le graphe d'une fonction T -périodique est invariant par la translation de vecteur $T\vec{i}$.

Définition. (notation a))

- f est croissante si et seulement si $\forall x, y \in D, [x \leq y \implies f(x) \leq f(y)]$.
- f est strictement croissante si et seulement si $\forall x, y \in D, [x < y \implies f(x) < f(y)]$.
- f est décroissante si et seulement si $\forall x, y \in D, [x \leq y \implies f(x) \geq f(y)]$.
- f est strictement décroissante si et seulement si $\forall x, y \in D, [x < y \implies f(x) > f(y)]$.
- f est monotone si et seulement si f est croissante ou décroissante.
- f est strictement monotone si et seulement si f est strictement croissante ou strictement décroissante.

Propriété. Graphiquement, les antécédents de λ par f sont les abscisses des points d'intersection du graphe de f avec la droite horizontale d'équation $y = \lambda$.

Propriété. Graphiquement, les solutions de l'inéquation $f(x) \geq \lambda$, en l'inconnue x , sont les abscisses des points du graphe de f situés au-dessus de la droite horizontale d'équation $y = \lambda$.

Définition. Une application $f : D \rightarrow E$ est majorée si et seulement si il existe $M \in \mathbb{R}$ tel que, pour tout $x \in D$, $f(x) \leq M$, c'est-à-dire si et seulement si le graphe de f est situé sous la droite horizontale d'équation $y = M$.

1.3 Opérations sur les fonctions

Définition. (notation b)) Soit f et g deux fonctions de \mathbb{R} dans \mathbb{R} . Soit $\lambda \in \mathbb{R}$.

- $f + g$ est la fonction de \mathbb{R} dans \mathbb{R} définie par $(f + g)(x) = f(x) + g(x)$.
On a $\mathcal{D}_{f+g} = \mathcal{D}_f \cap \mathcal{D}_g$.
- λf est la fonction de \mathbb{R} dans \mathbb{R} définie par $(\lambda f)(x) = \lambda f(x)$.
On a $\mathcal{D}_{\lambda f} = \mathcal{D}_f$.
- fg est la fonction de \mathbb{R} dans \mathbb{R} définie par $(fg)(x) = f(x) \times g(x)$.
On a $\mathcal{D}_{fg} = \mathcal{D}_f \cap \mathcal{D}_g$.
- $|f|$ est la fonction de \mathbb{R} dans \mathbb{R} définie par $|f|(x) = |f(x)|$. On a $\mathcal{D}_{|f|} = \mathcal{D}_f$.
- On définit de même $f - g$, $\frac{1}{f}$, $\frac{f}{g}$.

Définition. f est bornée si et seulement si $|f|$ est majorée.

Définition de la composition : (Notation b)) Soit f et g deux fonctions. On note $f(g(x)) = (f \circ g)(x)$: on définit ainsi une nouvelle fonction, $f \circ g$. C'est la composée de f et g .

Application réciproque :

Soit f une application de D dans E (notation a)). On dit que f est bijective si et seulement si f est injective et surjective. Dans ce cas, pour tout $y \in E$, il existe un unique $x_y \in D$ tel que $y = f(x_y)$. En notant $x_y = f^{-1}(y)$, on définit une application f^{-1} de E dans D , qui est également bijective. C'est la bijection réciproque de la bijection f . On a $(f^{-1})^{-1} = f$, $f \circ f^{-1} = Id_E$ et $f^{-1} \circ f = Id_D$, où Id_E est l'application de E dans E qui à x associe x .

Propriété. Si f est une bijection d'une partie E de \mathbb{R} vers une partie F de \mathbb{R} , alors le graphe de f^{-1} est le symétrique du graphe de f pour la symétrie orthogonale selon la première diagonale, c'est-à-dire la droite d'équation $y = x$.

Il faut savoir le démontrer.

Définition. Soit f et g deux applications définies sur D à valeurs dans \mathbb{R} .

On dit que f est inférieure à g sur D , et on note $f \leq g$, lorsque : $\forall x \in D, f(x) \leq g(x)$.

Remarque. La notation " $f < g$ " désignera parfois la condition $[\forall x \in D, f(x) < g(x)]$, et d'autres fois la condition $[(f \leq g) \text{ et } (f \neq g)]$, c'est-à-dire $[\forall x \in D, f(x) \leq g(x)]$ et $[\exists x \in D, f(x) < g(x)]$.

2 Trigonométrie

2.1 Les fonctions circulaires

Définition. Soit $\theta \in \mathbb{R}$. On admet que le complexe $e^{i\theta}$ est sur le cercle unité et que θ est l'angle $\widehat{M_1 M_0 M_{e^{i\theta}}}$ (en notant M_z le point d'affixe z).

On pose $\cos(\theta) = \operatorname{Re}(e^{i\theta})$ et $\sin(\theta) = \operatorname{Im}(e^{i\theta})$.

Ainsi $\cos(\theta)$ est l'abscisse du point $M_{e^{i\theta}}$ et $\sin(\theta)$ est son ordonnée.

Formules d'Euler : $\cos \theta = \frac{e^{i\theta} + e^{-i\theta}}{2}$ et $\sin \theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}$.

Propriété. Les fonctions \cos et \sin sont 2π -périodiques. \cos est paire. \sin est impaire.

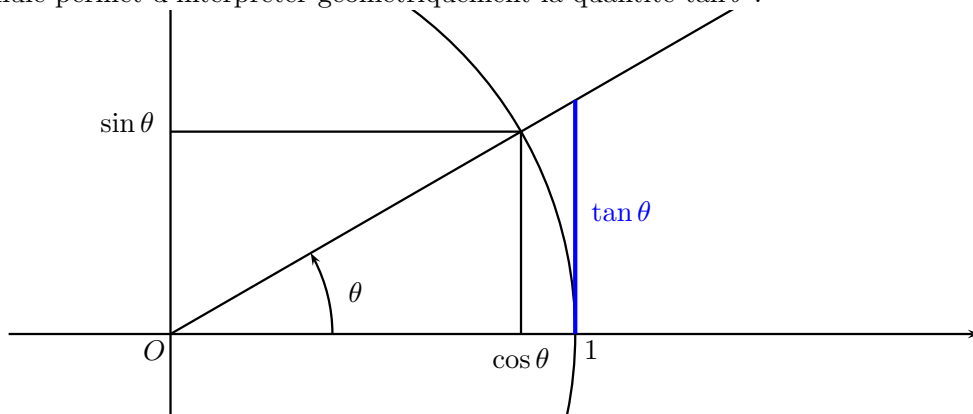
Définition des fonctions tangente et cotangente : $\tan \theta = \frac{\sin \theta}{\cos \theta}$ et $\cotan \theta = \frac{\cos \theta}{\sin \theta}$.

La fonction tangente est définie sur $\mathbb{R} \setminus (\frac{\pi}{2} + \pi\mathbb{Z})$.

Formules : Soit OAB un triangle rectangle en A . Par définition, l'hypoténuse est le côté opposé à l'angle droit. Notons $\theta = \widehat{AOB}$ l'angle au sommet O .

Alors $\cos \theta = \frac{OA}{OB} = \frac{\text{longueur du côté adjacent}}{\text{longueur de l'hypoténuse}}$, $\sin \theta = \frac{AB}{OB} = \frac{\text{longueur du côté opposé}}{\text{longueur de l'hypoténuse}}$
et $\tan \theta = \frac{AB}{OA} = \frac{\text{longueur du côté opposé}}{\text{longueur du côté adjacent}}$.

Cette dernière formule permet d'interpréter géométriquement la quantité $\tan \theta$:



2.2 Graphes des fonctions circulaires

Il faut savoir tracer les graphes des fonctions \cos , \sin et \tan .

2.3 Formulaire de trigonométrie

Il faut savoir établir chacune de ces formules.

Formule circulaire : Pour tout $\theta \in \mathbb{R}$, $\cos^2 \theta + \sin^2 \theta = 1$.

Formules de symétries : Lorsque les quantités qui interviennent sont définies,

$$\begin{array}{lll} \cos(-\theta) = \cos(\theta) & \sin(-\theta) = -\sin(\theta) & \tan(-\theta) = -\tan(\theta) \\ \cos(\pi - \theta) = -\cos(\theta) & \sin(\pi - \theta) = \sin(\theta) & \tan(\pi - \theta) = -\tan(\theta) \\ \cos(\pi + \theta) = -\cos(\theta) & \sin(\pi + \theta) = -\sin(\theta) & \tan(\pi + \theta) = \tan(\theta) \\ \cos(\frac{\pi}{2} - \theta) = \sin(\theta) & \sin(\frac{\pi}{2} - \theta) = \cos(\theta) & \tan(\frac{\pi}{2} - \theta) = \cotan(\theta) \\ \cos(\frac{\pi}{2} + \theta) = -\sin(\theta) & \sin(\frac{\pi}{2} + \theta) = \cos(\theta) & \tan(\frac{\pi}{2} + \theta) = -\cotan(\theta) \end{array}$$

Il faut être capable de visualiser toutes ces formules sur le cercle trigonométrique.

Formule d'addition :

$$\cos(a + b) = \cos a \cos b - \sin a \sin b \text{ et } \sin(a + b) = \sin a \cos b + \cos a \sin b.$$

$$\cos(a - b) = \cos a \cos b + \sin a \sin b \text{ et } \sin(a - b) = \sin a \cos b - \cos a \sin b,$$

$$\tan(a + b) = \frac{\tan a + \tan b}{1 - \tan a \tan b} \text{ et } \tan(a - b) = \frac{\tan a - \tan b}{1 + \tan a \tan b}.$$

Formules de duplication : $\cos(2a) = \cos^2 a - \sin^2 a = 2\cos^2 a - 1 = 1 - 2\sin^2 a$,

$$\sin(2a) = 2\sin a \cos a \text{ et } \tan(2a) = \frac{2\tan a}{1 - \tan^2 a}.$$

Premières formules de linéarisation :

$$\cos^2 a = \frac{\cos(2a) + 1}{2} \text{ et } \sin^2 a = \frac{1 - \cos(2a)}{2} \geq 0.$$

$$2 \cos a \cdot \cos b = \cos(a + b) + \cos(a - b),$$

$$2 \sin a \cdot \sin b = \cos(a - b) - \cos(a + b),$$

$$2 \sin a \cdot \cos b = \sin(a + b) + \sin(a - b).$$

Formules de factorisation :

$$\cos p + \cos q = 2 \cos \frac{p+q}{2} \cos \frac{p-q}{2},$$

$$\cos p - \cos q = -2 \sin \frac{p+q}{2} \sin \frac{p-q}{2},$$

$$\sin p + \sin q = 2 \sin \frac{p+q}{2} \cos \frac{p-q}{2},$$

$$\sin p - \sin q = 2 \sin \frac{p-q}{2} \cos \frac{p+q}{2}.$$

Il faut savoir les retrouver en utilisant les complexes.

Formules (hors programme) : en posant $u = \tan\left(\frac{\theta}{2}\right)$, on a

$$\cos \theta = \frac{1 - u^2}{1 + u^2}, \quad \sin \theta = \frac{2u}{1 + u^2}, \quad \tan \theta = \frac{2u}{1 - u^2}.$$

Propriété. Lignes trigonométriques à connaître :

θ	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$
$\cos \theta$	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0
$\sin \theta$	0	$\frac{1}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1
$\tan \theta$	0	$\frac{\sqrt{3}}{3}$	1	$\sqrt{3}$	non défini

La croissance de la fonction tangente sur $[0, \frac{\pi}{2}[$ aide à retenir la dernière ligne.

2.4 Equations trigonométriques

2.4.1 Résolution du système (S) : $(\cos x = c) \wedge (\sin x = s)$

2.4.2 Résolution de l'équation $\cos x = c$

Définition. L'application \cos réalise une bijection (décroissante) de $[0, \pi]$ dans $[-1, 1]$. On note \arccos l'application réciproque.

Propriété. Pour tout $u, v \in \mathbb{R}$, $\cos u = \cos v \iff u \equiv \pm v [2\pi]$.

Il faut savoir résoudre les équations suivantes : $\cos x = \frac{\sqrt{3}}{2}$ et $\cos x = \cos\left(\frac{\pi}{3} - 2x\right)$.

2.4.3 Résolution de l'équation $\sin x = s$

Définition. L'application \sin réalise une bijection (croissante) de $[-\frac{\pi}{2}, \frac{\pi}{2}]$ dans $[-1, 1]$. On note \arcsin l'application réciproque. **Il faut savoir tracer son graphe.**

Propriété. Pour tout $u, v \in \mathbb{R}$, $\sin u = \sin v \iff (u \equiv v [2\pi]) \vee (u \equiv \pi - v [2\pi])$.

2.4.4 Résolution de l'équation $\tan x = t$

Définition. \tan est une bijection (croissante) de $] -\frac{\pi}{2}, \frac{\pi}{2}[$ dans \mathbb{R} . On note \arctan l'application réciproque. **Il faut savoir tracer son graphe.**

Corollaire. Pour tout $u, v \in \mathbb{R}$, $\tan u = \tan v \iff u \equiv v [\pi]$.

2.4.5 Expressions de la forme $A \cos x + B \sin x$.

Technique à connaître : transformation de $A \cos x + B \sin x$ en $r \cos(x - \varphi)$.

Première méthode :

Soit $(A, B) \in \mathbb{R} \setminus \{(0, 0)\}$.

$$A \cos x + B \sin x = \sqrt{A^2 + B^2} \left(\frac{A}{\sqrt{A^2 + B^2}} \cos x + \frac{B}{\sqrt{A^2 + B^2}} \sin x \right).$$

Posons $c = \frac{A}{\sqrt{A^2 + B^2}}$ et $s = \frac{B}{\sqrt{A^2 + B^2}}$. On a $c^2 + s^2 = 1$, donc on sait qu'il existe $\varphi \in \mathbb{R}$ tel que

$c = \cos \varphi$ et $s = \sin \varphi$. Ainsi, en posant $r = \sqrt{A^2 + B^2}$,

$$A \cos x + B \sin x = r(\cos \varphi \cos x + \sin \varphi \sin x) = r \cos(x - \varphi).$$

r est appelé l'amplitude et φ la phase.

On remarquera que, par construction, $c + is = e^{i\varphi}$, donc $A + iB = re^{i\varphi}$.

Seconde méthode : lorsque $A \neq 0$. Il existe φ tel que $\tan \varphi = \frac{B}{A}$.

$$\text{Alors } A \cos x + B \sin x = A \left(\cos x + \frac{\sin \varphi}{\cos \varphi} \sin x \right) = \frac{A}{\cos \varphi} \cos(x - \varphi).$$

Sachez résoudre les équations suivantes :

$$-3 \cos x + 4 \sin x = 10 \text{ et } \sqrt{3} \cos x - \sin x = 2.$$

Semaine 2 : Résumé de cours

1 Dérivation et intégration

1.1 Pente de la tangente

Propriété. Pour une droite d'équation $y = px + y_0$, on dit que p est sa pente et que y_0 est l'ordonnée à l'origine.

On dispose également des droites “verticales”, d'équation $x = x_0$, où $x_0 \in \mathbb{R}$, qui sont de pente infinie. Deux droites affines du plan sont parallèles si et seulement si elles ont la même pente.

Propriété. Soit $f : \mathbb{R} \rightarrow \mathbb{R}$ une fonction. Pour tout $x_0, x_1 \in \mathcal{D}_f$, avec $x_0 \neq x_1$, la corde du graphe de f entre les abscisses x_0 et x_1 est par définition l'unique droite du plan passant par les points du graphe de f d'abscisses x_0 et x_1 .

Elle a pour équation : $y - f(x_0) = \frac{f(x_1) - f(x_0)}{x_1 - x_0} \times (x - x_0)$.

En particulier, la pente de cette droite est égale à $\frac{f(x_1) - f(x_0)}{x_1 - x_0}$.

Définition. Soit $f : \mathbb{R} \rightarrow \mathbb{R}$ une fonction définie sur un intervalle I et soit $x_0 \in I$.

On dit que f est dérivable en x_0 si et seulement si la quantité $\frac{f(x_1) - f(x_0)}{x_1 - x_0}$ possède une limite lorsque x_1 tend vers x_0 . Dans ce cas, cette limite est notée $f'(x_0)$ et est appelée la dérivée de f en x_0 .

Informellement, lorsque f est dérivable en x_0 , la corde du graphe de f entre les abscisses x_0 et x_1 tend vers la tangente en x_0 , d'équation : $y - f(x_0) = f'(x_0) \cdot (x - x_0)$.

Cela dit que la meilleure approximation de f , au voisinage de x_0 , parmi l'ensemble des applications affines, est $x \mapsto f(x_0) + f'(x_0) \cdot (x - x_0)$.

Il faut retenir que $f'(x_0)$, lorsqu'elle est définie, est la pente de la tangente au graphe de f en le point d'abscisse x_0 .

Définition. On dit que f est dérivable sur l'intervalle I si et seulement si elle est dérivable en chacun des réels de I . On dispose alors de l'application f' , définie au moins sur I .

On dit alors que f est de classe D^1 .

Lorsque f' est continue sur I , on dit que f est de classe C^1 sur I .

Définition. Si f' est définie sur un intervalle I , on dit que f est deux fois dérivable sur I lorsque f' est dérivable en tout point de I . La dérivée de la dérivée de f est notée f'' . On l'appelle la dérivée seconde de f .

Soit $n \in \mathbb{N}$. Par récurrence, la dérivée n -ième de f lorsqu'elle est définie est la dérivée de la dérivée $(n-1)$ -ième. On la note $f^{(n)}$. On dit alors que f est de classe D^n sur I .

On dit que f est de classe C^n sur I lorsque f est n fois dérivable sur I et que $f^{(n)}$ est continue.

On dit que f est de classe C^∞ sur I lorsque, pour tout $n \in \mathbb{N}$, f est C^n sur I .

Remarque. On convient que $f^{(0)} = f$, pour toute application f de \mathbb{R} dans \mathbb{R} .

1.2 Règles de dérivation

Règles générales **A savoir utiliser dans des calculs sans hésiter**

- Pour tout $\alpha, \beta \in \mathbb{R}$, $(\alpha f + \beta g)' = \alpha f' + \beta g'$.
- $(fg)' = f'g + fg'$.
- $\left(\frac{1}{f}\right)' = -\frac{f'}{f^2}$.
- $\left(\frac{f}{g}\right)' = \frac{f'g - g'f}{g^2}$.
- $(f \circ g)' = g' \times (f' \circ g)$.
- Pour tout $\alpha \in \mathbb{R}^*$, $(f^\alpha)' = \alpha f' \times f^{\alpha-1}$.
- Lorsque f est bijective, $(f^{-1})' = \frac{1}{f' \circ f^{-1}}$.

Les fonctions qui interviennent dans ces formules sont toutes supposées dérivables sur un intervalle. On se limite éventuellement à un sous-intervalle pour s'assurer que les quantités qui interviennent dans les formules sont bien définies.

Dérivées des fonctions usuelles **A connaître par coeur**

- $\forall \alpha \in \mathbb{R}^*$, $\frac{d}{dx}(x^\alpha) = \alpha x^{\alpha-1}$, $\frac{d}{dx}\left(\frac{1}{x}\right) = -\frac{1}{x^2}$, $\frac{d}{dx}(\sqrt{x}) = \frac{1}{2\sqrt{x}}$.
- $\cos' = -\sin$, $\sin' = \cos$.
- $\frac{d}{dx}(\tan x) = \frac{1}{\cos^2 x} = 1 + \tan^2 x$.
- $\arcsin' x = \frac{1}{\sqrt{1-x^2}}$, $\arccos' x = \frac{-1}{\sqrt{1-x^2}}$, $\arctan' x = \frac{1}{1+x^2}$.
- $\frac{d}{dx}(e^x) = e^x$, $\frac{d}{dx}(a^x) = (\ln a)a^x$ (où $a > 0$), $\ln'(x) = \frac{1}{x}$.

Dérivées d'ordre supérieur

- Si f est n fois dérivable, $\frac{d^n}{dx^n}(f(ax+b)) = a^n f^{(n)}(ax+b)$.
- $\cos^{(n)}(x) = \cos(x + n\frac{\pi}{2})$ et $\sin^{(n)}(x) = \sin(x + n\frac{\pi}{2})$.
- $\frac{d^n}{dx^n}\left(\frac{1}{1+x}\right) = \frac{(-1)^n n!}{(1+x)^{n+1}}$.

1.3 Dérivation et monotonie

Théorème. Soit f une fonction de I dans \mathbb{R} , où I est un **intervalle** de \mathbb{R} . On suppose que f est dérivable sur I .

- f est constante sur I si et seulement si f' est identiquement nulle sur I .
- f est croissante sur I si et seulement si $\forall x \in I$, $f'(x) \geq 0$.
- f est décroissante sur I si et seulement si $\forall x \in I$, $f'(x) \leq 0$.
- Si $f'(x)$ est de signe constant sur I et si $\{x \in I / f'(x) = 0\}$ est fini, alors f est strictement monotone.

Il faut savoir redémontrer les propriétés suivantes. Il faut aussi les connaître pour les utiliser éventuellement sans démonstration.

- pour tout $x > 0$, $\sin x < x$.
- Pour tout $x \in [-1, 1]$, $\arccos x + \arcsin x = \frac{\pi}{2}$.
- Pour tout $t \in \mathbb{R}^*$, $\arctan t + \arctan \frac{1}{t} = \operatorname{sgn}(t) \times \frac{\pi}{2}$.

1.4 Intégration

Définition. Soit $a, b \in \mathbb{R}$ avec $a < b$. Soit $f : [a, b] \rightarrow \mathbb{R}$ une application continue. On note $\int_a^b f(t)dt$ (prononcer “intégrale de a à b de $f(t) dt$ ”) l’aire comprise entre l’axe des abscisses (noté Ox) et le graphe de f , en comptant positivement les aires au dessus de l’axe Ox (donc lorsque $f(x) \geq 0$) et négativement les aires situées au dessous de l’axe Ox (lorsque $f(x) \leq 0$).

Convention : Avec les notations et hypothèses précédentes, on convient que

$$\int_b^a f(t)dt = - \int_a^b f(t)dt \text{ et que } \int_a^a f(t)dt = 0.$$

Propriété. Soit I un intervalle inclus dans \mathbb{R} .

Soit f et g deux applications continues de I dans \mathbb{R} .

Soit $a, b \in I$ (on peut avoir $a < b$, $b < a$ ou bien $a = b$).

- Linéarité : Pour tout $\alpha, \beta \in \mathbb{R}$, $\int_a^b (\alpha f + \beta g) = \alpha \int_a^b f + \beta \int_a^b g$.
- Relation de Chasles : Pour tout $c \in I$, $\int_a^b f(t)dt = \int_a^c f + \int_c^b f$.

Soit $a, b \in I$: **on suppose maintenant que** $a \leq b$.

- Positivité : si $f \geq 0$, alors $\int_a^b f(t)dt \geq 0$.
- Croissance de l’intégrale : si $f \leq g$, alors $\int_a^b f(t)dt \leq \int_a^b g(t)dt$.
- Inégalité triangulaire : $\left| \int_a^b f(t)dt \right| \leq \int_a^b |f(t)|dt$.

Propriété. Soit $a, b \in \mathbb{R}$ avec $a < b$ et soit $f : [a, b] \rightarrow \mathbb{R}$ une application **continue et positive**, telle que $\int_a^b f(t)dt = 0$. Alors f est identiquement nulle sur $[a, b]$.

1.5 Primitivation

Définition. Soit I un intervalle et f une application continue de I dans \mathbb{R} .

On dit que F est une primitive de f sur I si et seulement si F est dérivable et $F' = f$.

Propriété. Avec les hypothèses et notations précédentes, si F_0 est une primitive de f , alors les autres primitives de f sont exactement les applications $F_0 + k$, où k est une fonction constante.

Théorème : Soit I un intervalle de \mathbb{R} et f une application de I dans \mathbb{R} que l’on suppose continue.

Soit $x_0 \in I$. Alors $x \mapsto \int_{x_0}^x f(t)dt$ est l’unique primitive de f qui s’annule en x_0 .

Corollaire. Soit f une application continue d’un intervalle I dans \mathbb{R} .

Si F est une primitive de f , alors pour tout $a, b \in I$, $\int_a^b f(t)dt = F(b) - F(a) \triangleq [F(t)]_a^b$.

Corollaire. Si f est une application de classe C^1 sur $[a, b]$, $\int_a^b f'(t)dt = f(b) - f(a)$.

Notation. L’écriture “ $\int f(t)dt = F(t) + k, t \in I$ ” signifiera que f est continue sur I et que l’ensemble des primitives de f est $\{F + k/k \in \mathbb{R}\}$.

Il faut savoir calculer les primitives suivantes :

$$\int \cos t dt, \int x^\alpha dx \text{ (où } \alpha \in \mathbb{R} \setminus \{-1\}\text{)}, \int \cos^2 x dx, \int \frac{dx}{1+x^2} \text{ et } \int \frac{2x dx}{(x^2+1)^2}.$$

Propriété. Avec $a \neq 0$, si $\int f(t)dt = F(t) + k$, alors $\int f(at + b)dt = \frac{1}{a}F(at + b) + k$.

Remarque. Si f est une application continue d'un intervalle I dans \mathbb{R} et si $u : J \rightarrow I$ et $v : J \rightarrow I$ sont des applications dérivables sur un intervalle J , on calcule la dérivée de $t \mapsto \int_{u(t)}^{v(t)} f(x)dx$ en utilisant une primitive F de f :

$$\int_{u(t)}^{v(t)} f(x)dx = F(v(t)) - F(u(t)) \text{ a pour dérivée } v'(t)f(v(t)) - u'(t)f(u(t)).$$

2 Fonctions Logarithmes et puissances

2.1 Quelques théorèmes d'analyse

On montrera plus tard les théorèmes suivants :

Théorème de la limite monotone : On pose $\overline{\mathbb{R}} = \mathbb{R} \cup \{+\infty, -\infty\}$.

Soit $(m, M) \in \overline{\mathbb{R}}^2$ avec $m < M$. Notons $I =]m, M[$.

Soit f une application de I dans \mathbb{R} que l'on suppose monotone.

Alors la quantité $f(x)$ possède une limite dans $\overline{\mathbb{R}}$, lorsque x tend vers m (resp : M).

Théorème de la bijection : Soit f une application définie sur un intervalle I et à valeurs dans \mathbb{R} . On suppose que f est continue sur I .

Alors f est une bijection de I dans $f(I)$ si et seulement si f est strictement monotone.

Dans ce cas, $f(I)$ est un intervalle et l'application réciproque f^{-1} est une application également continue, strictement monotone, de même sens de variation que f , allant de $f(I)$ dans I .

Définition. Soit $f : I \rightarrow J$ où I et J sont deux intervalles. Soit $n \in \mathbb{N}^* \cup \{\infty\}$. On dit que f est un C^n -difféomorphisme si et seulement si f est une bijection de I sur J et si f et f^{-1} sont toutes deux de classe C^n .

Caractérisation d'un difféomorphisme : Soit f une application définie sur un intervalle I et à valeurs dans \mathbb{R} . Soit $n \in \mathbb{N}^* \cup \{\infty\}$. f est un C^n -difféomorphisme de I dans $f(I)$ si et seulement si f est de classe C^n et si, pour tout $x \in I$, $f'(x) \neq 0$.

2.2 Les fonctions ln et exp

La fonction Logarithme népérien : Pour tout $x > 0$, on pose $\ln(x) = \int_1^x \frac{dt}{t}$.

\ln est une bijection strictement croissante de \mathbb{R}_+^* dans \mathbb{R} . $\ln(1) = 0$.

Pour tout $x > 0$, $\frac{d}{dx}(\ln(x)) = \frac{1}{x}$.

Il existe un unique $e \in \mathbb{R}$ tel que $\ln(e) = 1$. e est le nombre de Neper : $e = 2,7 \pm 10^{-1}$.

Pour tout $x, y \in \mathbb{R}_+^*$ et $n \in \mathbb{Z}$,

$$- \ln(xy) = \ln x + \ln y : \text{A savoir démontrer.}$$

$$- \ln\left(\frac{1}{x}\right) = -\ln x, \ln\left(\frac{x}{y}\right) = \ln x - \ln y,$$

$$- \ln(x^n) = n \ln x,$$

$$- \ln(t) \xrightarrow{t \rightarrow 0} -\infty, \ln(t) \xrightarrow{t \rightarrow +\infty} +\infty, \frac{\ln(t)}{t} \xrightarrow{t \rightarrow +\infty} 0 : \text{A savoir démontrer.}$$

La fonction exponentielle : c'est la bijection réciproque de la fonction logarithme népérien.

\exp est une bijection strictement croissante de \mathbb{R} dans \mathbb{R}_+^* .

Pour tout $x \in \mathbb{R}_+^*$, $\exp(\ln x) = x$ et, pour tout $x \in \mathbb{R}$, $\ln(\exp(x)) = x$.

$$\forall x \in \mathbb{R}, \frac{d}{dx}(\exp(x)) = \exp(x).$$

Pour tout $x, y \in \mathbb{R}$ et $n \in \mathbb{Z}$,

- $e^{x+y} = e^x e^y$,
- $e^0 = 1$ et $e^1 = e$,
- $e^{-x} = \frac{1}{e^x}$, $e^{x-y} = \frac{e^x}{e^y}$,
- $e^{nx} = (e^x)^n$.
- $e^t \xrightarrow[t \rightarrow -\infty]{} 0$, $e^t \xrightarrow[t \rightarrow +\infty]{} +\infty$. $\frac{e^t}{t} \xrightarrow[t \rightarrow +\infty]{} +\infty$.

Représentation graphique de \ln et \exp : **A connaître**

Logarithmes et exponentielles en base a .

- Soit $a \in \mathbb{R}_+^* \setminus \{1\}$. $\forall x \in \mathbb{R}_+^*$, $\ln_a(x) \triangleq \frac{\ln x}{\ln a}$.
Pour tout $x, y \in \mathbb{R}_+^*$ et $b \in \mathbb{R}$,
 - $\ln_a(xy) = \ln_a x + \ln_a y$,
 - $\ln_a(1) = 0$ et $\ln_a(a) = 1$,
 - $\ln_a\left(\frac{1}{x}\right) = -\ln_a x$, $\ln_a\left(\frac{x}{y}\right) = \ln_a x - \ln_a y$,
 - $\ln_a(x^b) = b \ln_a x$,
- Soit $a \in \mathbb{R}_+^*$. $\forall x \in \mathbb{R}$, $a^x \triangleq e^{x \ln a} = \exp_a(x)$.
 $\forall x \in \mathbb{R}$, $\ln_a(a^x) = x$ et $\forall x \in \mathbb{R}_+^*$, $a^{\ln_a x} = x$.
Pour tout $x \in \mathbb{R}$, $\frac{d}{dx}(a^x) = (\ln a)a^x$.
Pour tout $x, y \in \mathbb{R}$,
 - $a^{x+y} = a^x a^y$,
 - $a^0 = 1$ et $a^1 = a$, $a^x > 0$,
 - $a^{-x} = \frac{1}{a^x}$, $a^{x-y} = \frac{a^x}{a^y}$,
 - pour tout $b \in \mathbb{R}$, $a^{bx} = (a^x)^b$.
 - Pour tout $b > 0$, $a^x b^x = (ab)^x$.

2.3 Fonctions puissances

Définition. Un monôme de degré $n \in \mathbb{N}$ est une application de la forme $x \mapsto ax^n$, où a est un paramètre réel. Cette application est définie sur \mathbb{R} .

Une fonction polynomiale est une somme finie de monômes.

Lorsque $n \in \mathbb{Z}$ avec $n < 0$, $x \mapsto x^n$ est définie sur \mathbb{R}^* .

Représentation graphique de $x \mapsto x^n$ lorsque $n \in \mathbb{Z}$: **A connaître**.

Représentation graphique de $x \mapsto x^\alpha$ où $\alpha \in \mathbb{R} \setminus \mathbb{Z}$, lorsque x décrit \mathbb{R}_+^* : **A connaître**.

Convention : Pour tout $b \in \mathbb{R}_+^*$, $0^b = 0$ et $\boxed{0^0 = 1}$.

3 Etude d'une fonction

3.1 Plan d'étude

Plan d'étude d'une fonction f de \mathbb{R} dans \mathbb{R} :

1. Calcul du domaine de définition de f .
2. Si f est paire, impaire ou/et périodique, on peut réduire le domaine d'étude.
3. Calcul de $f'(x)$ et étude de son signe.
4. Tableau de variations de f . Indiquez notamment les limites de f aux bornes des intervalles.
5. Etude des branches infinies si $f(x) \xrightarrow[x \rightarrow \pm\infty]{} \pm\infty$.

Semaine 3 : Résumé de cours

1 Etude des branches infinies

Soit $\varepsilon \in \{-1, 1\}$. On suppose que $f(x) \xrightarrow{x \rightarrow \varepsilon\infty} \pm\infty$.

1. S'il existe $\mu \in \mathbb{R}$ tel que $\frac{f(x)}{x} \xrightarrow{x \rightarrow \varepsilon\infty} \mu$, on dit que le graphe de f admet une direction asymptotique de pente μ .
 - S'il existe $\alpha \in \mathbb{R}$ tel que $f(x) - \mu x \xrightarrow{x \rightarrow \varepsilon\infty} \alpha$, la droite affine d'équation $y = \mu x + \alpha$ est une asymptote de la courbe au voisinage de $\varepsilon\infty$.
 - Si $f(x) - \mu x \xrightarrow{x \rightarrow \varepsilon\infty} \pm\infty$, on dit que le graphe de f présente au voisinage de $\varepsilon\infty$ une branche parabolique de pente μ .
En particulier, lorsque $\frac{f(x)}{x} \xrightarrow{x \rightarrow \varepsilon\infty} 0$, on est en présence d'une branche parabolique horizontale.
 - Autres cas : il y a seulement une direction asymptotique.
2. Si $\frac{f(x)}{x} \xrightarrow{x \rightarrow \varepsilon\infty} \pm\infty$, le graphe de f admet une branche parabolique verticale.
3. Autres cas : on ne peut rien dire.

2 Déformations du graphe

Notation. f désigne une fonction de D dans \mathbb{R} , où $D \subset \mathbb{R}$.

Propriété. On fixe un réel a .

- Le graphe de $x \mapsto f(x) + a$ se déduit du graphe de f par la translation de vecteur $a\vec{j}$.
- Le graphe de $x \mapsto f(x + a)$ se déduit du graphe de f par la translation de vecteur $-a\vec{i}$. **A savoir établir.**
- Le graphe de $x \mapsto f(a - x)$ se déduit du graphe de f par la symétrie orthogonale selon la droite verticale d'abscisse $\frac{a}{2}$.
- Le graphe de $x \mapsto f(ax)$ se déduit du graphe de f par l'affinité orthogonale d'axe invariant Oy et de coefficient $\frac{1}{a}$, qui correspond, en identifiant un point avec le couple de ses coordonnées, à la transformation $(x, y) \mapsto (\frac{x}{a}, y)$ (**A savoir établir**). Ceci a pour effet,
 - lorsque $a > 1$, d'écraiser le graphe de f d'un facteur a vers l'axe des ordonnées, parallèlement à l'axe Ox ,
 - lorsque $0 < a < 1$, d'étirer le graphe de f d'un facteur $\frac{1}{a}$ autour de l'axe Oy , parallèlement à l'axe Ox .
- Le graphe de $x \mapsto af(x)$ se déduit du graphe de f par une affinité d'axe invariant Ox et de coefficient a , i.e par la transformation $(x, y) \mapsto (x, ay)$.

3 Trigonométrie hyperbolique

Définition. On définit les fonctions usuelles suivantes :

- cosinus hyperbolique : $\forall x \in \mathbb{R}, \operatorname{ch} x = \frac{e^x + e^{-x}}{2},$
- sinus hyperbolique : $\forall x \in \mathbb{R}, \operatorname{sh} x = \frac{e^x - e^{-x}}{2},$
- tangente hyperbolique : $\forall x \in \mathbb{R}, \operatorname{th} x = \frac{\operatorname{sh} x}{\operatorname{ch} x} = \frac{e^x - e^{-x}}{e^x + e^{-x}} = \frac{e^{2x} - 1}{e^{2x} + 1}.$

Propriété. Les fonctions sh, ch et th sont de classe C^∞ sur \mathbb{R} et $\operatorname{ch}' = \operatorname{sh}, \operatorname{sh}' = \operatorname{ch}, \operatorname{th}'(x) = 1 - \operatorname{th}^2 x = \frac{1}{\operatorname{ch}^2 x}.$

Il faut connaître les graphes de sh, ch et th.

Toute formule de la trigonométrie circulaire est associée avec une formule duale de la trigonométrie hyperbolique. Cependant, le programme officiel se limite à la formule suivante :

Formule : $\forall x \in \mathbb{R}, \operatorname{ch}^2 x - \operatorname{sh}^2 x = 1.$

Mais il n'est pas interdit de connaître quelques formules de trigonométrie hyperbolique :

- $\operatorname{ch}(a + b) = \operatorname{ch} a \operatorname{ch} b + \operatorname{sh} a \operatorname{sh} b,$
- $\operatorname{sh}(a + b) = \operatorname{sh} a \operatorname{ch} b + \operatorname{ch} a \operatorname{sh} b,$
- $\operatorname{ch}^2 a = \frac{\operatorname{ch}(2a) + 1}{2}, \operatorname{sh}^2 a = \frac{\operatorname{ch}(2a) - 1}{2} \geq 0.$

4 Applications trigonométriques réciproques

Les graphes des fonctions usuelles de ce chapitre sont à connaître.

4.1 Trigonométrie circulaire

La fonction arcsin : l'application $\sin : [-\frac{\pi}{2}, \frac{\pi}{2}] \longrightarrow [-1, 1]$ est surjective, continue et strictement croissante. On note arcsin son application réciproque, de $[-1, 1]$ dans $[-\frac{\pi}{2}, \frac{\pi}{2}]$. Elle est continue, impaire et strictement croissante sur $[-1, 1]$.

La restriction de sin à $] -\frac{\pi}{2}, \frac{\pi}{2}[$ est un C^∞ -difféomorphisme sur $] -1, 1[$, dont le C^∞ -difféomorphisme réciproque est la restriction de arcsin à $] -1, 1[$.

Pour tout $x \in] -1, 1[$, $\operatorname{arcsin}'(x) = \frac{1}{\sqrt{1-x^2}}.$

La fonction arccos : l'application $\cos : [0, \pi] \longrightarrow [-1, 1]$ est surjective, continue et strictement décroissante. On note arccos son application réciproque, de $[-1, 1]$ dans $[0, \pi]$. Elle est continue et strictement décroissante sur $[-1, 1]$.

La restriction de cos à $] 0, \pi[$ est un C^∞ -difféomorphisme sur $] -1, 1[$, dont le C^∞ -difféomorphisme réciproque est la restriction de arccos à $] -1, 1[$.

Pour tout $x \in] -1, 1[$, $\operatorname{arccos}'(x) = \frac{-1}{\sqrt{1-x^2}}.$

Propriété. $\forall t \in [-1, 1] \quad \cos(\operatorname{arccos} t) = t$ et $\sin(\operatorname{arcsin} t) = t$, mais en général, $\operatorname{arccos}(\cos t) \neq t$. Plus précisément, $\operatorname{arccos}(\cos t) = t \iff t \in [0, \pi]$.

Ainsi, lorsque $t \notin [0, \pi]$, $\operatorname{arccos}(\cos t) = t_0$ où $t_0 \in [0, \pi]$ et $\cos t = \cos t_0$.

La fonction arctan : l'application $\tan :] -\frac{\pi}{2}, \frac{\pi}{2}[\longrightarrow \mathbb{R}$ est un C^∞ -difféomorphisme strictement croissant, dont le C^∞ -difféomorphisme réciproque est noté.

Pour tout $x \in \mathbb{R}$, $\operatorname{arctan}'(x) = \frac{1}{1+x^2}.$

4.2 Trigonométrie hyperbolique

Les fonctions réciproques des fonctions ch, sh et th ne sont pas au programme.

La fonction argsh : sh est un C^∞ -difféomorphisme de \mathbb{R} dans \mathbb{R} , dont le difféomorphisme réciproque est noté argsh (“argument sinus hyperbolique”). Ainsi argsh est une application C^∞ , impaire, strictement croissante. $\argsh'(x) = \frac{1}{\sqrt{1+x^2}}$.

A savoir établir : Pour tout $x \in \mathbb{R}$, $\argsh x = \ln(x + \sqrt{1+x^2})$.

La fonction argch : L'application ch est une bijection continue strictement croissante de \mathbb{R}_+ dans $[1, +\infty[$. Son application réciproque est notée argch. C'est une bijection continue strictement croissante de $[1, +\infty[$ dans \mathbb{R}_+ .

ch est un C^∞ -difféomorphisme de \mathbb{R}_+^* dans $]1, +\infty[$, donc argch est C^∞ sur $]1, +\infty[$.

$\argch'(x) = \frac{1}{\sqrt{x^2-1}}$. Pour tout $x \in [1, +\infty[$, $\argch x = \ln(x + \sqrt{x^2-1})$.

La fonction argth : th est un C^∞ -difféomorphisme de \mathbb{R} dans $] -1, 1[$, dont le difféomorphisme réciproque est noté argth. Ainsi argth est une application C^∞ , impaire, strictement croissante de $] -1, 1[$ dans \mathbb{R} . $\argth'(x) = \frac{1}{1-x^2}$. Pour tout $x \in] -1, 1[$, $\argth x = \frac{1}{2} \ln\left(\frac{1+x}{1-x}\right)$.

5 Calculs d'intégrales

5.1 Changement de variables

Théorème. On suppose que f est une application continue d'un intervalle I dans \mathbb{R} , et que φ est une application **de classe** C^1 d'un intervalle J dans I . Alors,

$$\forall (\alpha, \beta) \in J^2 \quad \boxed{\int_{\alpha}^{\beta} f(\varphi(t))\varphi'(t)dt = \int_{\varphi(\alpha)}^{\varphi(\beta)} f(x)dx.} \quad (1)$$

Lorsque l'on remplace un membre de cette égalité par l'autre, on dit que l'on effectue le changement de variable $x = \varphi(t)$.

Démonstration à connaître.

Propriété. Soit $a \in \mathbb{R}_+^*$ et soit f une application continue sur $[-a, a]$.

Si f est paire, alors $\int_{-a}^a f(t) dt = 2 \int_0^a f(t) dt$. Si f est impaire, $\int_{-a}^a f(t) dt = 0$.

Théorème. Soit $T \in \mathbb{R}_+^*$. On suppose que f est une fonction continue et T -périodique définie sur \mathbb{R} .

Alors, $\forall t_0 \in \mathbb{R} \quad \int_0^T f(t) dt = \int_{t_0}^{T+t_0} f(t) dt$.

Démonstration à connaître.

5.2 Intégration par parties

Théorème. Soit $u : I \rightarrow \mathbb{R}$ et $v : I \rightarrow \mathbb{R}$ deux applications de classe C^1 sur I .

Pour tout $(a, b) \in I^2$, $\int_a^b u(t)v'(t) dt = [u(t)v(t)]_a^b - \int_a^b u'(t)v(t) dt$.

Théorème. Soit $u : I \rightarrow \mathbb{R}$ et $v : I \rightarrow \mathbb{R}$ deux applications de classe C^1 sur I .

Alors, $\int u(t)v'(t) dt = u(t)v(t) - \int u'(t)v(t) dt, \quad t \in I$.

Semaine 4 : Résumé de cours

1 Fondations

1.1 Ensembles et éléments

Axiome d'extensionnalité : Si E et F sont deux ensembles, alors $E = F$ si et seulement si pour tout $x \in E$, $x \in F$ et pour tout $x \in F$, $x \in E$.

Définition. $\{a\}$ est un singleton.
Lorsque $a \neq b$, $\{a, b\}$ est appelé une paire.

Définition. Un prédicat P sur un ensemble E est une application de E dans $\{V, F\}$, où V symbolise le vrai et F le faux.

Définition d'un ensemble en compréhension : Si E est un ensemble et P un prédicat sur E , alors $F = \{x \in E / P(x)\}$ est un ensemble.
De plus, pour tout $x \in E$, $x \in F \iff P(x)$.

Le paradoxe de Russell :

Notons A la collection de tous les ensembles et posons $B = \{x \in A / x \notin x\}$. Alors $B \in B$ si et seulement si $B \notin B$, ce qui est impossible. Cela signifie que A n'est pas un ensemble !

À connaître.

1.2 Quantificateurs

Définition du quantificateur universel :

Soit E un ensemble et P un prédicat sur E . La propriété " $\forall x \in E, P(x)$ " signifie que pour tous les éléments x de E , $P(x)$ est vraie, c'est-à-dire que $\{x \in E / P(x)\}$ est égal à E .

Définition du quantificateur existentiel :

Avec les mêmes notations, la propriété " $\exists x \in E, P(x)$ " signifie qu'il existe au moins un $x \in E$ tel que $P(x)$ est vraie, c'est-à-dire que $\{x \in E / P(x)\} \neq \emptyset$.

Existence et unicité : La propriété " $\exists! x \in E, P(x)$ " signifie qu'il existe un unique $x \in E$ tel que $P(x)$ est vraie, c'est-à-dire que $\{x \in E / P(x)\}$ est un singleton.

Remarque. L'emploi des quantificateurs en guise d'abréviations est exclu : l'usage d'un " $\forall x$ " est toujours suivi d'un " $\in E, P(x)$ " (ou plus rarement d'un " $, P(x)$ "), où P est un prédicat sur E .

Remarque. Soit P un prédicat sur un ensemble E . Alors dans les phrases

" $\forall x \in E, P(x)$ " et " $\exists x \in E, P(x)$ ", on peut remplacer la variable x par y , ou n'importe quel autre symbole. On dit que, dans les phrases " $\forall x \in E, P(x)$ " et " $\exists x \in E, P(x)$ ", x est une variable muette ou bien que c'est une variable liée.

Dans la propriété " $\exists y \in \mathbb{R}, x = y^2$ ", y est une variable liée, et par opposition, on dit que x est une variable libre.

1.3 Parties d'un ensemble

Définition. Soit E et F deux ensembles.

On dit que F est inclus dans E et l'on note $F \subset E$ si et seulement si tout élément de F est un élément de E , c'est-à-dire si et seulement si $\forall x \in F, x \in E$.

Transitivité de l'inclusion : Si $A \subset B$ et $B \subset C$, alors $A \subset C$.

Définition. Si E est un ensemble, on note $\mathcal{P}(E)$ l'ensemble de ses parties.

1.4 Opérateurs sur les ensembles

Définition. Soit E et F deux ensembles :

- **Intersection :** $x \in E \cap F$ si et seulement si $(x \in E \text{ et } x \in F)$.
- **Réunion :** $x \in E \cup F$ si et seulement si $(x \in E \text{ ou } x \in F)$.
- **Différence ensembliste :** $E \setminus F = \{x \in E / x \notin F\}$.
- **Différence symétrique :** $E \Delta F = (E \setminus F) \cup (F \setminus E) = (E \cup F) \setminus (E \cap F)$.
- **Complémentaire de F dans E :** Si F est une partie de E , le complémentaire de F dans E est $\overline{F} = E \setminus F$, que l'on note plus rarement \complement_E^F .

Propriété. Si F et G sont deux parties d'un ensemble E , alors $F \setminus G = F \cap \overline{G}$.

Propriété. Associativité de l'intersection et de la réunion : Soit A, B, C trois ensembles. Alors, $A \cap (B \cap C) = (A \cap B) \cap C$ et $A \cup (B \cup C) = (A \cup B) \cup C$.

Définition. Soit I un ensemble et $(E_i)_{i \in I}$ une famille d'ensembles. On définit $\bigcup_{i \in I} E_i$ et $\bigcap_{i \in I} E_i$ par :

$$x \in \bigcup_{i \in I} E_i \iff (\exists i \in I, x \in E_i) \text{ et } x \in \bigcap_{i \in I} E_i \iff (\forall i \in I, x \in E_i).$$

Cette dernière définition n'est pas correcte lorsque $I = \emptyset$.

Distributivité de l'intersection par rapport à la réunion :

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C). \quad A \cap \bigcup_{i \in I} B_i = \bigcup_{i \in I} (A \cap B_i).$$

Il faut savoir le démontrer.

Distributivité de la réunion par rapport à l'intersection :

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C). \quad A \cup \bigcap_{i \in I} B_i = \bigcap_{i \in I} (A \cup B_i) \text{ (avec } I \neq \emptyset \text{)}.$$

Notation. Soit $(E_i)_{i \in I}$ une famille d'ensembles deux à deux disjoints, c'est-à-dire telle que, pour tout $i, j \in I$ avec $i \neq j$, $E_i \cap E_j = \emptyset$.

Alors $\bigcup_{i \in I} E_i$ est appelée une réunion disjointe et elle est notée $\bigsqcup_{i \in I} E_i$.

1.5 L'ensemble \mathbb{N} des entiers naturels

On admet qu'il existe un ensemble, noté \mathbb{N} , satisfaisant les axiomes de Peano suivants :

- \mathbb{N} est muni d'un élément particulier noté 0 et d'une application "successeur", notée s de \mathbb{N} dans \mathbb{N} .
- 0 n'est le successeur d'aucun entier : $\forall n \in \mathbb{N}, s(n) \neq 0$.
- s est une application injective : pour tout $n, m \in \mathbb{N}$, si $s(n) = s(m)$, alors $n = m$.
- Pour toute partie F de \mathbb{N} , si $0 \in F$ et si pour tout $n \in F$, $s(n) \in F$, alors $F = \mathbb{N}$.

Principe de récurrence : Soit $R(n)$ un prédicat sur \mathbb{N} .

Si $R(0)$ est vraie et si pour tout $n \in \mathbb{N}$, $R(n)$ implique $R(s(n))$, alors pour tout $n \in \mathbb{N}$, $R(n)$ est vraie.

Addition entre entiers : Pour tout $m \in \mathbb{N}$, on pose

$0 + m = m$ et

$\forall n \in \mathbb{N}, s(n) + m = s(n + m)$.

Ces conditions définissent l'addition entre entiers.

Propriétés de l'addition :

- 0 est neutre : $\forall m \in \mathbb{N}, m + 0 = 0 + m = m$.
- Associativité : $\forall n, m, k \in \mathbb{N}, (n + m) + k = n + (m + k)$.
- Commutativité : $\forall n, m \in \mathbb{N}, n + m = m + n$.

1.6 Produit cartésien

Définition. Si a et b sont deux objets, posons $(a, b) = \{\{a\}, \{a, b\}\}$. On l'appellera le “couple de composantes a et b ”. Alors, $(a, b) = (c, d)$ si et seulement si $a = c$ et $b = d$.

Il faut savoir le démontrer.

Définition. Si A et B sont deux ensembles, on pose $A \times B = \{(a, b) / a \in A \text{ et } b \in B\}$.

$A \times B$ s'appelle le produit cartésien de A et B .

Définition. Un couple est aussi un 2-uplet. Pour $n \geq 3$, on définit récursivement la notion de n -uplet (ou n -liste) en écrivant : $(a_1, \dots, a_n) = ((a_1, \dots, a_{n-1}), a_n)$.

Alors, $(a_1, \dots, a_n) = (b_1, \dots, b_n)$ si et seulement si $\forall i \in \{1, \dots, n\}, a_i = b_i$.

Notation. \mathbb{N}^* désigne $\mathbb{N} \setminus \{0\}$.

Définition. Soit $n \in \mathbb{N}^*$. Si A_1, \dots, A_n sont n ensembles, on pose

$A_1 \times \dots \times A_n = \{(a_1, \dots, a_n) / \forall i \in \{1, \dots, n\}, a_i \in A_i\}$.

Si E est un ensemble, on note $E^n = \underbrace{E \times \dots \times E}_{n \text{ fois}}$.

Remarque. Convention, lorsque $n = 1$, le “1-uplet” (a) est égal à a .

Avec cette convention, $E^1 = E$.

Commutativité de deux quantificateurs universels :

Soit E et F deux ensembles. Notons $P(x, y)$ un prédicat défini sur $E \times F$. Alors

$$\begin{aligned} [\forall (x, y) \in E \times F, P(x, y)] &\iff [\forall x \in E, \forall y \in F, P(x, y)] \\ &\iff [\forall y \in F, \forall x \in E, P(x, y)] \end{aligned}$$

Commutativité de deux quantificateurs existentiels : De même,

$$\begin{aligned} [\exists (x, y) \in E \times F, P(x, y)] &\iff [\exists x \in E, \exists y \in F, P(x, y)] \\ &\iff [\exists y \in F, \exists x \in E, P(x, y)] \end{aligned}$$

ATTENTION :

Un quantificateur universel ne commute pas avec un quantificateur existentiel.

“ $\forall x \in E, \exists y \in F, P(x, y)$ ” si et seulement si il existe une application

$x \mapsto y(x)$ de E dans F tel que, pour tout $x \in E, P(x, y(x))$,

et “ $\exists y \in F, \forall x \in E, P(x, y)$ ” si et seulement si il existe une application **constante**

$x \mapsto y_0$ de E dans F , telle que pour tout $x \in E, P(x, y_0)$.

On voit qu'en général, la seconde affirmation implique la première mais que la réciproque est fausse.

2 Formules propositionnelles

2.1 Syntaxe

Définition par induction des formules propositionnelles : on part d'un ensemble \mathcal{V} dont les éléments sont appelés des variables propositionnelles. On utilise également les “connecteurs logiques” suivants : $\wedge, \vee, \implies, \iff, \neg$.

L'ensemble F des formules propositionnelles est défini par induction structurale :

- Les variables propositionnelles sont des formules propositionnelles.
- si $P, Q \in F$, alors $(P \wedge Q), (P \vee Q), (P \implies Q), (P \iff Q)$ et $\neg P$ sont aussi des formules propositionnelles.

Plus précisément, si l'on note $F_0 = \mathcal{V}$, et pour tout $n \in \mathbb{N}$,

$$F_{n+1} = F_n \cup \{\neg P / P \in F_n\} \cup \{(P \alpha Q) / P, Q \in F_n \text{ et } \alpha \in \{\wedge, \vee, \implies, \iff\}\}, \text{ alors } F = \bigcup_{n \in \mathbb{N}} F_n.$$

Remarque. Une formule propositionnelle s'appelle aussi une proposition, une assertion, une formule, un énoncé, une expression booléenne, etc.

Définition. Si P et Q sont deux formules propositionnelles, $P \wedge Q$ (prononcer “ P et Q ”) s'appelle la conjonction de P et de Q , $P \vee Q$ (prononcer “ P ou Q ”) s'appelle la disjonction de P et de Q , $P \implies Q$ s'appelle une implication, $P \iff Q$ est une équivalence, et $\neg P$ est la négation de la proposition P .

2.2 Sémantique

Définition. Une distribution de valeurs de vérité sur l'ensemble \mathcal{V} des variables propositionnelles est une application de \mathcal{V} dans l'ensemble $\{V, F\}$.

Définition. Soit v une distribution de valeurs de vérité sur l'ensemble \mathcal{V} . On prolonge v sur l'ensemble des formules propositionnelles construites à partir de \mathcal{V} de la manière suivante : pour toutes formules propositionnelles P et Q ,

- $v(P \wedge Q) = 1$ si et seulement si $v(P) = v(Q) = 1$.
- $v(P \vee Q) = 1$ si et seulement si $v(P) = 1$ ou $v(Q) = 1$.
- $v(P \implies Q) = 0$ si et seulement si $v(P) = 1$ et $v(Q) = 0$.
- $v(P \iff Q) = 1$ si et seulement si $v(P) = v(Q)$.
- $v(\neg P) = 1$ si et seulement si $v(P) = 0$.

Définition. La définition précédente est équivalente à la donnée des “tables de vérité” des connecteurs logiques $\wedge, \vee, \implies, \iff$ et \neg :

P	Q	$P \wedge Q$	$P \vee Q$	$P \implies Q$
V	V	V	V	V
V	F	F	V	F
F	V	F	V	V
F	F	F	F	V

Définition. Lorsque $P \implies Q$, on dit que P est une *condition suffisante* pour Q et que Q est une *condition nécessaire* pour P .

Lorsque $P \iff Q$, on dit que P est une *condition nécessaire et suffisante* pour Q .

Définition. Une tautologie est une formule propositionnelle qui est toujours vraie, quelle que soit la distribution de valeurs de vérité des variables propositionnelles qui interviennent dans la formule.

Exemple. Quelques tautologies à connaître (A, B, C désignent des formules propositionnelles quelconques) :

1. $(A \vee (B \vee C)) \iff ((A \vee B) \vee C)$: associativité de \vee (\wedge est aussi associatif),
2. $(A \wedge (B \vee C)) \iff ((A \wedge B) \vee (A \wedge C))$: distributivité de \wedge par rapport à \vee ,
3. $(A \vee (B \wedge C)) \iff ((A \vee B) \wedge (A \vee C))$: distributivité de \vee par rapport à \wedge ,
4. $(A \wedge (A \vee B)) \iff A$: première loi d'absorption,
5. $((A \vee (A \wedge B)) \iff A$: seconde loi d'absorption,
6. $(\neg(A \vee B)) \iff (\neg A \wedge \neg B)$: loi de Morgan,
7. $(\neg(A \wedge B)) \iff (\neg A \vee \neg B)$: loi de Morgan,
8. $(A \implies B) \iff (\neg A) \vee B$ (une définition de l'implication),

9. $\neg(A \implies B) \iff A \wedge (\neg B)$,
10. $(A \implies B) \iff (\neg B \implies \neg A)$: contraposition.
11. $((A \implies B) \wedge (B \implies C)) \implies (A \implies C)$ (règle du modus ponens).

Il faut savoir le démontrer.

Définition. On dit que deux propositions P et Q sont logiquement équivalentes si et seulement si la proposition $P \iff Q$ est une tautologie. On notera alors $P \equiv Q$

Ainsi, lorsque l'on ne s'intéresse qu'à la valeur booléenne des propositions, on peut remplacer toute proposition par une proposition qui lui est logiquement équivalente.

Exemple. $(A \wedge (B \vee C)) \equiv ((A \wedge B) \vee (A \wedge C))$.
 $\neg(A \implies B) \equiv A \wedge \neg B$ et $A \implies B \equiv \neg A \vee B$.

Définition. La contraposée de l'implication $A \implies B$ est égale à $\neg B \implies \neg A$.
Toute implication est logiquement équivalente à sa contraposée.

2.3 Négation d'une proposition

- ◇ $\neg(A \vee B)$ est logiquement équivalente à $(\neg A) \wedge (\neg B)$,
- $\neg(A \wedge B)$ est logiquement équivalente à $(\neg A) \vee (\neg B)$.
- ◇ $\neg(\neg A)$ est logiquement équivalente à A .
- ◇ $\neg(A \implies B)$ est logiquement équivalente à $A \wedge (\neg B)$.
- ◇ Une équivalence est la conjonction de deux implications, donc
- $\neg(A \iff B)$ est logiquement équivalente à $[\neg(A \implies B)] \vee [\neg(B \implies A)]$.

Propriété. Soit P un prédicat sur un ensemble E .

$\neg[\forall x \in E, P(x)] \iff [\exists x \in E, \neg P(x)]$
et $\neg[\exists x \in E, P(x)] \iff [\forall x \in E, \neg P(x)]$.

Exemple. **Savoir nier** qu'une suite $(x_n)_{n \in \mathbb{N}}$ de réels converge vers 0 :

$\neg[\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, [n \geq N \implies |x_n| \leq \varepsilon]] \equiv \dots$

Propriété. Soit A et B deux ensembles de E .

Soit $(E_i)_{i \in I}$ une famille de parties de E , avec $I \neq \emptyset$. Alors,

- $\overline{\overline{A}} = A, \quad \overline{A \cup B} = \overline{A} \cap \overline{B}, \quad \overline{A \cap B} = \overline{A} \cup \overline{B},$
- $A \subset B \iff \overline{B} \subset \overline{A},$
- $\overline{\bigcap_{i \in I} E_i} = \bigcup_{i \in I} \overline{E_i}, \quad \overline{\bigcup_{i \in I} E_i} = \bigcap_{i \in I} \overline{E_i}.$

Semaine 5 : Résumé de cours

1 Relations binaires

1.1 Définitions

Définition. Une relation binaire R sur $E \times F$ est une partie de $E \times F$, mais on notera “ xRy ” au lieu de “ $(x, y) \in R$ ”. Le graphe de R est $\{(x, y) \in E \times F / xRy\}$, donc le graphe de R est ... égal à R .

Définition. Lorsque $E = F$, on dit que

- R est réflexive si et seulement si $\forall x \in E, xRx$,
- R est symétrique si et seulement si $\forall x, y \in E, (xRy) \implies (yRx)$,
- R est antisymétrique si et seulement si $\forall x, y \in E, [(xRy) \wedge (yRx) \implies x = y]$,
- et R est transitive si et seulement si $\forall x, y, z \in E, [(xRy) \wedge (yRz) \implies (xRz)]$.

1.2 Relations d'ordre

Définition. Une relation binaire R sur un ensemble E est appelée une relation d'ordre si et seulement si R est réflexive, antisymétrique et transitive.

Exemple. Si A est un ensemble, la relation d'inclusion est une relation d'ordre sur $\mathcal{P}(A)$.

Définition. Une relation d'ordre R sur un ensemble E est totale si et seulement si pour tout couple (x, y) de E^2 , x et y sont comparables, c'est-à-dire $(xRy) \vee (yRx)$. Sinon, on dit que l'ordre est partiel.

Exemple. La relation d'inclusion sur $\mathcal{P}(A)$ n'est pas totale dès que A possède plus de deux éléments.

Définition. Soit F une partie de E et $m \in E$. On dit que m est un majorant de F si et seulement si pour tout $a \in F, a \preceq m$. On définit de même la notion de minorant d'une partie de E .

On dit qu'une partie est majorée si et seulement si elle possède au moins un majorant.

On dit qu'une partie est minorée si et seulement si elle possède au moins un minorant.

On dit qu'une partie est bornée si et seulement si elle est majorée et minorée.

Définition. Si F est une partie de E et $m \in E$, on dit que m est le maximum de F si et seulement si m majore F et $m \in F$. On le note $\max(F)$. On définit de même le minimum de F .

Définition. La borne supérieure de F est le minimum de l'ensemble des majorants (lorsqu'il existe). On le note $\sup(F)$. La borne inférieure de F est le maximum de l'ensemble des minorants (lorsqu'il existe). On le note $\inf(F)$.

Définition. Soit F une partie de E et m un élément de F .

m est maximal dans F si et seulement si $\forall x \in F (x \succeq m \implies x = m)$, i.e $\forall x \in F, \neg(x \succ m)$.

m est minimal dans F si et seulement si $\forall x \in F (x \preceq m \implies x = m)$, i.e $\forall x \in F, \neg(x \prec m)$.

Propriété. Lorsque la relation d'ordre est totale, toute partie F de E possède au plus un élément maximal et dans ce cas, c'est le maximum de F . Idem avec minimal et minimum.

Exercice. Si E est un ensemble fini et non vide, pour tout ordre défini sur E , montrer que E possède au moins un élément minimal.

A connaître.

1.3 L'ordre naturel et la soustraction

L'ordre naturel : Pour tout $n, m \in \mathbb{N}$,
on convient que $n \leq m$ si et seulement si $\exists k \in \mathbb{N}, m = n + k$.
Dans ce cas, k est unique. On le note $k = m - n$.
La relation binaire \leq ainsi définie est un ordre total sur \mathbb{N} .

Définition. On vient de montrer que, si n est un entier naturel, pour tout $h, k \in \mathbb{N}$, $n + h = n + k$ implique $h = k$. On dit que n est régulier.
Il faut savoir le démontrer.

Propriété. Soit $m, n \in \mathbb{N}$. Si $m < n$, alors $m + 1 \leq n$.

1.4 Multiplication dans \mathbb{N} et relation de divisibilité

Multiplication entre entiers : Pour tout $m \in \mathbb{N}$, on pose
 $0 \times m = 0$ et $\forall n \in \mathbb{N}, s(n) \times m = n \times m + m$.
Ces conditions définissent l'addition entre entiers.

Propriétés de la multiplication :

- 0 est absorbant : $\forall m \in \mathbb{N}, m \times 0 = 0 \times m = 0$.
- 1 est neutre : $\forall m \in \mathbb{N}, m \times 1 = 1 \times m = m$.
- Distributivité de la multiplication par rapport à l'addition :
 $\forall n, m, p \in \mathbb{N}, n(m + p) = (nm) + (np) = nm + np$: les dernières parenthèses sont inutiles si l'on convient que la multiplication est prioritaire devant l'addition.
- Associativité : $\forall n, m, k \in \mathbb{N}, (n \times m) \times k = n \times (m \times k)$.
- Commutativité : $\forall n, m \in \mathbb{N}, n \times m = m \times n$.

La relation d'ordre est compatible avec la multiplication :

Pour tout $a, b, c, d \in \mathbb{N}$, si $a \leq b$ et $c \leq d$, alors $ac \leq bd$.

Propriété. Soit $n, k \in \mathbb{N}$.
Si $nk = 0$, alors $n = 0$ ou $k = 0$.
Si $nk = 1$, alors $n = k = 1$.

Définition. Soit $n, m \in \mathbb{N}$. On dit que n divise m , que n est un diviseur de m , ou encore que m est un multiple de n si et seulement si il existe $k \in \mathbb{N}$ tel que $m = kn$. On note $n|m$.

Remarque. Tout entier divise 0 mais 0 ne divise que lui-même.

Définition. un nombre premier est un entier n supérieur à 2 dont les seuls diviseurs sont 1 et n .

Propriété. La relation de divisibilité est une relation d'ordre partiel sur \mathbb{N} .

Il faut savoir le démontrer.

1.5 Maximum et minimum dans \mathbb{N}

Propriété. Toute partie non vide et majorée de \mathbb{N} possède un maximum.

Il faut savoir le démontrer.

Propriété. Soit $a, b \in \mathbb{N}$ avec $b \neq 0$. Il existe un unique couple $(q, r) \in \mathbb{N}^2$ tel que $a = bq + r$ et $0 \leq r < b$. On dit que q et r sont le quotient et le reste de la division euclidienne de a par b .

Il faut savoir le démontrer.

Propriété. Toute partie non vide de \mathbb{N} possède un minimum.

Il faut savoir le démontrer.

Remarque. Un ensemble ordonné dont toute partie non vide possède un plus petit élément est appelé un ensemble bien ordonné.

Principe de la descente infinie : pour montrer que “ $\forall n \in \mathbb{N}, R(n)$ ”, une alternative à la récurrence est de raisonner par l’absurde en supposant qu’il existe $n \in \mathbb{N}$ tel que $\neg[R(n)]$. Ainsi, l’ensemble $F = \{n \in \mathbb{N} / \neg R(n)\}$ possède un minimum n_0 . On peut parfois aboutir à une contradiction en construisant un entier vérifiant $m < n_0$ et $m \in F$.

1.6 Relations d’équivalence

Définition. Une relation binaire sur un ensemble E est une relation d’équivalence si et seulement si R est réflexive, symétrique et transitive.

Exemple fondamental : Soit E et F deux ensembles et $f : E \longrightarrow F$ une application.

Convenons que, pour tout $x, y \in E$, $x R y \iff f(x) = f(y)$.

Alors R est une relation d’équivalence sur E .

Définition. Soit R une relation d’équivalence sur E .

Si $x \in E$, on note \bar{x} l’ensemble des $y \in E$ tels que $x R y$.

\bar{x} s’appelle la classe d’équivalence de x .

On désigne par E/R l’ensemble des classes d’équivalence : $E/R = \{\bar{x} / x \in E\}$.

E/R s’appelle l’ensemble quotient de E par R .

Propriété. pour tout $x, y \in E$, $x R y \iff \bar{x} = \bar{y}$.

Il faut savoir le démontrer.

Définition. Une partition \mathcal{P} de E est une partie de $\mathcal{P}(E)$ telle que :

- pour tout $A, B \in \mathcal{P}$, $A \neq B \implies A \cap B = \emptyset$,
- pour tout $A \in \mathcal{P}$, $A \neq \emptyset$,
- et $\bigcup_{A \in \mathcal{P}} A = E$.

Théorème. Si R est une relation d’équivalence sur E , son ensemble quotient E/R est une partition de E . Réciproquement, si \mathcal{P} est une partition de E , il existe une unique relation d’équivalence R sur E telle que $\mathcal{P} = E/R$: Elle est définie par $\forall x, y \in E$, $[x R y \iff (\exists C \in \mathcal{P}, x, y \in C)]$. En résumé, la donnée d’une relation d’équivalence sur E est équivalente à la donnée d’une partition de E .

Il faut savoir démontrer la première phrase.

Semaine 6 : Résumé de cours

1 Axiome du choix

En voici deux énoncés équivalents.

- Pour tout ensemble I , pour toute famille $(E_i)_{i \in I}$ d'ensembles tous non vides, il existe une famille $(x_i)_{i \in I}$ telle que, pour tout $i \in I$, $x_i \in E_i$.
- Pour tout ensemble E , pour toute relation d'équivalence sur E , il existe un ensemble R tel que l'intersection de R avec chaque classe d'équivalence est un singleton.

2 L'art de la démonstration

La structure d'une démonstration se construit avant tout en fonction de la structure de la propriété à démontrer. En conséquence, on regarde d'abord la cible à atteindre et seulement lorsque c'est nécessaire les hypothèses dont on dispose pour y parvenir. On ne sait pas a priori sous quelles formes ces hypothèses seront utilisées.

2.1 Démontrer une disjonction

Pour montrer $P \vee Q$, on peut supposer que P est fausse et démontrer Q , ou bien supposer que Q est fausse et montrer P .

2.2 Démonstration par disjonction de cas

Pour démontrer une propriété dépendant de certains paramètres, on peut être amené à étudier plusieurs cas selon les valeurs de ces paramètres. Il importe que la réunion des différents cas étudiés recouvre toutes les valeurs possibles des paramètres.

2.3 Résoudre une équation

Définition. Si P est un prédicat sur un ensemble E , “résoudre l'équation $P(x)$, en l'inconnue $x \in E$ ”, c'est calculer $\{x \in E / P(x)\}$ qu'on appelle alors l'ensemble des solutions de l'équation. “calculer” signifie “donner l'ensemble des solutions sous la forme la plus simple possible”.

Remarque. La plupart des équations sont de la forme “ $f(x) = g(x)$ ”, où f et g sont deux applications de E dans un autre ensemble F .

Lorsque $F = \mathbb{R}$, on rencontre parfois des équations de la forme “ $f(x) \leq g(x)$ ”, ou “ $f(x) < g(x)$ ”. Dans ce cas, on parle plutôt d'*inéquations*.

Méthode :

- Précisez d'abord pour quelles valeurs $x \in E$ l'équation a bien un sens. Par exemple, pour une équation de la forme “ $f(x) = g(x)$ ”, il faudra d'abord rechercher les domaines de définition de f et de g .

- Autant que possible, raisonnez par équivalence comme dans l'exemple précédent. Cependant le fait de raisonner par équivalence impose parfois trop de lourdeur à la rédaction. Lorsqu'on choisit de raisonner par implication, après avoir montré que $P(x) \implies x \in S$, pour une certaine partie S de E , il restera à rechercher quels sont les éléments de S qui sont effectivement solutions.

2.4 Implication

Pour montrer $[P \implies Q]$, on suppose que P est vraie (hypothèse supplémentaire) et on démontre Q .

Raisonnement par contraposition : l'implication $P \implies Q$ est logiquement équivalente à $(\neg Q) \implies (\neg P)$, qui est appelée sa contraposée. Ainsi, pour démontrer $P \implies Q$, on peut raisonner par contraposition, c'est-à-dire démontrer $(\neg Q) \implies (\neg P)$: on suppose que Q est fausse et on démontre que P est fausse.

Le raisonnement par l'absurde : cela consiste à supposer que R est fausse et à aboutir à une contradiction, souvent de la forme $S \wedge (\neg S)$.

Pour montrer que $[P \iff Q]$, on montre souvent $[P \implies Q]$ puis la réciproque $[Q \implies P]$.

Dans des cas simples, on peut raisonner par une succession d'équivalences.

Pour montrer que les propriétés P_1, \dots, P_k sont équivalentes, on peut se contenter de montrer le cycle d'implications $P_1 \implies P_2 \implies \dots \implies P_k \implies P_1$. Mais la liste P_1, \dots, P_k n'est pas toujours donnée dans l'ordre idéal. Il convient donc parfois de la réordonner.

2.5 Quantificateurs

Pour montrer que $[\forall x \in E, P(x)]$, le plus souvent, on prend x quelconque dans E , en écrivant "soit $x \in E$ ", puis on démontre $P(x)$.

Pour montrer que $[\exists x \in E, P(x)]$, la méthode directe consiste à construire un élément x de E satisfaisant $P(x)$.

On peut aussi raisonner par l'absurde, en supposant que $[\forall x \in E, \neg(P(x))]$ et en recherchant une contradiction. Il faut cependant que cette nouvelle hypothèse se marie bien avec les autres hypothèses.

Pour montrer que $\neg(\forall x \in E, P(x))$, on peut rechercher un x dans E tel que $P(x)$ est fausse. Dans ce contexte, x est appelé un contre-exemple du prédicat $P(x)$.

2.6 Existence et unicité

Comment montrer une propriété de la forme $[\exists! x \in E, P(x)]$?

Dans de nombreux exercices et problèmes, l'énoncé d'une telle propriété se présente sous la forme : "montrer qu'il existe $x \in E$ tel que $P(x)$, puis montrer que x est unique".

Sur le plan ontologique, tout objet mathématique est unique, mais ce n'est pas du tout ce qui est demandé par l'énoncé. La propriété " x est unique" dépend de P .

En mathématiques, l'unicité est toujours prononcée relativement à un prédicat. Par exemple, 2 est l'unique entier premier et pair, mais 2 n'est pas l'unique entier pair inférieur à 10.

Pour montrer qu'il existe un unique $x \in E$ tel que $P(x)$, il est souvent préférable de séparer l'existence et l'unicité. Pour l'unicité, il faut montrer que $\{x \in E/P(x)\}$ ne possède pas deux éléments distincts, par exemple en supposant qu'il existe $x, y \in E$ vérifiant $P(x)$ et $P(y)$ et en prouvant que $x = y$.

Mais il y a d'autres méthodes :

- On peut montrer que $\{x \in E/P(x)\}$ est un singleton.
- On peut résoudre l'équation " $P(x)$ " en l'inconnue x pour montrer qu'elle admet une seule solution.
- On peut raisonner par analyse-synthèse :

2.7 Démonstration par analyse-synthèse

Ce mode de raisonnement est envisageable lorsque la propriété à démontrer est de la forme $[\exists x \in E, P(x)]$. Il se décompose en deux parties :

◊ **L'analyse** : on suppose qu'il existe $x \in E$ tel que $P(x)$.

C'est a priori très étrange, car on suppose justement ce qu'il faut démontrer !

A partir du fait que x vérifie $x \in E$ et $P(x)$, on cherche à préciser quelles sont les valeurs possibles pour x .

Il est fréquent que l'analyse conduise à une seule valeur possible pour x .

◊ **La synthèse** : Parmi ces différentes valeurs possibles, on en recherche une qui vérifie $P(x)$.

2.8 Démonstrations par récurrence

Principe de récurrence :

Soit $n_0 \in \mathbb{N}^*$. Soit $R(n)$ un prédicat défini pour tout entier $n \geq n_0$.

Si $R(n_0)$ est vraie et si pour tout $n \geq n_0$, $R(n)$ implique $R(n+1)$,

alors pour tout $n \in \mathbb{N}$ tel que $n \geq n_0$, $R(n)$ est vraie.

Principe de récurrence ascendante finie : Soit $n, m \in \mathbb{N}$ avec $n \leq m$.

Soit $R(k)$ un prédicat défini pour $k \in \llbracket n, m \rrbracket$.

Si $R(n)$ est vraie et si pour tout $k \in \llbracket n, m-1 \rrbracket$, $R(k)$ implique $R(k+1)$,

alors $R(k)$ est vraie pour tout $k \in \llbracket n, m \rrbracket$.

Principe de récurrence descendante finie : Soit $n, m \in \mathbb{N}$ avec $n \leq m$.

Soit $R(k)$ un prédicat défini pour $k \in \llbracket n, m \rrbracket$.

Si $R(m)$ est vraie et si pour tout $k \in \llbracket n+1, m \rrbracket$, $R(k)$ implique $R(k-1)$,

alors $R(k)$ est vraie pour tout $k \in \llbracket n, m \rrbracket$.

Principe de récurrence forte :

Soit $n_0 \in \mathbb{N}$. Soit $R(n)$ un prédicat défini pour tout entier $n \geq n_0$.

Si $R(n_0)$ est vraie et si pour tout $n \geq n_0$, $[\forall k \in \{n_0, \dots, n\}, R(k)]$ implique $R(n+1)$,

alors pour tout $n \in \mathbb{N}$ tel que $n \geq n_0$, $R(n)$ est vraie.

Principe de récurrence double :

Soit $n_0 \in \mathbb{N}$. Soit $R(n)$ un prédicat défini pour tout entier $n \geq n_0$.

Si $R(n_0)$ et $R(n_0+1)$ sont vraies et si

pour tout $n \geq n_0$, $[R(n) \wedge R(n+1)]$ implique $R(n+2)$,

alors pour tout $n \in \mathbb{N}$ tel que $n \geq n_0$, $R(n)$ est vraie.

3 \mathbb{Z}

3.1 Construction de \mathbb{Z}

Définition. $\mathbb{Z} = \mathbb{N}^2 / R$, où R est la relation d'équivalence suivante sur \mathbb{N}^2 :

$\forall a, b, c, d \in \mathbb{N}, (a, b)R(c, d) \iff a + d = b + c$.

Si $(\overline{a, b}), (\overline{c, d}) \in \mathbb{Z}$, on pose $\overline{a, b} + \overline{c, d} \triangleq \overline{a + c, b + d}$

et $\overline{a, b} \times \overline{c, d} \triangleq \overline{ac + bd, ad + bc}$.

3.2 L'anneau \mathbb{Z}

Propriété. L'addition sur \mathbb{Z} vérifie les propriétés suivantes :

- $0 \triangleq \overline{(0,0)}$ est neutre : $\forall m \in \mathbb{Z}, m + 0 = 0 + m = m$.
- Associativité : $\forall n, m, k \in \mathbb{Z}, (n + m) + k = n + (m + k)$.
- Commutativité : $\forall n, m \in \mathbb{Z}, n + m = m + n$.
- Tout élément possède un symétrique : $\forall n \in \mathbb{Z}, \exists m \in \mathbb{Z}, n + m = 0$.

On résume ces propriétés en disant que $(\mathbb{Z}, +)$ est un groupe commutatif.

Propriété. La multiplication sur \mathbb{Z} vérifie les propriétés suivantes :

- $1 \triangleq \overline{(1,0)}$ est neutre : $\forall m \in \mathbb{Z}, m \times 1 = 1 \times m = m$.
- Distributivité de la multiplication par rapport à l'addition :
 $\forall n, m, p \in \mathbb{Z}, n(m + p) = nm + np$.
- Associativité : $\forall n, m, k \in \mathbb{Z}, (n \times m) \times k = n \times (m \times k)$.
- Commutativité : $\forall n, m \in \mathbb{Z}, n \times m = m \times n$.

On résume ces propriétés et le fait que $(\mathbb{Z}, +)$ est un groupe commutatif en disant que $(\mathbb{Z}, +, \times)$ est un anneau commutatif.

3.3 L'ordre de \mathbb{Z}

Compatibilité de la relation d'ordre avec l'addition :

$$\forall x, y, x', y' \in \mathbb{Z}, [x \leq y] \wedge [x' \leq y'] \implies x + x' \leq y + y'.$$

Identification de \mathbb{N} avec une partie de \mathbb{Z} : on identifie $n \in \mathbb{N}$ avec $\overline{(n,0)}$.

Règle des signes :

- $\forall n \in \mathbb{Z}, n \geq 0 \iff n \in \mathbb{N}$.
- $\forall n, m \in \mathbb{Z}, ([n \geq 0] \wedge [m \geq 0]) \implies nm \geq 0$.
- $\forall n \in \mathbb{Z}, n \geq 0 \iff -n \leq 0$.
- $\forall x, y, a \in \mathbb{Z}, \begin{cases} \text{si } a \geq 0, & x \leq y \implies ax \leq ay, \\ \text{si } a \leq 0, & x \leq y \implies ax \geq ay. \end{cases}$

Propriété. Toute partie non vide majorée de \mathbb{Z} possède un maximum.

Toute partie non vide minorée de \mathbb{Z} possède un minimum.

Définition. Soit $n \in \mathbb{Z}$.

Le signe de n au sens large est

- 1 ou bien “positif” lorsque $n \geq 0$,
- -1 ou bien “négatif” lorsque $n \leq 0$.

Le signe de n au sens strict est

- 1 ou bien “strictement positif” lorsque $n > 0$,
- 0 ou bien “nul” lorsque $n = 0$,
- -1 ou bien “strictement négatif” lorsque $n < 0$.

Définition. Pour tout $n \in \mathbb{Z}$, on note $|n| = \max\{-n, n\}$.

Propriété. Pour tout $n \in \mathbb{Z}, n \leq |n|$, avec égalité si et seulement si $n \geq 0$. De plus $|n|^2 = n^2$.

Propriété. $\forall n, m \in \mathbb{Z}, |nm| = |n||m|$.

Propriété. \mathbb{Z} est un anneau intègre, c'est-à-dire que, pour tout $n, m \in \mathbb{Z}$,
 $nm = 0 \implies [(n = 0) \vee (m = 0)]$.

Remarque. Soit D une partie de \mathbb{R} .

L'ensemble des applications de D dans \mathbb{R} , noté $\mathcal{F}(D, \mathbb{R})$, muni de l'addition et du produit entre fonctions, est un anneau. Les éléments neutres sont respectivement l'application identiquement nulle et l'application constante égale à 1.

Cependant cet anneau n'est pas intègre car on peut avoir $fg = 0$ alors que $f \neq 0$ et $g \neq 0$.

Cet exemple est à connaître.

Propriété. Soit $n, m \in \mathbb{Z}^2$. $nm \geq 0$ si et seulement si n et m sont de même signe au sens large.

Propriété. Soit $a, b, n \in \mathbb{Z}$ tels que $an \leq bn$. Si $n > 0$ alors $a \leq b$ et si $n < 0$, alors $a \geq b$.

Inégalité triangulaire : $\forall n, m \in \mathbb{Z}$, $|n + m| \leq |n| + |m|$, avec égalité si et seulement si n et m sont de même signe.

Il faut savoir le démontrer.

3.4 Les sous-groupes de \mathbb{Z}

Division euclidienne dans \mathbb{Z} : Pour tout $a, b \in \mathbb{Z}$ avec $b \neq 0$, il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leq r < |b|$. q et r sont appelés les quotient et reste.

Définition. Une partie G de \mathbb{Z} est un sous-groupe de \mathbb{Z} si et seulement si

- $G \neq \emptyset$,
- $\forall (x, y) \in G^2$, $x + y \in G$,
- $\forall x \in G$, $-x \in G$.

Propriété. Soit G un sous-groupe de \mathbb{Z} .

Pour tout $n \in \mathbb{Z}$ et $g \in G$, $ng \in G$.

Pour tout $n \in G$, $n\mathbb{Z} \subset G$.

Il faut savoir le démontrer.

Corollaire. Soit G un sous-groupe de \mathbb{Z} . Alors $\boxed{1 \in G \iff G = \mathbb{Z}}$.

Théorème. Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les $n\mathbb{Z}$, où $n \in \mathbb{N}$.

Il faut savoir le démontrer.

Propriété. Une intersection de sous-groupes de \mathbb{Z} est un sous-groupe de \mathbb{Z} .

Il faut savoir le démontrer.

Définition. Soit B une partie de \mathbb{Z} . Le groupe engendré par B est l'intersection des sous-groupes de \mathbb{Z} contenant B . C'est le plus petit sous-groupe contenant B . On le note $Gr(B)$.

Propriété. Soient B et C deux parties de \mathbb{Z} telles que $C \subset B$. Alors $Gr(C) \subset Gr(B)$.

Propriété. $Gr(B) = \left\{ \sum_{i=1}^n a_i b_i / n \in \mathbb{N}, (a_1, \dots, a_n) \in \mathbb{Z}^n, (b_1, \dots, b_n) \in B^n \right\}$.

Il faut savoir le démontrer.

3.5 Divisibilité

Définition. Soit $n, m \in \mathbb{Z}$. $n|m$ si et seulement si il existe $k \in \mathbb{Z}$ tel que $m = kn$.

Propriété. Soit $a, b \in \mathbb{Z}$ avec $b \neq 0$. Alors b divise a si et seulement si le reste de la division euclidienne de a par b vaut 0.

Remarque. Tout entier relatif divise 0 mais 0 ne divise que lui-même.

Remarque. Si $n, m \in \mathbb{Z}$, n divise m si et seulement si $|n|$ divise $|m|$ dans \mathbb{N} .

Propriété. Soit $a, b, c \in \mathbb{Z}$.

- si $b|a$, alors pour tout $\alpha \in \mathbb{Z}$, $b|\alpha a$.
- Si $b|a$ et $b|c$, alors $b|(a + c)$.
- Si $b|a$ et $d|c$, alors $bd|ac$.
- si $b|a$, pour tout $p \in \mathbb{N}$, $b^p|a^p$.

Propriété. Soit $p \in \mathbb{N}$ et $b, a_1, \dots, a_p, c_1, \dots, c_p \in \mathbb{Z}$.

Si pour tout $i \in \{1, \dots, p\}$, $b \mid a_i$, alors $b \mid \sum_{i=1}^p c_i a_i$.

Propriété. Pour tout $(a, b) \in \mathbb{Z}^2$, $a \mid b \iff b\mathbb{Z} \subseteq a\mathbb{Z}$.

Propriété. La relation de divisibilité est réflexive et transitive.

Remarque. La relation de divisibilité n'est pas un ordre sur \mathbb{Z} car $-1 \mid 1$ et $1 \nmid -1$.

Définition. Soit $a, b \in \mathbb{Z}$. On dit que a et b sont premiers entre eux (ou étrangers) si et seulement si les seuls diviseurs communs de a et b sont 1 et -1 .

Définition. Soit $n \in \mathbb{N}$ avec $n \geq 2$ et $a_1, \dots, a_n \in \mathbb{Z}$.

- a_1, \dots, a_n sont deux à deux premiers entre eux si et seulement si, pour tout $i, j \in \{1, \dots, n\}$ avec $i \neq j$, a_i et a_j sont premiers entre eux.
- a_1, \dots, a_n sont globalement premiers entre eux si et seulement si les seuls diviseurs communs de a_1, \dots, a_n sont 1 et -1 .

Propriété. Si $p \in \mathbb{P}$ et $a \in \mathbb{Z}$, alors ou bien $p \mid a$, ou bien p et a sont premiers entre eux.

Propriété. Soit $p \in \mathbb{N} \setminus \{0, 1\}$. Les propriétés suivantes sont équivalentes :

1. p est premier.
2. p est premier avec tout entier qu'il ne divise pas.
3. p est premier avec tout nombre premier contenu dans $\llbracket 2, \sqrt{p} \rrbracket$.

Il faut savoir le démontrer.

le crible d'Ératosthène : pour dresser la liste ordonnée des nombres premiers inférieurs à n , initialement, on pose $L = \llbracket 2, n \rrbracket$ et on positionne un curseur sur 2. On supprime de L les multiples de 2, sauf 2, puis on déplace le curseur sur l'entier suivant de L : il s'agit de 3, car il n'a pas été supprimé. On supprime de L tous les multiples de 3, sauf 3, etc. Ainsi, à chaque itération, on déplace le curseur sur le premier entier suivant qui est encore dans L et l'on supprime de L tous les multiples du curseur, sauf le curseur. On arrête l'algorithme dès que le curseur est strictement supérieur à \sqrt{n} .

Théorème. \mathbb{P} est de cardinal infini.

Il faut savoir le démontrer.

3.6 Congruence

Définition. Relation de congruence : Soit $k \in \mathbb{Z}$. $\forall n, m \in \mathbb{Z}$, $n \equiv m [k] \iff k \mid (n - m)$.

C'est la relation de congruence modulo k , qui est une relation d'équivalence.

Propriété. Soit $a, b \in \mathbb{Z}$ avec $b \neq 0$: il existe $r \in \{0, \dots, |b| - 1\}$ tel que $a \equiv r [b]$.
 r est le reste de la division euclidienne de a par b .

Notation. La classe d'équivalence de n modulo k est $\bar{n} = \{n + kh / h \in \mathbb{Z}\} \triangleq n + k\mathbb{Z}$.

Compatibilités de la congruence avec l'addition et la multiplication :

Pour tout $n, m, h, k \in \mathbb{Z}$,

- $n \equiv m [k] \implies h + n \equiv h + m [k]$ et
- $n \equiv m [k] \implies hn \equiv hm [k]$.

Corollaire : $\forall a, b, k \in \mathbb{Z}$, $\forall n \in \mathbb{N}$, $(a \equiv b [k] \implies a^n \equiv b^n [k])$.

Petit théorème de Fermat : (Admis pour le moment) Si $p \in \mathbb{P}$ et $a \in \mathbb{Z}$,
 $(a \not\equiv 0 [p]) \implies a^{p-1} \equiv 1 [p]$, donc dans tous les cas, $a^p \equiv a [p]$.

Définition. Soit $x_0 \in \mathbb{R}$. Pour tout $x, y \in \mathbb{R}$, on dit que x est congru à y modulo x_0 et on note $x \equiv y [x_0]$ si et seulement si il existe $k \in \mathbb{Z}$ tel que $x - y = kx_0$. La relation de congruence modulo x_0 est une relation d'équivalence sur \mathbb{R} . Elle est compatible avec l'addition entre réels mais pas avec la multiplication entre réels.

3.7 PGCD

Définition. Soit $(a, b) \in \mathbb{Z}^2$. $a\mathbb{Z} + b\mathbb{Z}$ est le sous-groupe de \mathbb{Z} engendré par $\{a, b\}$, donc il existe un unique $d \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. On dit que d est le PGCD de a et b . On note $d = \text{PGCD}(a, b) = a \wedge b$.

Propriété. Pour la relation d'ordre de divisibilité dans \mathbb{N} , $a \wedge b = \inf_{|} \{|a|, |b|\}$.

Il faut savoir le démontrer.

Remarque. Lorsque a ou b est un entier relatif non nul, au sens de l'ordre naturel sur \mathbb{N} , $a \wedge b$ est aussi le plus grand diviseur commun de a et b .

Propriété. a et b sont premiers entre eux si et seulement si $a \wedge b = 1$.

Définition. Plus généralement, si $k \in \mathbb{N}^*$ et si $a_1, \dots, a_k \in \mathbb{Z}$, on dit que d est le PGCD de a_1, \dots, a_k si et seulement si $d \in \mathbb{N}$ et $d\mathbb{Z} = a_1\mathbb{Z} + \dots + a_k\mathbb{Z} = \text{Gr}\{a_1, \dots, a_k\}$. Alors $d = \inf_{|} \{a_1, \dots, a_k\}$.

Si B est une partie quelconque de \mathbb{Z} , on dit que d est le PGCD de B si et seulement si $d \in \mathbb{N}$ et $d\mathbb{Z} = \text{Gr}(B)$. Alors $d = \inf_{|}(B)$.

Propriété. Soit $k \in \mathbb{N}$, $a_1, \dots, a_k \in \mathbb{Z}$ et $h \in \{1, \dots, k\}$.

— Commutativité du PGCD :

$\text{PGCD}(a_1, \dots, a_k)$ ne dépend pas de l'ordre de a_1, \dots, a_k .

— Associativité du PGCD :

$\text{PGCD}(a_1, \dots, a_k) = \text{PGCD}(a_1, \dots, a_h) \wedge \text{PGCD}(a_{h+1}, \dots, a_k)$.

— Distributivité de la multiplication par rapport au PGCD : pour tout $\alpha \in \mathbb{Z}$,

$\text{PGCD}(\alpha a_1, \dots, \alpha a_k) = |\alpha| \text{PGCD}(a_1, \dots, a_k)$.

Il faut savoir le démontrer.

3.8 PPCM

Définition. Soit $(a, b) \in \mathbb{Z}^2$. $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de \mathbb{Z} , donc il existe un unique entier naturel m tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. On dit que m est un PPCM de a et b et on note $m = a \vee b$.

Propriété. Soit $(a, b) \in \mathbb{Z}^2$. $a \vee b = \sup_{|} \{|a|, |b|\}$.

Remarque. Lorsque a et b sont des entiers relatifs non nuls, $a \vee b = \min_{\leq} \{k \in \mathbb{N}^* / a|k \text{ et } b|k\}$.

Définition. Plus généralement, si $k \in \mathbb{N}^*$ et si $a_1, \dots, a_k \in \mathbb{Z}$, on dit que m est le PPCM de a_1, \dots, a_k si et seulement si $m \in \mathbb{N}$ et $m\mathbb{Z} = a_1\mathbb{Z} \cap \dots \cap a_k\mathbb{Z}$. Alors $m = \sup_{|} \{a_1, \dots, a_k\}$.

Si B est une partie quelconque de \mathbb{Z} , on dit que m est le PPCM de B si et seulement si $m \in \mathbb{N}$ et $m\mathbb{Z} = \bigcap_{b \in B} b\mathbb{Z}$. Alors $m = \sup_{|}(B)$.

Remarque. Dans ce contexte, on convient que si $B = \emptyset$, $\bigcap_{b \in B} b\mathbb{Z} = \mathbb{Z}$, donc 1 est le PPCM de \emptyset .

Ainsi, toute partie de \mathbb{N} possède une borne supérieure et une borne inférieure pour la relation d'ordre de divisibilité. On dit que l'ensemble ordonné $(\mathbb{N}, |)$ est un treillis complet.

Propriété. Soit $k \in \mathbb{N}$, $a_1, \dots, a_k \in \mathbb{Z}$ et $h \in \{1, \dots, k\}$.

— Commutativité du PPCM :

$\text{PPCM}(a_1, \dots, a_k)$ ne dépend pas de l'ordre de a_1, \dots, a_k .

— Associativité du PPCM :

$\text{PPCM}(a_1, \dots, a_k) = \text{PPCM}(a_1, \dots, a_h) \vee \text{PPCM}(a_{h+1}, \dots, a_k)$.

- Distributivité de la multiplication par rapport au PPCM :
pour tout $\alpha \in \mathbb{Z}$, $PPCM(\alpha a_1, \dots, \alpha a_k) = |\alpha| PPCM(a_1, \dots, a_k)$.

3.9 Les théorèmes de l'arithmétique

Théorème de Bézout. Soit $(a, b) \in \mathbb{Z}^2$.

a et b sont premiers entre eux si et seulement si : $\exists (u, v) \in \mathbb{Z}^2$ $ua + vb = 1$.

Il faut savoir le démontrer.

Théorème de Bézout (généralisation). Soit $n \in \mathbb{N}$ avec $n \geq 2$ et $a_1, \dots, a_n \in \mathbb{Z}$.

a_1, \dots, a_n sont globalement premiers entre eux si et seulement si :

$\exists u_1, \dots, u_n \in \mathbb{Z}$, $u_1 a_1 + \dots + u_n a_n = 1$.

Propriété. Soit $(a, b) \in \mathbb{Z}^2$. Posons $d = a \wedge b$.

Alors il existe $(a', b') \in \mathbb{Z}^2$, avec a' et b' premiers entre eux, tel que $a = a'd$ et $b = b'd$.

Théorème de Gauss. Soit $(a, b, c) \in \mathbb{Z}^3$. Si $a|bc$ avec a et b premiers entre eux, alors $a|c$.

Il faut savoir le démontrer.

Corollaire. Soit $p, a, b \in \mathbb{Z}$. Si $p | ab$ et si p est premier, alors $p | a$ ou $p | b$.

Corollaire. Soit $(a, b, c) \in \mathbb{Z}^3$, $n \in \mathbb{N}^*$ et $a_1, \dots, a_n \in \mathbb{Z}$.

◇ Si $a \wedge b = a \wedge c = 1$, alors $a \wedge bc = 1$.

◇ On en déduit que, si $a \wedge b = 1$, $\forall (k, l) \in (\mathbb{N}^*)^2$ $a^k \wedge b^l = 1$.

◇ Si $a|b$, $c|b$ et $a \wedge c = 1$ alors $ac|b$. Par récurrence, on en déduit que

si pour tout $i \in \{1, \dots, n\}$, $a_i|b$ et si $i \neq j \implies a_i \wedge a_j = 1$, alors $a_1 \times \dots \times a_n | b$.

◇ $|ab| = (a \wedge b)(a \vee b)$. En particulier, $a \wedge b = 1 \implies a \vee b = |ab|$.

Il faut savoir le démontrer.

Théorème fondamental de l'arithmétique. Pour tout $a \in \mathbb{N}^*$, il existe une unique famille $(\nu_p)_{p \in \mathbb{P}} \in \mathbb{N}^{(\mathbb{P})}$ (i.e telle que $\{p \in \mathbb{P} / \nu_p \neq 0\}$ est fini) telle que $a = \prod_{p \in \mathbb{P}} p^{\nu_p}$.

C'est la décomposition de a en facteurs premiers. ν_p s'appelle la valuation p -adique de a .

Il faut savoir le démontrer.

Propriété. si $a = \prod_{p \in \mathbb{P}} p^{\nu_p}$ et $b = \prod_{p \in \mathbb{P}} p^{\mu_p}$, Alors $a | b \iff [\forall p \in \mathbb{P}, \nu_p \leq \mu_p]$.

De plus, $a \wedge b = \prod_{p \in \mathbb{P}} p^{\min(\nu_p, \mu_p)}$ et $a \vee b = \prod_{p \in \mathbb{P}} p^{\max(\nu_p, \mu_p)}$.

Lemme d'Euclide. Soient $(a, b) \in \mathbb{Z}^2$ avec $b \neq 0$. Notons q et r les quotient et reste de la division euclidienne de a par b . Alors $a \wedge b = b \wedge r$.

Algorithme d'Euclide. Soit $a_0, a_1 \in \mathbb{N}^*$ avec $a_0 > a_1$.

Pour $i \geq 1$, tant que $a_i \neq 0$, on note a_{i+1} le reste de la division euclidienne de a_{i-1} par a_i .

On définit ainsi une suite strictement décroissante d'entiers naturels $(a_i)_{0 \leq i \leq N}$ telle que $a_N = 0$.

Alors $a_0 \wedge a_1 = a_{N-1}$.

De plus, lorsque $a_0 \wedge a_1 = 1$, cet algorithme permet de calculer des entiers s_0 et t_0 tels que $1 = s_0 a_0 + t_0 a_1$.

À connaître précisément.

Exercice. Soit $a, b, c \in \mathbb{Z}$ avec a et b non nuls.

Résoudre l'équation de Bézout (B) : $au + bv = c$ en l'inconnue $(u, v) \in \mathbb{Z}^2$.

À connaître.

Semaine 7 : Résumé de cours

1 \mathbb{Q}

Définition. On définit une relation binaire R sur $\mathbb{Z} \times \mathbb{Z}^*$ par $(a, b)R(c, d) \iff ad = bc$. C'est une relation d'équivalence. On pose $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/R$.

Pour tout $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, on note $\frac{a}{b} = \overline{(a, b)}$.

Pour l'écriture $\frac{a}{b}$, on dit que a est son numérateur et que b est son dénominateur.

Pour tout $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*$, on pose $\frac{a}{b} \times \frac{c}{d} \triangleq \frac{ac}{bd}$ et $\frac{a}{b} + \frac{c}{d} \triangleq \frac{ad + cb}{bd}$.

On définit ainsi une addition et une multiplication sur \mathbb{Q} .

Propriété. $(\mathbb{Q}, +, \times)$ est un corps, c'est-à-dire que

- $(\mathbb{Q}, +, \times)$ est un anneau,
- \mathbb{Q} n'est pas réduit à $\{0\}$ (on note $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$),
- \mathbb{Q} est commutatif,
- tout élément non nul de \mathbb{Q} est inversible : $\forall x \in \mathbb{Q}^*, \exists y \in \mathbb{Q}^*, xy = 1$.

Propriété. Comme tout corps, \mathbb{Q} est intègre, c'est-à-dire que, pour tout $x, y \in \mathbb{Q}$, $xy = 0 \implies [(x = 0) \vee (y = 0)]$.

La démonstration dans un corps quelconque est à connaître.

Propriété. L'application $\begin{matrix} \mathbb{Z} & \longrightarrow & \mathbb{Q} \\ n & \longmapsto & \frac{n}{1} \end{matrix}$ permet d'identifier \mathbb{Z} avec une partie de \mathbb{Q} .

On parvient à prolonger l'ordre de \mathbb{Z} en un ordre sur \mathbb{Q} , qui reste compatible avec l'addition et qui vérifie la règle des signes pour le produit.

On prolonge aussi sur \mathbb{Q} la notion de valeur absolue ainsi que ses propriétés vues dans \mathbb{Z} .

Propriété. Pour tout $x \in \mathbb{Q}$, il existe un unique couple (a, b) tel que $x = \frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, tels que a et b sont premiers entre eux. On dit alors que $\frac{a}{b}$ est la forme irréductible de x .

Démonstration à connaître.

Exercice. Montrer que $\sqrt{2}$ est irrationnel.

A connaître.

\mathbb{Q} est archimédien :

Soit x et y deux rationnels strictement positifs. Alors il existe $n \in \mathbb{N}$ tel que $x < ny$.

2 L'ensemble \mathbb{R} des réels

2.1 Corps totalement ordonnés

Définition. Soit $(K, +, \times)$ un corps muni d'une relation d'ordre \preceq .

On dit que $(K, +, \times, \preceq)$ est un corps ordonné si et seulement si

- *Compatibilité avec l'addition* : $\forall x, y, z \in K, [x \preceq y] \implies [x + z \preceq y + z]$.
- *Compatibilité avec le produit, règle des signes* :
 $\forall x, y \in K, [0 \preceq x] \wedge [0 \preceq y] \implies [0 \preceq xy]$.

2.2 Bornes supérieures

Définition. Soit E un ensemble muni d'une relation d'ordre \preceq . Soit $A \subset E$.

Lorsque l'ensemble des majorants de A possède un plus petit élément, ce minimum est appelé la borne supérieure de A , et noté $\sup A$.

Lorsque l'ensemble des minorants de A possède un plus grand élément, ce maximum est appelé la borne inférieure de A , et noté $\inf A$.

Propriété. Soit (E, \preceq) un ensemble ordonné et $A \subset E$.

Si A possède un maximum, alors A possède une borne supérieure et $\sup A = \max A$.

Cependant, il est "fréquent" que A ne possède pas de maximum, mais possède une borne supérieure. Dans ce cas, $\sup A \notin A$.

Propriété. Soit (E, \preceq) un ensemble ordonné et soit $A, B \in \mathcal{P}(E)$.

Si A et B possèdent des bornes supérieures : si $B \subset A$, alors $\sup(B) \leq \sup(A)$.

Si A et B possèdent des bornes inférieures : si $B \subset A$, alors $\inf(B) \geq \inf(A)$.

Démonstration à connaître.

2.3 Une caractérisation de \mathbb{R} .

Caractérisation de \mathbb{R} : (admise)

Il existe au moins un corps K totalement ordonné dans lequel toute partie non vide majorée admet une borne supérieure.

De plus si K' est un autre corps totalement ordonné dans lequel toute partie non vide majorée admet une borne supérieure, il existe une bijection f de K dans K' telle que f est un morphisme de corps ordonnés, c'est-à-dire :

- $\forall x, y \in K, x \leq y \implies f(x) \leq f(y)$,
- $\forall x, y \in K, f(x + y) = f(x) + f(y)$,
- $\forall x, y \in K, f(xy) = f(x)f(y)$,
- $f(1_K) = 1_{K'}$.

Cela signifie que, quitte à renommer x en $f(x)$, K et K' sont égaux, tant que dans K et K' on se contente d'utiliser leurs structures de corps totalement ordonnés.

Ainsi, à un morphisme bijectif près, il existe un unique corps totalement ordonné dans lequel toute partie non vide majorée admet une borne supérieure. Il est noté \mathbb{R} et ses éléments sont appelés les réels.

Il existe un morphisme injectif de corps ordonné de \mathbb{Q} dans \mathbb{R} , qui permet d'identifier \mathbb{Q} avec une partie de \mathbb{R} .

Propriété. Toute partie non vide minorée de \mathbb{R} possède une borne inférieure.

Il faut savoir le démontrer.

Passage à la borne supérieure (resp : inférieure) : Soit (E, \preceq) un ensemble ordonné et soit A une partie de E possédant une borne supérieure.

◇ Soit $e \in E$. Alors $\sup(A) \leq e \iff [\forall a \in A, a \leq e]$.

Le fait de passer de la propriété " $\forall a \in A, a \leq e$ " à l'affirmation " $\sup(A) \leq e$ " s'appelle le *passage à la borne supérieure*.

◇ Il faut savoir le justifier : si $[\forall a \in A, a \leq e]$, alors e est un majorant de A , or $\sup(A)$ est le plus petit des majorants, donc $\sup(A) \leq e$.

◇ ATTENTION, en général, $\sup(A) \notin A$, donc le passage à la borne supérieure ne se réduit pas au fait d'appliquer la propriété " $\forall a \in A, a \leq e$ " avec $a = \sup(A)$.

◇ De même, si B est une partie de E possédant une borne inférieure, le principe du passage à la borne inférieure consiste à passer de la propriété, " $\forall a \in A, a \geq e$ " à " $\inf(A) \geq e$ ".

Propriété. Soit A une partie non vide majorée de \mathbb{R} . Soit $s \in \mathbb{R}$. Alors

$s = \sup(A) \iff [\forall a \in A, a \leq s] \wedge [\forall \varepsilon > 0, \exists a \in A, s - \varepsilon < a]$.

Démonstration à connaître.

Exercice. Soit A une partie de \mathbb{R} non vide et majorée. Montrer qu'il existe une suite $(x_n)_{n \in \mathbb{N}}$ d'éléments de A qui converge vers $\sup(A)$.

A savoir faire.

Propriété. Soit A une partie non vide minorée de \mathbb{R} . Soit $m \in \mathbb{R}$. Alors
 $m = \inf(A) \iff [\forall a \in A, a \geq m] \wedge [\forall \varepsilon > 0, \exists a \in A, m + \varepsilon > a]$.

2.4 La droite réelle achevée

Définition. On appelle droite réelle achevée l'ensemble $\overline{\mathbb{R}} \triangleq \mathbb{R} \cup \{-\infty, +\infty\}$, sur lequel l'ordre dans \mathbb{R} est prolongé par les conditions : $\forall x \in \mathbb{R}, -\infty < x < +\infty$.

Propriété. $(\overline{\mathbb{R}}, \leq)$ est un ensemble totalement ordonné dans lequel toute partie possède une borne inférieure et une borne supérieure. En particulier, toute partie A de \mathbb{R} possède une borne supérieure dans $\overline{\mathbb{R}}$. De plus, $\sup(A) = +\infty \iff A$ non majorée et $\sup(A) = -\infty \iff A = \emptyset$.

2.5 Les intervalles

Définition.

- Pour tout $a, b \in \overline{\mathbb{R}}$, l'intervalle $]a, b[$ est défini par $]a, b[= \{x \in \mathbb{R} / a < x < b\}$.
- Pour tout $a, b \in \mathbb{R}$, l'intervalle $[a, b]$ est défini par $[a, b] = \{x \in \mathbb{R} / a \leq x \leq b\}$.
- Si $a \in \mathbb{R}$ et $b \in \overline{\mathbb{R}}$, les intervalles $[a, b[$ et $]b, a]$ sont définis par :
 $[a, b[= \{x \in \mathbb{R} / a \leq x < b\}$ et $]b, a] = \{x \in \mathbb{R} / b < x \leq a\}$.
- En particulier, $\mathbb{R} =]-\infty, +\infty[$ et $\emptyset =]0, -1[$ sont des intervalles.

Définition.

- Un intervalle est ouvert si et seulement si il est de la première forme $]a, b[$ avec $a, b \in \overline{\mathbb{R}}$.
- On dit qu'un intervalle est fermé si et seulement si son complémentaire est une réunion d'un ou deux d'intervalles ouverts.
- Ainsi, $[a, b]$ est fermé lorsque $a, b \in \mathbb{R}$, mais $[a, +\infty[$ est aussi fermé (avec $a \in \mathbb{R}$).
- \emptyset et \mathbb{R} sont à la fois ouverts et fermés.
- $[0, 1[$ n'est ni ouvert ni fermé. On dit qu'il est semi-ouvert ou semi-fermé.
- Les intervalles fermés bornés sont de la forme $[a, b]$ avec $a, b \in \mathbb{R}$. On les appelle aussi des segments.

Définition. Une partie A de \mathbb{R} est convexe si et seulement si pour tout $a, b \in A$ avec $a < b$, $[a, b] \subset A$.

Théorème. Les parties convexes de \mathbb{R} sont exactement ses intervalles.

Il faut savoir le démontrer.

Corollaire. Une intersection d'intervalles de \mathbb{R} est un intervalle de \mathbb{R} .

Propriété. Si une famille d'intervalles est d'intersection non vide, l'union de ces intervalles est encore un intervalle.

Il faut savoir le démontrer.

2.6 la valeur absolue

Propriété. Le signe au sens large du produit de deux réels est égal au produit des signes de ces réels.

Définition. Pour tout $x \in \mathbb{R}$, on note $|x| = \max\{-x, x\}$.

$\forall x, y \in \mathbb{R}, |xy| = |x||y|$.

Inégalité triangulaire : $\forall x, y \in \mathbb{R}, |x + y| \leq |x| + |y|$, avec égalité si et seulement si x et y sont de même signe.

Corollaire de l'inégalité triangulaire : $\forall x, y \in \mathbb{R}, ||x| - |y|| \leq |x - y|$.

A savoir démontrer.

Formule : Pour tout $a, b \in \mathbb{R}$,

$$\min(a, b) = \frac{(a + b) - |a - b|}{2} \text{ et } \max(a, b) = \frac{(a + b) + |a - b|}{2}.$$

Distance entre réels : Lorsque $x, y \in \mathbb{R}$, la quantité $d(x, y) = |x - y|$ est appelée la distance entre les deux réels x et y . Elle vérifie l'inégalité triangulaire : $d(x, z) \leq d(x, y) + d(y, z)$.

2.7 Propriétés usuelles des réels

Propriété. \mathbb{R} est archimédien : Pour tout $a, b \in \mathbb{R}_+^*$, $\exists n \in \mathbb{N}, na > b$.

Définition. Soit A une partie de \mathbb{R} . On dit que A est dense dans \mathbb{R} si et seulement si pour tout $x, y \in \mathbb{R}$ avec $x < y$, il existe $a \in A$ tel que $x \leq a \leq y$.

Propriété. A est dense dans \mathbb{R} si et seulement si, pour tout $x \in \mathbb{R}$, il existe une suite $(a_n)_{n \in \mathbb{N}}$ d'éléments de A telle que $a_n \xrightarrow{n \rightarrow +\infty} x$.

Il faut savoir le démontrer.

Propriété. \mathbb{Q} et $\mathbb{R} \setminus \mathbb{Q}$ sont denses dans \mathbb{R} .

Définition. Soit $x \in \mathbb{R}$. On appelle partie entière de x le plus grand entier relatif inférieur ou égal à x . Elle est notée $[x]$. C'est l'unique entier n tel que $n \leq x < n + 1$.

On appelle partie entière supérieure de x le plus petit entier supérieur ou égal à x . Elle est notée $\lceil x \rceil$. C'est l'unique entier n tel que $n - 1 < x \leq n$.

Une inégalité très utile : Pour tout $x, y \in \mathbb{R}$, $|xy| \leq \frac{x^2 + y^2}{2}$.

A savoir établir.

3 Développement décimal

3.1 Développement décimal d'un entier naturel

Propriété. Si (x_n) une suite strictement croissante d'entiers naturels, on montre par récurrence que pour tout $n \in \mathbb{N}$, $x_n \geq n$.

Définition. Les chiffres en base 10 sont $0, 1, \dots, 9$.

Théorème. Pour tout $n \in \mathbb{N}$, il existe une unique suite presque nulle de chiffres $(a_k)_{k \in \mathbb{N}} \in \{0, \dots, 9\}^{(\mathbb{N})}$ telle que $n = \sum_{k \in \mathbb{N}} a_k 10^k$.

Remarque. On peut généraliser et développer en base a où a est un entier supérieur ou égal à 2.

CNS de divisibilité : Soit $n \in \mathbb{N}$, dont le développement décimal est noté

$n = \sum_{k \in \mathbb{N}} a_k 10^k$. On note $s = \sum_{k \in \mathbb{N}} a_k$ la somme des chiffres de n .

- n est divisible par 2 si et seulement si $a_0 \in \{0, 2, 4, 6, 8\}$.
- n est divisible par 5 si et seulement si $a_0 \in \{0, 5\}$.
- n est divisible par 10 si et seulement si $a_0 = 0$.

- n est divisible par 3 si et seulement si $s \equiv 0 \pmod{3}$.
- n est divisible par 9 si et seulement si $s \equiv 0 \pmod{9}$.
- n est divisible par 11 si et seulement si $\sum_{k \in \mathbb{N}} (-1)^k a_k \equiv 0 \pmod{11}$.

Il faut savoir le démontrer.

3.2 L'ensemble \mathbb{D} des nombres décimaux

Définition. $\mathbb{D} = \left\{ \frac{n}{10^k} / n \in \mathbb{Z} \text{ et } k \in \mathbb{N} \right\}$. C'est une partie stricte de \mathbb{Q} dont les éléments sont appelés les nombres décimaux.

Propriété. Soit $x \in \mathbb{Q}$. x est un nombre décimal si et seulement si son écriture irréductible est de la forme $x = \frac{p}{2^h 5^k}$, où $p \in \mathbb{Z}$ et $h, k \in \mathbb{N}$.

Remarque. $(\mathbb{D}, +, \times)$ est un anneau.

Propriété. $d \in \mathbb{D}$ si et seulement si il existe une famille presque nulle de chiffres indexée par \mathbb{Z} , $(a_k)_{k \in \mathbb{Z}} \in \{0, \dots, 9\}^{(\mathbb{Z})}$ telle que $d = \sum_{k \in \mathbb{Z}} a_k 10^k$.

3.3 Approximation d'un réel

Définition. Soit $x, \alpha \in \mathbb{R}$ et $\varepsilon \in \mathbb{R}_+^*$.

- On dit que α est une valeur approchée de x à ε près si et seulement si $d(x, \alpha) \leq \varepsilon$.
On note alors $x = \alpha \pm \varepsilon$.
- On dit que α est une valeur approchée de x à ε près par défaut si et seulement si $\alpha \leq x \leq \alpha + \varepsilon$,
- On dit que α est une valeur approchée de x à ε près par excès si et seulement si $\alpha - \varepsilon \leq x \leq \alpha$.

Propriété. Soit $x \in \mathbb{R}$ et $p \in \mathbb{N}$. Posons $\alpha = \frac{\lfloor 10^p x \rfloor}{10^p}$. $\alpha \in \mathbb{D}$.

Alors α est une valeur approchée de x par défaut à 10^{-p} près, et $\alpha + 10^{-p}$ est une valeur approchée de x par excès à 10^{-p} près.

Il faut savoir le démontrer.

Corollaire. \mathbb{D} est dense dans \mathbb{R} .

Semaine 8 : Résumé de cours

1 Développement d'un réel en base quelconque

Notation. On fixe un entier naturel a supérieur ou égal à 2.

Propriété. Soit $(v_n)_{n \geq 1}$ une suite d'entiers telle que, pour tout $n \in \mathbb{N}^*$, $0 \leq v_n \leq a - 1$.

Pour tout $n \in \mathbb{N}$, posons $x_n = \sum_{k=1}^n v_k a^{-k}$. La suite (x_n) est croissante et majorée, donc elle converge

vers une limite x que l'on notera $x = \sum_{n=1}^{+\infty} v_n a^{-n}$. Dans ces conditions, on dit que $(v_n)_{n \geq 1}$ est un développement de x en base a et on note $x = 0, \overline{v_1 v_2 \cdots v_n v_{n+1} \cdots}$.

De plus, $x \in [0, 1]$ et $[x = 1 \iff (\forall n \in \mathbb{N}^*, v_n = a - 1)]$.

Il faut savoir le démontrer.

Notation. Posons $\mathcal{V} = \{(v_n)_{n \geq 1} / \forall n \in \mathbb{N}^* v_n \in \mathbb{N} \cap [0, a[\text{ et } \forall N \in \mathbb{N}^* \exists n \geq N v_n \neq a - 1\}$. Ainsi, les éléments de \mathcal{V} sont les suites de chiffres qui ne sont pas tous égaux à $a - 1$ à partir d'un certain rang.

Théorème. Tout réel de $[0, 1[$ admet un unique développement en base a dans \mathcal{V} .

Remarque. Soit $x \in \mathbb{R}_+$. On peut écrire $x = [x] + \{x\}$, où $[x] \in \mathbb{N}$ et où $\{x\} = x - [x] \in [0, 1[$ est la partie fractionnaire de x . On obtient le développement en base a du réel x en concaténant le développement en base a de l'entier $[x]$ avec celui du réel $\{x\} \in [0, 1[$.

Théorème hors programme : caractérisation d'un rationnel. Soit $x \in [0, 1[$.

Notons $x = 0, \overline{v_1 \cdots v_n \cdots}$ le développement en base a de x .

x est un rationnel si et seulement si son développement en base a est périodique à partir d'un certain rang, c'est-à-dire si et seulement si il existe $N \in \mathbb{N}^*$ et $p \in \mathbb{N}^*$ tel que $\forall n > N, v_n = v_{n+p}$.

Il faut savoir le démontrer.

2 Applications

2.1 Généralités

Définition. Une fonction f de E dans F est un triplet $f = (E, F, \Gamma)$, où E et F sont des ensembles et où Γ est une relation binaire sur $E \times F$ telle que

$\forall x \in E, \forall y, z \in F, (x \Gamma y) \wedge (x \Gamma z) \implies (y = z)$, c'est-à-dire telle que pour tout $x \in E$, il existe au plus un $y \in F$ en relation avec x . On note alors " $y = f(x)$ " au lieu de $x \Gamma y$ ou bien $(x, y) \in \Gamma$.

- Le domaine de définition de f est $\{x \in E / \exists y \in F, x \Gamma y\}$. On le notera \mathcal{D}_f .
- Une application de E dans F est une fonction telle que $\mathcal{D}_f = E$.
- E s'appelle l'ensemble de départ de f et F l'ensemble d'arrivée.
- Γ s'appelle le graphe de f . $\Gamma = \{(x, y) \in E \times F / x \Gamma y\} = \{(x, f(x)) / x \in \mathcal{D}_f\}$.
- Lorsque $y = f(x)$, où $x \in E$ et $y \in F$,
 - on dit que y est l'image de x par f et

— que x est un antécédent de y par f .

Propriété. Soit f une fonction de E vers F et soit g une fonction de E' vers F' . Alors $f = g$ si et seulement si $E = E'$, $F = F'$, $\mathcal{D}_f = \mathcal{D}_g$ et pour tout $x \in \mathcal{D}_f$, $f(x) = g(x)$.

Définition. Soit E et I deux ensembles. La famille $(e_i)_{i \in I}$ d'éléments de E indexée par I est l'unique application de I dans E dont le graphe est $\{(i, e_i)/i \in I\}$. Il s'agit d'une autre façon de noter une application, parfois mieux adaptée.

Définition. Une *suite* est une famille d'éléments indexée par \mathbb{N} , ou éventuellement par $\{n \in \mathbb{N}/n \geq n_0\}$ (où $n_0 \in \mathbb{N}$).

Définition. Si E et F sont deux ensembles, le triplet (E, F, \emptyset) est une fonction de E dans F , que l'on appelle la fonction vide. Elle est définie sur \emptyset .

Le triplet $(\emptyset, F, \emptyset)$ est une application à valeurs dans F , appelée l'application vide.

La famille (d'éléments de E) $(e_i)_{i \in \emptyset}$ désigne l'application vide $(\emptyset, E, \emptyset)$, que l'on appelle aussi la famille vide d'éléments de E .

Notation. L'application identité sur E est définie par : $\forall x \in E, Id_E(x) = x$.

Définition. Soit E un ensemble et A une partie de E . L'indicatrice de A dans E est l'unique application, notée $\mathbf{1}_A$, de E dans $\{0, 1\}$ telle que $\mathbf{1}_A(x) = 1$ si $x \in A$ et $\mathbf{1}_A(x) = 0$ si $x \in E \setminus A$.

Propriété. Soit E un ensemble et A et B deux parties de E . En définissant naturellement la somme, la différence et le produit de deux applications de E dans \mathbb{R} , on vérifie que : $\mathbf{1}_{E \setminus A} = \mathbf{1}_E - \mathbf{1}_A$, $\mathbf{1}_{A \cap B} = \mathbf{1}_A \cdot \mathbf{1}_B$ et $\mathbf{1}_{A \cup B} = \mathbf{1}_A + \mathbf{1}_B - \mathbf{1}_A \cdot \mathbf{1}_B$.

Il faut savoir le démontrer.

Définition. Soit f une application de E vers F . On suppose que F est muni d'une relation d'ordre \preceq . Soit A une partie de E . Les majorant, borne supérieure, minimum etc. de f sur A sont par définition les majorant, borne supérieure, minimum etc. de $f(A)$.

Définition. Soit I un ensemble quelconque et soit $(f_i)_{i \in I}$ une famille d'éléments d'un ensemble F . On suppose que F est muni d'une relation d'ordre \preceq . Les majorant, borne supérieure, minimum etc. de $(f_i)_{i \in I}$ sont par définition les majorant, borne supérieure, minimum etc. de $\{f_i/i \in I\}$.

Notation. On note $\mathcal{F}(E, F)$ ou bien F^E l'ensemble des applications de E dans F .

F^I est donc aussi l'ensemble des familles indexées par I d'éléments de l'ensemble F .

Définition. Soient E et F deux ensembles, E' une partie de E et F' une partie de F .

- Soit f une application de E dans F . La restriction de f à E' est l'unique application de E' dans F telle que $\forall x \in E', f|_{E'}(x) = f(x)$.
- Soit f une application de E' dans F . On appelle prolongement de f sur E toute application g de E dans F telle que $g|_{E'} = f$.
- Si pour tout $x \in E, f(x) \in F'$, la corestriction de f à F' est l'unique application de E dans F' telle que : pour tout $x \in E, f|^{F'}(x) = f(x)$.
- Si, pour tout $x \in E', f(x) \in F', f|_{E'}^{F'}$ désigne l'application de E' dans F' telle que, pour tout $x \in E', (f|_{E'}^{F'})(x) = f(x)$.

Définition. Soit f une application d'un ensemble E dans lui-même. Une partie A de E est stable par f si et seulement si elle vérifie l'une des propriétés équivalentes suivantes :

- $\forall x \in A, f(x) \in A$,
- $f(A) \subset A$,
- $f|_A^A$ est définie.

Définition. Soit f une application de E dans F et g une application de F dans G . La composée de g et de f est l'unique application $g \circ f$ de E dans G définie par : $\forall x \in E, (g \circ f)(x) = g(f(x))$.

Associativité de la composition : Soit f une application de E dans F , g une application de F dans G et h une application de G dans H . Alors $h \circ (g \circ f) = (h \circ g) \circ f$. On peut donc noter $h \circ g \circ f$ cette fonction.

2.2 Applications croissantes et décroissantes

Définition. Soit f une application d'un ensemble ordonné (E, \leq_E) dans un ensemble ordonné (F, \leq_F) .

- f est croissante si et seulement si $[\forall x, y \in E, x \leq_E y \implies f(x) \leq_F f(y)]$.
- f est strictement croissante si et seulement si $\forall x, y \in E, x <_E y \implies f(x) <_F f(y)$.
- f est décroissante si et seulement si elle est croissante de (E, \leq_E) dans (F, \geq_F) .
- f est strictement décroissante si et seulement si $\forall x, y \in E, x <_E y \implies f(x) >_F f(y)$.
- f est monotone si et seulement si f est croissante ou décroissante.
- f est strictement monotone si et seulement si f est strictement croissante ou strictement décroissante.

Propriété.

- La composée de deux applications croissantes est croissante.
- La composée de deux applications décroissantes est croissante.
- La composée d'une application croissante et d'une application décroissante est décroissante.

Il faut savoir le démontrer.

Propriété. Soit f et g deux fonctions de \mathbb{R} dans \mathbb{R} .

- Si f et g sont croissantes, alors $f + g$ est croissante.
- Si f et g sont décroissantes, alors $f + g$ est décroissante.
- Si f est croissante, $-f$ est décroissante.
- Si f et g sont à valeurs positives et croissantes (resp : décroissantes), alors fg est croissante (resp : décroissante).
- Si f et g sont à valeurs strictement positives et sont strictement croissantes (resp : strictement décroissantes), alors fg est strictement croissante (resp : strictement décroissante).

Il faut savoir le démontrer.

Définition. Soit f et g deux applications d'un ensemble E dans un ensemble ordonné (F, \leq) . On écrit $f \leq g$ si et seulement si, pour tout $x \in E$, $f(x) \leq g(x)$.

On définit ainsi une relation d'ordre sur $\mathcal{F}(E, F)$.

2.3 Images directes et réciproques

Définition. Soit f une application de E dans F .

- Si A est une partie de E , l'image directe de A par f est $f(A) \triangleq \{f(x)/x \in A\}$.
Ainsi, $\forall y \in F, y \in f(A) \iff [\exists x \in A, y = f(x)]$.
 $f(A)$ est l'ensemble des images par f des éléments de A .
- Si B est une partie de F , l'image réciproque de B par f est $f^{-1}(B) \triangleq \{x \in E/f(x) \in B\}$. Ainsi, $\forall x \in E, x \in f^{-1}(B) \iff f(x) \in B$.
 $f^{-1}(B)$ est l'ensemble des antécédents par f des éléments de B .

Propriétés des images directes : Soit f une application de E dans F , $(A_i)_{i \in I}$ une famille de parties de E , A et A' deux parties de E .

- $A \subset A' \implies f(A) \subset f(A')$.
- $f\left(\bigcup_{i \in I} A_i\right) = \bigcup_{i \in I} f(A_i)$.
- $f\left(\bigcap_{i \in I} A_i\right) \subset \bigcap_{i \in I} f(A_i)$, mais l'inclusion réciproque est fautive en général.
- $f(E \setminus A) \supset f(E) \setminus f(A)$, mais l'inclusion réciproque est fautive en général.

Il faut savoir le démontrer.

Propriétés des images réciproques : Soit f une application de E dans F , $(B_i)_{i \in I}$ une famille de parties de F , B et B' deux parties de F .

- $B \subset B' \implies f^{-1}(B) \subset f^{-1}(B')$.
- $f^{-1}\left(\bigcup_{i \in I} B_i\right) = \bigcup_{i \in I} f^{-1}(B_i)$.
- $f^{-1}\left(\bigcap_{i \in I} B_i\right) = \bigcap_{i \in I} f^{-1}(B_i)$.
- $f^{-1}(F \setminus B) = E \setminus f^{-1}(B)$.

Il faut savoir le démontrer.

Propriété. Avec les notations de la propriété précédente,

$A \subset f^{-1}(f(A))$ et $f(f^{-1}(B)) \subset B$, mais les inclusions réciproques peuvent être fausses.

Il faut savoir le démontrer.

2.4 Injectivité et surjectivité

Définition. Soit $f : E \longrightarrow F$. f est injective si et seulement si $\forall x, y \in E, [f(x) = f(y) \implies x = y]$, c'est-à-dire si et seulement si, pour tout couple d'éléments distincts de E , leurs images sont différentes, ou encore si et seulement si tout élément de F possède au plus un antécédent.

Définition. Soit $f : E \longrightarrow F$. f est surjective si et seulement si $\forall y \in F, \exists x \in E, y = f(x)$, c'est-à-dire si et seulement si $f(E) = F$, ou encore si et seulement si tout élément de F possède au moins un antécédent.

Définition. On dit que f est bijective si et seulement si f est injective et surjective, c'est-à-dire si et seulement si tout élément de l'ensemble d'arrivée possède un unique antécédent dans l'ensemble de départ.

Propriété. Soit f une application de E dans F . Sur E , on définit la relation binaire R par : $xRy \iff f(x) = f(y)$. R est une relation d'équivalence. Alors l'application $\bar{f} : E/R \longrightarrow f(E)$ est une bijection.

Il faut savoir le démontrer.

Propriété. La composée de deux injections est une injection.

La composée de deux surjections est une surjection.

La composée de deux bijections est une bijection.

Il faut savoir le démontrer.

Propriété. Soit f une application de E dans F et g une application de F dans G .

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

Si $g \circ f$ est surjective, alors g est surjectif.

Définition et propriété :

◇ Soit f une bijection de E dans F . Pour tout $y \in F$, notons $f^{-1}(y)$ l'unique antécédent de y par f . Alors f^{-1} est une bijection de F dans E , appelée la bijection réciproque de f .

◇ On vérifie que $f \circ f^{-1} = Id_F$ et $f^{-1} \circ f = Id_E$.

◇ Réciproquement, s'il existe une application g de F dans E telle que $f \circ g = Id_F$ et $g \circ f = Id_E$, alors f et g sont des bijections et $g = f^{-1}$.

◇ $(f^{-1})^{-1} = f$.

Il faut savoir le démontrer.

Propriété. Si $f : E \longrightarrow F$ et $g : F \longrightarrow G$ sont bijectives, alors $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Remarque. La notation f^{-1} , pour une application f , est utilisée selon deux sens *différents*, qu'il est important de bien distinguer :

- Lorsque f est une application *quelconque* de E dans F , si B est une partie de F , alors $f^{-1}(B) = \{x \in E / f(x) \in B\}$.

— Lorsque f est une *bijection* de E dans F , pour tout $y \in F$, $f^{-1}(y)$ est l'unique antécédent de y par f .

En particulier, dès que l'on utilise une expression de la forme $f^{-1}(y)$ où y est un *élément* de l'ensemble d'arrivée de f , on suppose nécessairement que f est une bijection.

Lorsque $y \in F$, il importe de bien distinguer $f^{-1}(y)$ qui représente, pour une bijection f , l'unique antécédent de y , et $f^{-1}(\{y\})$ qui représente, pour une application f quelconque, l'ensemble des antécédents de y . Cet ensemble peut être vide lorsque f n'est pas surjective, il peut contenir plus de deux éléments lorsque f n'est pas injective.

Propriété. Si f est une bijection de E dans F , alors pour tout $B \subset F$, $f(f^{-1}(B)) = B$ et, pour tout $A \subset E$, $f^{-1}(f(A)) = A$.

Propriété. (HP) Les applications injectives sont simplifiables à gauche et les applications surjectives sont simplifiables à droite.

Il faut savoir le démontrer.

Propriété. Si $E \neq \emptyset$, alors $f : E \rightarrow F$ est injective si et seulement si il existe $g : F \rightarrow E$ telle que $g \circ f = Id_E$.

Il faut savoir le démontrer.

Propriété. $f : E \rightarrow F$ est surjective si et seulement si il existe $g : F \rightarrow E$ telle que $f \circ g = Id_F$.

Il faut savoir le démontrer.

3 Lois internes

Définition. Une loi interne sur E est une application f de $E \times E$ dans E . Dans ce contexte la notation *préfixe* " $f(x, y)$ " est remplacée par la notation *infixe* " $x f y$ ", où $x, y \in E$.

On dit que (E, f) est un magma (hors programme).

Définition. Soit Δ une loi interne sur E . Δ est associative si et seulement si pour tout $x, y, z \in E$, $(x \Delta y) \Delta z = x \Delta (y \Delta z)$. On dit alors que (E, Δ) est un magma associatif. Dans ce cas, si $x_1, \dots, x_p \in E$, la quantité $x_1 \Delta x_2 \Delta \dots \Delta x_p$ ne dépend pas des différentes façons de la parenthéser.

Définition. Soit Δ une loi interne sur E et soit $e \in E$. On dit que e est un élément neutre de (E, Δ) si et seulement si, pour tout $x \in E$, $x \Delta e = e \Delta x = x$. Si E possède un élément neutre, il est unique. On dit alors que (E, Δ) est un magma unitaire, ou bien unifère.

Définition. Un monoïde est un magma associatif unitaire. Il est commutatif, ou abélien, si et seulement si pour tout x, y , $x \Delta y = y \Delta x$.

Remarque. l'usage est de confondre le monoïde (E, Δ) et l'ensemble sous-jacent E .

Notation. Si (E, Δ) est un monoïde d'élément neutre e , on convient que $x_1 \Delta x_2 \Delta \dots \Delta x_p = e$, lorsque $p = 0$.

Définition. Soit (E, \times) un monoïde d'élément neutre 1_E et $x \in E$. On dit que x est inversible à droite (resp : à gauche) si et seulement si il existe $y \in E$ tel que $yx = 1_E$ (resp : $xy = 1_E$).

Si x est inversible à gauche et à droite, il existe un unique $y \in E$ tel que $xy = yx = 1_E$. On note $y = x^{-1}$, c'est le symétrique de x .

Il faut savoir le démontrer.

Propriété.

Si x et y sont inversibles dans le monoïde (E, \times) , alors xy est aussi inversible et $(xy)^{-1} = y^{-1}x^{-1}$.

Définition. Un groupe est un monoïde dans lequel tout élément est inversible.

Définition. On appelle *anneau* tout triplet $(A, +, \cdot)$, où A est un ensemble et où “+” et “.” sont deux lois internes sur A telles que

- $(A, +)$ est un groupe abélien (l'élément neutre étant noté 0 ou 0_A),
- “.” est une loi associative, admettant un élément neutre noté 1 ou 1_A ,
- la loi “.” est *distributive* par rapport à la loi “+”, c'est-à-dire que $\forall (x, y, z) \in A^3$ $x.(y + z) = (x.y) + (x.z)$ et $(x + y).z = (x.z) + (y.z)$.

4 Cardinal d'un ensemble

Définition. Soit E un ensemble. S'il existe $n \in \mathbb{N}$ tel que \mathbb{N}_n est en bijection avec E , alors n est unique. On dit que n est le cardinal de E . Il est noté $\text{card}(E)$ ou bien $\#E$, ou encore $|E|$. En cas d'inexistence d'un tel entier n , on dit que E est infini.

Exemple. Pour tout $n, m \in \mathbb{Z}$, $\text{Card}(\llbracket n, m \rrbracket) = m - n + 1$.

Propriété. Soit A un ensemble de cardinal $n \in \mathbb{N}$ et soit B un ensemble quelconque. B est fini de cardinal n si et seulement si il existe une bijection de A sur B .

Propriété. Soit A un ensemble fini de cardinal $n \in \mathbb{N}$. Soit B une partie de A . Alors B est un ensemble fini et $|B| \leq |A|$, avec égalité si et seulement si $B = A$.

Propriété. Soit A une partie de \mathbb{N} . A est finie si et seulement si elle est majorée. En particulier, \mathbb{N} est infini.

Semaine 9 : Résumé de cours

1 Cardinaux d'ensembles usuels

Propriété. Pour tout $n \in \mathbb{N}^*$, une réunion *disjointe* de n ensembles finis est finie et son cardinal est égal à la somme des cardinaux de ces ensembles.

Propriété. Soit E un ensemble fini et A une partie de E . Alors $|E \setminus A| = |E| - |A|$.

Propriété. Soit E un ensemble fini et R une relation d'équivalence sur E . Alors E/R est aussi de cardinal fini, inférieur au cardinal de E .

Formule :

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Il faut savoir le démontrer.

Propriété. Formule du crible : (Hors programme)

$$\begin{aligned} \# \left(\bigcup_{i=1}^n E_i \right) &= \sum_{i=1}^n \# E_i - \sum_{1 \leq i < j \leq n} \#(E_i \cap E_j) + \cdots + (-1)^{k+1} \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} \# \left(\bigcap_{j=1}^k E_{i_j} \right) \\ &\quad + \cdots + (-1)^{n+1} \# \left(\bigcap_{i=1}^n E_i \right). \end{aligned}$$

Propriété. Le cardinal du produit cartésien de n ensembles finis est égal au produit des cardinaux de ces ensembles.

Il faut savoir le démontrer.

Formule : $|\mathcal{F}(E, F)| = |F|^{|E|}$.

Il faut savoir le démontrer.

Propriété. Si E est de cardinal n , alors $\mathcal{P}(E)$ est de cardinal 2^n .

Il faut savoir le démontrer.

2 Sommes et produits finis

Formules :

- Pour tout $a \in G$ et $n \in \mathbb{N}$, $\sum_{k=1}^n a = na$.
- Pour tout $n \in \mathbb{N}$, $\sum_{k=1}^n k = \frac{n(n+1)}{2}$.
- Pour tout $n \in \mathbb{N}$, $\sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}$.
- Pour tout $n \in \mathbb{N}$, $\sum_{k=1}^n k^3 = \left(\frac{n(n+1)}{2} \right)^2$.

Notation. Pour tout $n \in \mathbb{N}$, \mathcal{S}_n désigne l'ensemble des bijections de \mathbb{N}_n dans \mathbb{N}_n , que l'on appelle des permutations sur \mathbb{N}_n .

Commutativité généralisée : Soit $n \in \mathbb{N}$ et $x_1, \dots, x_n \in G$. Alors, $\forall \sigma \in \mathcal{S}_n$, $\sum_{i=1}^n x_i = \sum_{j=1}^n x_{\sigma(j)}$.

Définition. Soit A un ensemble fini et $(x_a)_{a \in A}$ une famille de G indexée par A .

Notons $n = |A|$. Il existe une bijection f de \mathbb{N}_n dans A . On pose $\sum_{a \in A} x_a \triangleq \sum_{i=1}^n x_{f(i)}$.

Cette quantité ne dépend pas de la bijection f .

Il faut savoir le démontrer.

Propriété d'additivité : Soit A un ensemble fini, $(x_a)_{a \in A}$ et $(y_a)_{a \in A}$ deux familles d'éléments de G indexées par A . Alors $\sum_{a \in A} (x_a + y_a) = \left(\sum_{a \in A} x_a \right) + \left(\sum_{a \in A} y_a \right)$.

Distributivité généralisée : Soit A un ensemble fini, $\lambda \in \mathbb{C}$ et $(x_a)_{a \in A}$ une famille de *complexes* indexée par A . Alors $\sum_{a \in A} (\lambda x_a) = \lambda \sum_{a \in A} x_a$.

Changement de variable dans une somme finie : Soit B un ensemble fini, $(x_b)_{b \in B}$ une famille d'éléments de G . Soit φ une bijection d'un ensemble A dans B . Alors $\sum_{b \in B} x_b = \sum_{a \in A} x_{\varphi(a)}$.

Il faut savoir le démontrer.

Formule : calcul d'une somme géométrique .

Soit $q \in \mathbb{C} \setminus \{1\}$, soit $m, n \in \mathbb{N}$ avec $m \leq n$. Alors $\sum_{k=m}^n q^k = \frac{q^m - q^{n+1}}{1 - q}$.

Il faut savoir le démontrer.

Théorème. Soit (G, \times) un groupe commutatif fini. Alors, pour tout $g \in G$, $g^{|G|} = 1_G$.

Il faut savoir le démontrer.

Remarque. Ce théorème est encore vrai lorsque G n'est pas commutatif (cf plus loin).

Sommation par paquets : Soit A un ensemble fini et $(x_a)_{a \in A}$ une famille d'éléments de G . On suppose qu'il existe un ensemble fini B et une famille $(A_b)_{b \in B}$ de parties de A telles que $A = \bigsqcup_{b \in B} A_b$.

Alors $\sum_{a \in A} x_a = \sum_{b \in B} \sum_{a \in A_b} x_a$.

Sommation par paquets, seconde formulation : Soit A un ensemble fini et $(x_a)_{a \in A}$ une famille d'éléments de G . Soit R une relation d'équivalence sur A . Alors $\sum_{a \in A} x_a = \sum_{c \in A/R} \sum_{a \in c} x_a$.

3 Applications et cardinaux

Notation. Considérons une application f de E dans F , où E est de cardinal fini.

Propriété. Soit E un ensemble fini et f une application de E dans un ensemble quelconque F . Alors $f(E)$ est fini. De plus,

$|f(E)| \leq |E|$, avec égalité si et seulement si f est injective, et

$|f(E)| \leq |F|$, avec égalité si et seulement si f est surjective.

Il faut savoir le démontrer.

Propriété. Soit E et F deux ensembles finis *de même cardinal*. Soit f une application de E dans F . Alors f injective $\iff f$ surjective $\iff f$ bijective.

Propriété. Soit A et B deux ensembles.

S'il existe une injection de A dans B et si B est fini, alors A est fini et $|A| \leq |B|$.

S'il existe une surjection de A dans B et si A est fini, alors B est fini et $|A| \geq |B|$.

Principe des tiroirs : Si l'on doit ranger p objets dans n tiroirs et que $p > n$, alors il existe au moins 2 objets qui seront dans le même tiroir.

Plus généralement, si $p > cn$, où $c \in \mathbb{N}^*$, il existe un tiroir qui contient plus de $c + 1$ objets.

Il faut savoir le démontrer.

Principe des bergers : Soit E et F des ensembles finis et $f : E \rightarrow F$ une application. On suppose que tout élément de F possède exactement k antécédents par f . Alors $|E| = k|F|$.

Il faut savoir le démontrer.

4 Listes et combinaisons

Vocabulaire : Soit E un ensemble et $p \in \mathbb{N}$.

- Une p -liste (aussi appelée un p -uplet) d'éléments de E est un élément de E^p .
- Un p -arrangement d'éléments de E est une p -liste dont les éléments sont deux à deux distincts.
- Une p -combinaison de E est une partie de E de cardinal p .

Propriété. Le nombre de p -listes d'éléments de E est égal à n^p (c'est $|E|^p$).

Propriété. Si $a = (e_1, \dots, e_p)$ est un p -arrangement de E , l'application $f_a : \mathbb{N}_p \rightarrow E$ définie par $i \mapsto e_i$ est une injection. De plus, $a \mapsto f_a$ est une bijection de l'ensemble A_p des p -arrangements de E vers l'ensemble I_p des injections de \mathbb{N}_p dans E .

Il faut savoir le démontrer.

Théorème. Le nombre de p -arrangements dans un ensemble de cardinal n est égal à

$n(n-1) \cdots (n-p+1) = \frac{n!}{(n-p)!}$. C'est aussi le nombre d'injections d'un ensemble à p éléments vers un ensemble à n éléments.

Corollaire. Pour tout $n \in \mathbb{N}$, $|\mathcal{S}_n| = n!$. Plus généralement, factorielle de n est le nombre de bijections d'un ensemble de cardinal n dans un autre ensemble de cardinal n .

Théorème. Le nombre de p -combinaisons d'éléments d'un ensemble de cardinal n , c'est-à-dire le nombre de parties de p éléments incluses dans un ensemble de cardinal n est égal à

$$\binom{n}{p} \triangleq \frac{A_{n,p}}{p!} = \frac{n!}{(n-p)!p!}.$$

Cette quantité s'appelle le coefficient binomial " p parmi n ".

Il faut savoir le démontrer.

5 Les coefficients binomiaux

Formule : $\forall n, p \in \mathbb{N}$ avec $0 \leq p \leq n$, $\binom{n}{p} = \binom{n}{n-p}$.

Formule comité-président : Pour tout $n, k \in \mathbb{N}^*$ avec $k \leq n$, $k \binom{n}{k} = n \binom{n-1}{k-1}$.

La preuve combinatoire est à connaître.

Formule comité-bureau : si $p \leq k \leq n$, $\binom{k}{p} \times \binom{n}{k} = \binom{n}{p} \times \binom{n-p}{k-p}$.

La preuve combinatoire est à connaître.

Formule du triangle de Pascal : $\forall n, p \in \mathbb{N}$ avec $1 \leq p < n$, $\binom{n}{p} = \binom{n-1}{p} + \binom{n-1}{p-1}$.

La preuve combinatoire est à connaître.

Remarque. Il est souvent pratique de convenir que, pour tout $n, p \in \mathbb{Z}$ tels que $\neg(0 \leq p \leq n)$, $\binom{n}{p} = 0$.

Représentation graphique du triangle de Pascal : À connaître.

Formule du binôme de Newton : On se place dans un anneau $(A, +, \times)$. Soit a_1 et a_2 deux éléments de A qui commutent, c'est-à-dire tels que $a_1 a_2 = a_2 a_1$. Alors

$$\forall n \in \mathbb{N}, (a_1 + a_2)^n = \sum_{k=0}^n \binom{n}{k} a_1^k a_2^{n-k}.$$

Les deux preuves sont à connaître.

Formule du multinôme : (Hors programme). Soit $p, n \in \mathbb{N}^*$. Soit a_1, \dots, a_p p éléments d'un anneau A qui commutent deux à deux. Alors

$$(a_1 + \dots + a_p)^n = \sum_{\substack{i_1, \dots, i_p \in \mathbb{N} \\ \text{tel que } i_1 + \dots + i_p = n}} \frac{n!}{i_1! \times \dots \times i_p!} a_1^{i_1} \times \dots \times a_p^{i_p}.$$

Semaine 10 : Résumé de cours

1 Sommes finies (suite)

Formule de Leibniz : Soient f et g deux applications d'un intervalle I dans \mathbb{R} . Si f et g sont n fois dérivables sur I , alors fg est n fois dérivable sur I et $(fg)^{(n)} = \sum_{k=0}^n \binom{n}{k} f^{(k)} g^{(n-k)}$.

Il faut savoir le démontrer.

1.1 Sommes et produits : quelques techniques

1.1.1 Télécopage

$$\sum_{k=m}^n (u_{k+1} - u_k) = u_{n+1} - u_m \text{ et } \sum_{k=m+1}^{n+1} (u_{k-1} - u_k) = u_m - u_{n+1}.$$

1.1.2 Séparation des indices pairs et impairs

$$\sum_{k=0}^n u_k = \sum_{\substack{0 \leq k \leq n \\ k \text{ pair}}} u_k + \sum_{\substack{0 \leq k \leq n \\ k \text{ impair}}} u_k = \sum_{p=0}^{\lfloor \frac{n}{2} \rfloor} u_{2p} + \sum_{p=0}^{\lfloor \frac{n-1}{2} \rfloor} u_{2p+1}.$$

1.1.3 Fonction génératrice

Soit $m, n \in \mathbb{N}$ avec $m \leq n$ et soit $(u_k)_{m \leq k \leq n}$ une famille de complexes. La fonction génératrice de cette famille est l'application polynomiale $P : x \mapsto \sum_{k=m}^n u_k x^k$.

Si P est connu, on peut en déduire plusieurs sommes : $\sum_{k=m}^n u_k = P(1)$, $\sum_{k=m}^n k u_k = P'(1)$,

$$\sum_{k=m}^n k(k-1)u_k = P''(1), \quad \sum_{k=m}^n \frac{u_k}{k+1} = \int_0^1 P(t) dt \text{ etc.}$$

1.1.4 Quelques formules

Somme arithmétique : Une suite (u_n) de complexes est arithmétique de raison r si et seulement si $\forall n \in \mathbb{N}, u_{n+1} = u_n + r$. Dans ce cas, pour tout $n \in \mathbb{N}$, $u_n = u_0 + nr$ et $\sum_{k=m}^n u_k = \frac{u_m + u_n}{2} (n - m + 1)$.

Formule de Bernoulli : Soit $(A, +, \times)$ un anneau. Soit a et b deux éléments de A qui commutent (i.e $ab = ba$). Alors, pour tout $n \in \mathbb{N}$, $a^{n+1} - b^{n+1} = (a - b) \sum_{k=0}^n a^k b^{n-k}$.

Il faut savoir le démontrer.

Somme géométrique : Une suite (u_n) de complexes est géométrique de raison r si et seulement si

$$\forall n \in \mathbb{N}, u_{n+1} = ru_n. \text{ Dans ce cas, } u_n = u_0 r^n \text{ et } \sum_{k=m}^n u_k = \frac{u_{n+1} - u_m}{r - 1}.$$

1.1.5 Sommes doubles

$$\sum_{\substack{m \leq k \leq n \\ p \leq \ell \leq q}} u_{k,\ell} = \sum_{k=m}^n \sum_{\ell=p}^q u_{k,\ell} = \sum_{\ell=p}^q \sum_{k=m}^n u_{k,\ell}.$$

Propriété. Dans un anneau, $\sum_{\substack{m \leq k \leq n \\ p \leq \ell \leq q}} v_k w_\ell = \left(\sum_{k=m}^n v_k \right) \left(\sum_{\ell=p}^q w_\ell \right).$

1.1.6 Sommes triangulaires

$$\sum_{m \leq k \leq \ell \leq n} u_{k,\ell} = \sum_{k=m}^n \sum_{\ell=k}^n u_{k,\ell} = \sum_{\ell=m}^n \sum_{k=m}^{\ell} u_{k,\ell}.$$

Il faut savoir le démontrer.

1.1.7 Produits

Toutes les propriétés précédentes, lorsqu'elles étaient valables dans un monoïde commutatif $(G, +)$ sont valables en notation multiplicative dans un monoïde commutatif (G, \times) .

1.2 Intégration par parties itérée

Intégration par parties itérée : (Hors programme).

Soit I un intervalle de \mathbb{R} , $n \in \mathbb{N}$, f et g deux applications de classe C^n de I dans \mathbb{R} . Alors, pour tout

$$a, b \in I, \int_a^b f^{(n)}(t)g(t)dt = \left[\sum_{i=0}^{n-1} f^{(n-1-i)}(t)g^{(i)}(t)(-1)^i \right]_a^b + (-1)^n \int_a^b f(t)g^{(n)}(t)dt.$$

Démonstration à connaître.

Formule de Taylor avec reste intégral :

Soit I un intervalle de \mathbb{R} , $n \in \mathbb{N}$, f une application de classe C^{n+1} de I dans \mathbb{R} . Alors, pour tout

$$a, b \in I, f(b) = f(a) + \sum_{k=1}^n \frac{(b-a)^k}{k!} f^{(k)}(a) + \int_a^b \frac{(b-t)^n}{n!} f^{(n+1)}(t)dt.$$

Démonstration à connaître.

Exemple d'application : (Hors programme)

Sous les hypothèses et notations de la formule précédente, fixons $a, b \in I$ avec $a \leq b$.

Soit $m, M \in \mathbb{R}$ tels que, pour tout $t \in [a, b]$, $m \leq f^{(n+1)}(t) \leq M$.

$$\text{Alors } m \frac{(b-a)^{n+1}}{(n+1)!} \leq f(b) - \sum_{k=0}^n \frac{(b-a)^k}{k!} f^{(k)}(a) \leq M \frac{(b-a)^{n+1}}{(n+1)!}.$$

Démonstration à connaître.

Inégalité de Taylor-Lagrange :

Soit $a, b \in \mathbb{R}$ avec $a \neq b$. On se place sur $I = [\min(a, b), \max(a, b)]$.

Soit $n \in \mathbb{N}$ et f une application de classe C^{n+1} de I dans \mathbb{R} .

Soit $M \in \mathbb{R}$ tel que, pour tout $t \in I$, $|f^{(n+1)}(t)| \leq M$. Alors

$$\left| f(b) - f(a) - \sum_{k=1}^n \frac{(b-a)^k}{k!} f^{(k)}(a) \right| \leq M \frac{|b-a|^{n+1}}{(n+1)!}.$$

Formule de Taylor-Young : Soit $n \in \mathbb{N}^*$, I un intervalle de \mathbb{R} , $x_0 \in I$ et $f : I \rightarrow \mathbb{R}$ une application de classe C^{n+1} . Alors $f(x) = \sum_{k=0}^n \frac{f^{(k)}(x_0)}{k!} (x - x_0)^k + (x - x_0)^n \varepsilon(x)$, où $\varepsilon(x) \xrightarrow{x \rightarrow x_0} 0$.

A savoir démontrer lorsque $x_0 = 0$.

Remarque. On admettra que cette formule est valable dès que f est n fois dérivable en x_0 .

2 Les complexes (début)

2.1 Construction de \mathbb{C}

Propriété. \mathbb{C} est un corps, dont \mathbb{R} est un sous-corps et dont les lois sont définies par

$$\forall a, b, c, d \in \mathbb{R}, \quad \begin{cases} (a + ib) + (c + id) &= (a + c) + i(b + d) \\ (a + ib) \times (c + id) &= (ac - bd) + i(ad + bc) \end{cases}$$

Si $z \neq 0$, l'inverse de $z = a + ib$ est $\frac{a - ib}{a^2 + b^2}$.

Définition. $\forall z \in \mathbb{C}$, $\exists! a, b \in \mathbb{R}$, $z = a + ib$. On note $a = \operatorname{Re}(z)$ et $b = \operatorname{Im}(z)$.

L'écriture du complexe z sous la forme $z = \operatorname{Re}(z) + i\operatorname{Im}(z)$ s'appelle l'écriture algébrique de z .

Définition. Les imaginaires purs sont les ib où $b \in \mathbb{R}$.

Propriété. Comme pour tout corps, \mathbb{C} est intègre, c'est-à-dire que, pour tout $z, z' \in \mathbb{C}$, si $zz' = 0$, alors $z = 0$ ou $z' = 0$.

Propriété. $\frac{1}{i} = -i$.

Linéarité des parties réelle et imaginaire : Pour tout $z, z' \in \mathbb{C}$ et $\alpha \in \mathbb{R}$, $\operatorname{Re}(\alpha z + z') = \alpha \operatorname{Re}(z) + \operatorname{Re}(z')$ et $\operatorname{Im}(\alpha z + z') = \alpha \operatorname{Im}(z) + \operatorname{Im}(z')$.

2.2 Le plan complexe

Définition. On considère un plan P affine euclidien orienté, rapporté à un repère orthonormé direct $R = (O, \vec{i}, \vec{j})$. Soit $(x, y) \in \mathbb{R}^2$. On peut alors définir le complexe $z = x + iy$ et le point M de P dont les coordonnées dans le repère R sont (x, y) . On dit que z est l'afixe du point M et que M est l'image du complexe z .

Si l'on note $M(z)$ l'image du complexe z , l'application $z \mapsto M(z)$ est une bijection de \mathbb{C} dans P qui permet parfois d'identifier \mathbb{C} avec P (muni de son repère R).

On dit également que z est l'afixe du vecteur \overrightarrow{OM} et que \overrightarrow{OM} est le vecteur image de z .

Si l'on note $\vec{u}(z)$ le vecteur image de z , l'application $z \mapsto \vec{u}(z)$ est une bijection de \mathbb{C} dans l'ensemble des vecteurs de P .

Pour ces raisons, \mathbb{C} est souvent appelé le plan complexe.

Interprétation géométrique de l'addition entre complexes :

Soit $z, z' \in \mathbb{C}$. Avec les notations précédentes, notons \vec{u}_z et $\vec{u}_{z'}$ les vecteurs images de z et z' . Alors le vecteur $\vec{u}_z + \vec{u}_{z'}$ a pour affixe $z + z'$.

Ainsi, si l'on identifie \mathbb{C} avec l'ensemble des vecteurs de P , l'addition entre complexes correspond à l'addition entre vecteurs du plan.

Si l'on visualise les deux complexes z et z' par deux points M_z et $M_{z'}$ du plan P , le complexe $z + z'$ est donc le point qui complète $O, M_z, M_{z'}$ en un parallélogramme.

Interprétation géométrique de la différence de deux complexes :

Avec les mêmes notations, $z' - z$ est l'affixe du vecteur $\overrightarrow{M(z)M(z')}$.

Définition. L'homothétie de centre Ω et de rapport $\lambda \in \mathbb{R}$ est la transformation suivante du plan :

$$\begin{aligned} P &\longrightarrow P \\ M &\longmapsto \Omega + \lambda \overrightarrow{\Omega M}. \end{aligned}$$

Interprétation géométrique du produit d'un complexe par un réel :

Soit $z \in \mathbb{C}$ et $\alpha \in \mathbb{R}$. Alors αz est l'affixe du vecteur $\alpha \overrightarrow{OM(z)}$.

Ainsi, αz est aussi l'affixe de l'image de $M(z)$ par l'homothétie de centre O et de rapport α .

2.3 La conjugaison

Définition. Soit $x, y \in \mathbb{R}$. Le conjugué du complexe z est le complexe $\bar{z} \triangleq x - iy$.

Géométriquement, \bar{z} est le symétrique de z selon l'axe Ox des réels.

Propriété. $z \in \mathbb{R} \iff z = \bar{z}$ et $z \in i\mathbb{R} \iff \bar{z} = -z$.

Propriété. Pour tout $z \in \mathbb{C}$, $\operatorname{Re}(z) = \frac{z + \bar{z}}{2}$ et $\operatorname{Im}(z) = \frac{z - \bar{z}}{2i}$.

Propriété. Pour tout $z, z' \in \mathbb{C}$, $\overline{\bar{z}} = z$, $\overline{z + z'} = \bar{z} + \bar{z}'$ et $\overline{zz'} = \bar{z} \times \bar{z}'$, $\overline{\left(\frac{z}{z'}\right)} = \frac{\bar{z}}{\bar{z}'}$.

Corollaire. Pour tout $n \in \mathbb{Z}$ et $z \in \mathbb{C}^*$, $\overline{z^n} = \bar{z}^n$.

3 Le module

Définition. Soit $x, y \in \mathbb{R}$. Le module du complexe $z = x + iy$ est $|z| \triangleq \sqrt{x^2 + y^2}$.

Interprétation géométrique :

$|z|$ désigne la distance du point $M(z)$ à l'origine, ainsi que la norme du vecteur $\overrightarrow{u(z)}$.

La distance entre $M(z)$ et $M(z')$ est égale à $|z - z'|$.

Propriété. $\forall z \in \mathbb{C}$, $|z|^2 = z\bar{z}$.

Propriété. Pour tout $z \in \mathbb{C}^*$, $\frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{\bar{z}}{|z|^2}$.

Propriété. Pour tout $z, z' \in \mathbb{C}$,

- $|z| = |\bar{z}|$ (compatibilité du module avec la conjugaison) ;
- $|zz'| = |z| \times |z'|$ (compatibilité du module avec la multiplication) ;
- pour tout $n \in \mathbb{N}$, $|z^n| = |z|^n$;
- si $z \neq 0$, $\left|\frac{z'}{z}\right| = \frac{|z'|}{|z|}$.

Propriété. Le module est une norme sur \mathbb{C} , c'est-à-dire que l'application $|\cdot| : \mathbb{C} \longrightarrow \mathbb{R}$ vérifie les propriétés suivantes : Pour tout $z, z' \in \mathbb{C}$ et $\alpha \in \mathbb{R}$,

- $|z| \geq 0$ (positivité),
- $|z| = 0 \iff z = 0$ (séparation),
- $|\alpha z| = |\alpha| \times |z|$ (homogénéité),
- $|z + z'| \leq |z| + |z'|$ (inégalité triangulaire).

Il faut savoir le démontrer.

Semaine 11 (du 25 au 29 novembre) : Résumé de cours

Les complexes (suite)

1 Le module (suite)

Distance entre complexes : Lorsque $x, y \in \mathbb{C}$, la quantité $d(x, y) = |x - y|$ est appelée la distance entre les deux complexes x et y .

La fonction distance vérifie les propriétés suivantes : pour tout $x, y, z \in \mathbb{C}$,

- Positivité : $d(x, y) \in \mathbb{R}_+$.
- $d(x, y) = 0 \iff x = y$: d permet de *séparer* les complexes.
- Symétrie : $d(x, y) = d(y, x)$.
- Inégalité triangulaire : $d(x, z) \leq d(x, y) + d(y, z)$.

Définition. Soit $a \in \mathbb{C}$ et $r \in \mathbb{R}_+$.

- La boule fermée de centre a et de rayon r est $B_f(a, r) = \{z \in \mathbb{C} / |z - a| \leq r\}$. C'est le disque de centre a et de rayon r .
- Lorsque $r > 0$, la boule ouverte de centre a et de rayon r est $B_o(a, r) = \{z \in \mathbb{C} / d(a, z) < r\}$. C'est le disque ouvert de centre a et de rayon r .
- La sphère de centre a et de rayon r est $S(a, r) = \{z \in \mathbb{C} / d(a, z) = r\}$. C'est le cercle de centre a et de rayon r .

Définition. $S(0, 1)$ s'appelle la sphère unité ou bien le cercle unité. Il est noté \mathbb{U} .

Propriété. $\text{Pour tout } z \in \mathbb{C}, z \in \mathbb{U} \iff \bar{z} = \frac{1}{z}.$

Théorème.

Pour tout $z, z' \in \mathbb{C}$, $|z + z'| \leq |z| + |z'|$, avec égalité si et seulement si $z' = 0$ ou bien $\frac{z}{z'} \in \mathbb{R}_+$.

Il faut savoir le démontrer.

Généralisation : (hors programme) $|z_1 + \dots + z_n| \leq |z_1| + \dots + |z_n|$, avec égalité si et seulement si, pour tout i, j tels que $1 \leq i < j \leq n$, $(z_j = 0) \vee (\frac{z_i}{z_j} \in \mathbb{R}_+)$.

Il faut savoir le démontrer.

Corollaire de l'inégalité triangulaire :

- Pour tout $z, z' \in \mathbb{C}$, $||z| - |z'|| \leq |z - z'|$.
- Pour tout $a, b, c \in \mathbb{C}$, $|d(a, b) - d(b, c)| \leq d(a, c)$.

Il faut savoir le démontrer.

Définition. Une partie A de \mathbb{C} est bornée si et seulement si il existe $R \in \mathbb{R}_+$ tel que, pour tout $a \in A$, $|a| \leq R$, c'est-à-dire si et seulement si A est incluse dans un disque centré en 0.

2 Fonctions à valeurs dans \mathbb{C}

2.1 Fonctions bornées

Définition. Soit E un ensemble quelconque et f une application de E dans \mathbb{C} .

On dit que f est bornée sur E si et seulement si $\{f(x)/x \in E\}$ est une partie bornée de \mathbb{C} .

Notation. Soit f une application d'un ensemble E dans \mathbb{C} .

On note $\operatorname{Re}(f) : E \rightarrow \mathbb{R}$ et $\operatorname{Im}(f) : E \rightarrow \mathbb{R}$
 $x \mapsto \operatorname{Re}(f(x))$ et $x \mapsto \operatorname{Im}(f(x))$. On les appelle les parties réelle et imaginaire de l'application f .

Propriété. Avec ces notations, f est bornée sur E si et seulement si $\operatorname{Re}(f)$ et $\operatorname{Im}(f)$ sont bornées.

2.2 Dérivation

Définition. Soit I un intervalle inclus dans \mathbb{R} et $f : I \rightarrow \mathbb{C}$ une application. On verra plus loin que f est continue (resp : dérivable, k fois dérivable, de classe C^k où $k \in \mathbb{N}^* \cup \{\infty\}$) si et seulement si les applications $\operatorname{Re}(f)$ et $\operatorname{Im}(f)$ sont continues (resp : dérivables, k fois dérivables, de classe C^k où $k \in \mathbb{N}^* \cup \{\infty\}$). De plus, lorsque f est k fois dérivable, où $k \in \mathbb{N}^*$, on verra que, pour tout $t \in I$, $f^{(k)}(t) = [\operatorname{Re}(f)]^{(k)}(t) + i[\operatorname{Im}(f)]^{(k)}(t)$.

Propriété. Les formules suivantes, déjà admises pour des fonctions de \mathbb{R} dans \mathbb{R} sont aussi valables pour des fonctions de \mathbb{R} dans \mathbb{C} , ainsi que nous le démontrerons plus tard.

Les fonctions qui interviennent dans ces formules sont toutes supposées dérivables sur un intervalle. On se limite éventuellement à un sous-intervalle pour s'assurer que les quantités qui interviennent dans les formules sont bien définies. :

- Pour tout $\alpha, \beta \in \mathbb{C}$, $(\alpha f + \beta g)' = \alpha f' + \beta g'$.
- $(fg)' = f'g + fg'$.
- $\left(\frac{1}{f}\right)' = -\frac{f'}{f^2}$.
- $\left(\frac{f}{g}\right)' = \frac{f'g - g'f}{g^2}$.
- Si $g : \mathbb{R} \rightarrow \mathbb{R}$, alors $(f \circ g)' = g' \times (f' \circ g)$.
- Pour tout $n \in \mathbb{Z}$, $(f^n)' = nf' \times f^{n-1}$.

Formule de Leibniz : Soient f et g deux applications d'un intervalle I dans \mathbb{C} . Si f et g sont n fois dérivables sur I , alors fg est n fois dérivable sur I et

$$(fg)^{(n)} = \sum_{k=0}^n \binom{n}{k} f^{(k)} g^{(n-k)}.$$

2.3 Intégration

Définition. Soit I un intervalle de \mathbb{R} . Soit $f : I \rightarrow \mathbb{C}$ une application continue. Pour tout $a, b \in I$, on pose

$$\int_a^b f(t) dt = \int_a^b \operatorname{Re}(f(t)) dt + i \int_a^b \operatorname{Im}(f(t)) dt.$$

Remarque. Ainsi, $\operatorname{Re}\left(\int_a^b f(t) dt\right) = \int_a^b \operatorname{Re}(f(t)) dt$ et $\operatorname{Im}\left(\int_a^b f(t) dt\right) = \int_a^b \operatorname{Im}(f(t)) dt$.

On admettra pour le moment que les intégrales vérifient les propriétés suivantes :

Propriété. Soit I un intervalle inclus dans \mathbb{R} .

Soit f et g deux applications continues de I dans \mathbb{C} . Soit $a, b \in I$.

- Linéarité : Pour tout $\alpha, \beta \in \mathbb{C}$, $\int_a^b (\alpha f + \beta g) = \alpha \int_a^b f + \beta \int_a^b g$.
- Relation de Chasles : Pour tout $c \in I$, $\int_a^b f(t) dt = \int_a^c f + \int_c^b f$.
- Inégalité triangulaire : $\left| \int_a^b f(t) dt \right| \leq \int_{\min(a,b)}^{\max(a,b)} |f(t)| dt$.

Définition. Soit I un intervalle de \mathbb{R} et f une application de I dans \mathbb{C} que l'on suppose continue.

On dit que F est une primitive de f sur I si et seulement si F est dérivable et $F' = f$.

Si F_0 est une primitive de f , alors les autres primitives de f sont exactement les applications $F_0 + k$, où k est une fonction constante.

Théorème : Soit I un intervalle de \mathbb{R} et f une application de I dans \mathbb{C} que l'on suppose continue.

Soit $x_0 \in I$. Alors $x \mapsto \int_{x_0}^x f(t) dt$ est l'unique primitive de f qui s'annule en x_0 .

Corollaire. Soit f une application continue d'un intervalle I dans \mathbb{C} .

Si F est une primitive de f , alors pour tout $a, b \in I$, $\int_a^b f(t) dt = F(b) - F(a) \triangleq [F(t)]_a^b$.

Corollaire. Si f est C^1 de I dans \mathbb{C} , pour tout $a, b \in I$, $\int_a^b f'(t) dt = f(b) - f(a)$.

Notation. L'écriture " $\int f(t) dt = F(t) + k, t \in I$ " signifiera que f est continue de I dans \mathbb{C} et que l'ensemble des primitives de f est $\{F + k/k \in \mathbb{C}\}$.

Changement de variable : si $f : I \rightarrow \mathbb{C}$ est continue et si $\varphi : J \rightarrow I$ est de classe C^1 , alors $\forall (\alpha, \beta) \in J^2$

$$\int_{\alpha}^{\beta} f(\varphi(t)) \varphi'(t) dt = \int_{\varphi(\alpha)}^{\varphi(\beta)} f(x) dx. \text{ Cette égalité correspond au changement de variable } x = \varphi(t).$$

Intégration par parties : soit $u : I \rightarrow \mathbb{C}$ et $v : I \rightarrow \mathbb{C}$ deux applications de classe C^1 sur I .

$$\text{Pour tout } (a, b) \in I^2, \int_a^b u(t) v'(t) dt = [u(t) v(t)]_a^b - \int_a^b u'(t) v(t) dt.$$

$$\text{On a aussi : } \int u(t) v'(t) dt = u(t) v(t) - \int u'(t) v(t) dt, \quad t \in I.$$

La formule d'intégration par parties itérée reste valable pour des fonctions de I dans \mathbb{C} , ainsi que la formule de Taylor avec reste intégral, l'inégalité de Taylor-Lagrange et celle de Taylor-Young.

3 L'exponentielle complexe

3.1 En théorie

Définition. Une suite $(z_n)_{n \in \mathbb{N}}$ de complexes converge vers $\ell \in \mathbb{C}$ si et seulement si

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, |z_n - \ell| \leq \varepsilon.$$

On dit que $(z_n)_{n \in \mathbb{N}}$ est convergente si et seulement si il existe $\ell \in \mathbb{C}$ tel que $z_n \xrightarrow[n \rightarrow +\infty]{} \ell$.

Définition. La série de complexes $\sum z_n$ converge si et seulement si la suite de ses sommes partielles

$$\left(\sum_{k=0}^n z_k \right)_{n \in \mathbb{N}} \text{ est une suite convergente. On note alors } \sum_{n=0}^{+\infty} z_n = \lim_{n \rightarrow +\infty} \sum_{k=0}^n z_k.$$

Propriété. Si $\sum z_n$ est une série convergente de complexes, alors $z_n \xrightarrow[n \rightarrow +\infty]{} 0$.

La réciproque est fautive : on peut avoir $z_n \xrightarrow[n \rightarrow +\infty]{} 0$ alors que la série $\sum z_n$ diverge.

Il faut savoir le démontrer.

Théorème. Si $\sum |z_n|$ converge alors $\sum z_n$ est une série convergente. On dit alors que la série $\sum z_n$ est absolument convergente.

Définition. On a vu, grâce à l'inégalité de Taylor-Lagrange, que pour tout $t \in \mathbb{R}$,

$e^t = \lim_{n \rightarrow +\infty} \sum_{k=0}^n \frac{t^k}{k!}$. Ainsi, pour tout complexe $z \in \mathbb{C}$, la série $\left(\sum \frac{z^n}{n!}\right)_{n \in \mathbb{N}}$ est absolument convergente.

Ceci permet de prolonger l'exponentielle réelle sur \mathbb{C} , en convenant que $\forall z \in \mathbb{C}, e^z = \lim_{n \rightarrow +\infty} \sum_{k=0}^n \frac{z^k}{k!}$.

Propriété. Soit $(z_n)_{n \in \mathbb{N}}$ une suite de complexes qui converge vers $\ell \in \mathbb{C}$. Alors $\overline{z_n} \xrightarrow[n \rightarrow +\infty]{} \overline{\ell}$.

Il faut savoir le démontrer.

Propriété. Pour tout $z \in \mathbb{C}$, $\overline{(e^z)} = e^{\overline{z}}$.

Il faut savoir le démontrer.

Propriété. Pour tout $u, v \in \mathbb{C}$, $e^u e^v = e^{u+v}$.

Il faut savoir le démontrer.

Corollaire. Pour tout $z \in \mathbb{C}$, $e^z \neq 0$ et $\frac{1}{e^z} = e^{-z}$.

Propriété. $|e^z| = e^{\operatorname{Re}(z)}$.

Il faut savoir le démontrer.

Théorème. $e^z \in \mathbb{U} \iff z \in i\mathbb{R}$.

Formules d'Euler :

$$\cos \theta \triangleq \operatorname{Re}(e^{i\theta}) = \frac{e^{i\theta} + e^{-i\theta}}{2} \quad \text{et} \quad \sin \theta \triangleq \operatorname{Im}(e^{i\theta}) = \frac{e^{i\theta} - e^{-i\theta}}{2i}.$$

De plus,

$$e^{i\theta} = \cos \theta + i \sin \theta.$$

Propriété. Pour tout $\theta \in \mathbb{R}$, $\cos \theta = \sum_{n=0}^{+\infty} (-1)^n \frac{\theta^{2n}}{(2n)!}$ et $\sin \theta = \sum_{n=0}^{+\infty} (-1)^n \frac{\theta^{2n+1}}{(2n+1)!}$.

Il faut savoir le démontrer.

Corollaire. \sin est une fonction impaire et \cos est une fonction paire.

\cos et \sin sont de classe C^∞ et $\cos' = -\sin$, $\sin' = \cos$.

Il faut savoir le démontrer.

Formule circulaire : Pour tout $\theta \in \mathbb{R}$, $\cos^2 \theta + \sin^2 \theta = 1$.

Formule d'addition : $\cos(a+b) = \cos a \cos b - \sin a \sin b$ et $\sin(a+b) = \sin a \cos b + \cos a \sin b$.

Définition. On appelle série alternée toute série réelle de la forme $\sum (-1)^n \alpha_n$ ou $\sum (-1)^{n+1} \alpha_n$, où pour tout $n \in \mathbb{N}$, $\alpha_n \in \mathbb{R}_+$.

Théorème spécial des séries alternées (TSSA).

Soit $\sum a_n$ une série alternée. On dit qu'elle est spéciale alternée lorsque la suite $(|a_n|)$ est décroissante et tend vers 0. Dans ce cas, $\sum a_n$ est convergente.

De plus, pour tout $n \in \mathbb{N}$, $\sum_{k=n}^{+\infty} a_k$ est du signe de son premier terme a_n et $|\sum_{k=n+1}^{+\infty} a_k| \leq |a_{n+1}|$.

Propriété. L'application \cos est strictement décroissante sur $]0, 2]$ et elle possède un unique zéro sur $]0, 2]$, que l'on notera $\frac{\pi}{2}$: c'est la **définition** de π .

Propriété. Pour tout $x \in \mathbb{R}$, $\cos(x + \frac{\pi}{2}) = -\sin(x)$ et $\sin(x + \frac{\pi}{2}) = \cos(x)$.

On dispose des tableaux de variations suivants :

x	0	$\frac{\pi}{2}$	π	$\frac{3\pi}{2}$	2π
$\cos(x)$	1 ↘	0 ↘	-1 ↗	0 ↗	1
$\sin(x)$	0 ↗	1 ↘	0 ↘	-1 ↗	0

2π est la plus petite période de \cos , ainsi que de \sin .

Propriété. Soit $(a, b) \in \mathbb{R}^2$ tel que $a^2 + b^2 = 1$.

Il existe un unique $\theta \in [0, 2\pi[$ tel que $a = \cos(\theta)$ et $b = \sin(\theta)$.

Corollaire. Soit $\theta, \varphi \in \mathbb{R}$ tels que $\cos \theta = \cos \varphi$ et $\sin \theta = \sin \varphi$. Alors $\theta \equiv \varphi [2\pi]$.

Paramétrage du cercle unité : l'application $\begin{matrix} \mathbb{R} & \longrightarrow & \mathbb{U} \\ t & \longmapsto & e^{it} \end{matrix}$ est périodique et sa plus petite période est 2π . Sa restriction à $[0, 2\pi[$ est bijective.

Définition. Soit $a, b \in \mathbb{R}$ avec $a < b$ et $\begin{matrix} M : [a, b] & \longrightarrow & \mathbb{C} \\ t & \longmapsto & M(t) \end{matrix}$ une application de classe C^1 .

Notons $C = \{M(t)/t \in [a, b]\}$: C est une courbe dans le plan complexe, dont l'application M est un paramétrage. Par définition, la longueur de C est égale à $\int_a^b |M'(t)| dt$.

Propriété. Soit $\theta \in [0, 2\pi]$. Notons $C_\theta = \{e^{it}/t \in [0, \theta]\}$: C_θ est une portion du cercle unité. Sa longueur est égale à θ .

3.2 Arguments d'un complexe

Propriété. Si $z = a + ib$, où $(a, b) \in \mathbb{R}^2$, $e^z = e^a(\cos(b) + i \sin(b))$.

Définition. Pour tout $z \in \mathbb{C}$, il existe $\rho, \theta \in \mathbb{R}$ tels que $z = \rho e^{i\theta}$. On dit alors que (ρ, θ) est un couple de coordonnées polaires du point $M(z)$ (l'image du complexe z).

On peut imposer $\rho \geq 0$. Dans ce cas, $\rho = |z|$. On dit alors que θ est un argument de z et l'on note $\theta = \arg(z)$.

Lorsque $z \neq 0$, on peut imposer $\rho > 0$ et $\theta \in [0, 2\pi[$. Dans ce cas, le couple (ρ, θ) est unique.

Définition. Un complexe z possède ainsi deux écritures usuelles :

- l'écriture algébrique : $z = a + ib$ avec $a, b \in \mathbb{R}$, ou bien $z = \operatorname{Re}(z) + i \operatorname{Im}(z)$;
- l'écriture trigonométrique (ou exponentielle, ou polaire) : $z = \rho e^{i\theta}$, avec $\rho \in \mathbb{R}_+$ et $\theta \in \mathbb{R}$ (l'angle θ n'est défini que modulo 2π), ou bien $z = |z| e^{i \arg(z)}$.

Les relations suivantes font le lien entre ces deux écritures :

lorsque $z = a + ib = \rho e^{i\theta}$ avec $a, b, \rho, \theta \in \mathbb{R}$ et $\rho \geq 0$,

$$\rho = \sqrt{a^2 + b^2}, \quad \cos \theta = \frac{a}{\sqrt{a^2 + b^2}}, \quad \sin \theta = \frac{b}{\sqrt{a^2 + b^2}}, \quad \tan \theta = \frac{b}{a}.$$

De plus, si $\theta \in]-\pi, \pi[$, alors $\theta = 2 \arctan\left(\frac{b}{a + \sqrt{a^2 + b^2}}\right)$.

Il faut savoir le démontrer.

Propriétés de l'argument : Si z, z_1, z_2 sont trois complexes non nuls, alors

- $\arg(z_1 z_2) \equiv \arg(z_1) + \arg(z_2) [2\pi]$;
- $\arg\left(\frac{1}{z}\right) \equiv \arg(\bar{z}) \equiv -\arg(z) [2\pi]$;

- $\arg\left(\frac{z_1}{z_2}\right) \equiv \arg(z_1) - \arg(z_2) [2\pi]$;
- pour tout $n \in \mathbb{Z}$, $\arg(z^n) \equiv n \arg(z) [2\pi]$;
- $\arg(-z) \equiv \arg(z) + \pi [2\pi]$;
- $(\arg(z_1) \equiv \arg(z_2) [2\pi]) \iff \frac{z_1}{z_2} \in \mathbb{R}_+^*$.

Remarque. Pour tout $z \in \mathbb{C}$, $\arg(e^z) \equiv \operatorname{Im}(z) [2\pi]$.

Interprétation géométrique du produit dans \mathbb{C} : Fixons $z_0 = \rho_0 e^{i\theta_0}$, où $\rho_0 \in \mathbb{R}_+$ et $\theta_0 \in \mathbb{R}$.

La multiplication par z_0 , c'est-à-dire l'application $z \mapsto zz_0$ est la composée de $h : z \mapsto \rho_0 z$ avec $r : z \mapsto ze^{i\theta_0}$. h s'interprète géométriquement comme une homothétie de centre O et de rapport ρ_0 et r comme la rotation de centre O et d'angle θ_0 .

Propriété. Soit $(\rho, \theta) \in \mathbb{R}_+^* \times \mathbb{R}$. Pour tout $z \in \mathbb{C}$, $e^z = \rho e^{i\theta} \iff (\exists k \in \mathbb{Z}, z = \ln(\rho) + i\theta + 2ik\pi)$.

En particulier, l'application exponentielle $\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C}^* \\ z & \longmapsto & e^z \end{array}$ est surjective et $2i\pi$ périodique.

Il faut savoir le démontrer.

Formule de Moivre : Pour tout $n \in \mathbb{N}$ et $t \in \mathbb{R}$, $e^{int} = (\cos t + i \sin t)^n$.

Propriété. Pour tout $z \in \mathbb{C}$, $\frac{d}{dt}(e^{zt}) = ze^{zt}$.

Définition. Pour tout $\alpha \in \mathbb{C}$ et $x \in \mathbb{R}_+^*$, on note $x^\alpha \triangleq e^{\alpha \ln x}$.

Propriété. Pour tout $\alpha \in \mathbb{C}$, $\frac{d}{dt}(t^\alpha) = \alpha t^{\alpha-1}$.

Technique de l'angle moyen : $e^{i\alpha} + e^{i\beta} = e^{i\frac{\alpha+\beta}{2}}(e^{i\frac{\alpha-\beta}{2}} + e^{i\frac{-\alpha+\beta}{2}}) = 2e^{i\frac{\alpha+\beta}{2}} \cos\left(\frac{\alpha-\beta}{2}\right)$

et $e^{i\alpha} - e^{i\beta} = e^{i\frac{\alpha+\beta}{2}}(e^{i\frac{\alpha-\beta}{2}} - e^{i\frac{-\alpha+\beta}{2}}) = 2ie^{i\frac{\alpha+\beta}{2}} \sin\left(\frac{\alpha-\beta}{2}\right)$.

3.3 Linéarisation

Définition. Linéariser une expression trigonométrique, c'est transformer un produit de quantités en sin et cos en une somme de sin ou cos. Une méthode de linéarisation consiste à suivre les étapes suivantes :

- On remplace chaque occurrence en cos ou sin par son expression issue des formules d'Euler ;
- On développe les différents produits qui apparaissent alors ;
- On regroupe les différents termes à l'aide des formules d'Euler pour faire apparaître une somme de cos et de sin.

3.4 Antilinéarisation

Exercice. **Il faut savoir le démontrer.**

Montrer que, pour tout $n \in \mathbb{N}$, il existe un unique polynôme T_n tel que, pour tout $\theta \in \mathbb{R}$, $T_n(\cos \theta) = \cos n\theta$. T_n est appelé le n -ième polynôme de Tchebychev de première espèce.

Exercice. De même, $\sin(n+1)\theta = (\sin \theta)S_n(\cos \theta)$. S_n est le n -ième polynôme de Tchebychev de seconde espèce.

Semaine 12 (du 2 au 6 décembre) : Résumé de cours

Les complexes (fin)

1 Équations polynomiales

1.1 Racines n -ièmes d'un complexe

Les racines n -ièmes de $a \in \mathbb{C}^*$ sont les solutions de l'équation $z^n = a$ en l'inconnue $z \in \mathbb{C}^*$.

Posons $a = re^{i\varphi}$. Alors, en notant $z_0 = r^{\frac{1}{n}} e^{i\frac{\varphi}{n}}$ on a $z_0^n = a$. Ainsi,

$$z^n = a \iff z^n = z_0^n \iff \left(\frac{z}{z_0}\right)^n = 1 \iff \frac{z}{z_0} \in \mathbb{U}_n \iff (\exists k \in \{0, \dots, n-1\}, z = r^{\frac{1}{n}} e^{i\frac{2k\pi + \varphi}{n}}).$$

a possède donc exactement n racines n -ièmes, disposées selon un polygone régulier à n côtés, inscrit dans le cercle de centre O et de rayon $|a|^{\frac{1}{n}}$.

1.2 Équations du second degré

1.2.1 Racines carrées

$a = re^{i\varphi}$ (avec $r > 0$) possède exactement deux racines carrées égales à $\pm\sqrt{r}e^{i\frac{\varphi}{2}}$.

Lorsque $a = x + iy$ avec $x, y \in \mathbb{R}$, on peut déterminer les racines carrées de a selon le procédé suivant :

$$\text{Si } z = \alpha + i\beta, \text{ alors } z^2 = a \iff \begin{cases} x &= \alpha^2 - \beta^2 \\ \sqrt{x^2 + y^2} &= \alpha^2 + \beta^2 \\ \text{sgn}(y) &= \text{sgn}(\alpha\beta) \end{cases}.$$

1.2.2 Racines d'un trinôme

Formule : Soit $a, b, c \in \mathbb{C}$ avec $a \neq 0$. Les solutions de l'équation $az^2 + bz + c = 0$ sont $\frac{-b \pm \delta}{2a}$, où δ est une racine carrée du discriminant $\Delta = b^2 - 4ac$.

Ces deux racines sont égales si et seulement si $\Delta = 0$. Dans ce cas, l'unique racine vaut $\frac{-b}{2a}$. On dit que c'est une racine double.

Il faut savoir le démontrer.

Propriété. Soit $a, b, c \in \mathbb{C}$ avec $a \neq 0$. Notons z_1 et z_2 les deux racines (éventuellement égales à une racine double) du trinôme $aX^2 + bX + c$. Alors
$$\boxed{z_1 + z_2 = -\frac{b}{a} \text{ et } z_1 z_2 = \frac{c}{a}}.$$

Propriété. Soit $s, p \in \mathbb{C}$.

$$\begin{cases} z_1 + z_2 = s \\ z_1 z_2 = p \end{cases} \text{ si et seulement si } \{z_1, z_2\} \text{ est l'ensemble des racines du trinôme } X^2 - sX + p.$$

2 Géométrie du plan complexe

2.1 Distances et angles

Propriété. Soit A, B, C trois points du plan usuel, d'affixes respectifs $a, b, c \in \mathbb{C}$.

- Le vecteur \overrightarrow{AB} est d'affixe $b - a$;
- La distance AB entre A et B est égale à $|b - a|$;
- L'angle orienté $(\widehat{CA, CB})$ vérifie $(\widehat{CA, CB}) \equiv \arg\left(\frac{b - c}{a - c}\right) [2\pi]$.

Il faut savoir démontrer la dernière propriété.

2.2 Orthogonalité et colinéarité

Propriété. Soit \vec{u} et \vec{v} deux vecteurs non nuls d'affixes $u = a + ib$ et $v = c + id$.

- $\vec{u} // \vec{v} \iff \frac{u}{v} \in \mathbb{R} \iff \operatorname{Im}(\bar{u}v) = 0 \iff ad - bc \stackrel{\Delta}{=} \begin{vmatrix} a & c \\ b & d \end{vmatrix} \stackrel{\Delta}{=} \det(\vec{u}, \vec{v}) = 0$.
 $\det(\vec{u}, \vec{v})$ est le déterminant (auss appelé le produit mixte) des deux vecteurs \vec{u} et \vec{v} .
- $\vec{u} \perp \vec{v} \iff \frac{u}{v} \in i\mathbb{R} \iff \operatorname{Re}(\bar{u}v) = 0 \iff ac + bd \stackrel{\Delta}{=} \langle \vec{u}, \vec{v} \rangle = 0$.
 $\langle \vec{u}, \vec{v} \rangle$ est le produit scalaire des deux vecteurs \vec{u} et \vec{v} .

Il faut savoir le démontrer.

Corollaire. Soit A, B, C trois points du plan usuel, d'affixes respectifs $a, b, c \in \mathbb{C}$.

- (A, B et C sont alignés) $\iff \frac{a - b}{c - b} \in \mathbb{R} \iff \operatorname{Im}((a - b)(c - b)) = 0$, c'est-à-dire
 $C \in (AB) \iff \arg(c - a) \equiv \arg(b - a) [\pi] \iff (\exists t \in \mathbb{R}, c = (1 - t)a + tb)$.
- (Le triangle ABC est rectangle en B) $\iff \frac{a - b}{c - b} \in i\mathbb{R} \iff \operatorname{Re}((a - b)(c - b)) = 0$.

2.3 Équation d'un cercle

Notons C le cercle de centre $\alpha = a + ib \in \mathbb{C}$ et de rayon $r > 0$. Alors

$$z = x + iy \in C \iff |z - \alpha| = r \iff (z - \alpha)(\bar{z} - \bar{\alpha}) = r^2 \iff x^2 + y^2 - 2ax - 2by = r^2 - a^2 - b^2.$$

Réciproquement, un ensemble admettant une équation cartésienne de la forme

$x^2 + y^2 - 2ax - 2by = c$ est un cercle éventuellement réduit à un point ou à l'ensemble vide.

3 Les similitudes

3.1 Les similitudes directes

Définition. Une application $f : \mathbb{C} \longrightarrow \mathbb{C}$ est une isométrie si et seulement si elle conserve les distances, c'est-à-dire si et seulement si, pour tout $z, z' \in \mathbb{C}$, $|f(z) - f(z')| = |z - z'|$.

Définition. La translation de vecteur $b \in \mathbb{C}$ est la transformation $t_b : z \longmapsto z + b$. Elle est bijective, d'application réciproque t_{-b} , elle ne possède aucun point fixe lorsque $b \neq 0$, c'est une isométrie.

Définition. La rotation de centre $z_0 \in \mathbb{C}$ et d'angle $\theta \in \mathbb{R}$ est la transformation $r_{z_0, \theta} : z \longmapsto e^{i\theta}(z - z_0) + z_0$. Elle est bijective, d'application réciproque $r_{z_0, -\theta}$, elle admet z_0 comme unique point fixe lorsque $\theta \notin 2\pi\mathbb{Z}$, c'est une isométrie.

Définition. L'homothétie de centre $z_0 \in \mathbb{C}$ et de rapport $\lambda \in \mathbb{R}^*$ est la transformation

$h_{z_0, \lambda} : z \longmapsto \lambda(z - z_0) + z_0$. Elle est bijective, d'application réciproque $h_{z_0, \frac{1}{\lambda}}$, elle admet z_0 comme unique point fixe lorsque $\lambda \neq 1$.

Définition. La similitude directe de centre $z_0 \in \mathbb{C}$, d'angle $\theta \in \mathbb{R}$ et de rapport $\lambda \in \mathbb{R}^*$ est $s_{z_0, \theta, \lambda} = h_{z_0, \lambda} \circ r_{z_0, \theta} = r_{z_0, \theta} \circ h_{z_0, \lambda} = z \mapsto \lambda e^{i\theta}(z - z_0) + z_0$. Elle est bijective, d'application réciproque $s_{z_0, -\theta, \frac{1}{\lambda}}$, elle admet z_0 comme unique point fixe lorsque $\lambda e^{i\theta} \neq 1$, elle conserve les proportions (pour tout $z, z' \in \mathbb{C}$, en posant $s = s_{z_0, \theta, \lambda}$, $|s(z) - s(z')| = |\lambda||z - z'|$), elle conserve les angles (pour tout a, b, c deux à deux distincts, $(\overrightarrow{s(a)s(b)}, \overrightarrow{s(a)s(c)}) = (\overrightarrow{ab}, \overrightarrow{ac})$) : **Il faut savoir le démontrer.**

Définition. On dit que f est une similitude affine directe si et seulement si c'est une application de \mathbb{C} dans \mathbb{C} de la forme $z \mapsto az + b$, où $a \in \mathbb{C}^*$ et $b \in \mathbb{C}$.

On dit que c'est une similitude vectorielle directe lorsque $f(0) = 0$.

Propriété. Soit $f : z \mapsto az + b$ une similitude directe.

Lorsque $a = 1$, c'est une translation.

Lorsque $a \neq 1$, f possède un unique point fixe $z_0 \in \mathbb{C}$ et f est la similitude directe de centre z_0 , d'angle $\arg(a)$ et de rapport $|a|$.

Il faut savoir le démontrer.

Propriété. L'ensemble S^+ des similitudes affines directes est un sous-groupe de $\mathcal{S}(\mathbb{C})$, dont l'ensemble des similitudes vectorielles directes est un sous-groupe.

Il faut savoir le démontrer.

Propriété. L'application qui à la similitude $z \mapsto az + b$ associe a (resp : $|a|$) est un morphisme de groupes, dont le noyau est le sous-groupe des translations (resp : des rotations et des translations).

Corollaire. Une composée, quel que soit l'ordre, de translations, de rotations dont la somme des angles est égale à θ et d'homothéties dont le produit des rapports est égal à λ est une similitude directe de la forme $z \mapsto \lambda e^{i\theta}z + b$.

3.2 Les similitudes indirectes

Définition. Soit D une droite affine du plan usuel. La réflexion d'axe D est la symétrie orthogonale par rapport à D .

Propriété. la conjugaison $z \mapsto \bar{z}$ est la réflexion d'axe Ox .

Remarque. La suite de ce paragraphe est hors programme.

Propriété. Soit $\theta \in \mathbb{R}$. L'application $z \mapsto e^{2i\theta}\bar{z}$ est la réflexion (vectorielle) selon la droite (vectorielle) $e^{i\theta}\mathbb{R}$.

Il faut savoir le démontrer.

Propriété. Soit $\theta \in \mathbb{R}$ et $z_0 \in \mathbb{C}$. L'application $z \mapsto e^{2i\theta}(\bar{z} - \bar{z}_0) + z_0$ est la réflexion (affine) selon la droite (affine) $z_0 + e^{i\theta}\mathbb{R}$.

Il faut savoir le démontrer.

Propriété. Soit $\theta \in \mathbb{R}$ et $z_0 \in \mathbb{C}$. Notons r_D la réflexion selon la droite D .

r_D est involutive, D est l'ensemble de ses points fixes, r_D est une isométrie, r_D transforme les angles en leurs opposés : pour tout a, b, c deux à deux distincts, $(\overrightarrow{s(a)s(b)}, \overrightarrow{s(a)s(c)}) = -(\overrightarrow{ab}, \overrightarrow{ac})$.

Définition. On dit que f est une similitude affine indirecte si et seulement si c'est une application de \mathbb{C} dans \mathbb{C} de la forme $z \mapsto a\bar{z} + b$, où $a \in \mathbb{C}^*$ et $b \in \mathbb{C}$.

On dit que c'est une similitude vectorielle indirecte lorsque $f(0) = 0$.

Une similitude affine indirecte f transforme les angles en leurs opposés et conserve les proportions : $\frac{|f(z) - f(z')|}{|z - z'|}$ est une constante indépendante de $(z, z') \in \mathbb{C}^2$ avec $z \neq z'$.

Définition. Une réflexion glissée d'axe D est la composée commutative d'une réflexion d'axe D avec une translation selon un vecteur parallèle à D .

Propriété. La composée d'une homothétie et d'une réflexion glissée est une similitude affine indirecte.

Propriété. Soit $f : z \mapsto \lambda e^{2i\theta} \bar{z} + b$ une similitude affine indirecte. C'est la composée d'une homothétie de rapport λ avec une réflexion glissée selon une droite parallèle au vecteur $e^{i\theta}$.

Définition. On note S^- l'ensemble des similitudes indirectes et $S = S^- \sqcup S^+$.
 S est un sous-groupe de $\mathcal{S}(\mathbb{C})$.

La composée de k éléments de S^+ avec h éléments de S^- , quel que soit l'ordre, est un élément de S^+ si h est pair et de S^- si h est impair.

Propriété. (Admise pour le moment) : Soit $f : \mathbb{C} \rightarrow \mathbb{C}$ une application. $f \in S$ si et seulement si il existe $\lambda \in \mathbb{R}_+^*$ tel que, pour tout $z, z' \in \mathbb{C}$, $|f(z) - f(z')| = \lambda|z - z'|$.

Propriété. L'application qui associe à toute similitude $z \mapsto az + b$ ou $z \mapsto a\bar{z} + b$ la quantité $|a|$ est un morphisme de groupes, donc le noyau est le sous-groupe des isométries noté I .

Propriété. Posons $I^+ = I \cap S^+$ et $I^- = I \cap S^-$.

I^+ est l'ensemble des translations et des rotations.

I^- est l'ensemble des réflexions glissées.

Propriété. Soit $D = z_0 + e^{i\theta} \mathbb{R}$ et $D' = z'_0 + e^{i\theta'} \mathbb{R}$ deux droites affines.

Si $\theta \not\equiv \theta' [\pi]$, alors $D \cap D'$ est un singleton $\{z_0\}$ et $r_{D'} \circ r_D$ est la rotation de centre z_0 et d'angle $2(\theta' - \theta) = 2(\widehat{D, D'})$.

Sinon, D et D' sont parallèles et $r_{D'} \circ r_D$ est une translation.

Semaine 13 (du 9 au 13 décembre) : Résumé de cours

1 La structure de groupe

1.1 Définitions

Définition. (G, \cdot) est un groupe si et seulement si G est muni d'une loi interne " \cdot " qui vérifie

- l'associativité : pour tout $x, y, z \in G$, $x(yz) = (xy)z$;
- l'existence d'un élément neutre 1_G : pour tout $x \in G$, $1_G \cdot x = x \cdot 1_G = x$;
- l'existence, pour tout $x \in G$, d'un symétrique x^{-1} tel que : $xx^{-1} = x^{-1}x = 1_G$.

Définition. Pour un groupe, "commutatif" et "abélien" sont synonymes.

Notation. On utilise principalement deux notations pour désigner la loi interne d'un groupe :

◇ *Notation multiplicative* : dans un groupe (G, \cdot) , l'élément neutre est noté 1 ou 1_G , le symétrique de $x \in G$ est noté x^{-1} et si $x_1, \dots, x_n \in G$, on note $x_1 \times \dots \times x_n = \prod_{i=1}^n x_i$, en convenant que ce produit vaut 1_G lorsque $n = 0$ (produit vide).

◇ *Notation additive* : dans un groupe abélien $(G, +)$, l'élément neutre est noté 0 ou 0_G , le symétrique de $x \in G$ est noté $-x$ et si $x_1, \dots, x_n \in G$, on note $x_1 + \dots + x_n = \sum_{i=1}^n x_i$, en convenant que cette somme vaut 0_G lorsque $n = 0$ (somme vide).

Définition. Si (G, \cdot) est un groupe fini, le cardinal de G est appelé l'**ordre** de G .

1.2 Calculs dans un groupe

Propriété. Soit (G, \cdot) un groupe et $a \in G$. Alors a est régulier (ou simplifiable) à gauche et à droite, c'est-à-dire que $\forall x, y \in G$, $[ax = ay \implies x = y]$ et $[xa = ya \implies x = y]$.

Propriété. Dans un groupe (G, \cdot) , $(x_1 \times \dots \times x_n)^{-1} = x_n^{-1} \times \dots \times x_1^{-1}$.

Propriété. Dans un groupe abélien $(G, +)$, on pose $x - y \triangleq x + (-y)$.

On dispose des formules : $x - (y + z) = x - y - z$ et $x - (y - z) = x - y + z$.

1.3 Construction de groupes

1.3.1 Groupe produit

Définition. Le groupe produit des n groupes $((G_i, \cdot_i))_{i \in \{1, \dots, n\}}$ est (G, \cdot) , où $G = G_1 \times \dots \times G_n$ et où la loi " \cdot " est définie par : $(x_1, \dots, x_n) \cdot (y_1, \dots, y_n) = (x_1 \cdot_1 y_1, \dots, x_n \cdot_n y_n)$.

1.3.2 Produit fonctionnel

Définition. Soit (G, \cdot) un groupe et A un ensemble quelconque. Pour tout $f, g \in G^A$, on convient que $f.g$ est l'application de A dans G définie par : $\forall a \in A, (f.g)(a) = f(a).g(a)$.

Alors G^A est un groupe, dont l'élément neutre est l'application constante $a \mapsto 1_G$ et pour lequel le symétrique de $f \in G^A$ est

$$f^{-1} : \begin{array}{ccc} A & \longrightarrow & G \\ a & \longmapsto & [f(a)]^{-1}. \end{array}$$

1.3.3 Le groupe symétrique

Propriété. Si E est un ensemble, alors l'ensemble des bijections de E dans E est un groupe pour la loi de composition. On l'appelle le groupe symétrique de E et on le note $\mathcal{S}(E)$. Son élément neutre est l'application identité Id_E et, pour tout $f \in \mathcal{S}(E)$, le symétrique de f est la bijection réciproque de f , dont la notation f^{-1} est en cohérence avec cette propriété.

1.4 Sous-groupes

1.4.1 Définition

Propriété et définition : Soit (G, \cdot) un groupe et H une partie de G .

H est un groupe pour la restriction de la loi " \cdot " à $H \times H$, avec le même élément neutre 1_G si et seulement si

- $H \neq \emptyset$;
- $\forall (x, y) \in H^2, xy \in H$ (stabilité du produit);
- $\forall x \in H, x^{-1} \in H$ (stabilité du symétrique).

Cet ensemble de conditions est équivalent à

- $H \neq \emptyset$;
- $\forall (x, y) \in H^2, xy^{-1} \in H$.

Dans ce cas, on dit que H est un **sous-groupe** de G .

Propriété de transitivité : Un sous-groupe d'un sous-groupe d'un groupe G est un sous-groupe de G .

1.4.2 Groupe engendré par une partie

Propriété. Soit I un ensemble non vide, éventuellement infini. Soient G un groupe et $(H_i)_{i \in I}$ une famille de sous-groupes de G . Alors l'intersection $\bigcap_{i \in I} H_i$ est un sous-groupe de G .

Il faut savoir le démontrer.

Définition. Soit G un groupe et A une partie de G .

Notons \mathcal{S} l'ensemble des sous-groupes de G contenant A . \mathcal{S} est non vide car $G \in \mathcal{S}$.

Alors $\bigcap_{H \in \mathcal{S}} H$ est un sous-groupe de G contenant A et, par construction, c'est le plus petit sous-groupe contenant A . On le note $Gr(A)$.

Propriété. Si $A \subset B$, alors $Gr(A) \subset Gr(B)$.

Propriété. Soit (G, \cdot) un groupe et A une partie de G . Notons $A^{-1} = \{a^{-1} / a \in A\}$.

Alors $Gr(A) = \left\{ \prod_{i=1}^n a_i / n \in \mathbb{N}, \forall i \in \{1, \dots, n\}, a_i \in A \cup A^{-1} \right\}$.

Il faut savoir le démontrer.

Définition. Si H et K sont deux sous-groupes d'un groupe abélien $(G, +)$, on note $H + K = \{h + k / (h, k) \in H \times K\}$. C'est le groupe engendré par $H \cup K$.

Définition. Soit G un groupe et A une partie de G .
 A est une **partie génératrice** de G si et seulement si $Gr(A) = G$.

1.4.3 Puissances d'un élément d'un groupe

Définition. Soit (G, \cdot) un groupe et $a \in G$. On définit la famille $(a^n)_{n \in \mathbb{Z}}$ par les relations suivantes :

- Initialisation : $a^0 = 1_G$ (encore le produit vide) ;
- Itération : pour tout $n \in \mathbb{N}$, $a^{n+1} = a \cdot a^n$ (donc pour $n \in \mathbb{N}^*$, $a^n = \underbrace{a \times \cdots \times a}_{n \text{ fois}}$) ;
- Symétrique : pour tout $n \in \mathbb{Z}$ avec $n < 0$, $a^n = (a^{-n})^{-1}$.

Formules : pour tout $n, m \in \mathbb{Z}$, $a^n a^m = a^{n+m}$ et $(a^n)^m = a^{nm}$.
 Si $ab = ba$ (on dit que a et b commutent), pour tout $n \in \mathbb{Z}$, $(ab)^n = a^n b^n$.

Remarque. Si a et b commutent, alors pour tout $n, k \in \mathbb{Z}$, a^n et b^k commutent également entre eux.
Il faut savoir le démontrer.

En notation additive, dans le cadre des groupes commutatifs, ce qui précède devient :

Définition. soit $(G, +)$ un groupe commutatif et a un élément de G . On **définit** la famille $(na)_{n \in \mathbb{Z}}$ par les relations suivantes :

- Initialisation : $0.a = 0_G$;
- Itération : pour tout $n \in \mathbb{N}$, $(n+1).a = a + (n.a)$
 (donc pour $n \in \mathbb{N}^*$, $n.a = \underbrace{a + \cdots + a}_{n \text{ fois}}$) ;
- Symétrique : pour tout $n \in \mathbb{Z}$ avec $n < 0$, $n.a = -((-n).a)$.

Propriété. Soit $(G, +)$ un groupe abélien et $a, b \in G$. Pour tout $n, m \in \mathbb{Z}$,
 $(n.a) + (m.a) = (n+m).a$, $m.(n.a) = (nm).a$ et $n.(a+b) = (na) + (nb)$.

Propriété. Soit $(G, +)$ un groupe abélien et A une partie de G .

Alors $Gr(A) = \left\{ \sum_{a \in A} n_a.a / (n_a)_{a \in A} \in \mathbb{Z}^{(A)} \right\}$.

Remarque. En particulier, $Gr(\{x_1, \dots, x_p\}) = \left\{ \sum_{i=1}^p n_i x_i / (n_i)_{1 \leq i \leq p} \in \mathbb{Z}^p \right\}$.

1.4.4 Groupe monogène

Propriété. Soit (G, \cdot) un groupe et $a \in G$. Alors le groupe engendré par la partie $\{a\}$ est $Gr(\{a\}) = \{a^n / n \in \mathbb{Z}\}$. On le note plus simplement $Gr(a)$.

Propriété. Soit $(G, +)$ un groupe abélien et $a \in G$. Alors le groupe engendré par la partie $\{a\}$ est $Gr(\{a\}) = \{na / n \in \mathbb{Z}\}$. On le note $Gr(a)$. On peut donc écrire $Gr(a) = \mathbb{Z}.a$.

Propriété. Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$, où $n \in \mathbb{N}$.

Il faut savoir le démontrer.

Définition. Soit a un élément d'un groupe G . Lorsque $Gr(a)$ est de cardinal fini, ce cardinal est appelé l'ordre de a .

Définition. On dit qu'un groupe (G, \cdot) est **monogène** si et seulement si il existe $a \in G$ tel que $G = Gr(a)$. On dit alors que a est un **générateur** de G .

Remarque. Tout groupe monogène est abélien.

Définition. Un groupe G est dit **cyclique** si et seulement si G est monogène et fini.

Exemple. $\mathbb{U}_n = \{e^{2i\pi \frac{k}{n}} / k \in \{0, \dots, n-1\}\}$ est un groupe cyclique.

Propriété. Soit (G, \cdot) un groupe, $a \in G$ et $n \in \mathbb{N}^*$.

Les propriétés suivantes sont équivalentes :

- i) $\text{Gr}(a)$ est cyclique de cardinal n .
- ii) $\{k \in \mathbb{N}^* / a^k = 1\}$ est non vide et son minimum est égal à n .
- iii) Pour tout $k \in \mathbb{Z}$, $[a^k = 1 \iff k \in n\mathbb{Z}]$.
- iv) Les éléments de $\text{Gr}(a)$ sont exactement $1, a, \dots, a^{n-1}$ et ils sont deux à deux distincts.

Dans ce cas, n est l'ordre de a et de $\text{Gr}(a)$.

Il faut savoir le démontrer.

1.5 Morphisme de groupes

Définition. Soient (G, Δ) et (H, ∇) deux groupes.

Une application f de G dans H est un **morphisme** (on dit aussi un **homomorphisme**) de groupes si et seulement si

$$\forall (x, y) \in G^2 \quad f(x \Delta y) = f(x) \nabla f(y).$$

Un **isomorphisme** est un morphisme bijectif.

Un **endomorphisme** est un morphisme de G dans lui-même.

Un **automorphisme** est un endomorphisme bijectif.

Propriété. Si a est un élément de (G, \cdot) , alors $\begin{matrix} (\mathbb{Z}, +) & \longrightarrow & (G, \cdot) \\ n & \longmapsto & a^n \end{matrix}$ est un morphisme de groupes.

Propriété. Si f est un morphisme de (G, \cdot) dans (H, \cdot) , alors $f(1_G) = 1_H$ et pour tout $x \in G$, $f(x)^{-1} = f(x^{-1})$.

Propriété. En notation additive, si f est un morphisme entre deux groupes abéliens $(G, +)$ et $(H, +)$, alors $f(0_G) = 0_H$ et, pour tout $x \in G$, $-f(x) = f(-x)$.

Propriété. Soit φ un morphisme du groupe (G, \cdot) vers le groupe (G', \cdot) .

Alors, pour tout $n \in \mathbb{N}$ et $x_1, \dots, x_n \in G$, $\varphi\left(\prod_{i=1}^n x_i\right) = \prod_{i=1}^n \varphi(x_i)$.

De plus, pour tout $n \in \mathbb{Z}$ et $a \in G$, $\varphi(a^n) = \varphi(a)^n$.

Il faut savoir le démontrer.

Propriété. Soit φ un morphisme du groupe abélien $(G, +)$ vers le groupe abélien $(G', +)$. Alors,

pour tout $n \in \mathbb{N}$ et $x_1, \dots, x_n \in G$, $\varphi\left(\sum_{i=1}^n x_i\right) = \sum_{i=1}^n \varphi(x_i)$.

De plus, pour tout $n \in \mathbb{Z}$ et $a \in G$, $\varphi(na) = n\varphi(a)$.

Propriété. La composée de deux morphismes de groupes est un morphisme de groupes.

Propriété. Si $f : G \longrightarrow H$ est un isomorphisme de groupes, f^{-1} est encore un isomorphisme de groupes, de H dans G .

Propriété. Soit (G, \cdot) un groupe. On note $\text{Aut}(G)$ l'ensemble des automorphismes de G . C'est un sous-groupe de $\mathcal{S}(G)$.

Définition. Soit $\varphi : G \longrightarrow G$ un endomorphisme et H un sous-groupe de G . On peut définir $\varphi|_H^H$ si et seulement si H est stable par φ , c'est-à-dire si et seulement si $[\forall x \in H, \varphi(x) \in H]$. Dans ce cas, $\varphi|_H^H$ est aussi un **endomorphisme**, appelé l'endomorphisme induit par φ sur H , ou plus simplement la restriction de φ à H (il y a bien sûr ambiguïté).

Propriété. Soit f un morphisme de G dans H , G' un sous-groupe de G et H' un sous-groupe de H . Alors $f(G')$ est un sous-groupe de H et $f^{-1}(H')$ est un sous-groupe de G .

Il faut savoir le démontrer.

Définition. Soient (G, \cdot) et (H, \cdot) deux groupes, et f un morphisme de G dans H . On appelle **noyau** de f le sous-groupe de G suivant :

$$\boxed{Ker(f) = f^{-1}(\{1_H\}) = \{x \in G / f(x) = 1_H\}}.$$

On appelle **image** de f le sous-groupe de H suivant :

$$\boxed{Im(f) = f(G) = \{f(x) / x \in G\}}.$$

Remarque. En notation additive, Si f est un morphisme dont le groupe d'arrivée $(H, +)$ est abélien, alors $Ker(f) = f^{-1}(\{0_H\}) = \{x \in G / f(x) = 0_H\}$.

Propriété. Soient (G, \cdot) et (H, \cdot) deux groupes, et f un morphisme de G dans H .

$$\begin{array}{ll} f \text{ est injective si et seulement si} & Ker(f) = \{1_G\}, \\ f \text{ est surjective si et seulement si} & Im(f) = H. \end{array}$$

Propriété. Un groupe est monogène non cyclique si et seulement si il est isomorphe à $(\mathbb{Z}, +)$.

Il faut savoir le démontrer.

1.6 Groupe symétrique

Notation. Pour tout $n \in \mathbb{N}$, on pose $\mathbb{N}_n = \{k \in \mathbb{N} / 1 \leq k \leq n\}$. En particulier $\mathbb{N}_0 = \emptyset$.

Définition. Soit $n \in \mathbb{N}$. $\mathcal{S}(\mathbb{N}_n)$ s'appelle le groupe symétrique de degré n . Il est plus simplement noté \mathcal{S}_n . Ses éléments sont les bijections sur \mathbb{N}_n , que l'on appelle aussi des permutations.

Notation. Si $f \in \mathcal{S}_n$, on note $f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$.

Définition. Soient $k \in \mathbb{N}_n$ et $a_1, a_2 \dots a_k$ k éléments distincts de \mathbb{N}_n .

On note $(a_1 \ a_2 \ \dots \ a_k)$ la permutation f telle que : $\forall i \in \{1, \dots, k-1\} \ f(a_i) = a_{i+1}$, $f(a_k) = a_1$, les autres éléments de \mathbb{N}_n étant invariants par f .

On dit que $(a_1 \ \dots \ a_k)$ est un **cycle** de longueur k dont le **support** est $\{a_1, \dots, a_k\}$.

Définition. On appelle **transposition** tout cycle de longueur 2.

Si $a, b \in \mathbb{N}_n$ avec $a \neq b$, la transposition $(a \ b)$ échange a et b sans modifier les autres éléments de \mathbb{N}_n .

Propriété. Deux cycles dont les supports sont disjoints commutent toujours entre eux.

Théorème. Toute permutation de \mathcal{S}_n se décompose de manière unique en un produit (commutatif) de cycles dont les supports sont deux à deux disjoints.

Propriété. Pour tout $n \in \mathbb{N}^*$, pour toute permutation σ de \mathcal{S}_n , il existe $k \in \mathbb{N}$ et k transpositions τ_1, \dots, τ_k telles que $\sigma = \tau_1 \circ \dots \circ \tau_k$. Cependant une telle décomposition n'est pas unique.

La démonstration par récurrence est à connaître.

Formule : $(a_1 \ a_2 \ \dots \ a_k) = (a_1 \ a_2) \circ (a_2 \ a_3) \circ \dots \circ (a_{k-1} \ a_k)$.

Définition. Soit $n \in \mathbb{N}^*$ et soit $\sigma \in \mathcal{S}_n$. La décomposition de σ en un produit de transpositions $\tau_1 \circ \dots \circ \tau_k$ n'est pas unique, mais le nombre k de transpositions utilisées a toujours la même parité. Ainsi $(-1)^k$ ne dépend que de σ . On l'appelle la signature de σ et on le note $\varepsilon(\sigma)$.

Les permutations de signature 1 s'appellent les permutations paires,

Les permutations de signature -1 s'appellent les permutations impaires.

Propriété. L'application signature est l'unique morphisme de \mathcal{S}_n dans $(\{-1, 1\}, \times)$ qui envoie toute transposition sur -1 .

Propriété. Soit $n \in \mathbb{N}^*$. On note \mathcal{A}_n l'ensemble des permutations paires de \mathcal{S}_n . C'est un sous-groupe de \mathcal{S}_n , appelé le groupe alterné de degré n .

Propriété. Si $n \geq 2$, alors $|\mathcal{A}_n| = \frac{n!}{2}$.

Il faut savoir le démontrer.

2 La structure d'anneau

2.1 Définition

Définition. On appelle **anneau** tout triplet $(A, +, \cdot)$, où A est un ensemble et où “+” et “.” sont deux lois internes sur A telles que

- $(A, +)$ est un groupe abélien (l'élément neutre étant noté 0 ou 0_A),
- “.” est une loi associative, admettant un élément neutre noté 1 ou 1_A ,
- la loi “.” est **distributive** par rapport à la loi “+”, c'est-à-dire que $\forall (x, y, z) \in A^3$ $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ et $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$.

Définition. Un anneau $(A, +, \cdot)$ est commutatif ou abélien si et seulement si la loi “.” est commutative.

2.2 Calculs dans un anneau

Propriété. Si A est un anneau, pour tout $x, y \in A$ et $n \in \mathbb{Z}$, $0 \cdot x = x \cdot 0 = 0$, $(nx) \cdot y = x \cdot (ny) = n(xy)$. En particulier, $-x = (-1_A) \cdot x = x \cdot (-1_A)$.

Il faut savoir le démontrer.

Exemple. $\{0\}$ est un anneau en posant $0 + 0 = 0$ et $0 \cdot 0 = 0$. On l'appelle l'anneau nul.

Propriété. Si A n'est pas l'anneau nul, alors $1_A \neq 0_A$.

Exemples. Si A est un anneau, pour tout ensemble E , $\mathcal{F}(E, A)$ et $A^{\mathbb{N}}$ sont des anneaux.

Propriété. *Généralisation de la distributivité.* Soient A un anneau, et $n, p \in \mathbb{N}$.

Pour tout $(a_1, \dots, a_n) \in A^n$ et $(b_1, \dots, b_p) \in A^p$ $\left(\sum_{i=1}^n a_i\right) \cdot \left(\sum_{i=1}^p b_i\right) = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} a_i \cdot b_j$.

2.3 Puissances d'un élément

Notation. Dans ce paragraphe on fixe un anneau A .

Définition. $a \in A$ est inversible si et seulement s'il admet un symétrique (un inverse) pour la loi “.”.

Définition. Si $a \in A$. On définit la famille (a^n) par les relations suivantes :

- Initialisation : $a^0 = 1_A$;
- Itération : pour tout $n \in \mathbb{N}$, $a^{n+1} = a \cdot a^n$ (donc pour $n \in \mathbb{N}^*$, $a^n = \underbrace{a \times \dots \times a}_{n \text{ fois}}$) ;
- Lorsque a est inversible, pour tout $n \in \mathbb{Z}$ avec $n < 0$, on note $a^n = (a^{-n})^{-1}$.

Définition. $a \in A \setminus \{0\}$ est nilpotent si et seulement si il existe $n \in \mathbb{N}$ avec $n \geq 2$ tel que $a^n = 0$.

Propriété. Pour tout $n, m \in \mathbb{N}$ $a^n a^m = a^{n+m}$ et $(a^n)^m = a^{nm}$.

Lorsque a est inversible, c'est valable pour tout $n, m \in \mathbb{Z}$.

Propriété. Soit $a, b \in A$ tels que $ab = ba$ (on dit que a et b commutent).

Pour tout $n, m \in \mathbb{N}$, $(ab)^n = a^n b^n$. Lorsque a et b sont inversibles, c'est valable pour tout $n, m \in \mathbb{Z}$.

2.4 Les sous-anneaux

Définition. Soit $(A, +, \cdot)$ un anneau et $B \subset A$. B est un sous-anneau de A si et seulement si, en le munissant des restrictions sur B^2 des lois “+” et “.”, B est un anneau possédant les mêmes éléments neutres que ceux de A .

Propriété. B est un sous-anneau de A ssi $1_A \in B$, et $\forall (x, y) \in B^2$, $x - y \in B$ et $xy \in B$.

Propriété. Si A est un anneau, son plus petit sous-anneau est $\mathbb{Z}.1_A = \{n.1_A / n \in \mathbb{Z}\}$.

Il faut savoir le démontrer.

2.5 Les corps

Propriété. L'ensemble $U(A)$ des éléments inversibles d'un anneau A est un groupe multiplicatif.

Définition. Un anneau A est un **corps** si et seulement si

- A n'est pas réduit à $\{0_A\}$,
- A est commutatif,
- et tout élément de A différent de 0_A est inversible.

Définition. Soit $(\mathbb{K}, +, \cdot)$ un corps et $\mathbb{L} \subset \mathbb{K}$. \mathbb{L} est un sous-corps de \mathbb{K} si et seulement si, en le munissant des restrictions sur \mathbb{L}^2 des lois “+” et “.”, \mathbb{L} est un corps possédant les mêmes éléments neutres que ceux de \mathbb{K} .

Propriété. \mathbb{L} est un sous-corps de \mathbb{K} ssi c'est un sous-anneau de \mathbb{K} tel que : $\forall x \in \mathbb{L} \setminus \{0\} \quad x^{-1} \in \mathbb{L}$.

2.6 Formules

Notation. On fixe un anneau $(A, +, \cdot)$.

Formule du binôme de Newton. Si $a, b \in A$ avec $ab = ba$, alors $(a + b)^n = \sum_{i=0}^n \binom{n}{i} a^i b^{n-i}$.

Formule du multinôme (hors programme) : Soit b_1, \dots, b_p des éléments de A qui commutent deux à deux. Alors, pour tout $n \in \mathbb{N}$, $(b_1 + \dots + b_p)^n = \sum_{\alpha_1 + \dots + \alpha_p = n} \frac{n!}{\alpha_1! \dots \alpha_p!} b_1^{\alpha_1} \dots b_p^{\alpha_p}$.

Formule de Bernoulli : Si $a, b \in A$ avec $ab = ba$, alors $a^{n+1} - b^{n+1} = (a - b) \sum_{k=0}^n a^k b^{n-k}$.

Sommes partielles d'une série géométrique.

Si $x \in A$ et $m, n \in \mathbb{N}$ avec $m \leq n$, $(1_A - x) \cdot \sum_{i=m}^n x^i = x^m - x^{n+1}$.

2.7 Anneaux intègres

Définition. Soit A un anneau.

$a \in A \setminus \{0\}$ est un diviseur à gauche de 0 si et seulement s'il existe $b \in A \setminus \{0\}$ tel que $ab = 0$.

C'est un diviseur à droite de 0 si et seulement s'il existe $b \in A \setminus \{0\}$ tel que $ba = 0$.

Propriété. Un élément non nul d'un anneau est régulier à gauche si et seulement si ce n'est pas un diviseur à gauche de 0. Idem à droite.

Il faut savoir le démontrer.

Définition. Un anneau A est intègre si et seulement si il est commutatif et non nul et s'il n'admet aucun diviseur de 0, ni à gauche ni à droite, c'est-à-dire si et seulement si, pour tout $a, b \in A$, $ab = 0 \implies (a = 0) \vee (b = 0)$.

Propriété. Un corps est en particulier un anneau intègre.

2.8 Morphismes d'anneaux

Définition. Soient $(A, +_A, \cdot_A)$ et $(B, +_B, \cdot_B)$ deux anneaux.

Une application $f : A \longrightarrow B$ est un **morphisme d'anneaux** si et seulement si

- $f(1_A) = 1_B$,
- $\forall (x, y) \in A^2 \quad f(x +_A y) = f(x) +_B f(y)$,
- $\forall (x, y) \in A^2 \quad f(x \cdot_A y) = f(x) \cdot_B f(y)$.

Un **isomorphisme** est un morphisme bijectif.

Un **endomorphisme** est un morphisme de A dans lui-même.

Un **automorphisme** est un endomorphisme bijectif.

Remarque. Lorsque f est un morphisme d'anneaux, c'est un morphisme de groupes, d'où $\text{Im}(f)$ et $\text{Ker}(f) = f^{-1}(\{0\})$.

Propriété. Soient A et B deux anneaux et f un morphisme d'anneaux de A dans B .

Pour tout $a \in A$, $p \in \mathbb{N}$ et $n \in \mathbb{Z}$, $f(na) = nf(a)$, $f(a^p) = f(a)^p$.

Si a est inversible, alors $f(a)$ est inversible et $f(a^n) = f(a)^n$. En particulier, $f(a^{-1}) = f(a)^{-1}$.

Propriété. La composée de deux morphismes d'anneaux est un morphisme d'anneaux.

Propriété. Si f est un isomorphisme d'anneaux, f^{-1} est encore un isomorphisme d'anneaux.

Propriété. Soient $(A, +_A, \cdot_A)$ et $(B, +_B, \cdot_B)$ deux anneaux et $f : A \longrightarrow B$ un morphisme d'anneaux.

L'image directe par f de tout sous-anneau de A est un sous-anneau de B .

L'image réciproque selon f de tout sous-anneau de B est un sous-anneau de A .

Définition. Soit \mathbb{K} et \mathbb{L} deux corps et f une application de \mathbb{K} dans \mathbb{L} . On dit que f est un morphisme de corps si et seulement si c'est un morphisme d'anneaux.

Propriété. (hors programme) Un morphisme de corps est toujours injectif.

Il faut savoir le démontrer.

Propriété. Soit $f : \mathbb{K} \longrightarrow \mathbb{L}$ un morphisme de corps.

Si \mathbb{K}' est un sous-corps de \mathbb{K} , alors $f(\mathbb{K}')$ est un sous-corps de \mathbb{L} .

Si \mathbb{L}' est un sous-corps de \mathbb{L} , alors $f^{-1}(\mathbb{L}')$ est un sous-corps de \mathbb{K} .

2.9 Les anneaux produits

Définition. Soient $n \in \mathbb{N}^*$ et $((A_i, +, \cdot))_{i \in \{1, \dots, n\}}$ une famille de n anneaux.

L'anneau produit de cette famille est $(A, +, \cdot)$, où $A = A_1 \times \dots \times A_n$ et où les lois “+” et “.” sont définies par : pour tout $x = (x_1, \dots, x_n) \in A$ et $y = (y_1, \dots, y_n) \in A$,

$$x + y = (x_1 + y_1, \dots, x_n + y_n) \text{ et } x \cdot y = (x_1 \cdot y_1, \dots, x_n \cdot y_n).$$

Définition. Pour tout $i \in \mathbb{N}_n$, la $i^{\text{ème}}$ projection, $p_i : \begin{array}{ccc} A & \longrightarrow & A_i \\ (a_1, \dots, a_n) & \longmapsto & a_i \end{array}$ est un morphisme surjectif d'anneaux.

Semaine 14 (du 16 au 20 décembre) : Résumé de cours

1 Les idéaux

Définition. Une partie I d'un anneau A est un **idéal** de A à gauche (resp : à droite) si et seulement si $I \neq \emptyset$, $\forall (x, y) \in I^2$, $x + y \in I$ et $\forall (x, y) \in \boxed{A \times I}$, $x.y \in I$ (resp : $y.x \in I$).

On dit qu'un idéal est absorbant pour le produit.

Lorsque I est un idéal à gauche et à droite, on dit que c'est un idéal bilatère.

Notation. Pour la suite, on fixe un anneau $(A, +, \cdot)$ **que l'on suppose commutatif**.

Propriété. Tout idéal est un groupe pour la loi "+".

Propriété. Soit A un anneau commutatif et I un idéal de A . Alors $\boxed{1 \in I \iff I = A}$.

Propriété. Une intersection d'idéaux de A est un idéal de A .

Il faut savoir le démontrer.

Définition. Soit B une partie de A . L'idéal engendré par B est l'intersection des idéaux de A contenant B . C'est le plus petit idéal (au sens de l'inclusion) contenant B . On le note $Id(B)$.

Propriété. Soient B et C deux parties de A telles que $C \subset B$. Alors $Id(C) \subset Id(B)$.

Propriété. Si B est une partie de A , $Id(B) = \left\{ \sum_{i=1}^n a_i b_i / n \in \mathbb{N}, (a_1, \dots, a_n) \in A^n, (b_1, \dots, b_n) \in B^n \right\}$.

Il faut savoir le démontrer.

Définition. Un idéal I de A est principal si et seulement si il existe $b \in A$ tel que $I = Id(b)$.

Définition. Un anneau est principal si et seulement si c'est un anneau commutatif, intègre et dont tous les idéaux sont principaux.

Théorème. \mathbb{Z} est un anneau principal.

Théorème. Si \mathbb{K} est un corps, alors $\mathbb{K}[X]$ est un anneau principal.

Il faut savoir le démontrer.

Propriété. Soit I et J deux idéaux de A . Alors $I + J$ est un idéal de A .

Propriété. Soient A et B deux anneaux commutatifs et $f : A \longrightarrow B$ un morphisme d'anneaux. $Ker(f)$ est un idéal de A et si I est un idéal de B , $f^{-1}(I)$ est un idéal de A contenant $Ker(f)$.

Il faut savoir le démontrer.

2 Groupes quotients

Notation. On fixe un groupe (G, \cdot) et un sous-groupe H de G .

On note R_H la relation binaire définie sur G par : $\forall (x, y) \in G^2, [xR_H y \iff x^{-1}y \in H]$.

Propriété. R_H est une relation d'équivalence et, pour tout $x \in G$, la classe d'équivalence de x pour R_H est $\bar{x} = \{xh/h \in H\} \triangleq xH$. On note G/H l'ensemble des classes d'équivalence.

Exemple fondamental : lorsque $G = (\mathbb{Z}, +)$ et $H = n\mathbb{Z}$, où $n \in \mathbb{N}$:

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{k}/k \in \mathbb{Z}\}, \text{ où } \bar{k} = \{k + na/a \in \mathbb{Z}\}.$$

Théorème de Lagrange (Hors programme) : Si G est de cardinal fini, alors $|H|$ divise $|G|$.

Corollaire. (Hors programme) Si p est un nombre premier, tout groupe de cardinal p est cyclique.

Théorème. (au programme) : Si (G, \cdot) est un groupe fini, $\forall a \in G, a^{|G|} = 1_G$.

Notation. Pour la suite, on suppose que $(G, +)$ est un groupe **commutatif**.

Ainsi, pour tout $x, y \in G, xR_H y \iff y - x \in H$.

Théorème. En posant, pour tout $x, y \in G, \bar{x} + \bar{y} \triangleq \overline{x + y}$, on définit une loi “+” sur G/H pour laquelle G/H est un groupe commutatif.

Il faut savoir le démontrer.

Définition. $\begin{matrix} G & \longrightarrow & G/H \\ x & \longmapsto & \bar{x} \end{matrix}$ est un morphisme, que l'on appelle la surjection canonique.

Propriété. Soit $n \in \mathbb{N}$. Dans $(\mathbb{Z}/n\mathbb{Z}, +)$, on dispose des règles de calcul suivantes :

- Pour tout $a, b \in \mathbb{Z}, \bar{a} = \bar{b} \iff a \equiv b [n]$,
- Pour $a, b \in \mathbb{Z}, \bar{a} + n\bar{b} = \bar{a}$,
- $\bar{0} = 0_{\mathbb{Z}/n\mathbb{Z}}$,
- pour tout $k \in \mathbb{Z}, -\bar{k} = \overline{-k}$,
- pour tout $h, k \in \mathbb{Z}, \overline{h + k} = \bar{h} + \bar{k}$,
- pour tout $h, k \in \mathbb{Z}, \overline{hk} = \bar{h}\bar{k}$.

Propriété. Si $n = 0$, $\mathbb{Z}/n\mathbb{Z}$ est monogène non cyclique. Il est isomorphe à \mathbb{Z} .

Tout groupe monogène non cyclique est isomorphe à \mathbb{Z} .

Propriété. Si $n \geq 1$, $\mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique de cardinal n : $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$.

Si $G = Gr(a)$ est un autre groupe cyclique de cardinal n , il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$:

$$\begin{matrix} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & (G, \cdot) \\ \bar{k} & \longmapsto & a^k \end{matrix} \text{ est un isomorphisme.}$$

Il faut savoir le démontrer.

3 Anneaux quotients

Notation. On fixe un anneau commutatif $(A, +, \cdot)$ et un idéal I de A .

Propriété. $(A/I, +, \cdot)$ est un anneau commutatif en posant, pour tout $x, y \in A, \overline{x \cdot y} = \bar{x} \cdot \bar{y}$.

Propriété. Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, on dispose des règles supplémentaires de calculs suivantes :

- Pour tout $h, k \in \mathbb{Z}, \overline{hk} = \bar{h} \cdot \bar{k}$.
- $\bar{1} = 1_{\mathbb{Z}/n\mathbb{Z}}$.

Semaine 15 (du 6 au 10 janvier) : Résumé de cours

1 $\mathbb{Z}/n\mathbb{Z}$

1.1 Propriétés spécifiques de $\mathbb{Z}/n\mathbb{Z}$

Notation. On fixe $n \in \mathbb{N}$ avec $n \geq 2$.

Propriété. (hors programme) les sous-groupes (resp : les idéaux) de $\mathbb{Z}/n\mathbb{Z}$ sont les $\bar{k}\mathbb{Z}/n\mathbb{Z}$, où k est un diviseur de n . En particulier, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est principal.

Théorème. Soit $k \in \mathbb{Z}$. \bar{k} engendre le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ (resp : est inversible dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$) ssi $k \wedge n = 1$. Dans ce cas, il existe $u, v \in \mathbb{Z}$ tels que $uk + vn = 1$ et $\bar{u} = \bar{k}^{-1}$.

Il faut savoir le démontrer.

Théorème. Soit $n \geq 2$. $\mathbb{Z}/n\mathbb{Z}$ est un corps (resp : est intègre) si et seulement si $n \in \mathbb{P}$.

Il faut savoir le démontrer.

Notation. Lorsque $p \in \mathbb{P}$, le corps $\mathbb{Z}/p\mathbb{Z}$ est souvent noté \mathbb{F}_p .

1.2 Théorème chinois

Théorème des restes chinois : Si a et b sont deux entiers supérieurs à 2 et **premiers entre eux**,
 $f : \mathbb{Z}/ab\mathbb{Z} \longrightarrow (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$ est un isomorphisme d'anneaux.
 $\bar{k} \longmapsto (\bar{k}, \bar{k})$

Il faut savoir le démontrer, en incluant la preuve constructive de la surjectivité : pour $h, k \in \mathbb{Z}$, comment déterminer $\ell \in \mathbb{Z}$ tel que $\ell \equiv h [a]$ et $\ell \equiv k [b]$?

Théorème chinois (généralisation) : Soit $n \geq 2$ et a_1, \dots, a_n n entiers supérieurs à 2 et **deux à deux premiers entre eux** :

$\mathbb{Z}/(a_1 \times \dots \times a_n)\mathbb{Z} \longrightarrow (\mathbb{Z}/a_1\mathbb{Z}) \times \dots \times (\mathbb{Z}/a_n\mathbb{Z})$ est un isomorphisme d'anneaux.
 $\bar{k} \longmapsto (\bar{k}, \dots, \bar{k})$

Remarque. pour $h_1, \dots, h_n \in \mathbb{Z}$, on peut calculer $\ell \in \mathbb{Z}$ tel que, pour tout $i \in \{1, \dots, n\}$, $\ell \equiv h_i [a_i]$.
À connaître.

1.3 L'indicatrice d'Euler

Définition. Pour tout $n \in \mathbb{N}^*$, on pose $\varphi(n) = |U(\mathbb{Z}/n\mathbb{Z})|$.

Remarque. $\varphi(1) = 1$, car $\mathbb{Z}/1\mathbb{Z}$ est l'anneau nul, pour lequel 0 est inversible.

Pour $n \geq 2$, $\varphi(n) = \#\{k \in \{1, \dots, n-1\} / k \wedge n = 1\}$.

Propriété. $\varphi(1) = 1$ et si p est un nombre premier, alors $\varphi(p) = p - 1$.

Propriété. Si p est premier et si $k \in \mathbb{N}^*$, alors $\varphi(p^k) = p^k - p^{k-1}$.

Il faut savoir le démontrer.

Propriété. Soit a et b sont deux entiers supérieurs à 2. Si $a \wedge b = 1$, alors $\varphi(ab) = \varphi(a)\varphi(b)$.

Il faut savoir le démontrer.

Corollaire. Soit $n \in \mathbb{N}$ avec $n \geq 2$, de décomposition primaire $n = \prod_{i=1}^k p_i^{m_i}$.

Alors $\varphi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$.

Propriété d'Euler-Fermat : Soit $n \in \mathbb{N}$ avec $n \geq 2$ et $k \in \mathbb{Z}$. Si $k \wedge n = 1$, alors $k^{\varphi(n)} \equiv 1 [n]$.

Il faut savoir le démontrer.

Petit théorème de Fermat : Si p est un nombre premier, alors pour tout $k \in \mathbb{Z}$, $k^p \equiv k [p]$.

1.4 Compléments hors programme

Notation. On fixe $n \in \mathbb{N}$ avec $n \geq 2$.

Si G est un groupe, on note $\text{Aut}(G)$ l'ensemble de ses automorphismes.

Propriété. L'application
$$\begin{array}{ccc} U(\mathbb{Z}/n\mathbb{Z}) & \longrightarrow & \text{Aut}(\mathbb{Z}/n\mathbb{Z}) \\ x & \longmapsto & [y \longmapsto xy] \end{array}$$
 est un isomorphisme.

Il faut savoir le démontrer.

Corollaire. Si (G, \cdot) est un groupe cyclique d'ordre n , alors $\text{Aut}(G)$ et $U(\mathbb{Z}/n\mathbb{Z})$ sont isomorphes. En particulier, $(\text{Aut}(G), \circ)$ est un groupe abélien. Plus précisément, l'application
$$\begin{array}{ccc} U(\mathbb{Z}/n\mathbb{Z}) & \longrightarrow & \text{Aut}(G) \\ \bar{k} & \longmapsto & [g \longmapsto g^k] \end{array}$$
 est un isomorphisme.

Propriété. Soit (G, \cdot) un groupe fini d'ordre n . Alors $n = \sum_{d|n} r_d \varphi(d)$, où r_d désigne le nombre de sous-groupes cycliques de G de cardinal d .

Il faut savoir le démontrer.

Propriété. $n = \sum_{d|n} \varphi(d)$.

Au moins l'une des deux démonstrations proposées est à connaître.

Théorème. Si \mathbb{K} est un corps, tout sous-groupe fini de $(\mathbb{K} \setminus \{0\}, \times)$ est cyclique.

Il faut savoir le démontrer.

Corollaire. Si $p \in \mathbb{P}$, $(\mathbb{F}_p \setminus \{0\}, \times)$ est isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$, c'est-à-dire qu'il existe $x \in \mathbb{F}_p \setminus \{0\}$ tel que x est d'ordre $p-1$: on dit alors que x est une racine primitive de \mathbb{F}_p .

Corollaire. Soit (G, \cdot) un groupe de cardinal $p \in \mathbb{P}$. Alors $\text{Aut}(G)$ est cyclique.

1.5 Caractéristique d'un anneau (hors programme)

Notation. A désigne un anneau commutatif.

Définition. S'il existe $n \in \mathbb{N}^*$ tel que $n.1_A = 0_A$, la caractéristique de A est $\text{car}(A) \triangleq \min\{n \in \mathbb{N}^* / n.1_A = 0_A\}$. Sinon, on convient que $\text{car}(A) = 0$.

Propriété. Soit A un anneau de caractéristique n : pour tout $m \in \mathbb{Z}$, $m.1_A = 0_A \iff n|m$.

Exemples. L'anneau nul est l'unique anneau de caractéristique 1, $\text{car}(\mathbb{Z}/n\mathbb{Z}) = n$, $\text{car}(\mathbb{R}) = 0$.

Propriété. Deux anneaux isomorphes ont la même caractéristique.

Propriété. $\mathbb{Z}.1_A$, le plus petit sous-anneau de A , est isomorphe à \mathbb{Z} lorsque $\text{car}(A) = 0$ et à $\mathbb{Z}/n\mathbb{Z}$ lorsque $\text{car}(A) = n \in \mathbb{N}^*$.

Il faut savoir le démontrer.

Corollaire. Un anneau de caractéristique nulle est de cardinal infini, la réciproque étant fausse.

Propriété. Si A est intègre et $\text{car}(A) \neq 0$, alors $\text{car}(A) \in \mathbb{P}$.

Il faut savoir le démontrer.

Propriété. Si $\text{car}(A) = p \in \mathbb{P}$, alors $x \mapsto x^p$ est un endomorphisme sur A , dit de Frobenius.

Il faut savoir le démontrer.

Notation. Pour toute la suite de ce paragraphe, \mathbb{K} désigne un corps quelconque.

Propriété. La caractéristique d'un corps est ou bien nulle, ou bien un nombre premier.

Propriété. On appelle sous-corps premier de \mathbb{K} le plus petit sous-corps de \mathbb{K} .

- Si $\text{car}(\mathbb{K}) = p \in \mathbb{P}$, le sous-corps premier de \mathbb{K} est $\mathbb{Z}.1_{\mathbb{K}}$, il est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
- Si $\text{car}(\mathbb{K}) = 0$, le sous-corps premier de \mathbb{K} est $\{(p.1_{\mathbb{K}})(q.1_{\mathbb{K}})^{-1} / p \in \mathbb{Z}, q \in \mathbb{N}^*\}$. Il est isomorphe à \mathbb{Q} . En particulier, \mathbb{K} est de cardinal infini.

Propriété. Si \mathbb{K} est un corps fini de caractéristique p , l'endomorphisme de Frobenius $x \mapsto x^p$ sur \mathbb{K} est un automorphisme de corps. Lorsque $\mathbb{K} = \mathbb{F}_p$, c'est l'identité.

2 Equations différentielles linéaires d'ordre 1

\mathbb{K} désigne \mathbb{R} ou \mathbb{C} .

On s'intéresse aux équations différentielles $(E) : y' = a(t)y + b(t)$ et $(H) : y' = a(t)y$ en l'inconnue y , où I est un intervalle, et où a et b sont deux applications continues de I dans \mathbb{K} .

(H) est l'équation homogène (ou bien l'équation sans second membre, ESSM) associée à (E) .

Définition. les courbes intégrales de (E) sont les graphes des solutions de (E) .

Définition. Soit $y_0 \in \mathbb{K}$ et $t_0 \in I$. Le problème de Cauchy relatif à (E) et au couple (t_0, y_0) est la recherche des solutions y de (E) vérifiant la condition initiale $y(t_0) = y_0$.

Propriété. Notons S_H l'ensemble des solutions de (H) et S_E l'ensemble des solutions de (E) . Si y_0 est une solution de (E) , alors $S_E = \{y_0 + y / y \in S_H\} \stackrel{\Delta}{=} y_0 + S_H$. On dit que la solution générale de (E) s'obtient en ajoutant une solution particulière de (E) à la solution générale de (H) .

Il faut savoir le démontrer.

Principe de superposition des solutions : Si y_1 (resp : y_2) est solution de $(E_1) : y' = a(t)y + b_1(t)$ (resp : de $(E_2) : y' = a(t)y + b_2(t)$), alors pour tout $\alpha, \beta \in \mathbb{R}$, $\alpha y_1 + \beta y_2$ est solution de l'équation $y' = a(t)y + \alpha b_1(t) + \beta b_2(t)$.

Théorème. Notons A une primitive de a . Alors $y' = a(t)y \iff [\exists \lambda \in \mathbb{K} \quad \forall t \in I \quad y(t) = \lambda e^{A(t)}]$.

Il faut savoir le démontrer.

Méthode de variation de la constante : avec les notations précédentes, on pose $y(t) = \lambda(t)e^{A(t)}$. Alors $(E) \iff \lambda'(t)e^{A(t)} = b(t)$.

Propriété. Pour tout problème de Cauchy relatif à (E) , il y a existence et unicité d'une solution.

Semaine 16 (du 13 au 17 janvier) : Résumé de cours

Première partie

Equations différentielles (suite)

1 Équations différentielles linéaires d'ordre 2

1.1 Équations à coefficients quelconques

Une équation différentielle linéaire d'ordre 2 est de la forme $(E) : y'' = a(x)y' + b(x)y + c(x)$ où a, b, c sont trois applications continues d'un intervalle I dans $\mathbb{K} = \mathbb{R}$ ou \mathbb{C} .

L'équation homogène associée est $(H) : y'' = a(x)y' + b(x)y$.

Propriété. Notons S_H l'ensemble des solutions de (H) et S_E l'ensemble des solutions de (E) . Si y_0 est une solution de (E) , alors $S_E = \{y_0 + y/y \in S_H\} \stackrel{\Delta}{=} y_0 + S_H$.

Définition. Soit $(x_0, y_0, y'_0) \in I \times \mathbb{K} \times \mathbb{K}$. On appelle problème de Cauchy relatif à (E) et au triplet (x_0, y_0, y'_0) le problème de la recherche des solutions de (E) telles que $y(x_0) = y_0$ et $y'(x_0) = y'_0$.

Théorème de Cauchy-Lipschitz.

Pour tout $(x_0, y_0, y'_0) \in I \times \mathbb{K} \times \mathbb{K}$, il y a existence et unicité au problème de Cauchy relatif à (E) et au triplet (x_0, y_0, y'_0) .

Cas particulier où on connaît une solution φ_1 de (H) ne s'annulant pas sur I : on pose $y(x) = \lambda(x)\varphi_1(x)$. Alors (E) est équivalente à une équation linéaire d'ordre 1 en λ' .

Il faut savoir le démontrer.

1.2 Equations linéaires d'ordre 2 à coefficients constants

Ici, $(E) : y'' + ay' + by = f(x)$, où $f : I \rightarrow \mathbb{K}$ est continue, et où a et b sont des constantes. L'équation homogène associée est $(H) : y'' + ay' + by = 0$.

1.2.1 Résolution de (H) : **Il faut savoir le démontrer.**

$\chi = X^2 + aX + b$ est appelé le polynôme caractéristique de (H) ou de (E) .

- **Premier cas.** Si $\Delta = a^2 - 4b \neq 0$, χ admet deux racines complexes distinctes λ et μ .

Alors $(H) \iff \exists(u, v) \in \mathbb{K}^2 \ \forall x \in \mathbb{R} \ y(x) = ue^{\lambda x} + ve^{\mu x}$.

Cas particulier où $(a, b) \in \mathbb{R}^2$ avec $\Delta < 0$: alors $\lambda = \alpha + i\beta$ et $\mu = \alpha - i\beta$, avec $\alpha, \beta \in \mathbb{R}$ et $(H) \iff \exists(u, v) \in \mathbb{R}^2 \ \forall x \in \mathbb{R} \ y(x) = ue^{\alpha x} \cos \beta x + ve^{\alpha x} \sin \beta x$.

- **Deuxième cas.** Si $\Delta = 0$: χ admet une racine double notée λ .

Alors $(H) \iff \exists(u, v) \in \mathbb{K}^2 \ \forall x \in \mathbb{R} \ y(x) = e^{\lambda x}(u + xv)$.

1.2.2 Résolution de l'équation avec second membre

Théorème. On suppose qu'il existe $\lambda \in \mathbb{K}$ et un polynôme P de $\mathbb{K}[X]$ tels que $\forall x \in I \quad f(x) = e^{\lambda x} P(x)$. Alors (E) admet une solution particulière de la forme $x \mapsto Q(x)e^{\lambda x}$, où Q est une application polynomiale.

Plus précisément, (E) admet sur I une solution particulière de la forme $x \mapsto x^m e^{\lambda x} Q(x)$ où Q est un polynôme de $\mathbb{K}[X]$ de même degré que P , avec $m = 0$ lorsque λ n'est pas racine de χ , avec $m = 1$ lorsque λ est une racine simple de χ et avec $m = 2$ lorsque λ est une racine double de χ .

Remarque. Ce théorème est aussi valable pour les équations différentielles de la forme $(E) : y' + by = e^{\lambda x} P(x)$ où $P \in \mathbb{K}[X]$: (E) admet sur I une solution particulière de la forme $x \mapsto Q(x)e^{\lambda x}$, où Q est une application polynomiale.

Plus précisément, (E) admet une solution particulière de la forme $x \mapsto x^m e^{\lambda x} Q(x)$ où Q est un polynôme de $\mathbb{K}[X]$ de même degré que P , avec $m = 0$ lorsque $\lambda \neq -b$ et $m = 1$ lorsque $\lambda = -b$ (dans ce cas, $\chi = X + b$).

Remarque. Lorsque $f(x)$ est de la forme $f(x) = P(x) \cos(\omega x)$ où $\omega \in \mathbb{R}$, ou bien de la forme $f(x) = P(x) \sin(\omega x)$, on peut appliquer ce qui précède en se ramenant à $x \mapsto P(x)e^{i\omega x}$.

Remarque. Plus généralement, lorsque $f(x)$ est de la forme $P(x)e^{Q(x)}$, où P et Q sont des polynômes, on peut chercher une solution particulière de la forme $H(x)e^{Q(x)}$, où H est aussi un polynôme.

2 Equations à variables séparables (hors programme)

2.1 Equations à variables séparées

Notation.

Soient I et K deux intervalles infinis et soient $a : I \rightarrow \mathbb{R}$ et $b : K \rightarrow \mathbb{R}$ deux applications continues. L'équation différentielle $(E) : a(t) - b(y)y' = 0$ est appelée une équation à variables séparées.

Si A et B sont des primitives de a et de b respectivement,

$(E) \iff \frac{d(A(t) - B(y(t)))}{dt} = 0$, donc les courbes intégrales de (E) ont pour équations cartésiennes $A(x) = B(y) + C$, où $C \in \mathbb{R}$.

En pratique, on écrira $(E) \iff a(t)dt = b(y)dy \iff A(t) = B(y) + C$.

2.2 Cas général

Notation. Soient I et K deux intervalles infinis. Soient a et d deux applications continues de I dans \mathbb{R} et b et c deux applications continues de K dans \mathbb{R} . L'équation $(E) : a(t)c(y) - b(y)d(t)y' = 0$ est appelée une équation à variables séparables.

En divisant par $c(y)$ et $d(t)$ on se ramène à une équation à variables séparées.

• Plus précisément, soit $y : I \rightarrow \mathbb{R}$ une application dérivable. Quitte à restreindre l'intervalle I , on supposera que d ne s'annule pas sur I . Ainsi $(E) \iff \frac{a(t)}{d(t)}c(y) - y'b(y) = 0$.

Il faudra ensuite étudier les possibles raccordements des solutions en chaque zéro de d .

• Si $y_0 \in K$ est un zéro de c , l'application constante $y = y_0$ est une solution de (E) . Ainsi chaque zéro de c fournit une solution particulière.

On suppose ensuite que $\forall t \in I \quad c(y(t)) \neq 0$. Alors $(E) \iff \frac{a(t)}{d(t)} - y' \frac{b(y)}{c(y)} = 0$: c'est une équation à variables séparées, donc on est ramené au a). Il reste ensuite à étudier les possibles recollements de ces dernières solutions avec les solutions particulières $y = y_0$ où y_0 est un zéro de c .

Deuxième partie

Espaces vectoriels (début)

Notation. \mathbb{K} désigne un corps quelconque.

Notation. Symbole de Kronecker : $\delta_{i,j} = 0$ lorsque $i \neq j$ et $\delta_{i,i} = 1$ lorsque $i = j$.

3 La structure algébrique d'espace vectoriel

3.1 Définition et exemples

Définition.

Un \mathbb{K} -espace vectoriel est un triplet $(E, +, \cdot)$, où $(E, +)$ est un groupe abélien et “ \cdot ” est une application

$$\begin{aligned} \mathbb{K} \times E &\longrightarrow E \\ (\alpha, x) &\longmapsto \alpha.x \end{aligned} \text{ tel que, pour tout } x, y \in E \text{ et } \alpha, \beta \in \mathbb{K},$$

- $\alpha.(x + y) = (\alpha.x) + (\alpha.y)$,
- $(\alpha + \beta).x = (\alpha.x) + (\beta.x)$,
- $(\alpha \times \beta).x = \alpha.(\beta.x)$,
- $1_{\mathbb{K}}.x = x$.

Remarque. Lorsque E est un \mathbb{K} -espace vectoriel, ses éléments seront appelés des vecteurs et les éléments de \mathbb{K} seront appelés des scalaires.

Exemples.

◇ Soient E un \mathbb{K} -espace vectoriel et I un ensemble quelconque. Alors l'ensemble E^I des familles $(x_i)_{i \in I}$ d'éléments de E indexées par I est un \mathbb{K} -espace vectoriel si l'on convient que

$$(x_i)_{i \in I} + (y_i)_{i \in I} = (x_i + y_i)_{i \in I} \text{ et, pour tout } \alpha \in \mathbb{K}, \alpha.(x_i)_{i \in I} = (\alpha.x_i)_{i \in I}.$$

De même, l'ensemble $\mathcal{F}(I, E)$ des applications de I dans E est un \mathbb{K} -espace vectoriel si l'on convient que, pour tout $f, g \in \mathcal{F}(I, E)$ et $\alpha \in K$, pour tout $x \in I$,

$$(f + g)(x) \triangleq f(x) + g(x) \text{ et } (\alpha.f)(x) \triangleq \alpha.(f(x)).$$

◇ En particulier, pour tout $n \in \mathbb{N}^*$, \mathbb{R}^n est un \mathbb{R} -espace vectoriel.

◇ Si \mathbb{L} est un sous-corps de \mathbb{K} , alors \mathbb{K} est un \mathbb{L} -espace vectoriel.

◇ L'ensemble $\mathbb{K}^{\mathbb{N}}$ des suites de scalaires est un \mathbb{K} -espace vectoriel.

◇ $\mathbb{K}[X]$ est un \mathbb{K} -espace vectoriel.

Propriété. Soit E un \mathbb{K} -espace vectoriel. Soit $x, y \in E$ et $\lambda, \mu \in \mathbb{K}$:

- $0_{\mathbb{K}}.x = 0_E$ et $\lambda.0_E = 0_E$;
- $(-1_{\mathbb{K}}).x = -x$;
- $(\lambda - \mu)x = \lambda.x - \mu.x$;
- $\lambda x = 0 \iff (\lambda = 0) \vee (x = 0)$;
- $(\lambda x = \lambda y) \wedge (\lambda \neq 0) \implies x = y$;
- $(\lambda x = \mu x) \wedge (x \neq 0) \implies \lambda = \mu$.

Définition. Soient $n \in \mathbb{N}^*$ et $((E_i, +, \cdot))_{i \in \{1, \dots, n\}}$ une famille de n \mathbb{K} -espaces vectoriels.

On structure $E = E_1 \times \dots \times E_n$ en un \mathbb{K} -espace vectoriel en convenant que

- $\forall x = (x_1, \dots, x_n) \in E, \forall y = (y_1, \dots, y_n) \in E, x + y = (x_1 + y_1, \dots, x_n + y_n)$,
- $\forall \alpha \in \mathbb{K}, \forall x = (x_1, \dots, x_n) \in E, \alpha.x = (\alpha.x_1, \dots, \alpha.x_n)$.

3.2 Sous-espaces vectoriels

Propriété et définition : Soit E un \mathbb{K} -espace vectoriel et F une partie de E .

F est un **sous-espace vectoriel** de E si et seulement si

- $F \neq \emptyset$;
- $\forall (x, y) \in F^2$, $x + y \in F$ (stabilité de la somme de deux vecteurs);
- $\forall (\alpha, x) \in \mathbb{K} \times F$, $\alpha.x \in F$ (stabilité du produit externe).

Cet ensemble de conditions est équivalent à

- $F \neq \emptyset$;
- $\forall (\alpha, x, y) \in \mathbb{K} \times F \times F$, $\alpha.x + y \in F$ (stabilité par combinaison linéaire).

Exemples.

- Pour tout $n \in \mathbb{N}^*$, pour tout $(\alpha_1, \dots, \alpha_n) \in \mathbb{K}^n \setminus \{0\}$, $\left\{ (x_i)_{1 \leq i \leq n} / \sum_{i=1}^n \alpha_i x_i = 0 \right\}$ est un sous-espace vectoriel de \mathbb{K}^n .
- $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$, pour tout $n \in \mathbb{N}$.
- L'ensemble $C^p([0, 1], \mathbb{C})$ des applications de classe C^p de $[0, 1]$ dans \mathbb{C} , où $p \in \mathbb{N}$, est un sous-espace vectoriel de $\mathcal{F}([0, 1], \mathbb{C})$.
- L'ensemble $l^1(\mathbb{C}) = \{(a_n)_{n \in \mathbb{N}} / \sum a_n \text{ ACV} \}$ est un sous-espace vectoriel de $\mathbb{C}^{\mathbb{N}}$.

Définition. Soient E un \mathbb{K} -espace vectoriel et I un ensemble quelconque. Soit $(x_i)_{i \in I}$ une famille de E^I . On dit que c'est une famille presque nulle si et seulement si $\{i \in I / x_i \neq 0\}$ est un ensemble fini. On note $E^{(I)}$ l'ensemble des familles presque nulles de E^I . $E^{(I)}$ est un sous-espace vectoriel de E^I .

3.3 Sous-espace vectoriel engendré par une partie

Propriété. Une intersection d'une famille de sous-espaces vectoriels est un sous-espace vectoriel.

Il faut savoir le démontrer.

Définition. Soit E un \mathbb{K} -espace vectoriel et A une partie de E . Notons \mathcal{S} l'ensemble des sous-espaces vectoriels de E contenant A . Alors $\bigcap_{F \in \mathcal{S}} F$ est un sous-espace vectoriel de E contenant A et, par construction, c'est le plus petit sous-espace vectoriel contenant A . On le note $\text{Vect}(A)$.

Exemple. $\text{Vect}(\emptyset) = \{0\}$, puisque $\{0\}$ est le plus petit sous-espace vectoriel de E .

Si F est un sous-espace vectoriel d'un \mathbb{K} -espace vectoriel E , $\text{Vect}(F) = F$.

Propriété. Si $A \subset B$, alors $\text{Vect}(A) \subset \text{Vect}(B)$.

Propriété. Soient E un \mathbb{K} -espace vectoriel et A une partie de E . Alors $\text{Vect}(A)$ est l'ensemble des combinaisons linéaires de vecteurs de A : $\text{Vect}(A) = \left\{ \sum_{a \in A} \alpha_a a / (\alpha_a)_{a \in A} \in \mathbb{K}^{(A)} \right\}$.

Il faut savoir le démontrer.

Notation. Si $(x_i)_{i \in I} \in E^I$, on note $\text{Vect}(x_i)_{i \in I} = \text{Vect}(\{x_i / i \in I\})$.

En particulier, $\text{Vect}(x_1, \dots, x_n) = \left\{ \sum_{i=1}^n \alpha_i x_i / \alpha_1, \dots, \alpha_n \in \mathbb{K} \right\}$.

Si $u \in E \setminus \{0\}$, $\text{Vect}(u) = \{\alpha u / \alpha \in \mathbb{K}\}$ est appelé la droite vectorielle engendrée par le vecteur u .

Propriété. Soit E un \mathbb{K} -espace vectoriel et $A \subset E$. Si $x \in \text{Vect}(A)$, $\text{Vect}(A \cup \{x\}) = \text{Vect}(A)$.

Si $x = \lambda y + a$ avec $\lambda \in \mathbb{K}$ et $a \in \text{Vect}(A)$, alors $\text{Vect}(A \cup \{x\}) = \text{Vect}(A \cup \{y\})$.

Il faut savoir le démontrer.

Propriété. Soit $(x_i)_{i \in I}$ une famille de vecteurs d'un \mathbb{K} -espace vectoriel E . Alors $\text{Vect}(x_i)_{i \in I}$ n'est pas modifié si l'on effectue l'une des *opérations élémentaires* suivantes :

- échanger x_{i_0} et x_{i_1} , où $i_0, i_1 \in I$ avec $i_0 \neq i_1$;
- multiplier x_{i_0} par $\alpha \in \mathbb{K}$ avec $\alpha \neq 0$;
- ajouter à l'un des x_i une combinaison linéaire des autres x_j .

Il faut savoir le démontrer.

Définition. Soit $p \in \mathbb{N}^*$ et E_1, \dots, E_p p sous-espaces vectoriels de E .

$E_1 + \dots + E_p \triangleq \text{Vect}\left(\bigcup_{i=1}^p E_i\right)$. On vérifie que $E_1 + \dots + E_p = \left\{ \sum_{i=1}^p x_i \mid \forall i \in \{1, \dots, p\}, x_i \in E_i \right\}$.

Semaine 17 (du 20 au 24 janvier) : Résumé de cours

1 La structure d'espace vectoriel (fin)

1.1 Les applications linéaires

Définition. Soient E et F deux \mathbb{K} -espaces vectoriels. Une application f de E dans F est une application linéaire (on dit aussi un morphisme ou un homomorphisme de \mathbb{K} -espaces vectoriels) si et seulement si $\forall (\alpha, x, y) \in \mathbb{K} \times E \times E$ $f(\alpha x + y) = \alpha f(x) + f(y)$.

Un *isomorphisme* est un morphisme bijectif.

Un *endomorphisme* est un morphisme de E dans lui-même.

Un *automorphisme* est un endomorphisme bijectif.

Une *forme linéaire* est une application linéaire à valeurs dans \mathbb{K} .

Exemples.

$$\begin{aligned} & C([-1, 1], \mathbb{R}) \longrightarrow \mathbb{R} \\ \text{---} & \quad f \longmapsto \int_{-1}^1 f(t)t^2 dt \text{ est une forme linéaire.} \\ & D^2([0, 1], \mathbb{R}) \longrightarrow \mathcal{F}([0, 1], \mathbb{R}) \\ \text{---} & \quad f \longmapsto f'' \text{ est linéaire.} \\ & l^1(\mathbb{C}) \longrightarrow \mathbb{C} \\ \text{---} & \quad (a_n)_{n \in \mathbb{N}} \longmapsto \sum_{n \in \mathbb{N}} a_n \text{ est une forme linéaire.} \end{aligned}$$

Définition. Les homothéties (vectorielles) de E sont les applications de la forme $\lambda.Id_E$, où $\lambda \in \mathbb{K}$.

Notation.

- On note $L(E, F)$ l'ensemble des applications linéaires de E dans F .
- On pose $L(E) \triangleq L(E, E)$.
- On pose $L(E, \mathbb{K}) = E^*$; c'est l'ensemble des formes linéaires, appelé le dual de E .

Propriété. Les formes linéaires sur \mathbb{K}^n sont exactement les

$$\mathbb{K}^n \longrightarrow \mathbb{K} \quad (x_i)_{1 \leq i \leq n} \longmapsto \sum_{i=1}^n \alpha_i x_i$$

où $(\alpha_1, \dots, \alpha_n) \in \mathbb{K}^n$.

Il faut savoir le démontrer.

Propriété. Si $u \in L(E, F)$ et $(x_i)_{i \in I} \in E^I$, $\forall (\alpha_i)_{i \in I} \in \mathbb{K}^{(I)}$ $u\left(\sum_{i \in I} \alpha_i x_i\right) = \sum_{i \in I} \alpha_i u(x_i)$.

Propriété. Soit $u \in L(E, F)$ et $(x_i)_{i \in I} \in E^I$. Alors $u\left(\text{Vect}(x_i)_{i \in I}\right) = \text{Vect}(u(x_i))_{i \in I}$.

Il faut savoir le démontrer.

Propriété. La composée de deux applications linéaires est une application linéaire.

Propriété. Si $f : E \longrightarrow F$ est un isomorphisme, f^{-1} est encore un isomorphisme.

Propriété. Si E et F sont deux \mathbb{K} -espaces vectoriels, alors $L(E, F)$ est un \mathbb{K} -espace vectoriel.

Il faut savoir le démontrer.

Définition. Soient E un \mathbb{K} -espace vectoriel, $u \in L(E)$ et F un sous-espace vectoriel de E . On dit que F est **stable** par u , ou que u **stabilise** F si et seulement si $u(F) \subset F$.

Dans ce cas, l'**endomorphisme induit** par u sur F est
$$\begin{array}{ccc} v : F & \longrightarrow & F \\ x & \longmapsto & u(x) \end{array}$$
. C'est un élément de $L(F)$, que par abus, on note souvent $u|_F$ et que l'on appelle la restriction de u à F .

Propriété. Soient E et F deux \mathbb{K} -espaces vectoriels, E' un sous-espace vectoriel de E et F' un sous-espace vectoriel de F . Soit f un morphisme de E dans F .

Alors $f(E')$ est un sous-espace vectoriel de F et $f^{-1}(F')$ est un sous-espace vectoriel de E .

Il faut savoir le démontrer.

Propriété. Soit f une application linéaire entre deux \mathbb{K} -espaces vectoriels E et F .

Alors f est injective si et seulement si $\text{Ker}(f) = \{0\}$ et

f est surjective si et seulement si $\text{Im}(f) = F$.

Propriété. Soit E un \mathbb{K} -espace vectoriel et $(u, v) \in L(E)^2$.

Si u et v commutent, alors $\text{Im}(u)$ et $\text{Ker}(u)$ sont stables par v .

Il faut savoir le démontrer.

Propriété. Soit $u, v \in L(E)$. Alors $uv = 0 \iff \text{Im}(v) \subset \text{Ker}(u)$.

Il faut savoir le démontrer.

Définition. Soit E et F deux \mathbb{K} -espaces vectoriels et $f \in L(E, F)$. Soit $y \in F$.

L'équation $(E) : f(x) = y$ en l'inconnue $x \in E$ est appelée une équation linéaire.

Propriété. Avec les notations précédentes, l'équation sans second membre associée à (E) est l'équation $(H) : f(x) = 0$, dont l'ensemble des solutions est $\mathcal{S}_H = \text{Ker}(f)$: notamment l'ensemble des solutions de l'équation homogène est un \mathbb{K} -espace vectoriel.

L'équation (E) est compatible, c'est-à-dire qu'elle possède au moins une solution $x_0 \in E$, si et seulement si $y \in \text{Im}(f)$. Dans ce cas, $\mathcal{S}_E = x_0 + \mathcal{S}_H$: la solution générale de (E) s'obtient en ajoutant à une solution particulière de (E) la solution générale de (H) .

1.2 Espaces affines

Définition. On appelle **\mathbb{K} -espace affine** tout triplet $(\mathcal{E}, E, +_\mathcal{E})$, où \mathcal{E} est un ensemble non vide, E est un \mathbb{K} -espace vectoriel (dont la loi additive sera notée $+_E$) et où $+_\mathcal{E}$ est une application

$$\begin{array}{ccc} \mathcal{E} \times E & \longrightarrow & \mathcal{E} \\ (M, x) & \longmapsto & M +_\mathcal{E} x \end{array} \text{ telle que}$$

i) Pour tout $M \in \mathcal{E}$, l'application
$$\begin{array}{ccc} E & \longrightarrow & \mathcal{E} \\ x & \longmapsto & M +_\mathcal{E} x \end{array}$$
 est une bijection.

ii) $\forall (M, x, y) \in \mathcal{E} \times E \times E \quad (M +_\mathcal{E} x) +_\mathcal{E} y = M +_\mathcal{E} (x +_E y)$.

Les éléments de \mathcal{E} sont appelés des **points** et E est appelé la **direction** de \mathcal{E} .

Notation. Soient \mathcal{E} un espace affine de direction E et $(A, B) \in \mathcal{E}^2$.

D'après i), il existe un unique vecteur x tel que $A +_\mathcal{E} x = B$. On note $x = \overrightarrow{AB}$ ou encore $x = B -_\mathcal{E} A$.

Remarque. On peut établir que les règles de calcul relatives aux opérations " $+_\mathcal{E}$ " (point $+_\mathcal{E}$ vecteur) et " $-_\mathcal{E}$ " (point $-_\mathcal{E}$ point) sont formellement les mêmes que celles que vérifient l'addition et la soustraction sur \mathbb{R} . Par exemple, la relation de **Chasles** s'écrit : $\overrightarrow{AB} + \overrightarrow{BC} = (B - A) + (C - B) = C - A = \overrightarrow{AC}$.

Définition. Si A, B, C, D sont quatre points de \mathcal{E} , $ABCD$ est un **parallélogramme** ssi $\overrightarrow{AB} = \overrightarrow{DC}$.

Remarque. Dans les propriétés i) et ii) définissant un espace affine, lorsqu'un point M de \mathcal{E} intervient, c'est toujours quantifié de la manière suivante : " $\forall M \in \mathcal{E} \dots$ ". Ainsi, dans un espace affine, tous les points ont la même importance. C'est un espace homogène, contrairement aux espaces vectoriels. Les propriétés qui suivent montrent que cette différence entre la notion de \mathbb{K} -espace vectoriel et celle de \mathbb{K} -espace affine est la seule qui soit vraiment pertinente.

Propriété. Soient $(\mathcal{E}, E, +)$ un \mathbb{K} -espace affine et A un point de \mathcal{E} . \mathcal{E} est un espace vectoriel en convenant que, pour tout $(M, N, \alpha) \in \mathcal{E} \times \mathcal{E} \times \mathbb{K}$, $M + N = A + (\overrightarrow{AM} + \overrightarrow{AN})$ et $\alpha.M = A + (\alpha.\overrightarrow{AM})$.

Remarque. Cette propriété montre que tout \mathbb{K} -espace affine est assimilable à un \mathbb{K} -espace vectoriel dès lors que l'on a choisi un point A , qui jouera le rôle de vecteur nul.

Propriété réciproque. Soit E un \mathbb{K} -espace vectoriel. Le triplet $(E, E, +)$ est un \mathbb{K} -espace affine, que l'on dit canoniquement associé à l'espace vectoriel E .

Convention. En accord avec le programme, les seuls espaces affines que nous utiliserons sont les espaces affines canoniquement associés à un espace vectoriel.

1.3 La structure d'algèbre

Définition. $(A, +, \cdot, \star)$ est une \mathbb{K} -**algèbre** si et seulement si $(A, +, \cdot)$ est un \mathbb{K} -espace vectoriel, $(A, +, \star)$ est un anneau et si $\forall (\lambda, a, b) \in \mathbb{K} \times A \times A$ $\lambda.(a \star b) = (\lambda.a) \star b = a \star (\lambda.b)$.

On dit que A est commutative (ou abélienne) si et seulement si la loi \star est commutative.

On dit que A est intègre si et seulement si l'anneau $(A, +, \star)$ est un anneau intègre.

Exemples. $(\mathbb{K}[X], +, \cdot, \times)$ est une \mathbb{K} -algèbre commutative et intègre. $\mathcal{F}(I, \mathbb{K})$ et \mathbb{K}^I sont des algèbres.

Propriété. Si E est un \mathbb{K} -espace vectoriel, alors $(L(E), +, \cdot, \circ)$ est une \mathbb{K} -algèbre.

Le groupe des inversibles de $L(E)$ est noté $(GL(E), \circ)$.

Il faut savoir le démontrer.

Remarque. Plus généralement, si E, F et G sont 3 \mathbb{K} -espaces vectoriels, pour tout $\alpha \in \mathbb{K}$, pour tout $f, g \in L(F, G)$ et $h \in L(E, F)$, $(\alpha f + g) \circ h = \alpha f \circ h + g \circ h$ et pour tout $f, g \in L(E, F)$ et $h \in L(F, G)$, $h \circ (\alpha f + g) = \alpha h \circ f + h \circ g$.

Propriété. Soit $(A, +, \cdot, \star)$ une \mathbb{K} -algèbre. B est une **sous-algèbre** de $(A, +, \cdot, \star)$ si et seulement si $1_A \in B$ et pour tout $x, y \in B$ et $\lambda \in \mathbb{K}$, $x + y, x \star y, \lambda x \in B$.

Définition. Soient $(A, +, \cdot, \times)$ et $(B, +, \cdot, \times)$ deux \mathbb{K} -algèbres. Une application $f : A \rightarrow B$ est un **morphisme d'algèbres** si et seulement si $f(1_A) = 1_B$ et pour tout $x, y \in A$ et $\alpha \in \mathbb{K}$, $f(x + y) = f(x) + f(y)$, $f(x \times y) = f(x) \times f(y)$, $f(\alpha.x) = \alpha.f(x)$.

Exemple. Soit E un \mathbb{K} -espace vectoriel et $u \in GL(E)$. Alors l'application $w \mapsto u w u^{-1}$ est un automorphisme de l'algèbre $L(E)$. Ce type d'automorphisme est appelé un automorphisme *intérieur*.

Il faut savoir le démontrer.

Propriété. Une composée de morphismes d'algèbres est un morphisme d'algèbres.

L'application réciproque d'un isomorphisme d'algèbres est un isomorphisme d'algèbres.

L'image directe ou réciproque d'une sous-algèbre par un morphisme d'algèbres est une sous-algèbre.

2 Espaces vectoriels normés

2.1 Définition d'une norme

Définition. Soit E un \mathbb{K} -espace vectoriel. On appelle norme sur E toute application $\|\cdot\| : E \rightarrow \mathbb{R}$ telle que, pour tout $(x, y, \lambda) \in E \times E \times \mathbb{K}$,

- ◊ $\|x\| \geq 0$ (positivité).
- ◊ $\|x\| = 0 \implies x = 0$ ($\|\cdot\|$ est définie),
- ◊ $\|\lambda x\| = |\lambda| \|x\|$ ($\|\cdot\|$ est homogène), et
- ◊ $\|x + y\| \leq \|x\| + \|y\|$, cette dernière propriété étant appelée l'inégalité triangulaire.

Si $\|\cdot\|$ est une norme sur E , le couple $(E, \|\cdot\|)$ est appelé un espace vectoriel normé.

Remarque. Si E est un espace vectoriel normé, $\|0\| = 0$.

Corollaire de l'inégalité triangulaire. $\forall (x, y) \in E^2 \quad \|\|x\| - \|y\|\| \leq \|x - y\|$.

Il faut savoir le démontrer.

Définition.

Soient E un espace vectoriel normé et $u \in E$. u est unitaire si et seulement si $\|u\| = 1$.

Si $u \neq 0$, on appelle vecteur unitaire associé à u le vecteur $\frac{u}{\|u\|}$, qui est bien unitaire.

Définition. Soient E un espace vectoriel normé et F un sous-espace vectoriel de E .

La restriction à F de la norme de E fait de F un espace vectoriel normé.

Exemple. Sur \mathbb{R} et sur \mathbb{C} , $|\cdot|$ est une norme.

2.2 Les normes 1, 2 et ∞ .

2.2.1 Cas des sommes finies.

Propriété. Sur \mathbb{K}^n , on dispose de trois normes classiques.

$$\begin{aligned} \|\cdot\|_1 : \quad \mathbb{K}^n &\longrightarrow \mathbb{R}_+ \\ x = (x_1, \dots, x_n) &\longmapsto \|x\|_1 = \sum_{i=1}^n |x_i|, \\ \|\cdot\|_2 : \quad \mathbb{K}^n &\longrightarrow \mathbb{R}_+ \\ x = (x_1, \dots, x_n) &\longmapsto \|x\|_2 = \sqrt{\sum_{i=1}^n |x_i|^2}, \text{ et} \\ \|\cdot\|_\infty : \quad \mathbb{K}^n &\longrightarrow \mathbb{R}_+ \\ x = (x_1, \dots, x_n) &\longmapsto \|x\|_\infty = \max_{1 \leq i \leq n} |x_i|. \end{aligned}$$

Il faut savoir le démontrer.

Propriété. (Hors programme) Soit $p \in]1, +\infty[$.

$$\|\cdot\|_p : \quad \mathbb{K}^n \longrightarrow \mathbb{R}_+$$

Alors $x = (x_1, \dots, x_n) \longmapsto \|x\|_p = \left(\sum_{i=1}^n |x_i|^p \right)^{\frac{1}{p}}$ est une norme sur \mathbb{K}^n .

Il faut savoir le démontrer.

Remarque. $\forall x \in \mathbb{K}^n \quad \|x\|_p \xrightarrow{p \rightarrow +\infty} \|x\|_\infty$. Cela justifie la notation $\|\cdot\|_\infty$.

Propriété. Soient $p \in \mathbb{N}^*$ et E_1, \dots, E_p p \mathbb{K} -espaces vectoriels munis de normes respectivement notées $\|\cdot\|_{E_1}, \dots, \|\cdot\|_{E_p}$. Alors $E = E_1 \times \dots \times E_p$ est un espace vectoriel normé si on le munit de l'une des normes classiques suivantes.

$$\begin{aligned}
N_1 : \quad E &\longrightarrow \mathbb{R}_+ \\
x = (x_1, \dots, x_p) &\longmapsto N_1(x) = \sum_{i=1}^p \|x_i\|_{E_i} , \\
N_2 : \quad E &\longrightarrow \mathbb{R}_+ \\
x = (x_1, \dots, x_p) &\longmapsto N_2(x) = \sqrt{\sum_{i=1}^p \|x_i\|_{E_i}^2} , \text{ et} \\
N_\infty : \quad E &\longrightarrow \mathbb{R}_+ \\
x = (x_1, \dots, x_p) &\longmapsto N_\infty(x) = \max_{1 \leq i \leq p} \|x_i\|_{E_i} .
\end{aligned}$$

2.2.2 Cas des intégrales sur un intervalle compact

Propriété. Soient $(a, b) \in \mathbb{R}^2$ avec $a < b$. Sur $\mathcal{C}([a, b], \mathbb{K})$, on dispose de trois normes classiques.

$$\begin{aligned}
\|\cdot\|_1 : \mathcal{C}([a, b], \mathbb{K}) &\longrightarrow \mathbb{R}_+ \\
f &\longmapsto \|f\|_1 = \int_a^b |f(x)| dx , \\
\|\cdot\|_2 : \mathcal{C}([a, b], \mathbb{K}) &\longrightarrow \mathbb{R}_+ \\
f &\longmapsto \|f\|_2 = \sqrt{\int_a^b |f(x)|^2 dx} , \text{ et} \\
\|\cdot\|_\infty : \mathcal{C}([a, b], \mathbb{K}) &\longrightarrow \mathbb{R}_+ \\
f &\longmapsto \|f\|_\infty = \sup_{x \in [a, b]} |f(x)| .
\end{aligned}$$

Il faut savoir le démontrer.

Propriété. (Hors programme) Soit $p \in]1, +\infty[$.

$$\|\cdot\|_p : \mathcal{C}([a, b], \mathbb{K}) \longrightarrow \mathbb{R}_+$$

Alors $f \longmapsto \|f\|_p = \left(\int_a^b |f(x)|^p dx \right)^{\frac{1}{p}}$ est une norme sur $\mathcal{C}([a, b], \mathbb{K})$.

2.3 Distance

Définition. Soit E un espace vectoriel normé .

On appelle distance associée à la norme $\|\cdot\|$ de E , l'application $d : E^2 \longrightarrow \mathbb{R}_+$
 $(x, y) \longmapsto \|x - y\|$.

Définition. Soient E un espace vectoriel normé dont la distance associée est notée d et A une partie de E . La restriction de d à A^2 est appelée la distance induite par d sur A .

Propriété. Avec les notations précédentes, pour tout $x, y, z \in E$,

- $d(x, y) \in \mathbb{R}_+$ (positivité) ;
- $d(x, y) = 0 \iff x = y$ (séparation) ;
- $d(x, y) = d(y, x)$ (symétrie) ;
- $d(x, z) \leq d(x, y) + d(y, z)$ (inégalité triangulaire).

Définition. On appelle espace métrique tout couple (E, d) où E est un ensemble et où $d : E^2 \longrightarrow \mathbb{R}_+$ est une application telle que, pour tout $x, y, z \in E$,

- $d(x, y) = 0 \iff x = y$ (séparation) ;
- $d(x, y) = d(y, x)$ (symétrie) ;
- $d(x, z) \leq d(x, y) + d(y, z)$ (inégalité triangulaire).

Les seuls espaces métriques qui sont au programme sont les (A, d_A) où A est une partie d'un espace vectoriel normé E et où d_A est la distance induite sur A par la distance associée à la norme de E .

Propriété. Soit E un espace vectoriel normé dont la distance associée est notée d .

Alors $\forall (x, y, z) \in E^3 \quad d(x + z, y + z) = d(x, y)$.

Cette propriété ne se généralise pas aux espaces métriques.

Propriété. Corollaire de l'inégalité triangulaire.

Soit E un espace vectoriel normé dont la distance associée est notée d .

Alors $\forall (x, y, z) \in E^3 \quad |d(x, y) - d(y, z)| \leq d(x, z)$.

Définition. Soient E un espace vectoriel normé et $(a, r) \in E \times \mathbb{R}_+^*$.

La boule ouverte centrée en a de rayon r est l'ensemble $B_o(a, r) = \{x \in E / d(a, x) < r\}$.

La boule fermée de centre a et de rayon r est l'ensemble $B_f(a, r) = \{x \in E / d(a, x) \leq r\}$.

La sphère de centre a et de rayon r est l'ensemble $S(a, r) = \{x \in E / d(a, x) = r\}$.

Semaine 18 (du 27 au 31 janvier) : Résumé de cours

\mathbb{K} désigne \mathbb{R} ou \mathbb{C} .

1 Espaces vectoriels normés (suite)

1.1 Distance (suite)

Définition. Dans un espace métrique, la boule unité est la boule fermée de centre 0 et de rayon 1.

Propriété. (non généralisable aux espaces métriques)

Les boules d'un espace vectoriel normé sont des convexes.

Il faut savoir le démontrer.

Définition. Soient E un espace métrique, A et B deux parties non vides de E et $a \in E$.

On note $d(a, A) = \inf_{x \in A} d(a, x)$. C'est la distance de a à A .

On note $d(A, B) = \inf_{(x, y) \in A \times B} d(x, y)$. C'est la distance de A à B .

On appelle diamètre de A la quantité $\delta(A) = \sup_{(x, y) \in A^2} d(x, y) \in \mathbb{R}_+ \cup \{+\infty\}$.

Propriété. Dans un espace métrique, $\delta(B_f(a, r)) \leq 2r$.

Propriété. (non généralisable aux espaces métriques)

Soient E un espace vectoriel normé non nul et $(a, r) \in E \times \mathbb{R}_+^*$. Alors $\delta(B_f(a, r)) = 2r$.

Il faut savoir le démontrer.

Propriété. Dans un espace métrique, si $\emptyset \neq A \subset B$, alors $\delta(A) \leq \delta(B)$.

Définition et propriété. Soient E un espace vectoriel normé et A une partie de E . Les propriétés suivantes sont équivalentes.

i) $\{\|x\|/x \in A\}$ est borné.

ii) Pour tout $x_0 \in E$, $\{\|x - x_0\|/x \in A\}$ est borné.

iii) Pour tout $x_0 \in E$, il existe $R \in \mathbb{R}_+$ tel que $A \subset B_f(x_0, R)$.

iv) Il existe $(x_0, R) \in E \times \mathbb{R}_+$ tel que $A \subset B_f(x_0, R)$.

Dans ce cas, on dit que A est bornée.

Définition. Soient A un ensemble, E un espace vectoriel normé et $f : A \rightarrow E$ une application.

On dit que f est bornée si et seulement si $f(A)$ est une partie bornée de E .

Propriété. Soient A un ensemble non vide et E un espace vectoriel normé.

On note $\mathcal{B}(A, E)$ l'ensemble des applications bornées de A dans E .

Pour $f \in \mathcal{B}(A, E)$, on note $\|f\|_\infty = \sup_{a \in A} \|f(a)\|$.

Alors $(\mathcal{B}(A, E), \|\cdot\|_\infty)$ est un espace vectoriel normé.

Il faut savoir le démontrer.

Propriété. Soit E un espace vectoriel normé. On note $l^\infty(E)$ l'ensemble des suites bornées à valeurs dans E . Si $(x_n)_{n \in \mathbb{N}} \in l^\infty(E)$, on note $\|(x_n)\|_\infty = \sup_{n \in \mathbb{N}} \|x_n\|$.

Alors $(l^\infty(E), \|\cdot\|_\infty)$ est un espace vectoriel normé.

1.2 Applications k-Lipschitziennes

Définition. Soient E et F deux espaces métriques, $k \in \mathbb{R}_+$ et $f : E \rightarrow F$ une fonction dont le domaine de définition sera noté \mathcal{D}_f .

f est k -lipschitzienne si et seulement si $\forall (x, y) \in \mathcal{D}_f \quad d(f(x), f(y)) \leq kd(x, y)$.

Lorsque $k < 1$, on dit que f est k -contractante.

On dit que f est lipschitzienne si et seulement si il existe $k \in \mathbb{R}_+$ tel que f est k -lipschitzienne.

Propriété. Une composée d'applications lipschitziennes est lipschitzienne.

Propriété. Soit E un espace vectoriel normé. L'application $\|\cdot\|$ est 1-lipschitzienne.

Propriété. Soient E un espace vectoriel normé et A une partie non vide de E .

L'application $\begin{matrix} E & \longrightarrow & \mathbb{R}_+ \\ x & \longmapsto & d(x, A) \end{matrix}$ est 1-lipschitzienne.

Il faut savoir le démontrer.

Propriété. Soient E_1, \dots, E_p p espaces vectoriels normés dont les normes sont notées N_1, \dots, N_p . On note $E = E_1 \times \dots \times E_p$.

Soit $i \in \mathbb{N}_p$. L'application $i^{\text{ème}}$ projection $p_i : \begin{matrix} E & \longrightarrow & E_i \\ x = (x_1, \dots, x_p) & \longmapsto & x_i \end{matrix}$ est 1-lipschitzienne lorsque E est muni de l'une de ses trois normes classiques, $\|\cdot\|_1$, $\|\cdot\|_2$ ou $\|\cdot\|_\infty$.

Remarque. Sur $E = \mathcal{C}([0, 1], \mathbb{R})$, $f \mapsto f(0)$ n'est pas lipschitzienne pour N_1 .

Il faut savoir le démontrer.

1.3 Normes équivalentes

Définition. Dans un espace vectoriel normé E , deux normes $\|\cdot\|_1$ et $\|\cdot\|_2$ sont équivalentes si et seulement s'il existe $(\alpha, \beta) \in (\mathbb{R}_+^*)^2$ tel que $\forall x \in E \quad \|x\|_1 \leq \alpha \|x\|_2$ et $\|x\|_2 \leq \beta \|x\|_1$.

Propriété. Avec les notations précédentes, $\|\cdot\|_1$ et $\|\cdot\|_2$ sont équivalentes si et seulement si $Id_E : (E, \|\cdot\|_1) \rightarrow (E, \|\cdot\|_2)$ et $Id_E : (E, \|\cdot\|_2) \rightarrow (E, \|\cdot\|_1)$ sont lipschitziennes.

Exemple. Soient E_1, \dots, E_p p espaces vectoriels normés dont les normes sont notées N_1, \dots, N_p . Sur $E = E_1 \times \dots \times E_p$, les trois normes classiques, $\|\cdot\|_1$, $\|\cdot\|_2$ et $\|\cdot\|_\infty$ sont deux à deux équivalentes.

Il faut savoir le démontrer.

Propriété. Soit E un espace vectoriel normé. Sur l'ensemble des normes de E , la relation "être équivalente à" est une relation d'équivalence.

Propriété. Soient E un \mathbb{K} -espace vectoriel et $\|\cdot\|_1$ et $\|\cdot\|_2$ deux normes équivalentes sur E .

Une partie A de E est bornée pour $\|\cdot\|_1$ si et seulement si elle est bornée pour $\|\cdot\|_2$.

Propriété. Soient E et F deux \mathbb{K} -espaces vectoriels. On suppose que E (resp : F) est muni de deux normes équivalentes, notées $\|\cdot\|_1^E$ et $\|\cdot\|_2^E$ (resp : $\|\cdot\|_1^F$ et $\|\cdot\|_2^F$). Alors $f : E \rightarrow F$ est lipschitzienne pour $\|\cdot\|_1^E$ et $\|\cdot\|_1^F$ si et seulement si elle est lipschitzienne pour $\|\cdot\|_2^E$ et $\|\cdot\|_2^F$.

Il faut savoir le démontrer.

2 limite d'une suite dans un espace métrique

Notation. On fixe un espace métrique noté (E, d) .

Définition. Soient $(x_n) \in E^{\mathbb{N}}$ une suite de vecteurs de E et $l \in E$. La suite (x_n) converge vers l si et seulement si (1) : $\forall \varepsilon \in \mathbb{R}_+^* \exists N \in \mathbb{N} \forall n \in \mathbb{N} (n \geq N \implies d(x_n, l) \leq \varepsilon)$.

Remarque. Dans (1), les deux dernières inégalités peuvent être choisies strictes ou larges.

Remarque. Pour tout $n_0 \in \mathbb{N}$, la propriété " $x_n \xrightarrow{n \rightarrow +\infty} \ell$ " ne dépend pas du choix de x_0, \dots, x_{n_0} .

Propriété. Unicité de la limite.

Si (x_n) converge vers l et vers l' , alors $l = l'$. On note $l = \lim_{n \rightarrow +\infty} x_n$ ou $x_n \xrightarrow{n \rightarrow +\infty} l$.

Il faut savoir le démontrer.

Définition. Une suite de vecteurs de E est convergente si et seulement s'il existe $l \in E$ tel que $x_n \xrightarrow{n \rightarrow +\infty} l$. Sinon, on dit que la suite est divergente.

Propriété. Soient (x_n) une suite de vecteurs de E et $l \in E$.

Si $x_n \xrightarrow{n \rightarrow +\infty} l$, alors $\|x_n\| \xrightarrow{n \rightarrow +\infty} \|l\|$, mais la réciproque est fautive.

$x_n \xrightarrow{n \rightarrow +\infty} 0$ si et seulement si $\|x_n\| \xrightarrow{n \rightarrow +\infty} 0$.

$x_n \xrightarrow{n \rightarrow +\infty} l$ si et seulement si $d(x_n, l) \xrightarrow{n \rightarrow +\infty} 0$.

Principe des gendarmes : Soit $(x_n) \in E^{\mathbb{N}}$ et $\ell \in E$.

S'il existe une suite de réels (g_n) telle que $\forall n \in \mathbb{N}, d(x_n, \ell) \leq g_n$ et $g_n \xrightarrow{n \rightarrow +\infty} 0$, alors $x_n \xrightarrow{n \rightarrow +\infty} \ell$.

Propriété. Soit N une seconde norme sur E , équivalente à $\|\cdot\|$.

Alors, pour toute suite (x_n) de E et pour tout $l \in E$, $x_n \xrightarrow[n \rightarrow +\infty]{N} l \iff x_n \xrightarrow[n \rightarrow +\infty]{\|\cdot\|} l$.

Il faut savoir le démontrer.

Remarque. Sur $E = \mathcal{C}([0, 1], \mathbb{R})$, les $\|\cdot\|_1$, $\|\cdot\|_2$ et $\|\cdot\|_\infty$ sont deux à deux non équivalentes entre elles, où ces normes désignent respectivement la norme de la convergence en moyenne, celle de la convergence en moyenne quadratique et la norme de la convergence uniforme.

Il faut savoir le démontrer.

Propriété. Toute suite convergente est bornée.

2.1 Somme et produit de limites

Notation. On suppose que E est un espace vectoriel normé.

Les propriétés de ce paragraphe ne se généralisent pas aux espaces métriques.

Propriété. Soient (x_n) et (y_n) deux suites de E convergeant vers l et l' .

Alors la suite $(x_n + y_n)$ converge vers $l + l'$.

Propriété. Si $(x_n + y_n)$ converge, alors (x_n) et (y_n) ont la même nature.

Propriété. Soient $(\alpha_n) \in \mathbb{K}^{\mathbb{N}}$ et $(x_n) \in E^{\mathbb{N}}$.

Si l'une des suites est bornée et si l'autre tend vers 0, alors $\alpha_n x_n \xrightarrow{n \rightarrow +\infty} 0$.

Propriété. Soient (l_n) une suite de E qui converge vers $l \in E$ et (α_n) une suite de scalaires qui converge vers α . Alors la suite $(\alpha_n \cdot l_n)$ converge vers $\alpha \cdot l$.

Il faut savoir le démontrer.

Propriété. L'ensemble des suites convergentes de E noté $E_{cv}^{\mathbb{N}}$ est un sous-espace vectoriel de $l^\infty(E)$ et l'application
$$\begin{array}{ccc} E_{cv}^{\mathbb{N}} & \longrightarrow & E \\ (x_n) & \longmapsto & \lim_{n \rightarrow +\infty} x_n \end{array}$$
 est une application linéaire.

Propriété. Suites à valeurs dans un produit.

Soient $p \in \mathbb{N}^*$ et E_1, \dots, E_p p espaces vectoriels normés, leurs normes étant notées N_1, \dots, N_p . On note $E = E_1 \times \dots \times E_p$ que l'on munit de l'une des trois normes classiques.

Soient $(x_n)_{n \in \mathbb{N}} = ((x_{1,n}, \dots, x_{p,n}))_{n \in \mathbb{N}}$ une suite d'éléments de E et $l = (l_1, \dots, l_p) \in E$.

Alors (x_n) converge vers l si et seulement si, pour tout $i \in \mathbb{N}_p$, $(x_{i,n})$ converge vers l_i .

Il faut savoir le démontrer.

3 Suites de complexes

3.1 Premières propriétés

Propriété. Soit $(x_n) \in \mathbb{C}^{*\mathbb{N}}$ telle que $x_n \xrightarrow{n \rightarrow +\infty} \ell \in \mathbb{C} \setminus \{0\}$. Alors $\frac{1}{x_n} \xrightarrow{n \rightarrow +\infty} \frac{1}{\ell}$.

Il faut savoir le démontrer.

Propriété. Soit (z_n) une suite de complexes et $\ell \in \mathbb{C}$.

Alors $z_n \xrightarrow{n \rightarrow +\infty} \ell$ si et seulement si $\operatorname{Re}(z_n) \xrightarrow{n \rightarrow +\infty} \operatorname{Re}(\ell)$ et $\operatorname{Im}(z_n) \xrightarrow{n \rightarrow +\infty} \operatorname{Im}(\ell)$.

Dans ce cas, on a donc $\lim_{n \rightarrow +\infty} z_n = \lim_{n \rightarrow +\infty} \operatorname{Re}(z_n) + i \lim_{n \rightarrow +\infty} \operatorname{Im}(z_n)$.

3.2 Quelques suites définies par récurrence

3.2.1 Suites arithmético-géométriques

Propriété. Soit $a, b \in \mathbb{C}$ avec $a \neq 1$. Si pour tout $n \in \mathbb{N}$, $u_{n+1} = au_n + b$, on calcule $c \in \mathbb{C}$ tel que $c = ac + b$. Alors $u_n - c$ est géométrique.

3.2.2 Suites homographiques (hors programme)

Propriété. Soit $a, b, c, d \in \mathbb{C}$ avec $c \neq 0$.

Si pour tout $n \in \mathbb{N}$, $u_{n+1} = \frac{au_n + b}{cu_n + d}$, on résout l'équation $\ell = \frac{a\ell + b}{c\ell + d}$.

Si cette équation possède deux solutions α et β distinctes, alors $v_n = \frac{u_n - \beta}{u_n - \alpha}$ est géométrique.

Sinon, cette équation possède une unique solution α et $v_n = \frac{1}{u_n - \alpha}$ est arithmétique.

3.2.3 Suites récurrentes linéaires d'ordre 2

Propriété. Soient $(a, b) \in \mathbb{K}^2 \setminus \{(0, 0)\}$ et $(u_n) \in \mathbb{K}^{\mathbb{N}}$ telle que $u_{n+2} = au_{n+1} + bu_n$.

$\chi(X) = X^2 - aX - b$ est le polynôme caractéristique de (u_n) . On note $\Delta = a^2 + 4b$.

— Si $\Delta \neq 0$, en notant λ_1 et λ_2 les deux racines de χ , $\exists (C_1, C_2) \in \mathbb{C}^2 \ \forall n \in \mathbb{N}, \ u_n = C_1 \lambda_1^n + C_2 \lambda_2^n$.

— Si de plus $\mathbb{K} = \mathbb{R}$ et $\Delta < 0$, en posant $\lambda_1 = \rho e^{i\theta}$,

$\exists (D_1, D_2) \in \mathbb{R}^2 \ \forall n \in \mathbb{N}, \ u_n = \rho^n (D_1 \cos(n\theta) + D_2 \sin(n\theta))$.

— Si $\Delta = 0$, en notant λ la racine double, $\exists (C_1, C_2) \in \mathbb{K}^2 \ \forall n \in \mathbb{N}, \ u_n = \lambda^n (C_1 + nC_2)$.

Il faut savoir le démontrer.

4 Suites de réels

4.1 Limites infinies

Définition. $x_n \xrightarrow[n \rightarrow +\infty]{} +\infty \iff \forall M \geq 0, \exists N \in \mathbb{N}, \forall n \geq N, x_n \geq M.$

$x_n \xrightarrow[n \rightarrow +\infty]{} -\infty \iff \forall M \geq 0, \exists N \in \mathbb{N}, \forall n \geq N, x_n \leq -M.$

Définition. Lorsqu'une suite de réels tend vers $+\infty$ ou $-\infty$, elle est toujours divergente : on dit qu'elle diverge vers $+\infty$ ou $-\infty$. On distingue ainsi trois catégories de suites réelles :

- Les suites convergentes. Ce sont celles qui convergent vers un réel.
- Les suites divergentes de première espèce. Ce sont celles qui divergent vers $+\infty$ ou $-\infty$.
- Toutes les autres suites. On dit qu'elles sont divergentes de seconde espèce.

Propriété. Si $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ est strictement croissante, pour tout $n \in \mathbb{N}$, $\varphi(n) \geq n$, donc $\varphi(n) \xrightarrow[n \rightarrow +\infty]{} +\infty$.

Définition. Si (x_n) est dans un espace métrique, $x_n \xrightarrow[n \rightarrow +\infty]{} \infty \iff d(x_0, x_n) \xrightarrow[n \rightarrow +\infty]{} +\infty$.

Propriété. Composition des limites : Si (x_n) est dans un espace métrique et si $x_n \xrightarrow[n \rightarrow +\infty]{} \ell$, avec ℓ éventuellement infinie, pour tout $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ telle que $\varphi(n) \xrightarrow[n \rightarrow +\infty]{} +\infty$, $x_{\varphi(n)} \xrightarrow[n \rightarrow +\infty]{} \ell$.

Il faut savoir le démontrer.

Propriété. Dans un espace métrique, $x_n \xrightarrow[n \rightarrow +\infty]{} l$ si et seulement si $x_{2n} \xrightarrow[n \rightarrow +\infty]{} l$ et $x_{2n+1} \xrightarrow[n \rightarrow +\infty]{} l$.

Il faut savoir le démontrer.

Propriété. Soit $p \in \mathbb{N}^*$. Si, pour tout $i \in \{0, \dots, p-1\}$, $x_{pn+i} \xrightarrow[n \rightarrow +\infty]{} l$, alors $x_n \xrightarrow[n \rightarrow +\infty]{} l$.

Remarque. C'est encore vrai dans le cas de limites infinies.

Propriété. Avec des suites de réels, en prenant $\varepsilon, \varepsilon' \in \{-1, 1\}$,

- Si $x_n \xrightarrow[n \rightarrow +\infty]{} \varepsilon\infty$ et $y_n \xrightarrow[n \rightarrow +\infty]{} y \in \mathbb{R}$, alors $x_n + y_n \xrightarrow[n \rightarrow +\infty]{} \varepsilon\infty$.
- Si $x_n \xrightarrow[n \rightarrow +\infty]{} \varepsilon\infty$ et $y_n \xrightarrow[n \rightarrow +\infty]{} \varepsilon\infty$, alors $x_n + y_n \xrightarrow[n \rightarrow +\infty]{} \varepsilon\infty$, mais $x_n - y_n$ est une forme indéterminée du type $\infty - \infty$.
- Si $x_n \xrightarrow[n \rightarrow +\infty]{} \varepsilon\infty$, alors $-x_n \xrightarrow[n \rightarrow +\infty]{} -\varepsilon\infty$.
- Si $x_n \xrightarrow[n \rightarrow +\infty]{} \varepsilon\infty$ et $\alpha > 0$, alors $\alpha x_n \xrightarrow[n \rightarrow +\infty]{} \varepsilon\infty$.
- Si $x_n \xrightarrow[n \rightarrow +\infty]{} \varepsilon\infty$ et $y_n \xrightarrow[n \rightarrow +\infty]{} \ell \in \mathbb{R}_+$, alors $x_n y_n \xrightarrow[n \rightarrow +\infty]{} \varepsilon\infty$, sauf lorsque $\ell = 0$, qui est une forme indéterminée du type $0 \times \infty$.
- Si $x_n \xrightarrow[n \rightarrow +\infty]{} \varepsilon\infty$ et $y_n \xrightarrow[n \rightarrow +\infty]{} \varepsilon'\infty$, alors $x_n y_n \xrightarrow[n \rightarrow +\infty]{} \varepsilon\varepsilon'\infty$.
- Si $x_n \xrightarrow[n \rightarrow +\infty]{} \varepsilon\infty$ alors $\frac{1}{x_n} \xrightarrow[n \rightarrow +\infty]{} 0$.
- Si $x_n \xrightarrow[n \rightarrow +\infty]{} 0^+$ alors $\frac{1}{x_n} \xrightarrow[n \rightarrow +\infty]{} +\infty$.

Remarque. Lorsque u_n est de la forme $u_n = a_n^{b_n}$, il est indispensable d'écrire $u_n = e^{b_n \ln a_n}$ pour étudier sa limite. Par exemple, $u_n = (1 + \frac{1}{n})^n = e^{n \ln(1 + \frac{1}{n})} \xrightarrow[n \rightarrow +\infty]{} e$ car $\frac{\ln(1+x)}{x} \xrightarrow[x \rightarrow 0]{} 1$.

Semaine 19 (du 3 au 7 février) : Résumé de cours

\mathbb{K} désigne \mathbb{R} ou \mathbb{C} .

1 Suites de vecteurs (fin)

1.1 limites et relation d'ordre

Principe des gendarmes : Soit $(p_n), (g_n), (g'_n)$ trois suites de réels et $\ell \in \mathbb{R}$ tels que, pour tout $n \in \mathbb{N}$, $g_n \leq p_n \leq g'_n$, $g_n \xrightarrow[n \rightarrow +\infty]{} \ell$ et $g'_n \xrightarrow[n \rightarrow +\infty]{} \ell$.

Alors $p_n \xrightarrow[n \rightarrow +\infty]{} \ell$. Le principe des gendarmes s'adapte aux cas des limites infinies :

Lemme du tunnel : Soit (u_n) une suite de réels qui converge vers $\ell \in \mathbb{R}$.

Soit $a, b \in \mathbb{R}$ tels que $a < \ell < b$. Alors il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N$, $a < u_n < b$.

Il faut savoir le démontrer.

Propriété. Dans \mathbb{R} , si pour tout $n \in \mathbb{N}$, $a_n \leq b_n$, alors dans $\overline{\mathbb{R}}$, $\lim_{n \rightarrow +\infty} a_n \leq \lim_{n \rightarrow +\infty} b_n$.

Propriété. Soit X une partie non vide de \mathbb{R} . Il existe une suite de réels (x_n) telle que $x_n \xrightarrow[n \rightarrow +\infty]{} \sup(X) \in \mathbb{R} \cup \{+\infty\}$ (resp : $x_n \xrightarrow[n \rightarrow +\infty]{} \inf(X) \in \mathbb{R} \cup \{-\infty\}$).

Il faut savoir le démontrer.

1.2 Suites monotones

Théorème de la limite monotone : Soit (x_n) une suite croissante de réels.

Si (x_n) est majorée, alors cette suite est convergente. De plus $\lim_{n \rightarrow +\infty} x_n = \sup_{n \in \mathbb{N}} x_n$.

Si (x_n) n'est pas majorée, alors cette suite est divergente. De plus $\lim_{n \rightarrow +\infty} x_n = +\infty$.

Ainsi, dans tous les cas, on peut écrire que $x_n \xrightarrow[n \rightarrow +\infty]{} \sup_{n \in \mathbb{N}} x_n \in \mathbb{R} \cup \{+\infty\}$.

Il faut savoir le démontrer.

Théorème. Soit (x_n) une suite décroissante de réels.

Si (x_n) est minorée, alors cette suite est convergente. De plus $\lim_{n \rightarrow +\infty} x_n = \inf_{n \in \mathbb{N}} x_n$.

Si (x_n) n'est pas minorée, alors cette suite est divergente. De plus $\lim_{n \rightarrow +\infty} x_n = -\infty$.

Ainsi, dans tous les cas, on peut écrire que $x_n \xrightarrow[n \rightarrow +\infty]{} \inf_{n \in \mathbb{N}} x_n \in \mathbb{R} \cup \{-\infty\}$.

Propriété. Soit (x_n) une suite géométrique de réels de raison a , tel que $x_0 \neq 0$.

- Si $|a| < 1$, alors $x_n \xrightarrow[n \rightarrow +\infty]{} 0$.
- Si $a = 1$, x_n est constante.
- Si $a > 1$, $x_n \xrightarrow[n \rightarrow +\infty]{} \varepsilon \infty$, où ε est le signe de x_0
- Si $a \leq -1$, (x_n) diverge.

1.3 Suites adjacentes

Définition. Deux suites (x_n) et (y_n) de réels sont adjacentes si et seulement si l'une est croissante, l'autre est décroissante et si $x_n - y_n \xrightarrow{n \rightarrow +\infty} 0$.

Théorème. Si (x_n) et (y_n) sont adjacentes avec (x_n) est croissante, alors ces deux suites convergent vers une limite commune $\ell \in \mathbb{R}$. De plus, pour tout $(p, q) \in \mathbb{N}^2$, $x_p \leq \ell \leq y_q$.

Il faut savoir le démontrer.

Théorème des segments emboîtés : Soit $(I_n)_{n \in \mathbb{N}}$ une suite de segments, décroissante au sens de l'inclusion, dont les longueurs tendent vers 0. Alors $\bigcap_{n \in \mathbb{N}} I_n$ est un singleton.

Il faut savoir le démontrer.

1.4 Les suites extraites

On se place dans un espace métrique quelconque.

Définition. Les suites extraites de (x_n) sont les $(x_{\varphi(n)})$, où $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ est strictement croissante.

Propriété. Si une suite (x_n) converge vers ℓ , toutes ses suites extraites convergent vers ℓ .

Remarque. Cette propriété se généralise au cas des limites infinies.

Propriété. Une suite extraite d'une suite extraite de (x_n) est une suite extraite de (x_n) .

Il faut savoir le démontrer.

Définition. Les valeurs d'adhérence de (x_n) sont les limites des suites extraites convergentes de (x_n) .

Remarque. La limite d'une suite convergente est son unique valeur d'adhérence.

Si une suite admet au moins deux valeurs d'adhérence distinctes, elle est divergente.

Propriété. (hors programme). Les propriétés suivantes sont équivalentes :

- i) a est une valeur d'adhérence de (x_n) .
- ii) $\forall \varepsilon \in \mathbb{R}_+^* \quad \forall N \in \mathbb{N} \quad \exists n \geq N \quad d(x_n, a) < \varepsilon$.
- iii) $\forall \varepsilon > 0 \quad \text{Card}(\{n \in \mathbb{N} / x_n \in B_o(a, \varepsilon)\}) = +\infty$.

Il faut savoir le démontrer.

Lemme des pics : De toute suite de réels on peut extraire une suite monotone.

Il faut savoir le démontrer.

Théorème de Bolzano-Weierstrass :

Toute suite bornée de complexes possède au moins une valeur d'adhérence.

Il faut savoir le démontrer.

1.5 Suites de Cauchy (hors programme)

On se place dans un espace métrique quelconque.

Définition. $[(x_n)$ est une suite de Cauchy] $\iff [\forall \varepsilon \in \mathbb{R}_+^* \quad \exists N \in \mathbb{N} \quad \forall p \geq N \quad \forall q \geq N \quad d(x_p, x_q) \leq \varepsilon]$.

Propriété. Toute suite convergente est une suite de Cauchy.

Il faut savoir le démontrer.

Propriété. Toute suite de Cauchy de E est bornée.

Il faut savoir le démontrer.

Propriété. Si une suite de Cauchy possède une valeur d'adhérence alors elle est convergente.

Il faut savoir le démontrer.

Définition. E est un espace métrique complet si et seulement si toute suite de Cauchy de E est convergente.

Théorème. Si toute suite bornée de E possède au moins une valeur d'adhérence, alors E est complet.

Théorème. \mathbb{R} et \mathbb{C} sont complets.

2 Séries de vecteurs

Notation. \mathbb{K} désigne \mathbb{R} ou \mathbb{C} .

Définition. Un espace de Banach est un \mathbb{K} -espace vectoriel normé complet.

Notation. On fixe dans ce chapitre un espace de Banach noté E .

2.1 Séries, convergence et divergence

2.1.1 Définition d'une série de vecteurs

Définition. Soit $(a_n)_{n \in \mathbb{N}}$ une suite de vecteurs. On appelle série de terme général a_n , et on note $\sum a_n$, la suite de terme général $(a_n, \sum_{k=0}^n a_k)$. Ainsi, $\sum a_n$ est une suite d'éléments de E^2 .

Remarque. L'intérêt de cette définition un peu formelle est de distinguer les séries de vecteurs des suites de vecteurs.

Propriété. L'ensemble des séries de vecteurs, noté $\mathcal{S}(E)$ est un \mathbb{K} -espace vectoriel.

De plus, $\sum a_n + \alpha \sum b_n = \sum (a_n + \alpha b_n)$, lorsque $\sum a_n$ et $\sum b_n$ sont dans $\mathcal{S}(E)$ et lorsque $\alpha \in \mathbb{K}$.

Notation. $\sum_{k=0}^n a_k$ est appelée la somme partielle (des $n+1$ premiers termes) de $\sum a_n$.

Propriété. Soit (A_n) une suite de vecteurs. Il existe une unique série $\sum a_n$ dont la suite des sommes partielles est (A_n) . Il s'agit de la série $\sum (A_n - A_{n-1})$, en convenant que $A_{-1} = 0$. Cette série est appelée la série télescopique associée à la suite (A_n) .

Il faut savoir le démontrer.

Définition. Soient $n_0 \in \mathbb{N}^*$ et $(a_n)_{n \geq n_0}$ une suite de vecteurs.

$\sum_{n \geq n_0} a_n$ est la série $\sum b_n$ où $b_n = 0$ si $n < n_0$ et $b_n = a_n$ si $n \geq n_0$.

On dit que $\sum_{n \geq n_0} a_n$ est une série tronquée à l'ordre n_0 .

2.1.2 Convergence d'une série de vecteurs

Définition. $\sum a_n$ converge si et seulement si la suite des sommes partielles de $\sum a_n$ converge.

Dans ce cas, on note $\sum_{n=0}^{+\infty} a_n = \lim_{n \rightarrow +\infty} \sum_{k=0}^n a_k$.

Propriété. Pour tout $n_0 \in \mathbb{N}^*$, les séries $\sum a_n$ et $\sum_{n \geq n_0} a_n$ sont de même nature et en cas de

convergence, $\sum_{n=0}^{+\infty} a_n = \sum_{n=0}^{n_0-1} a_n + \sum_{n=n_0}^{+\infty} a_n$.

Corollaire. On ne change pas la nature de la série $\sum a_n$ si l'on modifie un nombre fini d'éléments de la suite (a_n) .

Définition. Si $\sum a_n$ converge, son n -ième reste de Cauchy est $R_n = \sum_{k=n+1}^{+\infty} a_k$. On a $R_n \xrightarrow{n \rightarrow +\infty} 0$.

Propriété. Soit (u_n) une suite de vecteurs. La série télescopique $\sum (u_{n+1} - u_n)$ converge si et seulement si la suite (u_n) converge et dans ce cas, $\sum_{n=0}^{+\infty} (u_{n+1} - u_n) = \lim_{n \rightarrow +\infty} u_n - u_0$.

Il faut savoir le démontrer.

Propriété. Si $\sum a_n$ et $\sum b_n$ convergent et si $\lambda \in \mathbb{K}$, alors $\sum (a_n + \lambda b_n)$ converge et $\sum_{n=0}^{+\infty} (a_n + \lambda b_n) = \sum_{n=0}^{+\infty} a_n + \lambda \sum_{n=0}^{+\infty} b_n$. Ainsi, l'ensemble des séries convergentes de vecteurs est un sous-

espace vectoriel de $\mathcal{S}(E)$, noté $\mathcal{S}_{conv}(E)$ et l'application
$$\begin{aligned} \mathcal{S}_{conv}(E) &\longrightarrow \mathbb{K} \\ \sum a_n &\longmapsto \sum_{n=0}^{+\infty} a_n \end{aligned}$$
 est linéaire.

Il faut savoir le démontrer.

Propriété. La somme d'une série convergente et d'une série divergente est une série divergente.

Remarque. On en déduit que, si la somme de deux séries est convergente, ces deux séries ont même nature. Cependant, il est possible qu'elles divergent toutes les deux. Par exemple, $\sum a_n + \sum (-a_n)$ converge, même lorsque $\sum a_n$ diverge.

Propriété. Si une série converge, son terme général tend vers 0. La réciproque est fausse.

Il faut savoir le démontrer.

Définition. Lorsque la suite a_n ne tend pas vers 0, on dit que la série $\sum a_n$ diverge grossièrement.

Propriété. La série géométrique $\sum a^n$ converge ssi $|a| < 1$ et dans ce cas $\sum_{n=0}^{+\infty} a^n = \frac{1}{1-a}$.

Propriété. Séries à valeurs dans un produit.

Soient $p \in \mathbb{N}^*$ et E_1, \dots, E_p p espaces vectoriels normés. On note $E = E_1 \times \dots \times E_p$ que l'on munit de l'une des trois normes classiques.

Soient $(x_n)_{n \in \mathbb{N}} = ((x_{1,n}, \dots, x_{p,n}))_{n \in \mathbb{N}}$ une suite d'éléments de E .

Alors la série $\sum x_n$ converge si et seulement si, pour tout $i \in \mathbb{N}_p$, $\sum x_{i,n}$ est convergente.

De plus, dans ce cas, $\sum_{n=0}^{+\infty} x_n = \left(\sum_{n=0}^{+\infty} x_{1,n}, \dots, \sum_{n=0}^{+\infty} x_{p,n} \right)$.

Propriété. Soit $\sum a_n$ une série de complexes. Elle converge si et seulement si les séries $\sum \operatorname{Re}(a_n)$ et $\sum \operatorname{Im}(a_n)$ convergent, et dans ce cas $\sum_{n=0}^{+\infty} a_n = \sum_{n=0}^{+\infty} \operatorname{Re}(a_n) + i \sum_{n=0}^{+\infty} \operatorname{Im}(a_n)$.

2.1.3 Convergence absolue

Définition. $\sum a_n \in \mathcal{S}(E)$ vérifie le critère de Cauchy si et seulement si

$$\forall \varepsilon \in \mathbb{R}_+^* \quad \exists N \in \mathbb{N} \quad \forall n \geq N \quad \forall p \in \mathbb{N} \quad \left\| \sum_{k=1}^p a_{n+k} \right\| \leq \varepsilon.$$

Propriété. $\sum a_n$ converge si et seulement si elle vérifie le critère de Cauchy.

Il faut savoir le démontrer.

Définition. $\sum a_n$ est absolument convergente si et seulement si la série $\sum \|a_n\|$ est convergente.

Propriété. Soit $\sum a_n \in \mathcal{S}(E)$. Si $\sum a_n$ est absolument convergente, alors elle converge

et $\|\sum_{n=0}^{+\infty} a_n\| \leq \sum_{n=0}^{+\infty} \|a_n\|$ (Inégalité triangulaire). La réciproque est fausse.

Il faut savoir le démontrer.

Définition. $\sum a_n$ est semi-convergente ssi elle converge sans être absolument convergente.

2.2 Séries à termes positifs

2.2.1 Théorèmes généraux

Théorème. Soit $\sum a_n \in \mathcal{S}(\mathbb{R}_+)$. Alors $\sum a_n$ converge si et seulement si la suite de ses sommes partielles est majorée, et dans ce cas, en posant pour tout $n \in \mathbb{N}$, $A_n = \sum_{k=0}^n a_k$, $\sum_{n=0}^{+\infty} a_n = \sup_{n \in \mathbb{N}} A_n$.

Il faut savoir le démontrer.

Remarque. Lorsque $\sum a_n \in \mathcal{S}(\mathbb{R}_+)$ diverge, on peut écrire que $\sum_{n=0}^{+\infty} a_n = +\infty$.

Propriété. Soient $\sum a_n, \sum b_n \in \mathcal{S}(\mathbb{R}_+)$ telles que $\forall n \in \mathbb{N} \ a_n \leq b_n$.

Si $\sum b_n$ converge, alors $\sum a_n$ converge et $\sum_{n=0}^{+\infty} a_n \leq \sum_{n=0}^{+\infty} b_n$.

Si $\sum a_n$ est divergente, alors $\sum b_n$ diverge.

Il faut savoir le démontrer.

Remarque. Lorsque $\sum a_n$ une série de complexes absolument convergente, on peut montrer qu'elle est convergente de manière élémentaire, sans utiliser la notion hors programme de suite de Cauchy.

Il faut savoir le démontrer.

Propriété. On note $l^1(\mathbb{K}) = \{(u_n)_{n \in \mathbb{N}} \in \mathbb{K}^{\mathbb{N}} / \sum |u_n| \text{ converge} \}$ et pour tout $u = (u_n)_{n \in \mathbb{N}} \in l^1(\mathbb{K})$, posons $\|u\|_1 = \sum_{n \in \mathbb{N}} |u_n|$. Alors $(l^1(\mathbb{K}), \|\cdot\|_1)$ est un \mathbb{K} -espace vectoriel normé.

Il faut savoir le démontrer.

Propriété. On note $l^2(\mathbb{K}) = \{(u_n)_{n \in \mathbb{N}} \in \mathbb{K}^{\mathbb{N}} / \sum |u_n|^2 \text{ converge} \}$ et pour tout $u = (u_n)_{n \in \mathbb{N}} \in l^2(\mathbb{K})$, posons $\|u\|_2 = \sqrt{\sum_{n \in \mathbb{N}} |u_n|^2}$. Alors $(l^2(\mathbb{K}), \|\cdot\|_2)$ est un \mathbb{K} -espace vectoriel normé.

Il faut savoir le démontrer.

Définition. Soit (a_n) et (b_n) deux suites d'un \mathbb{K} -espace vectoriel normé E .

- $a_n = O(b_n) \iff \exists C \in \mathbb{R}_+, \exists N \in \mathbb{N}, \forall n \geq N, \|a_n\| \leq C\|b_n\|$.
- $a_n = o(b_n) \iff \forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, \|a_n\| \leq \varepsilon\|b_n\|$.
- $a_n \sim b_n \iff a_n - b_n = o(b_n)$.

Remarque. Lorsque $E = \mathbb{C}$, si pour tout $n \in \mathbb{N}$, $b_n \neq 0$, alors

- $a_n = O(b_n) \iff \frac{a_n}{b_n}$ est bornée ;
- $a_n = o(b_n) \iff \frac{a_n}{b_n} \xrightarrow{n \rightarrow +\infty} 0$ et
- $a_n \sim b_n \iff \frac{a_n}{b_n} \xrightarrow{n \rightarrow +\infty} 1$.

Propriété. Soit $\sum a_n$ une série de vecteurs et $\sum b_n$ une série de **réels positifs**.

On suppose que $\|a_n\| = \mathbf{O}(b_n)$.

Si la série $\sum b_n$ converge, alors $\sum a_n$ est absolument convergente.

Si la série $\sum \|a_n\|$ diverge, alors $\sum b_n$ est divergente.

Remarque. En pratique, on utilise souvent ce théorème lorsque $a_n = o(b_n)$.

Théorème. Soient $\sum a_n, \sum b_n \in \mathcal{S}(\mathbb{R}_+)$ telles que $a_n \sim b_n$. Alors les deux séries ont la même nature.

Théorème. Soit $\sum a_n, \sum b_n \in \mathcal{S}(\mathbb{R})$. On suppose que b_n est positif à partir d'un certain rang ou bien que b_n est négatif à partir d'un certain rang. Si $a_n \sim b_n$, alors $\sum a_n$ et $\sum b_n$ ont la même nature.

méthode : pour étudier la nature d'une série, on commence par rechercher un équivalent de son terme général.

Semaine 20 (du 24 au 28 février) : Résumé de cours

On montrera plus tard le théorème suivant, dont l’énoncé peut être utilisé dès maintenant.

On dit que la suite a_n est négligeable devant la suite b_n si et seulement si $a_n = o(b_n)$.

De même, on dit que la fonction $f(x)$ est négligeable devant $g(x)$ lorsque x est au voisinage de a si et seulement si $f(x) = o(g(x))$ au voisinage de a , c’est-à-dire, en supposant que l’on peut diviser, si et

seulement si $\frac{f(x)}{g(x)} \xrightarrow{x \rightarrow a} 0$.

Théorème des croissances comparées : Soit $\alpha, \beta, \gamma \in \mathbb{R}_+^*$ et $a > 1$.

1. Les suites $\ln^\alpha(n)$, n^β , a^n et $n!$ tendent vers $+\infty$ et chacune est négligeable devant les suivantes.
2. Au voisinage de $+\infty$, les fonctions $\ln^\alpha x$, x^β et $e^{\gamma x}$ tendent vers $+\infty$ et chacune est négligeable devant les suivantes.
3. Au voisinage de 0^+ , $|\ln x|^\alpha = o\left(\frac{1}{x^\beta}\right)$.
4. Au voisinage de $-\infty$, $e^{\gamma x} = o\left(\frac{1}{|x|^\beta}\right)$.

1 Séries de Riemann

Technique de comparaison entre séries et intégrales (TCSI) : Soit $n_0 \in \mathbb{N}$.

Soit $f : [n_0, +\infty[\rightarrow \mathbb{R}$ une application décroissante et continue. La TCSI consiste en la présentation des trois étapes suivantes :

Première étape : Soit $k > n_0$. f étant décroissante, pour tout $t \in [k-1, k]$, $f(k) \leq f(t) \leq f(k-1)$.

Deuxième étape : En intégrant, on obtient $f(k) \leq \int_{k-1}^k f(t) dt \leq f(k-1)$.

Troisième étape : Soit $n > n_0$: en sommant, $\sum_{k=n_0+1}^n f(k) \leq \int_{n_0}^n f(t) dt \leq \sum_{k=n_0}^{n-1} f(k)$.

Théorème de comparaison entre séries et intégrales : Sous les mêmes notations et hypothèses, la série $\sum f(n)$ a même nature que la suite $\left(\int_{n_0}^n f(t) dt\right)_{n \geq n_0}$.

Il faut savoir le démontrer.

Propriété. La série de Riemann $\sum_{n \geq 1} \frac{1}{n^\alpha}$ converge si et seulement si $\alpha > 1$.

Il faut savoir le démontrer.

Critère de Riemann : Soient $\sum a_n \in \mathcal{S}(\mathbb{R}_+)$.

S’il existe $\alpha > 1$ tel que $n^\alpha a_n \xrightarrow{n \rightarrow +\infty} 0$, alors $\sum a_n$ converge.

S’il existe $\alpha \leq 1$ tel que $n^\alpha a_n \xrightarrow{n \rightarrow +\infty} +\infty$, alors $\sum a_n$ diverge.

Propriété. (Hors programme). $\sum_{k=1}^n \frac{1}{k} = \ln(n) + \gamma + o(1)$, où γ est la **constante d'Euler**.

Il faut savoir le démontrer.

Hors programme : séries de Bertrand. Soit $(\alpha, \beta) \in \mathbb{R}^2$.

La série $\sum_{n \geq 2} \frac{1}{n^\alpha \ln^\beta n}$ converge si et seulement si $\alpha > 1$ ou bien ($\alpha = 1$ et $\beta > 1$).

Il faut savoir le démontrer.

2 Critère de D'Alembert

Propriété. Critère de D'Alembert. Soit $\sum a_n$ une série de réels positifs, non nuls à partir d'un certain rang, telle que $\frac{a_{n+1}}{a_n} \xrightarrow{n \rightarrow +\infty} l \in \overline{\mathbb{R}}$.

- ◇ Si $l < 1$, $\sum a_n$ est convergente,
- ◇ Si $l > 1$ ou si $l = 1^+$, $\sum a_n$ diverge grossièrement.
- ◇ Lorsque $l = 1$, on ne peut conclure. C'est le cas douteux du critère de d'Alembert.

Il faut savoir le démontrer.

Hors programme : Si (a_n) et (b_n) sont deux suites de réels strictement positifs telles que, pour tout $n \in \mathbb{N}$, $\frac{a_{n+1}}{a_n} \leq \frac{b_{n+1}}{b_n}$, alors $a_n = \mathcal{O}(b_n)$.

Il faut savoir le démontrer.

Propriété. Formule de Stirling : $n! \sim \sqrt{2\pi n} e^{-n} n^n$.

3 Séries alternées

Définition. On appelle série alternée toute série réelle de la forme $\sum (-1)^n \alpha_n$ ou $\sum (-1)^{n+1} \alpha_n$, où pour tout $n \in \mathbb{N}$, $\alpha_n \in \mathbb{R}_+$.

Théorème des séries spéciales alternées (TSSA).

Soit $\sum a_n$ une série alternée telle que la suite $(|a_n|)$ est décroissante et tend vers 0. On dit dans ce cas que $\sum a_n$ est une série spéciale alternée. Alors $\sum a_n$ est convergente.

De plus pour tout $(n, N) \in \mathbb{N}^2$ avec $N \geq n$, la quantité $\sum_{k=n}^N a_k$ est du signe de son premier terme (qui est a_n) et a un module inférieur ou égal au module de son premier terme. C'est encore vrai lorsque $N = +\infty$, donc pour tout $n \in \{-1\} \cup \mathbb{N}$, le reste de Cauchy $\sum_{k=n+1}^{+\infty} a_k$ est du signe de son premier

terme (qui est a_{n+1}) et, pour tout $n \in \{-1\} \cup \mathbb{N}$, $|\sum_{k=n+1}^{+\infty} a_k| \leq |a_{n+1}|$.

Il faut savoir le démontrer.

4 Non commutativité des séries semi-convergentes.

$$\sum_{n=1}^{+\infty} \frac{(-1)^n}{n} = -\ln 2.$$

Il faut savoir le démontrer.

On peut démontrer (hors programme) que, si $\sum a_n$ est une série semi-convergente de réels, pour tout $\ell \in \mathbb{R}$, il existe une bijection $\sigma : \mathbb{N} \rightarrow \mathbb{N}$ telle que $\sum a_{\sigma(n)}$ converge et a pour somme ℓ .

Dans un chapitre ultérieur, on montrera que, lorsque $\sum a_n$ est une série absolument convergente, pour toute bijection σ de \mathbb{N} dans \mathbb{N} , $\sum a_{\sigma(n)}$ est aussi absolument convergente et $\sum_{n=0}^{+\infty} a_{\sigma(n)} = \sum_{n=0}^{+\infty} a_n$.

5 La transformation d'Abel (hors programme)

Transformation d'Abel : Si $(a_n), (x_n) \in \mathbb{C}^{\mathbb{N}}$, en posant $X_n = \sum_{k=0}^n x_k$,

pour tout $(p, q) \in \mathbb{N}^2$ avec $p \leq q$, $\sum_{n=p}^q a_n x_n = a_q X_q - a_p X_{p-1} - \sum_{n=p}^{q-1} (a_{n+1} - a_n) X_n$.

Il faut savoir le démontrer.

Remarque. Cette formule ressemble à l'intégration par parties.

Théorème d'Abel : Soient (a_n) une suite décroissante de réels qui tend vers 0 et $\sum x_n$ une série de complexes dont les sommes partielles sont bornées. Alors la série $\sum a_n x_n$ converge.

Il faut savoir le démontrer.

Semaine 21 (du 2 mars au 7) : Résumé de cours

1 Topologie dans un espace métrique

Pour tout ce chapitre, on fixe un espace métrique (E, d) non vide.

1.1 Ouverts et fermés

Définition. Soient $x \in E$ et V une partie de E .

V est un voisinage de x si et seulement s'il existe $r > 0$ tel que $B_o(x, r) \subset V$.

$\mathcal{V}(x)$ désignera l'ensemble des voisinages de x .

Remarque. Si E est un espace vectoriel normé, lorsqu'on remplace la norme sur E par une norme équivalente, pour tout $x \in E$, $\mathcal{V}(x)$ n'est pas modifié.

Propriété. La notion de voisinage satisfait les propriétés suivantes :

- ◇ Pour tout $x \in E$, $E \in \mathcal{V}(x)$.
- ◇ Pour tout $x \in E$ et tout $V \in \mathcal{V}(x)$, si $W \supset V$, alors $W \in \mathcal{V}(x)$.
- ◇ Si $x \in E$ et si $(V, W) \in \mathcal{V}(x)^2$, alors $V \cap W \in \mathcal{V}(x)$.

Il faut savoir le démontrer.

Propriété. Si $x \in E$, une intersection finie de voisinages de x est un voisinage de x .

Définition. Soit $U \subset E$. U est ouvert si et seulement si U est voisinage de tous ses points.

Propriété. La notion d'ouvert satisfait les propriétés suivantes :

- ◇ \emptyset et E sont des ouverts de E .
- ◇ Une intersection finie d'ouverts est un ouvert.
- ◇ Si I est un ensemble quelconque (éventuellement de cardinal infini) et si $(U_i)_{i \in I}$ est une famille d'ouverts de E , alors $\bigcup_{i \in I} U_i$ est un ouvert de E .

Il faut savoir le démontrer.

Propriété. Les ouverts sont exactement les réunions de boules ouvertes.

Il faut savoir le démontrer.

Définition. Une partie de E est un fermé de E si et seulement si son complémentaire est un ouvert.

Propriété. La notion de fermé satisfait les propriétés suivantes :

- ◇ \emptyset et E sont des fermés de E .
- ◇ Une réunion finie de fermés est un fermé.
- ◇ Si I est un ensemble quelconque (éventuellement de cardinal infini) et si $(F_i)_{i \in I}$ est une famille de fermés de E , alors $\bigcap_{i \in I} F_i$ est un fermé de E .

Propriété. Les boules fermées (donc en particulier les singletons) sont des fermés.

Il faut savoir le démontrer.

Corollaire. Toute partie de E de cardinal fini est un fermé de E .

1.2 Adhérence et intérieur

Définition. Soient $a \in E$ et A une partie de E . On dit que a est un point intérieur de A si et seulement si $A \in \mathcal{V}(a)$. On note $\overset{\circ}{A}$ l'ensemble des points intérieurs de A .

Ainsi, pour tout $a \in E$, $a \in \overset{\circ}{A} \iff A \in \mathcal{V}(a)$.

Propriété. Soit A une partie de E .

$\overset{\circ}{A}$ est la réunion des ouverts contenus dans A . C'est le plus grand ouvert inclus dans A .

Propriété. Soient A et B deux parties de E .

- ◇ $\overset{\circ}{A} \subset A$,
- ◇ $\overset{\circ}{A} = A$ si et seulement si A est un ouvert,
- ◇ $\overset{\circ}{\overset{\circ}{A}} = \overset{\circ}{A}$,
- ◇ $A \subset B \implies \overset{\circ}{A} \subset \overset{\circ}{B}$ et
- ◇ $\overset{\circ}{A \cap B} = \overset{\circ}{A} \cap \overset{\circ}{B}$.

Il faut savoir le démontrer.

Définition. Soient $a \in E$ et A une partie de E . On dit que a est un point adhérent de A si et seulement si, pour tout $V \in \mathcal{V}(a)$, $V \cap A \neq \emptyset$.

On note \overline{A} l'ensemble des points adhérents de A . \overline{A} est appelée l'adhérence de A .

Ainsi, pour tout $a \in E$, $a \in \overline{A} \iff [\forall V \in \mathcal{V}(a) \ V \cap A \neq \emptyset]$.

Propriété. Soit A une partie de E . $E \setminus \overline{A} = \overset{\circ}{E \setminus A}$ et $E \setminus \overset{\circ}{A} = \overline{E \setminus A}$.

Il faut savoir le démontrer.

Corollaire. Soit A une partie de E .

\overline{A} est l'intersection des fermés contenant A . C'est le plus petit fermé contenant A .

Propriété. Soient A et B deux parties de E .

- ◇ $\overline{\overline{A}} \supset A$,
- ◇ $\overline{\overline{A}} = A$ si et seulement si A est un fermé,
- ◇ $\overline{\overline{\overline{A}}} = \overline{A}$,
- ◇ $A \subset B \implies \overline{A} \subset \overline{B}$ et
- ◇ $\overline{A \cup B} = \overline{A} \cup \overline{B}$.

Il faut savoir le démontrer.

Propriété (hors programme) : Soit (x_n) une suite de points de E .

Pour tout $N \in \mathbb{N}$, notons $X_N = \{x_n / n \geq N\}$.

Alors l'ensemble des valeurs d'adhérence de (x_n) est $\bigcap_{N \in \mathbb{N}} \overline{X_N}$: il est fermé.

Il faut savoir le démontrer.

Définition. Soit A une partie de E . Soit $x \in A$.

On dit que x est isolé dans A si et seulement si il existe $V \in \mathcal{V}(x)$ tel que $V \cap A = \{x\}$, c'est-à-dire si et seulement si $x \notin \overline{A \setminus \{x\}}$.

Définition. Soit A une partie de E . Soit $x \in E$.

On dit que x est un point d'accumulation de A si et seulement si, pour tout $V \in \mathcal{V}(x)$, $(V \cap A) \setminus \{x\} \neq \emptyset$, c'est-à-dire si et seulement si $x \in \overline{A \setminus \{x\}}$.

Propriété. Les points adhérents de A sont les points de E situés à une distance nulle de A .

Il faut savoir le démontrer.

Définition. Une partie de E est dense dans E si et seulement si elle rencontre toutes les boules ouvertes de E .

Propriété. Une partie A de E est dense dans E si et seulement si $\overline{A} = E$.

Définition. Soit $A \subset E$. La frontière de A est $Fr(A) = \overline{A} \setminus \overset{\circ}{A} = \overline{A} \cap \overline{E \setminus A} = \overline{A} \cap (E \setminus \overset{\circ}{A})$.

Propriété. Soit A une partie de E . $[A \setminus Fr(A)] = \overset{\circ}{A} \subset A \subset \overline{A} = [A \cup Fr(A)]$.

Propriété. A ouvert $\iff A \cap Fr(A) = \emptyset$. A fermée $\iff Fr(A) \subset A$.

1.3 Caractérisation par les suites

Propriété. $a \in \overline{A}$ si et seulement s'il existe une suite d'éléments de A qui converge vers a .

Il faut savoir le démontrer.

Corollaire. A est dense dans E si et seulement si pour tout $l \in E$, il existe $(x_n) \in A^{\mathbb{N}}$ telle que $x_n \xrightarrow{n \rightarrow +\infty} l$.

Propriété. A est fermé si et seulement si toute suite convergente d'éléments de A a pour limite un élément de A .

1.4 Topologie induite sur une partie

Propriété. Les boules, ouverts, fermés et voisinages pour la topologie induite sur A sont respectivement les traces sur A des boules centrées dans A , des ouverts, des fermés et des voisinages pour la topologie de E .

Il faut savoir le démontrer.

Propriété. Si B est une partie de A , l'adhérence de B pour la topologie induite sur A est la trace sur A de l'adhérence de B pour la topologie globale sur E .

Propriété. Soit B une partie de A . B est dense dans A si et seulement si $A \subset \overline{B}$.

1.5 Les compacts

Définition. Une partie A de E est compacte si et seulement si toute suite d'éléments de A admet au moins une valeur d'adhérence dans A .

Propriété. Tout compact de E est fermé et borné.

Il faut savoir le démontrer.

Propriété. Soit A un compact de E et $B \subset A$: B est compact si et seulement s'il est fermé.

Théorème. Les compacts de \mathbb{R} et de \mathbb{C} sont exactement les parties fermées et bornées.

Théorème (hors programme) : Caractérisation de la compacité par la propriété de Borel Lebesgue. Soit A une partie de E . Les assertions suivantes sont équivalentes.

i) A est compact.

- ii) Pour tout ensemble I et pour toute famille d'ouverts $(U_i)_{i \in I}$ telle que $A \subset \bigcup_{i \in I} U_i$, il existe une partie J finie de I telle que $A \subset \bigcup_{i \in J} U_i$: de tout recouvrement de A par des ouverts, on peut en extraire un recouvrement fini.
- iii) Pour tout ensemble I et pour toute famille de fermés $(F_i)_{i \in I}$ telle que $A \cap \bigcap_{i \in I} F_i = \emptyset$, il existe une partie J finie de I telle que $A \cap \bigcap_{i \in J} F_i = \emptyset$.

Propriété. Si $(x_n) \in E^{\mathbb{N}}$ et $x_n \xrightarrow{n \rightarrow +\infty} l$, alors l'ensemble $\{x_n/n \in \mathbb{N}\} \cup \{l\}$ est un compact de E .

Il faut savoir le démontrer.

2 Continuité ponctuelle

On fixe deux espaces métriques E et F , ainsi qu'une fonction $f : E \rightarrow F$, dont le domaine de définition sera noté \mathcal{D}_f .

2.1 Limite en un point

Notation. On fixe une partie A de \mathcal{D}_f . On fixe également a , qui peut être infini. On suppose qu'il existe au moins une suite $(a_n) \in A^{\mathbb{N}}$ telle que $a_n \xrightarrow{n \rightarrow +\infty} a$. On fixe aussi l dans $F \cup \{\infty, +\infty, -\infty\}$.

2.1.1 Caractérisation séquentielle

Définition. $f(x)$ tend vers l lorsque x tend vers a en appartenant à A si et seulement si $\forall (x_n)_{n \in \mathbb{N}} \in A^{\mathbb{N}} \left(x_n \xrightarrow{n \rightarrow +\infty} a \implies f(x_n) \xrightarrow{n \rightarrow +\infty} l \right)$. Dans ce cas, on note $f(x) \xrightarrow[x \in A]{x \rightarrow a} l$.

Propriété. Lorsque E et F sont des espaces vectoriels normés, si l'on remplace l'une des normes sur E ou F par une norme équivalente, la condition $f(x) \xrightarrow[x \in A]{x \rightarrow a} l$ est inchangée.

Propriété. Unicité de la limite. Si $F \neq \mathbb{R}$, on impose que $l, l' \in F \cup \{\infty\}$ et si $F = \mathbb{R}$, on impose que $l, l' \in \mathbb{R} \cup \{+\infty, -\infty\}$: Si $f(x) \xrightarrow[x \in A]{x \rightarrow a} l$ et $f(x) \xrightarrow[x \in A]{x \rightarrow a} l'$, alors $l = l'$.

Propriété. On suppose que $F = \mathbb{C}$ et que $l \in \mathbb{C}$.

Alors $f(x) \xrightarrow[x \in A]{x \rightarrow a} l$ si et seulement si $(\operatorname{Re}(f)(x) \xrightarrow[x \in A]{x \rightarrow a} \operatorname{Re}(l)) \wedge (\operatorname{Im}(f)(x) \xrightarrow[x \in A]{x \rightarrow a} \operatorname{Im}(l))$.

Propriété. Si $A \subset B \subset \mathcal{D}_f$ et si $f(x) \xrightarrow[x \in B]{x \rightarrow a} l$, alors $f(x) \xrightarrow[x \in A]{x \rightarrow a} l$.

2.1.2 Caractérisation par " ε "

Propriété. Si $a \in E$ et $l \in F$,

$f(x) \xrightarrow[x \in A]{x \rightarrow a} l \iff \forall \varepsilon \in \mathbb{R}_+^* \exists \alpha \in \mathbb{R}_+^* \forall x \in A (d(x, a) \leq \alpha \implies d(f(x), l) \leq \varepsilon)$.

Il faut savoir le démontrer.

Remarque. Dans (1), on peut prendre les deux dernières inégalités indifféremment strictes ou larges.

Propriété. On peut adapter cette caractérisation dans le cas où a et l sont éventuellement infinis. On obtient par exemple :

- Si $l \in F$ et $E = \mathbb{R}$,

$$f(x) \xrightarrow[x \in A]{x \rightarrow +\infty} l \iff \forall \varepsilon \in \mathbb{R}_+^* \exists M \in \mathbb{R}_+^* \forall x \in A (x \geq M \implies \|f(x) - l\| < \varepsilon).$$
- Si $a \in E$ et $F = \mathbb{R}$,

$$f(x) \xrightarrow[x \in A]{x \rightarrow a} +\infty \iff \forall M \in \mathbb{R}_+^* \exists \alpha \in \mathbb{R}_+^* \forall x \in A (\|x - a\| \leq \alpha \implies f(x) \geq M).$$
- Si $a = \infty$ et $l \in F$, en choisissant $e_0 \in E$,

$$f(x) \xrightarrow[x \in A]{x \rightarrow \infty} l \iff \forall \varepsilon \in \mathbb{R}_+^* \exists M \in \mathbb{R}_+^* \forall x \in A (d(x, e_0) \geq M \implies d(f(x), l) \leq \varepsilon).$$
- Si $a = \infty$ et $l = \infty$, en fixant $e_0 \in E$ et $f_0 \in F$, $f(x) \xrightarrow[x \in A]{x \rightarrow \infty} \infty$ si et seulement si

$$\forall M \in \mathbb{R}_+^* \exists N \in \mathbb{R}_+^* \forall x \in A (d(x, e_0) \geq N \implies d(f(x), f_0) \geq M).$$

Remarque. Une suite $(x_n) \in E^{\mathbb{N}}$ peut être vue comme la fonction $\begin{matrix} \mathbb{N} & \longrightarrow & E \\ n & \longmapsto & x_n \end{matrix}$, définie sur \mathbb{N} qui est une partie non majorée de \mathbb{R} . La notion de limite d'une suite dans un espace métrique devient donc un cas particulier de la notion de limite d'une fonction en $+\infty$.

2.1.3 Caractérisation par voisinages

Définition. Dans \mathbb{R} , on appelle voisinage de $+\infty$ toute partie contenant un intervalle $]c, +\infty[$ où $c \in \mathbb{R}$ et voisinage de $-\infty$ toute partie contenant un intervalle $] -\infty, c[$.

Ainsi $\mathcal{V}(+\infty) = \{V \subset \mathbb{R} / \exists c \in \mathbb{R} \]c, +\infty[\subset V\}$ et $\mathcal{V}(-\infty) = \{V \subset \mathbb{R} / \exists c \in \mathbb{R} \] -\infty, c[\subset V\}$.

Définition. On suppose que E n'est pas borné. Soit $e \in E$. On appelle voisinage dans E de ∞ toute partie contenant le complémentaire d'une boule fermée centrée en e .

Ainsi $\mathcal{V}(\infty) = \{V \subset E / \exists R > 0 \ E \setminus B_f(e, R) \subset V\}$. On vérifie que $\mathcal{V}(\infty)$ ne dépend pas de e .

Propriété. Avec les définitions précédentes de voisinages, on a encore :

Une intersection de deux voisinages de a est un voisinage a .

Toute partie contenant un voisinage de a est un voisinage de a .

Remarque.

Avec ces nouvelles définitions, les hypothèses portant sur a et A énoncées au début du présent paragraphe se résument ainsi : tout voisinage V de a rencontre A .

Définition. On dit que $f|_A$ vérifie une certaine propriété au voisinage de a si et seulement s'il existe un voisinage V de a tel que $f|_{V \cap A}$ vérifie cette propriété.

Lorsqu'on énonce une propriété portant sur f au voisinage de $a \in E$, on dit que c'est une propriété locale (de f au voisinage de a). Lorsqu'on énonce une propriété portant sur f au voisinage de ∞ ou de $\pm\infty$, on dit que c'est une propriété asymptotique.

Propriété. $f(x) \xrightarrow[x \in A]{x \rightarrow a} l \iff \forall V \in \mathcal{V}(l) \exists U \in \mathcal{V}(a) \ f(U \cap A) \subset V$.

Il faut savoir le démontrer.

Propriété. Caractère local (ou asymptotique) de la notion de limite.

Pour tout $U_0 \in \mathcal{V}(a)$, $f(x) \xrightarrow[x \in A]{x \rightarrow a} l \iff f(x) \xrightarrow[x \in A \cap U_0]{x \rightarrow a} l$.

Ainsi la valeur de l'éventuelle limite de $f(x)$ lorsque x tend vers a pour x appartenant à A ne dépend pas du comportement global de f sur A mais seulement du comportement de $f|_A$ au voisinage de a . En particulier, si l'on modifie les valeurs de $f(x)$ lorsque $x \notin U_0$, on ne modifie pas la valeur logique de la proposition $f(x) \xrightarrow[x \in A]{x \rightarrow a} l$.

Définition. Soit $a \in E$ tel que $a \in \overline{\mathcal{D}_f \setminus \{a\}}$. Ainsi, a est un point d'accumulation de \mathcal{D}_f . S'il existe $l \in F$ tel que $f(x) \xrightarrow[x \in \mathcal{D}_f \setminus \{a\]}{x \rightarrow a} l$, on écrit que $f(x) \xrightarrow[x \neq a]{x \rightarrow a} l$ ou même $f(x) \xrightarrow{x \rightarrow a} l$.

Propriété. Soient A et B deux parties de \mathcal{D}_f qui rencontrent tout voisinage de a .

Alors, $(f(x) \xrightarrow[x \in A]{x \rightarrow a} l \text{ et } f(x) \xrightarrow[x \in B]{x \rightarrow a} l) \iff f(x) \xrightarrow[x \in A \cup B]{x \rightarrow a} l$.

Il faut savoir le démontrer.

Définition. Supposons que $E = \mathbb{R}$ et que $a \in \mathbb{R}$.

- Si $a \in \overline{\mathcal{D}_f \cap]a, +\infty[}$, et si $f(x) \xrightarrow[x \in \mathcal{D}_f \cap]a, +\infty[]{x \rightarrow a} l$, on note $f(x) \xrightarrow[x > a]{x \rightarrow a} l$ ou $f(x) \xrightarrow[x \rightarrow a^+]{x \rightarrow a} l$ et $l = \lim_{x \rightarrow a} f(x)$ ou $l = \lim_{x \rightarrow a^+} f(x)$. Il s'agit de la notion de limite à droite du réel a .

- De même, si $a \in \overline{\mathcal{D}_f \cap]-\infty, a[}$, et si $f(x) \xrightarrow[x \in \mathcal{D}_f \cap]-\infty, a[]{x \rightarrow a} l$, on note $f(x) \xrightarrow[x < a]{x \rightarrow a} l$ ou $f(x) \xrightarrow[x \rightarrow a^-]{x \rightarrow a} l$ et $l = \lim_{x \rightarrow a} f(x)$ ou $l = \lim_{x \rightarrow a^-} f(x)$. Il s'agit de la notion de limite à gauche du réel a .

Propriété. On suppose que $E = \mathbb{R}$ et $a \in \overline{\mathcal{D}_f \cap]-\infty, a[} \cap \overline{\mathcal{D}_f \cap]a, +\infty[}$.

Alors $f(x) \xrightarrow[x \rightarrow a]{x \rightarrow a} l$ si et seulement si $f(x) \xrightarrow[x > a]{x \rightarrow a} l$ et $f(x) \xrightarrow[x < a]{x \rightarrow a} l$.

2.2 Continuité en un point

Définition. Soit $a \in \mathcal{D}_f$. f est continue en a si et seulement si $f(x) \xrightarrow[x \in \mathcal{D}_f]{x \rightarrow a} f(a)$.

Propriété. On suppose que $F = \mathbb{C}$. Soit $a \in \mathcal{D}_f$.

f est continue en a si et seulement si $\operatorname{Re}(f)$ et $\operatorname{Im}(f)$ sont continues en a .

Propriété. f est continue en a si et seulement si l'une des propriétés suivantes est vérifiée :

- Pour toute suite (x_n) de points de \mathcal{D}_f telle que $x_n \xrightarrow[n \rightarrow +\infty]{} a$, $f(x_n) \xrightarrow[n \rightarrow +\infty]{} f(a)$.
- $\forall \varepsilon > 0 \exists \alpha > 0 \forall x \in \mathcal{D}_f (d(x, a) \leq \alpha \implies d(f(x), f(a)) \leq \varepsilon)$.
- $\forall V \in \mathcal{V}(f(a)) \exists U \in \mathcal{V}(a) f(U \cap \mathcal{D}_f) \subset V$.

Propriété. Soit $a \in \mathcal{D}_f$.

Si $a \notin \overline{\mathcal{D}_f \setminus \{a\}}$ (on dit que a est un point isolé de \mathcal{D}_f), f est toujours continue en a .

Si $a \in \overline{\mathcal{D}_f \setminus \{a\}}$, f est continue en a si et seulement si $f(x) \xrightarrow[x \in \mathcal{D}_f \setminus \{a\}]{x \rightarrow a} f(a)$.

Remarque. Soient $a \in \mathcal{D}_f$ et $U_0 \in \mathcal{V}(a)$. f est continue en a si et seulement si $f|_{\mathcal{D}_f \cap U_0}$ est continue en a . Ainsi la notion de continuité (au point a) est une notion locale.

Définition. On dit que f est continue si et seulement si elle est continue en chaque point de son domaine de définition.

Propriété. Les applications lipschitziennes sont continues.

Il faut savoir le démontrer.

Propriété. Soient A une partie de \mathcal{D}_f et $a \in A$. Si f est continue en a , alors $f|_A$ est aussi continue en a .

Corollaire. Soit A une partie incluse dans \mathcal{D}_f . Si f est continue, alors $f|_A$ est continue.

Définition. On suppose que $E = \mathbb{R}$. Soit $a \in \mathcal{D}_f$. On dit que f est continue à droite en a si et seulement si $f|_{[a, +\infty[\cap \mathcal{D}_f}$ est continue en a . On définit de même la notion de continuité à gauche.

Propriété. On suppose que $E = \mathbb{R}$. Soit $a \in \mathcal{D}_f$.

f est continue en a si et seulement si f est continue à droite et à gauche en a .

Semaine 22 (du 9 mars au 14) : Résumé de cours

1 Continuité ponctuelle (suite et fin)

1.1 Continuité en un point (suite et fin)

Définition. On suppose que f est continue. Soit $D \supset \mathcal{D}_f$. On dit que f se prolonge par continuité sur D si et seulement s'il existe une application $\tilde{f} : D \rightarrow F$ continue et telle que $\tilde{f}|_{\mathcal{D}_f} = f$.

Définition. Soit $a \in \overline{\mathcal{D}_f} \setminus \mathcal{D}_f$. f admet un prolongement par continuité en a si et seulement si f admet une limite finie en a . Dans ce cas, l'unique prolongement par continuité \tilde{f} de f est donné par $\tilde{f}(a) = \lim_{\substack{x \rightarrow a \\ x \neq a}} f(x)$.

Propriété. Soient $A \subset E$ et f et g deux applications continues de A dans F . Si f et g coïncident sur une partie dense dans A , alors $f = g$.

Il faut savoir le démontrer.

1.2 Théorèmes de composition

Notation. Dans ce paragraphe, on fixe un troisième espace métrique noté G et une seconde fonction $g : F \rightarrow G$, définie sur \mathcal{D}_g .

Propriété. Soit B une partie de \mathcal{D}_g telle que $f(A) \subset B$. Soit $m \in G \cup \{\infty, +\infty, -\infty\}$.

Pour que $g(f(x)) \xrightarrow[x \in A]{x \rightarrow a} m$, il suffit que $f(x) \xrightarrow[x \in A]{x \rightarrow a} l$ (auquel cas B rencontre tout voisinage de l) et que $g(y) \xrightarrow[y \in B]{y \rightarrow l} m$.

Corollaire. On suppose que $f(\mathcal{D}_f) \subset \mathcal{D}_g$ et on fixe $a \in \mathcal{D}_f$.

Si f est continue en a et g en $f(a)$, alors $g \circ f$ est continue en a .

Corollaire. On suppose que $f(\mathcal{D}_f) \subset \mathcal{D}_g$.

Si f et g sont continues, alors $g \circ f$ est continue (et définie sur \mathcal{D}_f).

Corollaire. On suppose que $f(A) \subset \mathcal{D}_g$. Si $f(x) \xrightarrow[x \in A]{x \rightarrow a} b$ et si g est continue en b , alors $g(f(x)) \xrightarrow[x \in A]{x \rightarrow a} g(b)$.

Propriété. Limite en un point d'une application à valeurs dans un produit.

Supposons que $F = F_1 \times \cdots \times F_q$, où F_1, \dots, F_q sont des espaces vectoriels normés et notons $f : E \rightarrow F$

$$x \mapsto f(x) = (f_1(x), \dots, f_q(x)).$$

Soient A une partie de \mathcal{D}_f , $a \in \overline{A}$ et $l = (l_1, \dots, l_q) \in F$. Alors,

$f(x) \xrightarrow[x \in A]{x \rightarrow a} l$ si et seulement si pour tout $i \in \mathbb{N}_q$, $f_i(x) \xrightarrow[x \in A]{x \rightarrow a} l_i$.

Propriété. Continuité en un point d'une application à valeurs dans un produit.

Supposons que $F = F_1 \times \cdots \times F_q$, où F_1, \dots, F_q sont des espaces vectoriels normés et notons

$$f: E \longrightarrow F$$

$$x \longmapsto f(x) = (f_1(x), \dots, f_q(x)). \text{ Soit } a \in \mathcal{D}_f. \text{ Alors,}$$

f est continue en a si et seulement si pour tout $i \in \mathbb{N}_q$, f_i est continue en a .

1.3 Opérations algébriques sur les limites**1.3.1 Somme de deux applications à valeurs vectorielles****Notation.**

Dans ce paragraphe, on fixe une seconde fonction $g: E \longrightarrow F$, définie sur \mathcal{D}_g .

On suppose que $A \subset \mathcal{D}_f \cap \mathcal{D}_g$.

Propriété. Si $f(x) \xrightarrow[x \in A]{x \rightarrow a} l$ et $g(x) \xrightarrow[x \in A]{x \rightarrow a} l'$, alors $(f + g)(x) \xrightarrow[x \in A]{x \rightarrow a} l + l'$.

Remarque. C'est valable dans le cadre des limites infinies, à condition d'éviter la forme indéterminée $\infty - \infty$, c'est-à-dire lorsque l et l' sont les deux éléments distincts de $\{+\infty, -\infty\}$.

Propriété. Soit $a \in \mathcal{D}_f \cap \mathcal{D}_g$. Si f et g sont continues en a , $f + g$ est continue en a .

Corollaire. La somme de deux applications continues est continue.

1.3.2 Produit d'une application scalaire par une application vectorielle

Notation. Dans ce paragraphe, on suppose que f est une application de E dans \mathbb{K} et que g est une application de E dans un \mathbb{K} -espace vectoriel normé F . Ainsi f est une "application scalaire" et g est une "application vectorielle". On suppose que $A \subset \mathcal{D}_f \cap \mathcal{D}_g$.

Propriété. Si $f(x) \xrightarrow[x \in A]{x \rightarrow a} l$ et $g(x) \xrightarrow[x \in A]{x \rightarrow a} l'$, alors $(fg)(x) \xrightarrow[x \in A]{x \rightarrow a} ll'$.

Remarque. C'est valable dans le cadre des limites infinies, à condition d'éviter la forme indéterminée $0 \times \infty$.

Propriété. Soit $a \in \mathcal{D}_f \cap \mathcal{D}_g$. Si f et g sont continues en a , fg est aussi continue en a .

Corollaire. Le produit d'une application scalaire continue par une application vectorielle continue est continue.

Propriété. Soit A une partie de E . L'ensemble $\mathcal{C}(A, F)$ des applications continues de A dans F est un \mathbb{K} -espace vectoriel. $\mathcal{C}(A, \mathbb{K})$ est une \mathbb{K} -algèbre.

Propriété. On suppose que f est une application de E dans \mathbb{K}^* .

Si $f(x) \xrightarrow[x \in A]{x \rightarrow a} l \in \mathbb{K}$ alors $(\frac{1}{f})(x) \xrightarrow[x \in A]{x \rightarrow a} \frac{1}{l}$.

Remarque. Cette propriété est valable avec des limites infinies dans les cas suivants :

- Si $l = \infty$, en convenant que $\frac{1}{\infty} = 0$.
- Si $\mathbb{K} = \mathbb{R}$ et $l = 0^+$ (c'est-à-dire que $l = 0$ et que f est strictement positive au voisinage de a), en convenant que $\frac{1}{0^+} = +\infty$.
- Si $\mathbb{K} = \mathbb{R}$ et $l = 0^-$, en convenant que $\frac{1}{0^-} = -\infty$.

1.4 Cas des fonctions à valeurs dans \mathbb{R} .

On suppose ici que $F = \mathbb{R}$.

Propriété : passage à la limite sur une inégalité large :

Si $\forall x \in A$ $f(x) \leq g(x)$, $f(x) \xrightarrow[x \in A]{x \rightarrow a} l$ et $g(x) \xrightarrow[x \in A]{x \rightarrow a} l'$, alors $l \leq l'$.

Principe du tunnel (pour des inégalités strictes) :

Si $f(x) \xrightarrow[x \in A]{x \rightarrow a} l \in \mathbb{R}$ et $\alpha < l < \beta$, alors, au voisinage de a , $\alpha < f(x) < \beta$.

Corollaire. Si $f(x) \xrightarrow[x \in A]{x \rightarrow a} l \in \mathbb{R}$ alors $f|_A$ est bornée au voisinage de a .

Propriété. Principe des gendarmes.

Si $\forall x \in A$ $h_1(x) \leq h_2(x) \leq h_3(x)$, $h_1(x) \xrightarrow[x \in A]{x \rightarrow a} l$ et $h_3(x) \xrightarrow[x \in A]{x \rightarrow a} l$, alors $h_2(x) \xrightarrow[x \in A]{x \rightarrow a} l$.

Remarque. On peut adapter le principe des gendarmes au cas où $l = \pm\infty$.

Il faut savoir le démontrer.

1.5 Cas des fonctions de \mathbb{R} dans \mathbb{R} .

Théorème de la limite monotone : Soit $(m, M) \in \overline{\mathbb{R}}^2$ avec $m < M$ et $f :]m, M[\rightarrow \mathbb{R}$.

Si f est croissante, alors $f(x) \xrightarrow[x \in I]{x \rightarrow M} \sup_{y \in I} f(y) \in \overline{\mathbb{R}}$ et $f(x) \xrightarrow[x \in I]{x \rightarrow m} \inf_{y \in I} f(y) \in \overline{\mathbb{R}}$.

Si f est décroissante, alors $f(x) \xrightarrow[x \in I]{x \rightarrow M} \inf_{y \in I} f(y) \in \overline{\mathbb{R}}$ et $f(x) \xrightarrow[x \in I]{x \rightarrow m} \sup_{y \in I} f(y) \in \overline{\mathbb{R}}$.

Il faut savoir le démontrer.

Propriété. Soit $(m, M) \in \overline{\mathbb{R}}^2$ avec $m < M$ et $f :]m, M[\rightarrow \mathbb{R}$ une application monotone. Pour tout $a \in I$, f possède en a une limite à droite, notée $f(a^+)$, et une limite à gauche, notée $f(a^-)$. De plus, si f est croissante, $f(a^-) \leq f(a) \leq f(a^+)$, et si f est décroissante, $f(a^-) \geq f(a) \geq f(a^+)$. f est discontinue en a si et seulement si $f(a^+) \neq f(a^-)$ et dans ce cas $|f(a^+) - f(a^-)|$ s'appelle le saut de discontinuité de f en a .

Il faut savoir le démontrer.

Exercice. Si f est une application strictement croissante d'un intervalle I dans \mathbb{R} , montrer que l'ensemble des points de discontinuité de f est au plus dénombrable.

Il faut savoir le démontrer.

2 Continuité globale

2.1 Cas des fonctions de \mathbb{R} dans \mathbb{R}

Notation. Dans ce paragraphe, on fixe un intervalle I d'intérieur non vide.

Théorème des valeurs intermédiaires (TVI) :

Soit $f : I \rightarrow \mathbb{R}$ une application continue à valeurs réelles. Soit $a, b \in I$ avec $a < b$. Alors, pour tout réel k compris entre $f(a)$ et $f(b)$, il existe $c \in [a, b]$ tel que $f(c) = k$.

Ainsi, l'image d'un intervalle par une application continue à valeurs réelles est un intervalle.

Il faut savoir le démontrer.

Exercice. Soit P une application polynomiale de \mathbb{R} dans \mathbb{R} de degré impair. Montrer que P possède au moins une racine réelle.

Il faut savoir le démontrer.

Théorème.

Une fonction continue de I dans \mathbb{R} est injective si et seulement si elle est strictement monotone.

Théorème de la bijection :

Soit $f : I \rightarrow \mathbb{R}$ une application continue et strictement monotone.

f est une bijection de I dans $f(I)$ et $f^{-1} : f(I) \rightarrow I$ est également **continue** et strictement monotone (de même sens de variation que f).

Remarque. Dans un tableau de variations, les flèches obliques signifient que l'application étudiée est continue et strictement monotone. Le théorème de la bijection affirme en particulier que toutes les valeurs intermédiaires sont atteintes exactement une fois.

Définition. Soit E et F deux espaces métriques. $f : E \rightarrow F$ est un homeomorphisme entre E et F si et seulement si f est une bijection telle que f et f^{-1} sont continues.

Deux espaces métriques sont homéomorphes si et seulement si il existe un homéomorphisme entre ces deux espaces.

2.2 Continuité et ouverts

Théorème. Soit E et F deux espaces métriques et soit $f : E \rightarrow F$ une application définie sur \mathcal{D}_f . Les propriétés suivantes sont équivalentes.

- i) f est continue.
- ii) L'image réciproque par f de tout ouvert de F est un ouvert pour la topologie induite sur \mathcal{D}_f .
- iii) L'image réciproque par f de tout fermé de F est un fermé pour la topologie induite sur \mathcal{D}_f .

Il faut savoir le démontrer.

2.3 Continuité d'une application linéaire

Notation. Dans ce paragraphe, E et F désignent 2 \mathbb{K} -espaces vectoriels normés.

Théorème. On suppose que $f \in L(E, F)$. Les assertions suivantes sont équivalentes.

- i) f est continue.
- ii) f est continue en 0.
- iii) f est bornée sur la boule unité de E .
- iv) f est bornée sur la sphère unité de E .
- v) $\exists k \in \mathbb{R}_+ \forall x \in E \|f(x)\| \leq k\|x\|$.
- vi) f est lipschitzienne.

Il faut savoir le démontrer.

Exercice. On note $\mathcal{LC}(E)$ l'ensemble des endomorphismes continus sur E .

1°) Montrer que $\mathcal{LC}(E)$ est un \mathbb{K} -espace vectoriel que l'on peut munir de la norme suivante :

$$\forall u \in \mathcal{LC}(E) \quad \|u\| = \sup_{\substack{x \in E \\ \|x\|_E \leq 1}} \|u(x)\|_E.$$

2°) Montrer que $\forall u \in \mathcal{LC}(E) \quad \forall x \in E \quad \|u(x)\|_E \leq \|u\| \|x\|_E$.

Montrer que $\forall (u, v) \in \mathcal{LC}(E)^2 \quad \|v \circ u\| \leq \|v\| \|u\|$.

Il faut savoir le démontrer.

2.4 Continuité et compacité

Propriété (hors programme) : f est continue si et seulement si ses restrictions aux compacts de E inclus dans \mathcal{D}_f sont continues.

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

Il faut savoir le démontrer.

Corollaire. Soient A un compact non vide de E et $f : A \rightarrow \mathbb{R}$ une application continue. Alors f est bornée et elle atteint ses bornes, c'est-à-dire qu'il existe $(x_m, x_M) \in A^2$ tel que, pour tout $x \in A$, $f(x_m) \leq f(x) \leq f(x_M)$.

Corollaire. L'image directe d'un segment de \mathbb{R} par une application continue à valeurs réelles est un segment.

2.5 La continuité uniforme

Notation. On fixe deux espaces métriques E et F ainsi qu'une application $f : E \rightarrow F$ définie sur $\mathcal{D}_f \subset E$.

Définition. f est uniformément continue sur \mathcal{D}_f si et seulement si $\forall \varepsilon \in \mathbb{R}_+^* \exists \alpha \in \mathbb{R}_+^* \forall (x, y) \in \mathcal{D}_f^2 (d(x, y) \leq \alpha \implies d(f(x), f(y)) \leq \varepsilon)$.

Propriété. Caractérisation séquentielle de la continuité uniforme.

f est uniformément continue si et seulement si pour tout couple $((x_n), (y_n))$ de suites d'éléments de \mathcal{D}_f tel que $d(x_n, y_n) \xrightarrow{n \rightarrow +\infty} 0$, $d(f(x_n), f(y_n)) \xrightarrow{n \rightarrow +\infty} 0$.

Il faut savoir le démontrer.

Propriété. La composée de deux applications uniformément continues est uniformément continue.

Propriété. "lipschitzienne" \implies "uniformément continue" \implies "continue", mais les réciproques sont fausses.

Théorème de Heine : Toute application continue sur un compact est uniformément continue.

Il faut savoir le démontrer.

Semaine 23 (du 16 mars au 20) : Résumé de cours

Comparaison au voisinage d'un point

\mathbb{K} désigne \mathbb{R} ou \mathbb{C} .

Notation. A est une partie d'un espace \mathbb{K} -espace vectoriel normé E . Soit $a \in E \cup \{+\infty, -\infty, \infty\}$. On suppose que tout voisinage de a rencontre A .

Sauf mention du contraire, les applications considérées dans ce chapitre sont définies sur A et sont à valeurs dans un \mathbb{K} -espace vectoriel normé.

1 La relation de domination

Définition. On dit que f est dominée par g au voisinage de a si et seulement si

(1) : $\exists V \in \mathcal{V}(a) \exists C \in \mathbb{R}_+^* \forall x \in V \cap A \|f(x)\| \leq C\|g(x)\|$.

On note alors $f(x) = \underset{x \in A}{\underset{x \rightarrow a}{\mathbf{O}}}(g(x))$ (notation de Landau) ou bien $f(x) \preceq g(x)$ (notation de Hardy).

Remarque. $f = \mathbf{O}(g)$ si et seulement si $\|f(x)\| = \mathbf{O}(\|g(x)\|)$.

Cas particulier des suites.

$x_n = \mathbf{O}(y_n)$ si et seulement si $\exists N \in \mathbb{N} \exists C \in \mathbb{R}_+^* \forall n \geq N \|x_n\| \leq C\|y_n\|$.

Propriété. S'il existe V voisinage de a tel que $g(x)$ ne s'annule jamais sur V ,

$f = \mathbf{O}(g)$ si et seulement si $x \mapsto \frac{\|f(x)\|}{\|g(x)\|}$ est bornée au voisinage de a .

Propriété. $\mathbf{O}(\mathbf{O}(f)) = \mathbf{O}(f)$ (**Il faut savoir le démontrer.**), $\mathbf{O}(f) + \mathbf{O}(f) = \mathbf{O}(f)$,

Lorsque $\varphi(A) \subset \mathbb{K}$, $\mathbf{O}(\varphi) \cdot \mathbf{O}(f) = \mathbf{O}(\varphi \cdot f)$. Si $\alpha \in \mathbb{R}_+^*$, lorsque $f(A) \subset \mathbb{R}_+^*$, $\mathbf{O}(f)^\alpha = \mathbf{O}(f^\alpha)$.

Propriété. Si $f(x) = \underset{x \in A}{\underset{x \rightarrow a}{\mathbf{O}}}(g(x))$ et si $g(x) \underset{x \in A}{\underset{x \rightarrow a}{\longrightarrow}} 0$, alors $f(x) \underset{x \in A}{\underset{x \rightarrow a}{\longrightarrow}} 0$.

Propriété. (Hors programme) Soient $(u_n), (v_n) \in \mathbb{R}_+^{\mathbb{N}}$.

S'il existe $N \in \mathbb{N}$ tel que $\forall n \geq N \frac{u_{n+1}}{u_n} \leq \frac{v_{n+1}}{v_n}$, alors $u_n = \mathbf{O}(v_n)$.

Il faut savoir le démontrer.

2 La relation de prépondérance

Définition. On dit que f est négligeable devant g au voisinage de a si et seulement si

(1) : $\forall \varepsilon \in \mathbb{R}_+^* \exists V \in \mathcal{V}(a) \forall x \in V \cap A \|f(x)\| \leq \varepsilon\|g(x)\|$.

On note alors $f(x) = \underset{x \in A}{\underset{x \rightarrow a}{o}}(g(x))$ (notation de Landau) ou bien $f(x) \ll g(x)$ (notation de Hardy).

Remarque. $f = o(g)$ si et seulement si $\|f(x)\| = o(\|g(x)\|)$.

Cas particulier des suites. $x_n = o(y_n)$ si et seulement si $\forall \varepsilon \in \mathbb{R}_+^* \exists N \in \mathbb{N} \forall n \geq N \|x_n\| \leq \varepsilon \|y_n\|$.

Propriété. S'il existe V voisinage de a tel que $g(x)$ ne s'annule jamais sur V ,

$f = o(g)$ si et seulement si $\frac{\|f(x)\|}{\|g(x)\|} \xrightarrow[x \in A]{x \rightarrow a} 0$.

Exemples. $f = o(1)$ si et seulement si $f(x) \xrightarrow[x \in A]{x \rightarrow a} 0$.

Exemple. Soit $\alpha, \beta \in \mathbb{R}$ avec $\alpha < \beta$. Alors en $+\infty$, $x^\alpha = o(x^\beta)$ et en 0^+ , $x^\beta = o(x^\alpha)$.

Propriété. $o(f) = \mathbf{O}(f)$, $o(\mathbf{O}(f)) = o(f)$ et $\mathbf{O}(o(f)) = o(f)$ (donc aussi $o(o(f)) = o(f)$).

$o(f) + o(f) = o(f)$ (**Il faut savoir le démontrer.**),

Lorsque $\varphi(A) \subset \mathbb{K}$, $o(\varphi) \cdot \mathbf{O}(f) = o(\varphi \cdot f)$ et $\mathbf{O}(\varphi) \cdot o(f) = o(\varphi \cdot f)$ (donc aussi $o(\varphi) \cdot o(f) = o(\varphi \cdot f)$).

Si $\alpha \in \mathbb{R}_+^*$, lorsque $f(A) \subset \mathbb{R}_+^*$, $o(f)^\alpha = o(f^\alpha)$.

Théorème des croissances comparées : Soit $\alpha, \beta, \gamma \in \mathbb{R}_+^*$ et $a > 1$.

1. Les suites $\ln^\alpha(n)$, n^β , a^n et $n!$ tendent vers $+\infty$ et chacune est négligeable devant les suivantes.
2. Au voisinage de $+\infty$, les fonctions $\ln^\alpha x$, x^β et $e^{\gamma x}$ tendent vers $+\infty$ et chacune est négligeable devant les suivantes.
3. Au voisinage de 0^+ , $|\ln x|^\alpha = o\left(\frac{1}{x^\beta}\right)$.
4. Au voisinage de $-\infty$, $e^{\gamma x} = o\left(\frac{1}{|x|^\beta}\right)$.

3 La relation d'équivalence

3.1 Définition

Définition. On dit que f est équivalente à g au voisinage de a si et seulement si $f - g = o(g)$. Ainsi,

$$\boxed{f(x) \underset[x \in A]{x \rightarrow a} \sim g(x) \iff f = g + o(g)}.$$

Propriété. On suppose qu'il existe V voisinage de a tel que $g(x)$ ne s'annule jamais sur V , que f et g sont à valeurs dans \mathbb{K} . Alors $f \sim g \iff \frac{f(x)}{g(x)} \xrightarrow[x \in A]{x \rightarrow a} 1$.

Exemple. Si $P(X) = \sum_{k=m}^n a_k X^k$ est un polynôme à coefficients complexes, avec $a_n \neq 0$ et $a_m \neq 0$, au voisinage de 0, $P(t) \sim a_m t^m$ et au voisinage de $+\infty$, $P(t) \sim a_n t^n$.

Propriété. La relation " \sim " est une relation d'équivalence sur $\mathcal{F}(A, F)$.

Propriété. Si $f(x) \xrightarrow[x \in A]{x \rightarrow a} l \in \mathbb{K}$ et si $l \neq 0$, alors $f(x) \sim l$.

3.2 Propriétés de stabilité de la relation d'équivalence

Propriété. Si $f(x) \sim g(x)$, alors $\|f(x)\| \sim \|g(x)\|$.

Propriété. Stabilité du produit.

Si $\varphi \sim \Psi$, avec φ et Ψ à valeurs dans \mathbb{K} , et si $f \sim g$, alors $\varphi \cdot f \sim \Psi \cdot g$.

Il faut savoir le démontrer.

Propriété. Si $g(x) \neq 0$ au voisinage de a et $f \sim g$, avec f et g à valeurs dans \mathbb{K} , alors $\frac{1}{f(x)} \sim \frac{1}{g(x)}$.

Propriété. On suppose que f et g sont à valeurs réelles.

Si $f \sim g$, alors f et g ont le même signe au voisinage de a au sens strict.

Propriété. Soient $\alpha \in \mathbb{R}$. On suppose que f et g sont à valeurs réelles.

Si $f \sim g$ et si g est strictement positive au voisinage de a , alors $f^\alpha(x) \sim g^\alpha(x)$.

Propriété. Si $f \sim g$ et si $g(x) \xrightarrow[x \in A]{x \rightarrow a} l \in F \cup \{\infty, \pm\infty\}$, alors $f(x) \xrightarrow[x \in A]{x \rightarrow a} l$.

Propriété. La condition $f = \mathbf{O}(g)$ (respectivement $f = o(g)$, $f \sim g$) est vraie si et seulement si elle l'est en remplaçant f et g par des applications équivalentes.

Propriété. (Hors programme) On suppose que f et g sont à valeurs réelles strictement positives. Si $g(x) \xrightarrow[x \in A]{x \rightarrow a} l \in \mathbb{R}_+ \setminus \{1\}$ et si $f(x) \sim g(x)$, alors $\ln(f(x)) \sim \ln(g(x))$.

Lorsque $g(x) \xrightarrow[x \in A]{x \rightarrow a} 1$, alors $\ln(g(x)) \sim g(x) - 1$.

Il faut savoir le démontrer.

Propriété. Changement de variable.

Soient F un second \mathbb{K} -espace vectoriel normé, $B \subset F$ et $b \in F \cup \{+\infty, -\infty, \infty\}$. On suppose que tout voisinage de b rencontre B . Soit $\varphi : B \rightarrow A$ une application telle que $\boxed{\varphi(t) \xrightarrow[t \in B]{t \rightarrow b} a}$.

Si $f(x) \xrightarrow[x \in A]{x \rightarrow a} g(x)$ (respectivement : $f(x) = \mathbf{O}(g(x))$, $f(x) = o(g(x))$), alors

$f \circ \varphi(t) \xrightarrow[t \in B]{t \rightarrow b} g \circ \varphi(t)$ (respectivement : $f \circ \varphi(t) = \mathbf{O}(g \circ \varphi(t))$, $f \circ \varphi(t) = o(g \circ \varphi(t))$).

Il faut savoir le démontrer.

3.3 Défauts de stabilité de la relation d'équivalence

En général, si $f(x) \sim g(x)$, $\varphi(f(x)) \not\sim \varphi(g(x))$.

L'équivalence de fonctions au voisinage d'un point n'est pas stable pour la somme.

Elever un équivalent à une puissance qui dépend de la variable n'est pas autorisé. Par exemple, au voisinage de $+\infty$, $1 + \frac{1}{n} \sim 1$, mais $(1 + \frac{1}{n})^n \xrightarrow[n \rightarrow +\infty]{} e$, donc $(1 + \frac{1}{n})^n \not\sim 1$.

3.4 Résumons : quelques méthodes de calculs d'équivalents

- ◇ Si $x_n \xrightarrow[n \rightarrow +\infty]{} l \in E$, avec $l \neq 0$, alors $x_n \sim l$.
- ◇ Si $x_n = a_n b_n$, chercher des équivalents de a_n et de b_n et en faire le produit.
- ◇ Si $x_n = \frac{a_n}{b_n}$, chercher des équivalents de a_n et de b_n et en faire le quotient.
- ◇ Si $x_n = a_n + b_n$, regarder si $a_n = o(b_n)$, auquel cas $x_n \sim b_n$, ou bien si $b_n = o(a_n)$, auquel cas $x_n \sim a_n$.

4 Les développements limités.

Dans ce paragraphe, les fonctions considérées sont définies sur une partie A de \mathbb{K} et sont à valeurs dans \mathbb{K} .

4.1 Définitions

Définition. Soient $f : A \rightarrow \mathbb{K}$ une application et $n \in \mathbb{N}$. On dit que f admet un développement limité au voisinage de a à l'ordre n (ou en $o(x^n)$) si et seulement s'il existe $P \in \mathbb{K}_n[X]$ tel que $f(a+x) \underset{x \rightarrow 0}{\sim} P(x) + o(x^n)$.

Si $P(X) = \sum_{k=m}^n a_k X^k$ avec $a_m \neq 0$, alors $f(x) \sim a_m x^m$: $a_m x^m$ est la partie principale de $f(x)$ en 0.

Remarque. Pour toute la suite de ce paragraphe, on suppose que $a = 0$ (on peut toujours s'y ramener par changement de variable) et que 0 est un point d'accumulation de A .

Définition. développements limités au sens fort.

Avec les notations précédentes, on dit que f admet un développement limité au sens fort au voisinage de 0 à l'ordre n (ou en $\mathbf{O}(x^{n+1})$) si et seulement s'il existe $P \in \mathbb{K}_n[X]$ tel que $f(x) = P(x) + \mathbf{O}(x^{n+1})$. Les propriétés qui suivent sont valables pour les développements limités au sens fort ou au sens faible, mais nous ne les énoncerons que dans le cas du sens faible.

Propriété. unicité du développement limité. Avec les notations précédentes, s'il existe $(P, Q) \in \mathbb{K}_n[X]^2$ tel que $f(x) = P(x) + o(x^n) = Q(x) + o(x^n)$, alors $P = Q$.

Il faut savoir le démontrer.

Propriété. On suppose que $f(x)$ admet un $\text{DL}_n(0)$ de la forme $f(x) = P(x) + o(x^n)$.

Si f est paire, P est pair, donc P ne contient que des monômes de degrés pairs.

De même, si f est impaire, P est impair, donc P ne contient que des monômes de degrés impairs.

4.2 Opérations sur les développements limités

Propriété. Les règles de calcul établies pour les “ o ” et les “ \mathbf{O} ” permettent d'additionner, de multiplier et de composer des développements limités entre eux.

Remarque. Il est souvent pratique d'écrire un DL $\sum_{k=m}^n a_k x^k + o(x^n)$ sous sa forme normalisée $a_m x^m (1 + \dots + o(x^{n-m}))$.

4.3 Applications

Position de la tangente : un calcul de développement limité permet de positionner le graphe d'une application f par rapport à sa tangente en a , localement en a .

Détermination des asymptotes obliques : lorsque $f(x) \xrightarrow{x \rightarrow +\infty} \infty$, s'il existe $c_0, c_1, c_2 \in \mathbb{R}$ tels qu'en $+\infty$, $f(x) = c_0 x + c_1 + c_2 \frac{1}{x} + o(\frac{1}{x})$, alors la droite d'équation $y = c_0 x + c_1$ est asymptote au graphe de f et le signe de c_2 permet de positionner, au voisinage de $+\infty$, le graphe de f par rapport à son asymptote.

5 Applications aux séries

Théorème.

Soient $\sum a_n \in \mathcal{S}(E)$, où E est un Banach, et $\sum b_n \in \mathcal{S}(\mathbb{R})$, avec b_n de signe constant à partir d'un certain rang.

- On suppose que $\sum b_n$ est convergente.

Pour tout $n \in \mathbb{N}$, on note $R_n = \sum_{k=n+1}^{+\infty} a_k$ (en cas de convergence) et $S_n = \sum_{k=n+1}^{+\infty} b_k$.

Ce sont les **restes de Cauchy** (à l'ordre n) des séries $\sum a_n$ et $\sum b_n$.

- ◊ Si $a_n = \mathbf{O}(b_n)$ alors $\sum a_n$ converge absolument et $R_n = \mathbf{O}(S_n)$,
- ◊ Si $a_n = o(b_n)$ alors $\sum a_n$ converge absolument et $R_n = o(S_n)$,
- ◊ Si $a_n \sim b_n$ alors $\sum a_n$ converge absolument et $R_n \sim S_n$.

- On suppose que $\sum b_n$ est divergente.

Pour tout $n \in \mathbb{N}$, on note $A_n = \sum_{k=0}^n a_k$ et $B_n = \sum_{k=0}^n b_k$.

- ◇ Si $a_n = \mathbf{O}(b_n)$ alors $A_n = \mathbf{O}(B_n)$,
- ◇ Si $a_n = o(b_n)$ alors $A_n = o(B_n)$,
- ◇ Si $a_n \sim b_n$ alors $A_n \sim B_n$.

Il faut savoir le démontrer.

Exercice. Moyenne de Césaro : Soit $(a_n) \in \mathbb{C}^{\mathbb{N}}$ telle que $a_n \xrightarrow{n \rightarrow +\infty} l \in \mathbb{C}$. Alors $\frac{1}{n+1} \sum_{k=0}^n a_k \xrightarrow{n \rightarrow +\infty} l$.

Il faut savoir le démontrer.

Exercice. La série de Bertrand $\sum_{n \geq 2} \frac{1}{n^\alpha \ln^\beta n}$ converge ssi $\alpha > 1$ ou ($\alpha = 1$ et $\beta > 1$).

Il faut savoir le démontrer.

Semaine 24 (du 23 mars au 27) : Résumé de cours

1 Dérivabilité

1.1 Interprétations d'une dérivée

Définition. f est dérivable au point a si et seulement si $\frac{f(t) - f(a)}{t - a} \xrightarrow[t \neq a, t \in I]{t \rightarrow a} \ell \in E$. Dans ce cas, ℓ est appelée la dérivée de f au point a . On note $f'(a) = \left[\frac{d}{dt}(f(t)) \right]_{t=a} = \lim_{\substack{t \rightarrow a \\ t \neq a, t \in I}} \frac{f(t) - f(a)}{t - a} \in E$.

Remarque. Informellement, lorsque $E = \mathbb{R}$, la corde du graphe de f entre les abscisses x_0 et x_1 , d'équation $y - f(x_0) = \frac{f(x_1) - f(x_0)}{x_1 - x_0} \times (x - x_0)$, tend vers la tangente au graphe de f en le point de coordonnées $(x_0, f(x_0))$, d'équation $y - f(x_0) = f'(x_0) \cdot (x - x_0)$. Parmi les droites non verticales du plan, la tangente est la meilleure approximation du graphe de f au voisinage de x_0 .

interprétation cinématique : $\left\| \frac{f(t) - f(a)}{t - a} \right\|$ est la vitesse moyenne du mobile ponctuel $f(t)$ entre les instants a et t , donc $\|f'(a)\|$ représente la vitesse instantanée du mobile à l'instant a .

1.2 Dérivées à gauche et à droite

Définition. On dit que f est dérivable à droite en a si et seulement si $f|_{I \cap [a, +\infty[}$ est dérivable en a .

On note alors $f'_d(a) = \lim_{\substack{t \rightarrow a \\ t > a, t \in I}} \frac{f(t) - f(a)}{t - a}$.

Théorème. Lorsque $a \in \overset{\circ}{I}$, f est dérivable en a si et seulement si f est dérivable à droite et à gauche en a et si l'on a $f'_d(a) = f'_g(a)$. Dans ce cas, $f'(a) = f'_d(a) = f'_g(a)$.

1.3 Dérivées et développements limités

Propriété. f est dérivable en a si et seulement s'il existe $l \in E$ tel que $f(t) = f(a) + (t - a)l + \underset[t \neq a, t \in I]{t \rightarrow a} o(t - a)$. Dans ce cas $l = f'(a)$.

Propriété. Si f est dérivable en a , elle est continue en a .

Remarque. Si f est seulement dérivable à droite et à gauche en a , alors f est continue en a .

2 Opérations sur les fonctions dérivables

Propriété. Dérivation d'une application à valeurs dans un produit. Supposons que

$E = \prod_{i=1}^p E_i$, et pour tout $t \in I$, notons $f(t) = (f_1(t), \dots, f_p(t))$. f est dérivable en a si et seulement si, pour tout $i \in \mathbb{N}_p$, f_i est dérivable en a . Dans ce cas $f'(a) = (f'_1(a), \dots, f'_p(a))$.

Propriété. Supposons que E est un espace vectoriel de dimension finie muni d'une base

$e = (e_1, \dots, e_p)$. Pour tout $t \in I$, notons $f(t) = \sum_{i=1}^p f_i(t)e_i$. f est dérivable en a si et seulement si,

pour tout $i \in \mathbb{N}_p$, f_i est dérivable en a et dans ce cas $f'(a) = \sum_{i=1}^p f'_i(a)e_i$.

Cas particulier. Si f est une application de I dans \mathbb{C} , f est dérivable en a si et seulement si $Im(f)$ et $Re(f)$ sont des applications dérivables en a . Dans ce cas $f'(a) = Re(f)'(a) + iIm(f)'(a)$.

Propriété. Soient F un second \mathbb{K} -espace vectoriel normé et u une application linéaire continue de E dans F . Si f est dérivable en a , alors $u \circ f$ est dérivable en a et $(u \circ f)'(a) = u(f'(a))$.

Propriété. Lorsque $\mathbb{K} = \mathbb{C}$, si f est dérivable, alors \overline{f} est dérivable et $\overline{f}' = \overline{f'}$.

Propriété de linéarité. Soit $(\alpha, \beta) \in \mathbb{K}^2$. Si f et g sont dérivables en a , alors $\alpha f + \beta g$ est dérivable en a et $(\alpha f + \beta g)'(a) = \alpha f'(a) + \beta g'(a)$.

Définition. Soient E, F et G trois \mathbb{K} -espaces vectoriels et $B : E \times F \rightarrow G$ une application. On dit que B est bilinéaire si et seulement si, pour tout $y \in F$, $x \mapsto B(x, y)$ est linéaire et si, pour tout $x \in E$, $y \mapsto B(x, y)$ est linéaire.

Théorème de dérivation d'un produit : Soient E, F et G trois \mathbb{K} -espaces vectoriels normés et $B : E \times F \rightarrow G$ une application bilinéaire continue. Soient f une application de I dans E et g une application de I dans F . On dispose de l'application $B(f, g) : I \rightarrow G$ définie par $t \mapsto B(f(t), g(t))$. Si f et g sont dérivables en a , $B(f, g)$ est dérivable en a et $B(f, g)'(a) = B(f'(a), g(a)) + B(f(a), g'(a))$.

Il faut savoir le démontrer.

Corollaire. $\left(\prod_{i=1}^p f_i \right)'(a) = \sum_{i=1}^p \left[f'_i(a) \prod_{\substack{1 \leq j \leq p \\ j \neq i}} f_j(a) \right]$.

Dérivation des fonctions composées. Soient $\varphi : I \rightarrow J$ et $f : J \rightarrow E$ deux applications.

Si φ est dérivable en a et f en $\varphi(a)$, alors $f \circ \varphi$ est dérivable en a et $(f \circ \varphi)'(a) = \varphi'(a)f'(\varphi(a))$.

Il faut savoir le démontrer.

Corollaire. $f' = (f'_n \circ f_{n-1} \circ \dots \circ f_1) \times (f'_{n-1} \circ f_{n-2} \circ \dots \circ f_1) \times \dots \times f'_1$.

Dérivée de l'inverse.

Soit $f : I \rightarrow \mathbb{K}^*$ une application dérivable en a . Alors $\frac{1}{f}$ est dérivable en a et $\left(\frac{1}{f} \right)'(a) = -\frac{f'(a)}{f(a)^2}$.

Dérivée logarithmique. Soit $f : I \rightarrow \mathbb{K}^*$ dérivable en a .

$\frac{f'(a)}{f(a)}$ est appelée la dérivée logarithmique de f en a . Lorsque $\mathbb{K} = \mathbb{R}$, elle est égale à $(\ln |f|)'(a)$.

Propriété. Si u et v sont dérivables de I dans \mathbb{K}^* , $\frac{(uv)'}{uv} = \frac{u'}{u} + \frac{v'}{v}$, $\frac{\left(\frac{u}{v} \right)'}{\left(\frac{u}{v} \right)} = \frac{u'}{u} - \frac{v'}{v}$

$\forall n \in \mathbb{N}^* \quad \frac{(u^n)'}{u^n} = n \frac{u'}{u}$, et, si u est à valeurs dans \mathbb{R}_+^* , $\forall \alpha \in \mathbb{R} \quad \frac{(u^\alpha)'}{u^\alpha} = \alpha \frac{u'}{u}$.

3 Dérivées d'ordre supérieur

3.1 Définition

Définition. $f^{(0)} = f$, $f^{(n)}(t) = (f^{(n-1)})'(t)$.

Propriété. Pour tout $p, q \in \mathbb{N}$, f est $p + q$ fois dérivable sur I si et seulement si $f^{(p)}$ est q fois dérivable sur I , auquel cas, $f^{(p+q)} = [f^{(p)}]^{(q)}$.

Remarque. On dit que f est n fois dérivable en a si et seulement si il existe une boule ouverte B centrée en a telle que $f|_{B \cap I}$ soit $n - 1$ fois dérivable et telle que $[f|_{B \cap I}]^{(n-1)}$ soit dérivable en a .

Définition. On dit que f est de classe D^n (resp : C^n) si et seulement si $f^{(n)}$ est une application définie sur I (resp : définie et continue).

On dit que f est de classe C^∞ si et seulement si f est de classe C^n pour tout $n \in \mathbb{N}$.

3.2 Opérations sur les dérivées supérieures

Propriété de linéarité. Soit $n \in \mathbb{N}$. Si f et g sont D^n , alors pour tout $(\alpha, \beta) \in \mathbb{K}^2$, $\alpha f + \beta g$ est D^n et $[\alpha f + \beta g]^{(n)} = \alpha f^{(n)} + \beta g^{(n)}$.

Formule de Leibniz : Soient E, F et G trois \mathbb{K} -espaces vectoriels normés et $B : E \times F \rightarrow G$ une application bilinéaire continue. Soient f une application de I dans E et g une application de I dans F . On dispose de l'application $B(f, g) : I \rightarrow G$

$$t \mapsto B(f(t), g(t)).$$
 Soit $a \in I$; Si f et g sont dérivables n fois en a , $B(f, g)$ est dérivable n fois en a

et $B(f, g)^{(n)}(a) = \sum_{k=0}^n C_n^k B(f^{(k)}(a), g^{(n-k)}(a)).$

Il faut savoir le démontrer.

Corollaire. Pour tout $n \in \mathbb{N} \cup \{\infty\}$, le produit de deux applications C^n est C^n .

Théorème de composition : Soient J un intervalle de \mathbb{R} d'intérieur non vide et E un \mathbb{K} -espace vectoriel normé. Soient $\varphi : I \rightarrow J$ et $f : J \rightarrow E$ deux applications.

Soit $n \in \mathbb{N} \cup \{\infty\}$. Si φ et f sont C^n alors $f \circ \varphi$ est C^n .

4 L'égalité des accroissements finis

Dans ce paragraphe, toutes les applications utilisées sont définies sur I et sont à valeurs dans \mathbb{R} .

4.1 Extremum et point critique

Définition. f admet un maximum local en a si et seulement s'il existe un voisinage V de a tel que $\forall t \in V \cap I \quad f(t) \leq f(a)$.

f présente en a un maximum local strict si et seulement s'il existe un voisinage V de a tel que $\forall t \in V \cap I \setminus \{a\} \quad f(t) < f(a)$.

Définition. Lorsque f est dérivable en $a \in \overset{\circ}{I}$, a est un point critique de f si et seulement si $f'(a) = 0$.

Théorème. Les extremums locaux de f sur $\overset{\circ}{I}$ sont des points critiques de f . Réciproque fausse.

Il faut savoir le démontrer.

4.2 Le lemme de Rolle

Lemme de Rolle. Soient $(a, b) \in \mathbb{R}^2$ avec $a < b$ et $f : [a, b] \rightarrow \mathbb{R}$ une application continue sur $[a, b]$ et dérivable sur l'ouvert $]a, b[$. Si $f(a) = f(b)$, il existe $c \in]a, b[$ tel que $f'(c) = 0$.

Il faut savoir le démontrer.

Remarque. C'est faux pour une application à valeur dans \mathbb{C} : prendre $\begin{matrix} [0, 2\pi] & \longrightarrow & \mathbb{C} \\ \theta & \longmapsto & e^{i\theta} \end{matrix}$.

Un exercice à connaître : On dit qu'un polynôme P de $\mathbb{R}[X]$ est simplement scindé dans $\mathbb{R}[X]$ si et seulement si il se décompose sous la forme $P(x) = \lambda \prod_{i=1}^n (x - \alpha_i)$, où $\lambda \in \mathbb{R}^*$ et $\alpha_1, \dots, \alpha_n \in \mathbb{R}$ avec $i \neq j \implies \alpha_i \neq \alpha_j$. Si P est simplement scindé dans $\mathbb{R}[X]$, alors P' l'est aussi.

Théorème de Rolle généralisé (Hors programme).

Soit $(a, b) \in \mathbb{R} \cup \{-\infty, +\infty\}$ avec $a < b$. Si f est dérivable sur $]a, b[$ et si

$\lim_{x \rightarrow a} f(x) = \lim_{x \rightarrow b} f(x) \in \mathbb{R} \cup \{-\infty, +\infty\}$, alors il existe $c \in]a, b[$ tel que $f'(c) = 0$.

Il faut savoir le démontrer.

4.3 L'égalité des accroissements finis

Théorème des accroissements finis (TAF). Soit $(a, b) \in \mathbb{R}^2$ avec $a \neq b$. Soit $f : [a, b] \rightarrow \mathbb{R}$ continue sur $[a, b]$ et dérivable sur $]a, b[$. Alors il existe c dans $]a, b[$ tel que $f(b) - f(a) = (b - a)f'(c)$.

Il faut savoir le démontrer.

4.4 Théorème de la limite de la dérivée

TLD : Si f est continue sur I , dérivable (resp : de classe C^1) sur $I \setminus \{a\}$ et s'il existe $l \in \mathbb{R}$ tel que $f'(x) \xrightarrow[x \in I \setminus \{a\}]{x \rightarrow a} l$, alors f est dérivable (resp : de classe C^1) sur I , avec $f'(a) = l$.

Il faut savoir le démontrer.

Remarque. Il faut savoir montrer que, si f est continue sur I , dérivable sur $I \setminus \{a\}$ et si $f'(x) \xrightarrow[x \in I \setminus \{a\}]{x \rightarrow a} +\infty$, alors f n'est pas dérivable en a .

Remarque. Ce théorème est encore valable pour une fonction à valeurs dans un \mathbb{K} -espace vectoriel de dimension finie.

TLD : Généralisation aux dérivées d'ordre supérieur. Soient $k \in \mathbb{N} \cup \{\infty\}$. Si f est continue sur I , à valeurs dans un \mathbb{K} -espace vectoriel de dimension finie, si f est de classe C^k sur $I \setminus \{a\}$ et si, pour tout $h \in [1, k] \cap \mathbb{N}$, il existe $l_h \in \mathbb{R}$ tel que $f^{(h)}(x) \xrightarrow[x \in I \setminus \{a\}]{x \rightarrow a} l_h$, alors f est de classe C^k sur I .

5 Formules de Taylor

5.1 L'égalité de Taylor-Lagrange (hors programme)

Théorème. Soient $n \in \mathbb{N}$ et $f : [a, b] \rightarrow \mathbb{R}$. Si f est C^n sur $[a, b]$ et $n + 1$ fois dérivable sur $]a, b[$, alors il existe $c \in]a, b[$ tel que $f(b) = f(a) + \sum_{k=1}^n \frac{(b-a)^k}{k!} f^{(k)}(a) + \frac{(b-a)^{n+1}}{(n+1)!} f^{(n+1)}(c)$.

Il faut savoir le démontrer.

5.2 L'inégalité des accroissements finis (IAF)

Théorème. Inégalité des accroissements finis (IAF)

Si $f : [a, b] \rightarrow \mathbb{K}$ est C^1 sur $[a, b]$, alors $|f(b) - f(a)| \leq \lambda |b - a|$, où $\lambda = \sup_{x \in [a, b]} |f'(x)|$.

Corollaire. Soient $k \in \mathbb{R}_+$ et $f : I \rightarrow \mathbb{K}$ de classe C^1 .

Alors f est k -lipschitzienne si et seulement si pour tout $x \in [a, b]$, $|f'(x)| \leq k$.

5.3 Formules de Taylor

5.3.1 TRI et inégalité de TL

Théorème. Formule de Taylor avec reste intégral. Soient $k \in \mathbb{N}$ et $f : [a, b] \rightarrow \mathbb{K}$ C^{k+1} .

Alors $f(b) = f(a) + \sum_{h=1}^k \frac{(b-a)^h}{h!} f^{(h)}(a) + \int_a^b \frac{(b-t)^k}{k!} f^{(k+1)}(t) dt$.

Théorème. Inégalité de Taylor-Lagrange. Soient $k \in \mathbb{N}$ et $f : [a, b] \rightarrow \mathbb{K}$ C^{k+1} .

Alors $|f(b) - f(a) - \sum_{h=1}^k \frac{(b-a)^h}{h!} f^{(h)}(a)| \leq \lambda \frac{|b-a|^{k+1}}{(k+1)!}$, où $\lambda = \sup_{x \in [a, b]} |f^{(k+1)}(x)|$.

5.3.2 Primitivation d'un développement limité

Lemme. Soit $k \in \mathbb{N}$. Au voisinage de a , $\int_a^x o((t-a)^k) dt = o((x-a)^{k+1})$.

Il faut savoir le démontrer.

Théorème. Primitivation d'un développement limité. Soient $a \in I$ et $f : I \rightarrow \mathbb{K}$ une application de classe C^1 . Soit $k \in \mathbb{N}$. Si, au voisinage de a ,

$f'(x) = \sum_{h=0}^k \alpha_h (x-a)^h + o((x-a)^k)$, alors $f(x) = f(a) + \sum_{h=0}^k \frac{\alpha_h}{h+1} (x-a)^{h+1} + o((x-a)^{k+1})$.

5.3.3 Formule de TY

Formule de Taylor-Young. Si f est k fois dérivable en a , alors au voisinage de a ,

$f(x) = f(a) + \sum_{h=1}^k \frac{(x-a)^h}{h!} f^{(h)}(a) + o((x-a)^k)$.

Propriété. (Hors programme?) Soit $f : I \rightarrow \mathbb{R}$ une application deux fois dérivable en un point a de $\overset{\circ}{I}$. On suppose que $f'(a) = 0$ et que $f''(a) > 0$. Alors a est un minimum local strict : il existe un voisinage V de a tel que pour tout $t \in V \cap I \setminus \{a\}$, $f(t) > f(a)$.

6 Monotonie et dérivabilité

Ici les applications utilisées sont à valeurs dans \mathbb{R} .

6.1 Sens de variation

Théorème. f est constante si et seulement si $f' = 0$, elle est croissante si et seulement si $f' \geq 0$ et elle est décroissante si et seulement si $f' \leq 0$.

Il faut savoir le démontrer.

Propriété. Soit $f : I \rightarrow \mathbb{R}$ dérivable et croissante. Alors f est strictement croissante si et seulement si $\{x \in I / f'(x) = 0\}$ est d'intérieur vide. En particulier, si $f(x) > 0$ pour tout $x \in I$ sauf pour un nombre fini d'éléments de I , alors f est strictement croissante.

6.2 Difféomorphismes

Théorème. Supposons que f est dérivable et strictement monotone. Soit $t \in I$.

f^{-1} est dérivable en $f(t)$ si et seulement si $f'(t) \neq 0$, et dans ce cas $(f^{-1})'(f(t)) = \frac{1}{f'(t)}$.

Lorsque $[\forall t \in I, f'(t) \neq 0]$, $(f^{-1})' = \frac{1}{f' \circ f^{-1}}$.

Il faut savoir le démontrer.

Définition. Soit $n \in \mathbb{N}^*$. $f : I \rightarrow J$ est un C^n -difféomorphisme si et seulement si f est bijective, de classe C^n et si f^{-1} est aussi de classe C^n .

Propriété. f est un C^n -difféomorphisme de I dans $f(I)$ si et seulement si f est de classe C^n et si $[\forall t \in I, f'(t) \neq 0]$.

Il faut savoir le démontrer.

7 Suites récurrentes d'ordre 1

On souhaite étudier une suite (x_n) vérifiant $\forall n \in \mathbb{N} \quad x_{n+1} = f(x_n)$.

En étudiant l'application f , supposons que l'on ait déterminé un intervalle I tel que $f : I \rightarrow I$ est continue et monotone, avec $x_0 \in I$.

Représentation graphique de (x_n) : À connaître.

Propriété. Les valeurs possibles pour la limite de x_n sont les points fixes de $f|_I$ et les bornes de I qui n'appartiennent pas à I .

Propriété. Si $f|_I$ est croissante, alors (x_n) est monotone.

Plus précisément, (x_n) est croissante si et seulement si $f(x_0) - x_0 \geq 0$,

et (x_n) est décroissante si et seulement si $f(x_0) - x_0 \leq 0$.

Il faut savoir le démontrer.

Propriété. On suppose que $f|_I$ est croissante. Soit $l \in I$ un point fixe de f .

Si $x_0 \leq l$, alors $\forall n \in \mathbb{N} \quad x_n \leq l$. Si $x_0 \geq l$, alors $\forall n \in \mathbb{N} \quad x_n \geq l$.

Il faut savoir le démontrer.

Propriété. On suppose que $f|_I$ est décroissante. Alors $(f \circ f)|_I$ est croissante, donc les deux suites (x_{2n}) et (x_{2n+1}) sont monotones et de sens contraires.

Il faut savoir le démontrer.

Propriété. Soit $f : I \rightarrow I$ une application de classe C^1 et $\ell \in I$ tel que $f(\ell) = \ell$.

Si $|f'(\ell)| < 1$, alors il existe $\varepsilon \in \mathbb{R}_+^*$ tel que, pour tout $x_0 \in]\ell - \varepsilon, \ell + \varepsilon[$, $x_n \xrightarrow[n \rightarrow +\infty]{} \ell$: ℓ est un point d'équilibre stable.

Si $|f'(\ell)| > 1$, alors il existe $\varepsilon \in \mathbb{R}_+^*$ tel que, pour tout $x_0 \in]\ell - \varepsilon, \ell + \varepsilon[$, il existe $N \in \mathbb{N}$ tel que $x_N \notin]\ell - \varepsilon, \ell + \varepsilon[$: ℓ est un point d'équilibre instable.

Il faut savoir le démontrer.

Plan d'étude d'une suite vérifiant $x_{n+1} = f(x_n)$:

- ◇ Représentez le tableau des variations de f .
- ◇ Lorsque le graphe de f est simple, visualisez le comportement de la suite (x_n) .
- ◇ Trouvez un intervalle I tel que $f(I) \subset I$ et $x_0 \in I$ et f est monotone et continue sur I .
- ◇ Recherchez les "limites éventuelles".
- ◇ Si f est croissante sur I , étudiez les signes de $f(x_0) - x_0$ et de $x_0 - l$ (où l est un point fixe), puis concluez.
- ◇ Si f est décroissante sur I , se ramener au cas précédent en considérant $f \circ f$, ou bien si l'on a conjecturé que $x_n \xrightarrow{n \rightarrow +\infty} \ell$ et si $|f'(\ell)| < 1$, majorez $|x_{n+1} - \ell| = |f(x_n) - f(\ell)|$ à l'aide du TAF.

8 Fonctions convexes

8.1 Sous-espaces affines

Définition. Soient \mathcal{E} un \mathbb{K} -espace affine de direction E et \mathcal{F} une partie de \mathcal{E} .

\mathcal{F} est un **sous-espace affine** de \mathcal{E} si et seulement si il existe $A \in \mathcal{E}$ et un sous-espace vectoriel F de E tel que $\mathcal{F} = A + F = \{A + x \mid x \in F\}$. Dans ce cas, $F = \{\overrightarrow{MN} \mid M, N \in \mathcal{F}\}$: on dit que F est la direction du sous-espace affine \mathcal{F} . De plus, pour tout $B \in \mathcal{F}$, $\mathcal{F} = B + F$.

Exemples. Un singleton est un sous-espace affine dirigé par $\{0\}$.

Une droite affine de \mathcal{E} est de la forme $\mathcal{D} = A + \mathbb{K}x$, où $A \in \mathcal{E}$ et $x \in E \setminus \{0\}$.

Propriété. Soit E et F deux \mathbb{K} -espaces vectoriels et $f \in L(E, F)$. Soit $y \in F$. L'ensemble des solutions de l'équation linéaire $(E) : f(x) = y$ en l'inconnue $x \in E$, est ou bien vide, ou bien un sous-espace affine de E .

Définition. Deux sous-espaces affines sont parallèles si et seulement si ils ont la même direction.

Propriété. Soient \mathcal{E} un \mathbb{K} -espace affine de direction E et $(\mathcal{E}_i)_{i \in I}$ une famille de sous-espaces affines de \mathcal{E} . Pour $i \in I$, on note E_i la direction de \mathcal{E}_i .

$\bigcap_{i \in I} \mathcal{E}_i$ est ou bien \emptyset , ou bien un sous-espace affine de \mathcal{E} de direction $\bigcap_{i \in I} E_i$.

Définition. Soit \mathcal{E} un \mathbb{K} -espace affine de direction E . Un repère de \mathcal{E} est un couple $R = (O, b)$, où O est un point de \mathcal{E} , appelé l'origine du repère et où b est une base de E . Si $M \in \mathcal{E}$, les coordonnées de M dans le repère R sont les coordonnées du vecteur \overrightarrow{OM} dans la base b .

Définition. Si \mathcal{F} est un sous-espace affine de direction F , $\dim(\mathcal{F}) = \dim(F)$.

8.2 Barycentres et convexité

Notation. On fixe un espace affine \mathcal{E} , p points A_1, \dots, A_p de \mathcal{E} et p scalaires $\lambda_1, \dots, \lambda_p$ dans \mathbb{K} .

Définition. On appelle fonction vectorielle de Leibniz l'application $\varphi : \mathcal{E} \rightarrow E$ définie par $\varphi(M) = \sum_{i=1}^p \lambda_i \overrightarrow{A_i M}$.

Définition. Lorsque $\sum_{i=1}^p \lambda_i = 0$, φ est constante, et lorsque $\sum_{i=1}^p \lambda_i \neq 0$, φ est bijective. L'unique point

G tel que $\varphi(G) = 0$ s'appelle alors le barycentre des $(A_i, \lambda_i)_{1 \leq i \leq p}$. On a donc $\sum_{i=1}^p \lambda_i \overrightarrow{GA_i} = 0$.

On en déduit que, pour tout $M \in \mathcal{E}$, $\overrightarrow{MG} = \frac{1}{\sum_{i=1}^p \lambda_i} \sum_{i=1}^p \lambda_i \overrightarrow{MA_i}$. On note $G \triangleq \frac{\lambda_1 A_1 + \dots + \lambda_p A_p}{\lambda_1 + \dots + \lambda_p}$.

Définition. Lorsque, pour tout $i \in \mathbb{N}_p$, $\lambda_i = 1$, G s'appelle l'isobarycentre des points A_1, \dots, A_p .

Propriété. Homogénéité du barycentre :

Si l'on remplace chaque λ_i par $\alpha \lambda_i$ où $\alpha \in \mathbb{K} \setminus \{0\}$, G n'est pas modifié.

Propriété. Associativité du barycentre : Soit $k \in \mathbb{N}_p$. Notons G' le barycentre des $(A_i, \lambda_i)_{1 \leq i \leq k}$

(on suppose que $\lambda' = \sum_{i=1}^k \lambda_i \neq 0$) et G'' le barycentre des $(A_i, \lambda_i)_{k+1 \leq i \leq p}$ (on suppose que

$\lambda'' = \sum_{i=k+1}^p \lambda_i \neq 0$). Alors G est le barycentre de $((G', \lambda'), (G'', \lambda''))$.

Il faut savoir le démontrer.

Propriété. Soit \mathcal{F} un sous-espace affine de \mathcal{E} . Si pour tout $i \in \mathbb{N}_p$, $A_i \in \mathcal{F}$, alors $G \in \mathcal{F}$.

Exemple. Si A et B sont deux points distincts de \mathcal{E} , la droite (AB) est égale à l'ensemble des barycentres de A et B .

Si A, B et C sont trois points non alignés de \mathcal{E} , l'ensemble des barycentres de A, B et C est l'unique plan affine contenant ces trois points.

Définition. On suppose que $\mathbb{K} = \mathbb{R}$.

Une partie \mathcal{C} de \mathcal{E} est convexe si et seulement si elle vérifie l'une des propriétés équivalentes suivantes :

1. Pour tout $(A_1, A_2) \in \mathcal{C}^2$, $[A_1, A_2] \subset \mathcal{C}$, où $[A_1, A_2]$ est le segment d'extrémités A_1 et A_2 , c'est-à-dire l'ensemble des barycentres de $((A_1, t), (A_2, 1-t))$, lorsque t décrit $[0, 1]$.
2. Pour tout $(A_1, A_2) \in \mathcal{C}^2$, pour tout $(\lambda_1, \lambda_2) \in \mathbb{R}_+^2 \setminus \{0\}$, le barycentre de $((A_1, \lambda_1), (A_2, \lambda_2))$ est dans \mathcal{C} .
3. Pour tout $p \in \mathbb{N}^*$, pour tout $(A_i)_{1 \leq i \leq p} \in \mathcal{C}^p$, pour tout $(\lambda_i)_{1 \leq i \leq p} \in \mathbb{R}_+^p \setminus \{0\}$, le barycentre de $(A_i, \lambda_i)_{1 \leq i \leq p}$ est dans \mathcal{C} .

Une partie est donc convexe ssi elle est stable par pour des barycentres pondérés positivement.

Exemple. Les sous-espaces affines sont des convexes.

Propriété. Une intersection de parties convexes est convexe.

Définition. Soit B une partie de \mathcal{E} . L'enveloppe convexe de B est le plus petit convexe de \mathcal{E} contenant B . C'est l'ensemble des barycentres d'un nombre fini de points de B affectés de pondérations positives.

8.3 Inégalités de convexité

Notation. On fixe une application $f : I \rightarrow \mathbb{R}$, où I est un intervalle de \mathbb{R} d'intérieur non vide.

Définition. f est convexe si et seulement si

$$\forall (x, y) \in I^2 \quad \forall \alpha \in [0, 1] \quad f(\alpha x + (1 - \alpha)y) \leq \alpha f(x) + (1 - \alpha)f(y).$$

f est concave si et seulement si $-f$ est convexe.

Interprétation géométrique. f est convexe si et seulement si, pour tout $x, y \in I$ avec $x < y$, le graphe de $f|_{[x, y]}$ est au dessous de la corde joignant les points $(x, f(x))$ et $(y, f(y))$.

Il faut savoir le démontrer.

Remarque. On peut également définir la stricte convexité et la stricte concavité, en remplaçant l'inégalité large par une inégalité stricte lorsque $\alpha \in]0, 1[$.

Propriété. f est concave et convexe si et seulement si elle est affine, i.e de la forme $x \mapsto \alpha x + \beta$.

Propriété. Une somme d'un nombre fini d'applications convexes est convexe.

Définition. $x_0 \in \overset{\circ}{I}$ est un point d'inflexion de f si et seulement si il existe $\varepsilon > 0$ tel que $f|_{I \cap]x_0 - \varepsilon, x_0]}$ est convexe (resp : concave) et $f|_{I \cap]x_0, x_0 + \varepsilon]}$ est concave (resp : convexe).

Propriété. L'épigraphe de f est $\{(x, y) \in \mathbb{R}^2 / x \in I \text{ et } y \geq f(x)\}$.
 f est convexe si et seulement si son épigraphe est une partie convexe de \mathbb{R}^2 .

Propriété. Inégalité de Jensen. f est convexe si et seulement si

$$\forall n \in \mathbb{N}^* \quad \forall (x_1, \dots, x_n) \in I^n \quad \forall (\lambda_1, \dots, \lambda_n) \in \mathbb{R}_+^n, \sum_{i=1}^n \lambda_i = 1 \implies f\left(\sum_{i=1}^n \lambda_i x_i\right) \leq \sum_{i=1}^n \lambda_i f(x_i).$$

Il faut savoir le démontrer.

Exercice. Si $(x_1, \dots, x_n) \in \mathbb{R}_+^n$, la moyenne géométrique $\prod_{i=1}^n x_i^{\frac{1}{n}}$ est inférieure à la moyenne arithmétique $\frac{1}{n} \sum_{i=1}^n x_i$.

Il faut savoir le démontrer.

8.4 Croissance des pentes

Propriété. Lorsque $x, y \in I$ avec $x \neq y$, on pose $p_x(y) = \frac{f(x) - f(y)}{x - y} = p_y(x)$: c'est la pente de la corde d'extrémités $(x, f(x))$ et $(y, f(y))$. Les propriétés suivantes sont équivalentes :

1. f est convexe sur I .
2. Pour tout $a, b, c \in I$ avec $a < b < c$, $p_a(b) \leq p_a(c)$.
3. Pour tout $a, b, c \in I$ avec $a < b < c$, $p_b(a) \leq p_b(c)$.
4. Pour tout $a, b, c \in I$ avec $a < b < c$, $p_c(a) \leq p_c(b)$.

Ainsi, f est convexe si et seulement si pour tout $x_0 \in I$ l'application p_{x_0} est croissante sur $I \setminus \{x_0\}$.

Il faut savoir le démontrer.

Propriété. (Hors programme) Si f est convexe sur I , elle est dérivable à droite et à gauche en tout point de $\overset{\circ}{I}$. En particulier, elle est continue sur $\overset{\circ}{I}$.

Il faut savoir le démontrer.

8.5 Fonctions convexes dérivables

Propriété. Si f est dérivable, alors f est convexe si et seulement si f' est croissante.

Il faut savoir le démontrer.

Propriété. Si f est dérivable, f est convexe si et seulement si son graphe est au dessus de ses tangentes.

Il faut savoir le démontrer.

Propriété. Si f est deux fois dérivable sur I , f est convexe si et seulement si $\forall x \in I \quad f''(x) \geq 0$.

Propriété. On suppose que f est deux fois dérivable sur $\overset{\circ}{I}$ et que $x_0 \in \overset{\circ}{I}$.

Si f'' change de signe au voisinage de x_0 , alors x_0 est un point d'inflexion de f .

Semaine 25 (du 30 mars au 3 avril) : Résumé de cours

1 L'algèbre des polynômes

1.1 Le groupe des polynômes

Notation. A désigne un anneau quelconque.

Définition. On note $A[X] \triangleq A^{(\mathbb{N})}$: c'est l'ensemble des suites presque nulles.

Si $P = (a_k) \in A[X]$, on convient de noter $P = \sum_{k \in \mathbb{N}} a_k X^k$.

Remarque. Par définition, deux polynômes sont égaux si et seulement si ils ont les mêmes coefficients.

Propriété. Si $P(X) = \sum_{k \in \mathbb{N}} a_k X^k$ et $Q(X) = \sum_{k \in \mathbb{N}} b_k X^k$, alors $P + Q = \sum_{k \in \mathbb{N}} (a_k + b_k) X^k$.

$(A[X], +)$ est un sous-groupe commutatif de $A^{\mathbb{N}}$ dont le neutre est le polynôme identiquement nul.

Définition. Si $P(X) = (a_k)_{k \in \mathbb{N}} \in A[X] \setminus \{0\}$, $\deg(P) = \max(\{k \in \mathbb{N} / a_k \neq 0\})$.
On convient que $\deg(0) = -\infty$.

Définition. Soit $P(X) = \sum_{k \in \mathbb{N}} a_k X^k \in A[X]$ un polynôme de degré $n \in \mathbb{N}$.

- a_k est le coefficient de P de degré k .
- a_0 est aussi appelé le coefficient constant du polynôme P .
- a_n est appelé le coefficient de plus haut degré de P , ou bien son coefficient dominant.
- On dit que P est unitaire (ou normalisé) si et seulement si $a_n = 1$.
- Le polynôme $a_k X^k$ est appelé un monôme.

Notation. Pour tout $n \in \mathbb{N}$, on note $A_n[X] = \{P \in A[X] / \deg(P) \leq n\}$. Ainsi, $A[X] = \bigcup_{n \in \mathbb{N}} A_n[X]$.

Propriété. $\deg(P + Q) \leq \sup(\deg(P), \deg(Q))$, avec égalité lorsque $\deg(P) \neq \deg(Q)$.

1.2 Produits de polynômes

Définition. $\left(\sum_{n \in \mathbb{N}} a_n X^n\right) \times \left(\sum_{n \in \mathbb{N}} b_n X^n\right) \triangleq \sum_{n \in \mathbb{N}} \left(\sum_{k=0}^n a_k b_{n-k}\right) X^n$.

Propriété. Pour tout $P, Q \in A[X]$, PQ est aussi un élément de $A[X]$.

Il faut savoir le démontrer.

Propriété. $(A[X], +, \times)$ est un anneau, avec $1_{A[X]} = (\delta_{k,0} 1_A)_{k \in \mathbb{N}}$.

Remarque. $\left(\sum_{n \in \mathbb{N}} a_n X^n\right) \times \left(\sum_{n \in \mathbb{N}} b_n X^n\right) \times \left(\sum_{n \in \mathbb{N}} c_n X^n\right) = \sum_{n \in \mathbb{N}} \left(\sum_{\substack{(i,j,k) \in \mathbb{N}^3 \\ i+j+k=n}} a_i b_j c_k\right) X^n$.

Propriété. L'application $i : A \longrightarrow A[X]$ est un morphisme injectif d'anneaux. On identifie A avec une partie de $A[X]$ en convenant que, pour tout $a \in A$, $a = i(a)$. Alors $A_0[X] = A$.

Remarque. Lorsque $b \in A$ et $P \in A[X]$, on dispose donc du produit bP .

Si $P = \sum_{k \in \mathbb{N}} a_k X^k$, on vérifie que $bP = \sum_{k \in \mathbb{N}} ba_k X^k$.

Propriété. $A[X]$ est commutatif intègre si et seulement si A est commutatif intègre.

Il faut savoir le démontrer.

Pour toute la suite de ce chapitre, on supposera que A est commutatif intègre.

Propriété. Pour tout $P, Q \in A[X]$, $\deg(PQ) = \deg(P) + \deg(Q)$.

Propriété. $U(A[X]) = U(A)$.

Il faut savoir le démontrer.

Définition. L'indéterminée X est le polynôme $(1_A \delta_{k,1})_{k \in \mathbb{N}}$. On a $X^n = (1_A \delta_{k,n})_{k \in \mathbb{N}}$.

Définition. (hors programme :) A est commutatif intègre, donc $A[X]$ est commutatif intègre, puis $(A[X])[Y]$ est aussi un anneau commutatif intègre. Ce dernier ensemble est l'anneau des polynômes à deux indéterminées à coefficients dans A . On le note plutôt $A[X, Y]$. Il est isomorphe à $A^{(\mathbb{N}^2)}$, en convenant que $(a_{h,k})_{(h,k) \in \mathbb{N}^2} = \sum_{\substack{0 \leq h \leq m \\ 0 \leq k \leq n}} a_{h,k} X^h Y^k$. Dans ces conditions, $X = (\delta_{h,1} \delta_{k,0})_{(h,k) \in \mathbb{N}^2}$ et $Y = (\delta_{h,0} \delta_{k,1})_{(h,k) \in \mathbb{N}^2}$.

On peut vérifier que, pour tout $p, q \in \mathbb{N}^2$, $X^p Y^q = (\delta_{h,p} \delta_{k,q})_{(h,k) \in \mathbb{N}^2}$.

En généralisant, on peut définir $A[X_1, \dots, X_p]$, l'anneau des polynômes à p indéterminées.

1.3 Applications polynomiales

Définition. Soit $P = \sum_{k \in \mathbb{N}} a_k X^k \in A[X]$ un polynôme. L'application polynomiale associée à P est

l'application $\tilde{P} : A \longrightarrow A$
 $x \longmapsto \sum_{k \in \mathbb{N}} a_k x^k$.

Propriété. L'application $\varphi : A[X] \longrightarrow \mathcal{F}(A, A)$
 $P \longmapsto \tilde{P}$ est un morphisme d'anneaux.

Notation. $Im(\varphi)$ est un sous-anneau de $\mathcal{F}(A, A)$. C'est l'anneau des applications polynomiales.

Théorème. Lorsque A est un corps, φ est injectif si et seulement si A est de cardinal infini.

Algorithme d'Hörner : Soit $P = \sum_{k \in \mathbb{N}} a_k X^k \in A[X]$ et $x \in A$. On peut disposer le calcul de $\tilde{P}(x)$ de

la manière suivante : $\tilde{P}(x) = (\dots((a_n x + a_{n-1})x + a_{n-2}x) + \dots + a_1)x + a_0$. Cet algorithme permet de calculer $\tilde{P}(x)$ avec n multiplications et n additions.

1.4 Composition de polynômes

Définition. Si $P = \sum_{k=0}^n a_k X^k \in A[X]$ et $Q \in A[X]$, $P \circ Q = \sum_{k=0}^n a_k Q^k = P(Q)$.

Propriété. Pour tout $P, Q, R \in A[X]$,

- $(P + Q) \circ R = P \circ R + Q \circ R$,
- $(PQ) \circ R = (P \circ R) \times (Q \circ R)$,
- $(P \circ Q) \circ R = P \circ (Q \circ R)$.

Propriété. Soit $P, Q \in A[X]$ Si $\deg(Q) \geq 1$, alors $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

Il faut savoir le démontrer.

Propriété. Pour tout $P, Q \in A[X]$, $\widetilde{P \circ Q} = \tilde{P} \circ \tilde{Q}$.

1.5 Dérivation formelle

Définition. Si $P = \sum_{k \in \mathbb{N}} a_k X^k \in A[X]$, on pose $P' \triangleq \sum_{k \in \mathbb{N}^*} k a_k X^{k-1} = \sum_{k \in \mathbb{N}} (k+1) a_{k+1} X^k$.

Remarque. On peut écrire $P' = \sum_{k \in \mathbb{N}} k a_k X^{k+1}$, si l'on convient que $0X^{-1} = 0$.

Définition. Si $P = \sum_{k \in \mathbb{N}} a_k X^k$, $P^{(0)} = P$ et

$$\text{pour tout } n \in \mathbb{N}, P^{(n)} = \sum_{k \geq n} \frac{k!}{(k-n)!} a_k X^{k-n} = \sum_{k \in \mathbb{N}} \frac{(k+n)!}{k!} a_{k+n} X^k.$$

Propriété. Pour tout $P \in \mathbb{R}[X]$ et $n \in \mathbb{N}$, $\widetilde{P^{(n)}} = \tilde{P}^{(n)}$.

Propriété. Pour tout $P \in A[X]$, $\deg(P') \leq \deg(P) - 1$.

Propriété. Pour tout $P \in A[X] \setminus \{0\}$, $P^{(\deg(P)+1)} = 0$.

Propriété. Soit $P, Q \in A[X]$, $a \in A$ et $n \in \mathbb{N}$.

- $(P + Q)' = P' + Q'$, et plus généralement, $(P + Q)^{(n)} = P^{(n)} + Q^{(n)}$.
- $(aP)' = aP'$, et plus généralement, $(aP)^{(n)} = aP^{(n)}$.
- $(PQ)' = P'Q + PQ'$

Propriété. Pour tout $n \in \mathbb{N}$ et $P_1, \dots, P_n \in A[X]$, $(P_1 \times \dots \times P_n)' = \sum_{i=1}^n P_i' \prod_{j \neq i} P_j$.

Formule de Leibniz : $(PQ)^{(n)} = \sum_{k=0}^n \binom{n}{k} P^{(k)} Q^{(n-k)}$.

Propriété. Pour tout $P, Q \in A[X]$, $(P \circ Q)' = Q' \times (P' \circ Q)$.

1.6 La structure d'algèbre de $\mathbb{K}[X]$.

Pour la suite de ce chapitre, \mathbb{K} désigne un corps.

Propriété. $\mathbb{K}[X]$ est une \mathbb{K} -algèbre.

Propriété. Pour tout $n \in \mathbb{N}$,

$\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$ de dimension finie égale à $n + 1$.

1.7 Division euclidienne entre polynômes

Théorème. Soit $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Alors il existe un unique couple $(P, Q) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$ avec $\deg(R) < \deg(B)$: Q est le quotient de la division euclidienne du dividende A par le diviseur B et que R en est le reste.

Il faut savoir le démontrer.

Définition. Soit $A \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. a est une racine de A si et seulement si $\tilde{A}(a) = 0$.

Propriété. Soit $A \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Le reste de la division euclidienne de A par $X - a$ est égal au polynôme constant $\tilde{A}(a)$.

Il faut savoir le démontrer.

Corollaire. a est racine de A si et seulement si il existe $Q \in \mathbb{K}[X]$ tel que $A = (X - a)Q$.

Propriété. Supposons que \mathbb{L} est un sous-corps de \mathbb{K} . Alors, pour tout $(A, B) \in \mathbb{L}[X] \times (\mathbb{L}[X] \setminus \{0\})$, les quotient et reste de la division euclidienne sont les mêmes que l'on regarde A et B comme des polynômes de $\mathbb{L}[X]$ ou de $\mathbb{K}[X]$.

2 Arithmétique

2.1 Divisibilité

Définition. Soient A un anneau commutatif et $(a, b) \in A^2$. $a|b$ si et seulement si $\exists m \in A$ $b = ma$. On dit alors que a est un **diviseur** de b et que b est un **multiple** de a .

Remarque. $0|a \iff a = 0$ et, pour tout $a \in A$, $a|0$.

Propriété. Soit $P, Q \in \mathbb{K}[X]$ tels que $P | Q$ et $Q \neq 0$. Alors $\deg(Q) \geq \deg(P)$.

Propriété. Soit $P, Q \in \mathbb{K}[X]$ avec $Q \neq 0$. $P | Q$ si et seulement si le reste de la division euclidienne de P par Q est nul.

Propriété. Soit \mathbb{L} un sous-corps d'un corps \mathbb{K} . Soit $P, Q \in \mathbb{L}[X]$. Alors $P | Q$ dans $\mathbb{L}[X]$ si et seulement si $P | Q$ dans $\mathbb{K}[X]$.

Il faut savoir le démontrer.

Propriété. Soient A un anneau commutatif et $a, b, c, d \in A$.

- Si $b | a$ et $b | c$, alors $b | (a + c)$.
- Si $b | a$ et $d | c$, alors $bd | ac$.
- si $b | a$, pour tout $p \in \mathbb{N}$, $b^p | a^p$.

Propriété. Soient A un anneau commutatif et $b, a_1, \dots, a_p, c_1, \dots, c_p \in A$.

Si pour tout $i \in \{1, \dots, p\}$, $b | a_i$, alors $b | \sum_{i=1}^p c_i a_i$.

Propriété. Soient A un anneau commutatif et $(a, b) \in A^2$. $a|b \iff bA \subseteq aA$.

Propriété. Soit A un anneau commutatif. La relation de divisibilité est réflexive et transitive.

Définition. Soient A un anneau commutatif et $(a, b) \in A^2$.

a et b sont **associés** si et seulement si $a|b$ et $b|a$.

La relation “être associé à” est une relation d'équivalence, on la notera “ \sim ”.

Propriété. Dans un anneau commutatif, si $a \sim b$ et $c \sim d$, alors $ac \sim bd$.

Hypothèse : Jusqu'à la fin de ce paragraphe, on suppose que A est intègre et commutatif.

Propriété. Soit $a, b \in A$. a et b sont associés si et seulement s'il existe $\lambda \in U(A)$ tel que $a = \lambda b$.

Il faut savoir le démontrer.

Exemple. Dans \mathbb{Z} , n et m sont associés si et seulement si $|n| = |m|$.

Dans $\mathbb{K}[X]$, P et Q sont associés si et seulement s'il existe $\lambda \in \mathbb{K}^*$ tel que $Q = \lambda P$.

Propriété. La relation de divisibilité est une relation d'ordre sur \mathbb{N} .

La relation de divisibilité est une relation d'ordre sur l'ensemble des polynômes unitaires de $\mathbb{K}[X]$.

Définition. Soit $p \in A$. p est irréductible dans A si et seulement si $p \notin U(A)$ et si, pour tout $a, b \in A$, $p = ab \implies (a \in U(A)) \vee (b \in U(A))$.

Ainsi p est irréductible dans A si et seulement si p n'est pas inversible et a pour seuls diviseurs les éléments associés à 1 ou à p .

Semaine 26 (du 20 avril au 24) : Résumé de cours

1 Arithmétique

1.1 Divisibilité (suite)

Remarque. Si p est irréductible, il est non nul.

Propriété. Les éléments irréductibles de \mathbb{Z} sont les nombres premiers et leurs opposés.

Exemple. Dans $\mathbb{K}[X]$ (où \mathbb{K} est un corps), un polynôme P est irréductible si et seulement si il est de degré supérieur ou égal à 1 et si, pour tout $A, B \in \mathbb{K}[X]$, $P = AB \implies (\deg(A) = 0) \vee (\deg(B) = 0)$.

Remarque. Dans $\mathbb{K}[X]$:

- tout polynôme de degré 1 est irréductible ;
- tout polynôme de degré ≥ 2 possédant une racine dans \mathbb{K} est réductible ;
- tout polynôme de degré 2 ou 3 sans racine dans \mathbb{K} est irréductible.

Il faut savoir le démontrer.

Définition. Soit $a, b \in A$. On dit que a et b sont premiers entre eux (ou étrangers) si et seulement si les seuls diviseurs communs de a et b sont les éléments inversibles.

Définition. Soit $n \in \mathbb{N}$ avec $n \geq 2$ et $a_1, \dots, a_n \in A$.

- a_1, \dots, a_n sont deux à deux premiers entre eux si et seulement si, pour tout $i, j \in \{1, \dots, n\}$ avec $i \neq j$, a_i et a_j sont premiers entre eux.
- a_1, \dots, a_n sont globalement premiers entre eux si et seulement si les seuls diviseurs communs de a_1, \dots, a_n sont les éléments inversibles de A .

Propriété. Soit $p \in A$ un élément irréductible et $a \in A : p|a$, ou bien p et a sont premiers entre eux.

Il faut savoir le démontrer.

1.2 PGCD

Théorème. Si \mathbb{K} est un corps, alors $\mathbb{K}[X]$ est un anneau principal.

Il faut savoir le démontrer.

Remarque. Soit A un anneau commutatif intègre. On dit qu'il est euclidien (hors programme) si et seulement si il existe $v : A \setminus \{0\} \rightarrow \mathbb{N}$ tel que, pour tout $(a, b) \in A \times (A \setminus \{0\})$, il existe $q, r \in A$ vérifiant $a = bq + r$ et $(r = 0) \vee (v(r) < v(b))$.

On peut montrer que si A est euclidien, alors A est principal. La réciproque est fausse (admis).

Notation. Jusqu'à la fin de ce chapitre "arithmétique", on fixe un anneau A que l'on suppose principal.

Remarque. On peut montrer que $\mathbb{Z}[i] = \{n + mi / (n, m) \in \mathbb{Z}^2\}$ est un anneau principal. C'est l'anneau des entiers de Gauss.

Définition. Soit $(a, b) \in A^2$. d est un PGCD de a et b si et seulement si $aA + bA = dA$.

Caractérisation du PGCD par divisibilité : d est un PGCD de $(a, b) \in A^2$ si et seulement si d est un diviseur commun de a et b et si, pour tout diviseur commun d' de a et b , d' divise d .

Il faut savoir le démontrer.

Propriété. a et b sont premiers entre eux si et seulement si 1 est un PGCD de a et b .

Définition. Plus généralement, si $k \in \mathbb{N}^*$ et si $a_1, \dots, a_k \in A$, on dit que d est un PGCD de a_1, \dots, a_k si et seulement si $dA = a_1A + \dots + a_kA$, i.e si et seulement si d est un commun diviseur de a_1, \dots, a_k tel que si d' est un autre commun diviseur de a_1, \dots, a_k , alors d' divise d .

Soit B une partie quelconque de A . d est un PGCD de B si et seulement si $dA = Id(B)$, i.e si et seulement si d est un diviseur commun des éléments de B tel que si d' est un autre diviseur commun des éléments de B , alors d' divise d .

Propriété. Lorsque $A = \mathbb{Z}$ (resp : $A = \mathbb{K}[X]$), en imposant au PGCD d'être positif (resp : unitaire) il est unique. On le note alors $a \wedge b$.

Propriété. Soit $k \in \mathbb{N}$, $a_1, \dots, a_k \in A$ et $h \in \{1, \dots, k\}$.

Alors, en convenant de noter $a \sim b$ lorsque a et b sont associés,

- Commutativité du PGCD :
pour tout $\sigma \in \mathcal{S}_k$, $PGCD(a_1, \dots, a_k) \sim PGCD(a_{\sigma(1)}, \dots, a_{\sigma(k)})$.
- Associativité du PGCD :
 $PGCD(a_1, \dots, a_k) \sim PGCD(PGCD(a_1, \dots, a_h), PGCD(a_{h+1}, \dots, a_k))$.
- Distributivité de la multiplication par rapport au PGCD : pour tout $\alpha \in A$,
 $PGCD(\alpha a_1, \dots, \alpha a_k) \sim \alpha PGCD(a_1, \dots, a_k)$.

Il faut savoir le démontrer.

1.3 PPCM

Définition. Soit $(a, b) \in A^2$. m est un PPCM de a et b si et seulement si $aA \cap bA = mA$.

Caractérisation du PPCM par divisibilité : m est un PPCM de $(a, b) \in A^2$ si et seulement si m est un multiple commun de a et b et si, pour tout multiple commun m' de a et b , m' est un multiple de m .

Définition. Plus généralement, si $k \in \mathbb{N}^*$ et si $a_1, \dots, a_k \in A$, m est un PPCM de a_1, \dots, a_k si et seulement si $mA = a_1A \cap \dots \cap a_kA$, i.e si et seulement si m est un commun multiple de a_1, \dots, a_k tel que si m' est un autre commun multiple de a_1, \dots, a_k , alors m' est un multiple de m .

Soit B est une partie quelconque de A . m est un PPCM de B si et seulement si $mA = \bigcap_{b \in B} bA$, i.e

si et seulement si m est un multiple commun des éléments de B tel que si m' est un autre multiple commun des éléments de B , alors m' est un multiple commun de m .

Remarque. Dans ce contexte, on convient que si $B = \emptyset$, $\bigcap_{b \in B} bA = A$, donc 1_A est un PPCM de \emptyset .

Propriété. Soit $k \in \mathbb{N}$, $a_1, \dots, a_k \in A$ et $h \in \{1, \dots, k\}$.

Alors, en convenant de noter $a \sim b$ lorsque a et b sont associés,

- Commutativité du PPCM :
pour tout $\sigma \in \mathcal{S}_k$, $PPCM(a_1, \dots, a_k) \sim PPCM(a_{\sigma(1)}, \dots, a_{\sigma(k)})$.
- Associativité du PPCM :
 $PPCM(a_1, \dots, a_k) \sim PPCM(PPCM(a_1, \dots, a_h), PPCM(a_{h+1}, \dots, a_k))$.
- Distributivité de la multiplication par rapport au PPCM :
pour tout $\alpha \in A$, $PPCM(\alpha a_1, \dots, \alpha a_k) \sim \alpha PPCM(a_1, \dots, a_k)$.

1.4 Les théorèmes de l'arithmétique

Théorème de Bézout. Soit $(a, b) \in A^2$.

a et b sont premiers entre eux si et seulement si : $\exists (u, v) \in A^2 \quad ua + vb = 1$.

Théorème de Bézout (généralisation). Soit $n \in \mathbb{N}$ avec $n \geq 2$ et $a_1, \dots, a_n \in A$.

a_1, \dots, a_n sont globalement premiers entre eux si et seulement si :

$\exists u_1, \dots, u_n \in A \quad , \quad u_1 a_1 + \dots + u_n a_n = 1$.

Propriété. Soit $(a, b) \in A^2$. Notons d un PGCD de a et b . Alors

il existe $(a', b') \in A^2$, avec a' et b' premiers entre eux, tel que $a = a'd$ et $b = b'd$.

Théorème de Gauss. Soit $(a, b, c) \in A^3$. Si $a|bc$ avec a et b premiers entre eux, alors $a|c$.

Corollaire. Soit $p, a, b \in A$. Si $p | ab$ avec p irréductible, alors $p | a$ ou $p | b$.

Propriété. Soit $(a, b, c) \in A^3$, $n \in \mathbb{N}^*$ et $a_1, \dots, a_n \in A$.

On désigne par $a \wedge b$ un PGCD de a et b et par $a \vee b$ un PPCM de a et b .

◇ Si $a \wedge b = a \wedge c = 1$, alors $a \wedge bc = 1$.

◇ Si $a \wedge b = 1$, $\forall (k, l) \in (\mathbb{N}^*)^2 \quad a^k \wedge b^l = 1$.

◇ Si $a|b$, $c|b$ et $a \wedge c = 1$ alors $ac|b$.

Si pour tout $i \in \{1, \dots, n\}$, $a_i|b$ et si $i \neq j \implies a_i \wedge a_j = 1$, alors $a_1 \times \dots \times a_n | b$.

◇ $ab \sim (a \wedge b)(a \vee b)$. En particulier, $a \wedge b = 1 \implies a \vee b \sim ab$.

Il faut savoir le démontrer.

1.5 $\mathbb{K}[X]$ est un anneau factoriel

Notation. On suppose ici que $A \in \{\mathbb{Z}, \mathbb{K}[X]\}$ (\mathbb{K} étant un corps quelconque).

Si $A = \mathbb{Z}$, on pose $\mathcal{P} = \mathbb{P}$, et si $A = \mathbb{K}[X]$, \mathcal{P} est l'ensemble des polynômes irréductibles et unitaires.

Théorème. Soit $a \in A$ avec $a \neq 0$. Il existe un unique couple $(u, (\nu_p)_{p \in \mathcal{P}})$, où $u \in U(A)$ et où $(\nu_p)_{p \in \mathcal{P}}$ est une famille presque nulle d'entiers, tel que $a = u \prod_{p \in \mathcal{P}} p^{\nu_p}$: c'est la **décomposition de a**

en facteurs irréductibles. ν_p s'appelle la valuation p -adique de a .

Il faut savoir le démontrer.

Propriété. Soit $(a, b) \in (A \setminus \{0\})^2$, dont les décompositions en facteurs irréductibles sont

$a = u \prod_{p \in \mathcal{P}} p^{\nu_p}$ et $b = v \prod_{p \in \mathcal{P}} p^{\mu_p}$. Alors $a | b \iff [\forall p \in \mathcal{P}, \nu_p \leq \mu_p]$.

De plus, $a \wedge b = \prod_{p \in \mathcal{P}} p^{\min(\nu_p, \mu_p)}$ et $a \vee b = \prod_{p \in \mathcal{P}} p^{\max(\nu_p, \mu_p)}$. En particulier, a et b sont premiers entre

eux si et seulement si aucun élément de \mathcal{P} n'intervient à la fois dans la décomposition en facteurs irréductibles de a et dans celle de b .

Lemme d'Euclide. Soient $(a, b) \in A^2$ avec $b \neq 0$, et q, r tels que $a = bq + r$. Alors $a \wedge b = b \wedge r$.

Algorithme d'Euclide. Soit $(a_0, a_1) \in A^2$.

• Pour $i \geq 1$, tant que $a_i \neq 0$, on note a_{i+1} le reste de la division euclidienne de a_{i-1} par a_i . On définit ainsi une suite finie $(a_i)_{0 \leq i \leq N}$ d'éléments de A telle que $a_N = 0$ et, pour tout $i \in \{0, \dots, N-1\}$, $a_0 \wedge a_1 = a_i \wedge a_{i+1}$. En particulier, pour $i = N-1$, on obtient $a_0 \wedge a_1 = a_{N-1}$.

• Supposons maintenant que $a_0 \wedge a_1 = a_{N-1} = 1$. D'après le théorème de Bézout, il existe $(s, t) \in A^2$ tel que $sa_0 + ta_1 = 1$. La suite de l'algorithme d'Euclide permet le calcul d'un tel couple (s, t) : Notons q_i le quotient de la division euclidienne de a_{i-1} par a_i . Ainsi, $a_{i+1} = a_{i-1} - q_i a_i$.

En particulier, avec $i = N-2$, on obtient $1 = a_{N-3} - q_{N-2} a_{N-2}$.

Supposons que, pour un entier $i \in \{1, \dots, N-3\}$, on dispose d'entiers s_i et t_i tels que $1 = s_i a_i + t_i a_{i+1}$.

Alors $1 = s_i a_i + t_i (a_{i-1} - a_i q_i) = (s_i - t_i q_i) a_i + t_i a_{i-1}$, ce qui donne des entiers s_{i-1} et t_{i-1} tels que $1 = s_{i-1} a_{i-1} + t_{i-1} a_i$.

Par récurrence descendante, on peut donc calculer des entier s_0 et t_0 tels que $1 = s_0 a_0 + t_0 a_1$.

Corollaire. Supposons que \mathbb{L} est un sous-corps de \mathbb{K} et soit $(A, B) \in \mathbb{L}[X] \times (\mathbb{L}[X] \setminus \{0\})$. Les PGCD et PPCM de A et B sont les mêmes, que l'on regarde A et B comme des polynômes de $\mathbb{L}[X]$ ou de $\mathbb{K}[X]$.

Exercice. Soit $a, b, c \in A$ avec a et b non nuls.

Résoudre l'équation de Bézout $(B) : au + bv = c$ en l'inconnue $(u, v) \in A^2$.

Il faut savoir le démontrer.

2 Racines d'un polynôme

2.1 Identification entre polynômes formels et applications polynomiales

Notation. On fixe un corps \mathbb{K} quelconque.

Propriété. Soit $P \in \mathbb{K}[X]$ et a_1, \dots, a_k k éléments de \mathbb{K} deux à deux distincts : a_1, \dots, a_k sont toutes racines de P si et seulement si P est un multiple de $(X - a_1) \times \dots \times (X - a_k)$.

Il faut savoir le démontrer.

Corollaire. Un polynôme non nul admet au plus $\deg(P)$ racines.

Principe de rigidité des polynômes : si $P \in \mathbb{K}[X]$ possède une infinité de racines, alors $P = 0$.

Propriété. Soit $n \in \mathbb{N}$ et $P, Q \in \mathbb{K}_n[X]$.

Si $\{x \in \mathbb{K} / \tilde{P}(x) = \tilde{Q}(x)\}$ contient au moins $n + 1$ scalaires, alors $P = Q$.

Théorème. On peut identifier l'ensemble $\mathbb{K}[X]$ des polynômes formels avec l'ensemble $\mathcal{P}_{\mathbb{K}}$ des applications polynomiales de \mathbb{K} dans \mathbb{K} si et seulement si \mathbb{K} est de cardinal infini.

Remarque. Si \mathbb{K} est fini de cardinal q , alors $\prod_{a \in \mathbb{K}} (X - a) = X^q - X$.

Il faut savoir le démontrer.

Semaine 27 (du 27 avril au 1er mai) : Résumé de cours

1 Racines d'un polynôme

1.1 Polynôme d'interpolation de Lagrange

Notation. Dans tout ce paragraphe, on fixe un corps quelconque \mathbb{K} , $n \in \mathbb{N}$ et une famille $a_0, \dots, a_n \in \mathbb{K}$ de $n+1$ scalaires deux à deux distincts.

Pour tout $i \in \{0, \dots, n\}$, posons $L_i = \prod_{\substack{0 \leq j \leq n \\ j \neq i}} \frac{X - a_j}{a_i - a_j}$.

Les L_i sont appelés les polynômes de Lagrange associés à (a_0, \dots, a_n) .

Propriété. Pour tout $i, k \in \{0, \dots, n\}$, $\widetilde{L}_i(a_k) = \delta_{i,k}$.

Propriété. Pour tout $P \in \mathbb{K}_n[X]$, $P = \sum_{i=0}^n \widetilde{P}(a_i) L_i$.

Il faut savoir le démontrer.

Théorème. Soit $(b_0, b_1, \dots, b_n) \in \mathbb{K}^{n+1}$ une famille quelconque de scalaires. Il existe un unique polynôme P_0 de degré inférieur ou égal à n tel que, pour tout $i \in \{0, \dots, n\}$, $\widetilde{P}_0(a_i) = b_i$. P_0 est appelé le polynôme d'interpolation de Lagrange (associé aux deux familles (a_0, a_1, \dots, a_n) et (b_0, b_1, \dots, b_n)).

On dispose de la formule suivante : $P_0 = \sum_{i=0}^n \left(b_i \prod_{\substack{0 \leq j \leq n \\ j \neq i}} \frac{X - a_j}{a_i - a_j} \right)$. Enfin, l'ensemble des polynômes P

vérifiant, pour tout $i \in \{0, \dots, n\}$, $\widetilde{P}(a_i) = b_i$, est égal à $P_0 + \left(\prod_{i=0}^n (X - a_i) \right) \mathbb{K}[X]$.

1.2 Polynôme dérivé

Notation. Dans ce paragraphe, on suppose que \mathbb{K} est un corps de caractéristique nulle.

Propriété. Pour tout $P \in \mathbb{K}[X]$ tel que $\deg(P) \geq 1$, $\deg(P') = \deg(P) - 1$.

Corollaire. Soit $P \in \mathbb{K}[X]$. P est un polynôme constant si et seulement si $P' = 0$.

Corollaire. Si $P \in \mathbb{K}[X]$, $\deg(P) \geq n \implies \deg(P^{(n)}) = \deg(P) - n$ et $P^{(n)} = 0 \iff \deg(P) < n$.

Formule de Taylor : Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors $P = \sum_{n \in \mathbb{N}} \frac{(X - a)^n}{n! \cdot 1_{\mathbb{K}}} P^{(n)}(a)$.

Il faut savoir le démontrer.

Corollaire. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $k \in \mathbb{N}$. Alors

le reste de la division euclidienne de P par $(X - a)^k$ est égal à $\sum_{h=0}^{k-1} \frac{(X - a)^h}{h! \cdot 1_{\mathbb{K}}} P^{(h)}(a)$.

1.3 Racines multiples

Notation. \mathbb{K} désigne un corps quelconque.

Définition. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$. a est une racine de P de multiplicité m si et seulement si il existe $Q \in \mathbb{K}[X]$ tel que $P(X) = (X - a)^m Q(X)$ avec $\tilde{Q}(a) \neq 0$.

Remarque. a n'est pas racine de P si et seulement si a est racine de P de multiplicité nulle.

Définition. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$.

a est racine de P de multiplicité au moins m si et seulement si $(X - a)^m \mid P$.

Ainsi, a est racine de P de multiplicité m si et seulement si elle est racine de P de multiplicité au moins m , mais n'est pas racine de P de multiplicité au moins $m + 1$.

Définition. On dit que $a \in \mathbb{K}$ est une racine simple (resp : double, triple) de $P \in \mathbb{K}[X]$ si et seulement si a est une racine de P de multiplicité 1 (resp : 2, 3).

Définition. Soit $P \in \mathbb{K}[X] \setminus \{0\}$. Posons $\{a_1, \dots, a_k\} = \{x \in \mathbb{K} / \tilde{P}(x) = 0\}$. Pour tout $h \in \mathbb{N}_k$, notons m_h la multiplicité de a_h pour le polynôme P . On dit alors que le nombre de racines de P ,

comptées avec multiplicité, est égal à $\sum_{h=1}^k m_h$.

Et k est le nombre de racines de P comptées sans multiplicité.

Propriété. Soit $P \in \mathbb{K}[X]$, $a_1, \dots, a_k \in \mathbb{K}$ et $m_1, \dots, m_k \in \mathbb{N}$. Pour tout $h \in \{1, \dots, k\}$, a_h est racine de P de multiplicité au moins m_h si et seulement si P est un multiple de $\prod_{h=1}^k (X - a_h)^{m_h}$.

Propriété. Soit $P \in \mathbb{K}[X]$ un polynôme non nul. Le nombre de racines de P , comptées avec multiplicité est inférieur ou égal au degré de P .

Hypothèse : Pour la suite de ce paragraphe, on suppose que $\text{car}(\mathbb{K}) = 0$.

Théorème. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$. a est racine de P de multiplicité au moins m si et seulement si $\forall i \in \{0, \dots, m-1\}$, $P^{(i)}(a) = 0$.

Il faut savoir le démontrer.

Corollaire. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$. a est racine de P de multiplicité m si et seulement si $\forall i \in \{0, \dots, m-1\}$, $P^{(i)}(a) = 0$ et $P^{(m)}(a) \neq 0$.

Corollaire. Si $a \in \mathbb{K}$ est racine de $P \in \mathbb{K}[X]$ de multiplicité $m \in \mathbb{N}^*$, alors a est racine de P' de multiplicité $m - 1$.

1.4 Polynômes scindés

Notation. \mathbb{K} désigne un corps quelconque.

Définition. $P \in \mathbb{K}[X] \setminus \{0\}$ est scindé dans $\mathbb{K}[X]$ si et seulement si sa décomposition en polynômes irréductibles dans $\mathbb{K}[X]$ ne fait intervenir que des polynômes de degré 1.

Propriété. Soit $P \in \mathbb{K}[X] \setminus \{0\}$. P est scindé dans $\mathbb{K}[X]$ si et seulement si le nombre de racines de P dans \mathbb{K} , comptées avec multiplicité, est égal au degré de P .

Il faut savoir le démontrer.

Définition. Soit $P \in \mathbb{K}[X] \setminus \{0\}$. On dit que P est simplement scindé dans $\mathbb{K}[X]$ si et seulement si P est scindé dans \mathbb{K} et si toutes ses racines sont simples.

Relations de Viète entre coefficients et racines : Soit $P \in \mathbb{K}[X]$ un polynôme **scindé** dans $\mathbb{K}[X]$ de degré n , avec $n \geq 1$. Alors P peut s'écrire sous les deux formes suivantes :

- $P(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$, avec $a_0, \dots, a_n \in \mathbb{K}$ et $a_n \neq 0$;
- $P(X) = a_n (X - \beta_1) \times \dots \times (X - \beta_n)$, où β_1, \dots, β_n est la liste des racines de P , comptées avec multiplicité. Alors, pour tout $p \in \{1, \dots, n\}$,

$$\sigma_p = (-1)^p \frac{a_{n-p}}{a_n}, \text{ où } \sigma_p = \sum_{1 \leq i_1 < \dots < i_p \leq n} \beta_{i_1} \times \dots \times \beta_{i_p}.$$

Les σ_p s'appellent les fonctions symétriques élémentaires des racines. En particulier,

- Pour $p = 1$, $\sum_{i=1}^n \beta_i = -\frac{a_{n-1}}{a_n}$. Il s'agit de la somme des racines de P , comptées avec multiplicités.
- Pour $p = n$, $\prod_{i=1}^n \beta_i = (-1)^n \frac{a_0}{a_n}$. Il s'agit du produit des racines de P , comptées avec multiplicités.

La suite de ce paragraphe est hors programme.

Définition. Soit $n \in \mathbb{N}^*$ et $A \in \mathbb{K}[X_1, \dots, X_n]$ un polynôme à n indéterminées. On dit que A est symétrique si et seulement si, pour tout $\sigma \in \mathcal{S}_n$, $A(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = A(X_1, \dots, X_n)$.

Exemples. Les polynômes de Newton : $X_1^p + \dots + X_n^p$, où $n, p \in \mathbb{N}^*$ sont symétriques.

Les polynômes symétriques élémentaires : pour tout $p \in \{1, \dots, n\}$,

$$\Sigma_p(X_1, \dots, X_n) = \sum_{1 \leq i_1 < i_2 < \dots < i_p \leq n} X_{i_1} \times \dots \times X_{i_p} \text{ est bien un polynôme symétrique.}$$

Propriété. (Admise) Soit $n \in \mathbb{N}^*$. On suppose que A est un polynôme symétrique de $\mathbb{L}[X_1, \dots, X_n]$ (où \mathbb{L} est un corps). Alors il existe $B \in \mathbb{L}[\Sigma_1, \dots, \Sigma_n]$ tel que $A = B(\Sigma_1, \dots, \Sigma_n)$.

Corollaire. Avec ces notations, si \mathbb{K} est un sur-corps de \mathbb{L} et si $P \in \mathbb{L}[X]$ est scindé dans $\mathbb{K}[X]$, alors en notant β_1, \dots, β_n les racines de P comptées avec multiplicité, $A(\beta_1, \dots, \beta_n) \in \mathbb{L}$.

Exemple. Soit $P \in \mathbb{Q}[X]$ un polynôme dont les racines complexes comptées avec multiplicité sont notées β_1, \dots, β_n . Alors pour tout $p \in \mathbb{N}^*$, $\beta_1^p + \dots + \beta_n^p \in \mathbb{Q}$.

1.5 Polynômes de $\mathbb{R}[X]$ et de $\mathbb{C}[X]$

Définition. Si $P = \sum_{k \in \mathbb{N}} a_k X^k \in \mathbb{C}[X]$, on note $\bar{P} = \sum_{k \in \mathbb{N}} \bar{a}_k X^k$.

Propriété. L'application $\frac{\mathbb{C}[X]}{P} \longrightarrow \frac{\mathbb{C}[X]}{\bar{P}}$ est un isomorphisme d'anneaux.

Propriété. Soit $P \in \mathbb{C}[X]$, $\alpha \in \mathbb{C}$ et $m \in \mathbb{N}$. α est racine de P de multiplicité m si et seulement si $\bar{\alpha}$ est racine de \bar{P} de multiplicité m .

Il faut savoir le démontrer.

Corollaire. Si $P \in \mathbb{R}[X]$ et si α est racine de P (resp : racine de multiplicité m), alors $\bar{\alpha}$ est aussi une racine de P (resp : racine de multiplicité m).

Théorème de d'Alembert : Tout polynôme à coefficients complexes de degré supérieur ou égal à 1 possède au moins une racine complexe.

Corollaire. Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.

Corollaire. Dans $\mathbb{C}[X]$, deux polynômes sont premiers entre eux si et seulement si ils n'ont aucune racine complexe commune.

Corollaire. Dans $\mathbb{C}[X]$, tout polynôme non nul est scindé.

Dans $\mathbb{C}[X]$, le nombre de racines, comptées avec multiplicité, de tout polynôme non nul est égal à son degré.

Propriété. Soit $P, Q \in \mathbb{C}[X] \setminus \{0\}$. Alors $P \mid Q$ si et seulement si toute racine de P est racine de Q avec une multiplicité pour Q supérieure ou égale à celle pour P .

Propriété. Les polynômes irréductibles de $\mathbb{R}[X]$ sont exactement les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif.

Il faut savoir le démontrer.

Propriété. Soit $P \in \mathbb{R}[X] \setminus \{0\}$. P est scindé dans $\mathbb{R}[X]$ si et seulement si toutes ses racines sont réelles.

2 Le corps des fractions rationnelles

2.1 Corps des fractions d'un anneau intègre commutatif

Théorème. Soit A un anneau intègre et commutatif. Il existe un corps K , unique à un isomorphisme près, tel que A est un sous-anneau de K , et tel que tout élément de K peut s'écrire sous la forme $\frac{a}{b}$ où $(a, b) \in A^2$ avec $b \neq 0$. a est appelé le numérateur et b le dénominateur de l'écriture $\frac{a}{b}$. K est appelé le *corps des fractions* de A . C'est le plus petit corps contenant A .

2.2 Forme irréductible

Notation. \mathbb{K} désigne un corps quelconque.

Définition. On note $\mathbb{K}(X)$ le corps des fractions de l'anneau intègre $\mathbb{K}[X]$. Les éléments de $\mathbb{K}(X)$ sont appelés des fractions rationnelles en l'indéterminée X .

Définition. Soit $F \in \mathbb{K}(X)$.

$\frac{P}{Q}$ est un représentant irréductible de F si et seulement si $F = \frac{P}{Q}$ et si $P \wedge Q = 1$.

$\frac{P}{Q}$ est un représentant unitaire de F si et seulement si $F = \frac{P}{Q}$ et si S est unitaire.

Propriété. Soit $F \in \mathbb{K}(X) \setminus \{0\}$.

F possède un unique représentant irréductible et unitaire. Si on le note $\frac{P}{Q}$, alors

les représentants irréductibles de F sont les $\frac{\lambda P}{\lambda Q}$ où $\lambda \in \mathbb{K}^*$,

et les représentants quelconques de F sont les $\frac{LP}{LQ}$ où $L \in \mathbb{K}[X] \setminus \{0\}$.

Il faut savoir le démontrer.

2.3 Degré

Définition. $\deg\left(\frac{P}{Q}\right) \triangleq \deg(P) - \deg(Q) \in \mathbb{Z} \cup \{-\infty\}$.

Propriété. Soit $F, G \in \mathbb{K}(X)$.

- $\deg(F + G) \leq \max(\deg(F), \deg(G))$, avec égalité lorsque $\deg(F) \neq \deg(G)$.
- $\deg(FG) = \deg(F) + \deg(G)$.
- $\deg(FG^{-1}) = \deg(F) - \deg(G)$.

2.4 Racines et pôles

Définition. Soit $F \in \mathbb{K}(X)$ une fraction rationnelle admettant pour représentant **irréductible** $\frac{A}{B}$.

- Les racines de F sont les racines de A . Pour tout $a \in \mathbb{K}$ et $m \in \mathbb{N}$, a est une racine de F de multiplicité m si et seulement si a est racine de A de multiplicité m .
- Les pôles de F sont les racines de B . Pour tout $a \in \mathbb{K}$ et $m \in \mathbb{N}$, a est un pôle de F de multiplicité m si et seulement si a est racine de B de multiplicité m .

Définition. Si $F = \frac{P}{Q} \in \mathbb{C}[X]$, on note $\overline{F} = \frac{\overline{P}}{\overline{Q}}$.

Propriété. L'application $\begin{array}{ccc} \mathbb{C}(X) & \longrightarrow & \mathbb{C}(X) \\ P & \longmapsto & \overline{P} \end{array}$ est un isomorphisme de corps.

Propriété. Soit $F \in \mathbb{C}(X)$, $\alpha \in \mathbb{C}$ et $m \in \mathbb{N}$. α est racine (resp : pôle) de F de multiplicité m si et seulement si $\overline{\alpha}$ est racine (resp : pôle) de \overline{F} de multiplicité m .

Corollaire. Si $F \in \mathbb{R}(X)$ et si α est racine de F (resp : racine de multiplicité m), alors $\overline{\alpha}$ est aussi une racine de F (resp : racine de multiplicité m).

2.4.1 Fonctions rationnelles

Définition. Soit $F \in \mathbb{K}(X)$ une fraction rationnelle admettant pour représentant **irréductible** $\frac{A}{B}$.

Notons \mathcal{P} l'ensemble de ses pôles.

La fonction rationnelle associée à F est l'application

$$\begin{array}{ccc} \tilde{F} : \mathbb{K} \setminus \mathcal{P} & \longrightarrow & \mathbb{K} \\ x & \longmapsto & \frac{\tilde{A}(x)}{\tilde{B}(x)} \end{array}$$

Propriété. Si deux fractions rationnelles coïncident pour une infinité de valeurs de \mathbb{K} , elles sont égales.

Il faut savoir le démontrer.

2.5 Composition

Définition. Si $P = \sum_{n \in \mathbb{N}} a_n X^n \in \mathbb{K}[X]$ et $F \in \mathbb{K}(X)$, $P \circ F = P(F) \triangleq \sum_{n \in \mathbb{N}} a_n F^n$.

Propriété. Pour tout $F \in \mathbb{K}(X)$, l'application $P \mapsto P(F)$ est un morphisme d'anneaux de $\mathbb{K}[X]$ dans $\mathbb{K}(X)$.

Lemme : Soit $P \in \mathbb{K}[X]$ et $F \in \mathbb{K}(X)$. Si $P \neq 0$ et si $F \notin \mathbb{K}$, alors $P \circ F \neq 0$.

Définition. Soit $F \in \mathbb{K}(X)$ et $G \in \mathbb{K}(X) \setminus \mathbb{K}$.

Si $F = \frac{P}{Q}$, alors on pose $F \circ G = F(G) = \frac{P(G)}{Q(G)}$.

Propriété. Pour tout $G \in \mathbb{K}(X) \setminus \mathbb{K}$, $F \mapsto F(G)$ est un endomorphisme du corps $\mathbb{K}(X)$.

Semaine 28 (du 4 au 8 mai) : Résumé de cours

1 Les fractions rationnelles (fin)

1.1 Dérivation

Définition. Soit $F = \frac{P}{Q} \in \mathbb{K}(X)$. On pose $F' \triangleq \frac{P'Q - Q'P}{Q^2} \in \mathbb{K}(X)$.

Définition. Par récurrence, on peut définir la dérivée n -ième formelle d'une fraction rationnelle.

Propriété. Pour tout $F \in \mathbb{K}(X)$ et $n \in \mathbb{N}$, $\widetilde{F^{(n)}} = \tilde{F}^{(n)}$.

Propriété. Pour tout $F \in \mathbb{K}[X]$, $\deg(F') \leq \deg(F) - 1$, avec égalité lorsque $\text{car}(\mathbb{K}) = 0$ et $\deg(F) \notin \{0, -\infty\}$.

Propriété. Soit $F, G \in \mathbb{K}(X)$, $a \in \mathbb{K}$ et $n \in \mathbb{N}$.

- $(F + G)' = F' + G'$, et plus généralement, $(F + G)^{(n)} = F^{(n)} + G^{(n)}$.
- $(aF)' = aF'$, et plus généralement, $(aF)^{(n)} = aF^{(n)}$.
- $(FG)' = F'G + FG'$.
- Si $G \neq 0$, $\left(\frac{F}{G}\right)' = \frac{F'G - G'F}{G^2}$.

Propriété. Pour tout $n \in \mathbb{N}$ et $F_1, \dots, F_n \in \mathbb{K}(X)$, $(F_1 \times \dots \times F_n)' = \sum_{i=1}^n F_i' \prod_{j \neq i} F_j$.

Formule de Leibniz : $(FG)^{(n)} = \sum_{k=0}^n \binom{n}{k} F^{(k)} G^{(n-k)}$.

Propriété. Pour tout $F, G \in \mathbb{K}(X)$, avec $G \notin \mathbb{K}$, $(F \circ G)' = G' \times (F' \circ G)$.

1.2 Décomposition en éléments simples.

1.2.1 Partie entière

Définition. Un élément simple de $\mathbb{K}(X)$ est une fraction rationnelle de la forme $\frac{P}{Q^m}$, où $m \in \mathbb{N}^*$ et $P, Q \in \mathbb{K}[X]$, avec Q irréductible et $\deg(P) < \deg(Q)$.

Propriété de la partie entière : Soit $F = \frac{A}{S} \in \mathbb{K}(X)$. Il existe un unique couple $(E, B) \in \mathbb{K}[X]^2$ tel que $F = E + \frac{B}{S}$ avec $\deg(B) < \deg(S)$. De plus, si $\frac{A}{S}$ est irréductible alors $\frac{B}{S}$ l'est également. E est la *partie entière* de F .

Il faut savoir le démontrer.

1.2.2 Divisions successives

Méthode des divisions successives pour décomposer en éléments simples une fraction de la forme $\frac{B}{S^m}$ où S est un polynôme irréductible de $\mathbb{K}[X]$:

A connaître.

1.2.3 Le théorème

Théorème de décomposition en éléments simples :

Soit $F \in \mathbb{K}(X)$. On peut toujours écrire F sous la forme $F = \frac{A}{S_1^{m_1} S_2^{m_2} \dots S_n^{m_n}}$, où S_1, S_2, \dots, S_n sont des polynômes irréductibles dans $\mathbb{K}[X]$, $m_1, \dots, m_n \in \mathbb{N}^*$ et $A \in \mathbb{K}[X]$. Alors il existe un unique $E \in \mathbb{K}[X]$ et une unique famille $(T_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m_i}}$ de polynômes de $\mathbb{K}[X]$ tels que

$$F = E + \sum_{i=1}^n \left(\sum_{j=1}^{m_i} \frac{T_{i,j}}{S_i^j} \right) \text{ avec pour tout } i \in \llbracket 1; n \rrbracket \text{ et } j \in \llbracket 1; m_i \rrbracket, \deg(T_{i,j}) < \deg(S_i).$$

Cette égalité s'appelle la décomposition en éléments simples de F sur \mathbb{K} .

Le polynôme E est la *partie entière* de F .

Pour $i \in \llbracket 1; n \rrbracket$, la somme $\sum_{j=1}^{m_i} \frac{T_{i,j}}{S_i^j}$ s'appelle la partie polaire de F relative au polynôme S_i .

1.2.4 Dérivée logarithmique

Propriété. Soit P un polynôme scindé dans $\mathbb{K}[X]$. Alors, en notant $\alpha_1, \dots, \alpha_n$ les racines de P et m_1, \dots, m_n leurs multiplicités respectives, $\frac{P'}{P} = \sum_{i=1}^n \frac{m_i}{X - \alpha_i}$.

1.2.5 Dans $\mathbb{C}(X)$ et $\mathbb{R}(X)$

Théorème de décomposition en éléments simples dans $\mathbb{C}(X)$:

Soit $F \in \mathbb{C}(X)$. On peut toujours écrire F sous la forme $F = \frac{A}{(X - \alpha_1)^{m_1} \dots (X - \alpha_n)^{m_n}}$, où $\alpha_1, \dots, \alpha_n$ sont des poles de F , $m_1, \dots, m_n \in \mathbb{N}^*$ sont leurs multiplicités et $A \in \mathbb{K}[X]$. Alors il existe un unique $E \in \mathbb{K}[X]$ et une unique famille $(\lambda_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m_i}}$ de complexes tels

$$\text{que } F = E + \sum_{i=1}^n \left(\sum_{j=1}^{m_i} \frac{\lambda_{i,j}}{(X - \alpha_i)^j} \right).$$

Pour $i \in \llbracket 1; n \rrbracket$, la somme $\sum_{j=1}^{m_i} \frac{\lambda_{i,j}}{(X - \alpha_i)^j}$ est la partie polaire de F relative au pôle α_i .

Théorème de décomposition en éléments simples dans $\mathbb{R}(X)$:

Soit $F \in \mathbb{R}(X)$. On peut toujours écrire F sous la forme

$$F = \frac{A}{\left(\prod_{i=1}^n (X - a_i)^{m_i} \right) \times \left(\prod_{i=1}^p (X^2 + b_i X + c_i)^{k_i} \right)},$$

où a_1, \dots, a_n sont des poles réels de F , $m_1, \dots, m_n \in \mathbb{N}^*$ sont leurs multiplicités, où pour tout $i \in \{1, \dots, p\}$, $b_i, c_i \in \mathbb{R}$ avec $b_i^2 - 4c_i < 0$ et où $A \in \mathbb{K}[X]$.

Alors il existe un unique $E \in \mathbb{K}[X]$ et trois uniques familles $(\lambda_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m_i}}$, $(f_{i,j})_{\substack{1 \leq i \leq p \\ 1 \leq j \leq k_i}}$ et $(g_{i,j})_{\substack{1 \leq i \leq p \\ 1 \leq j \leq k_i}}$ de réels tels que $F = E + \sum_{i=1}^n \left(\sum_{j=1}^{m_i} \frac{\lambda_{i,j}}{(X - \alpha_i)^j} \right) + \sum_{i=1}^p \left(\sum_{j=1}^{k_i} \frac{f_{i,j}X + g_{i,j}}{(X^2 + b_iX + c_i)^j} \right)$.

Méthode : En pratique, pour décomposer une fraction rationnelle F en éléments simples dans $\mathbb{R}(X)$ ou dans $\mathbb{C}(X)$,

1. on commence par l'écrire sous forme irréductible unitaire, $F = \frac{A}{B}$.
2. En effectuant la division euclidienne de A par B , on écrit $F = E + \frac{C}{B}$, où E est la partie entière de F . Lorsque $\deg(F) < 0$, il est évident que $E = 0$, donc on peut supprimer cette étape.
3. On scinde B en produit de polynômes irréductibles unitaires.
4. On écrit la DES de $\frac{C}{B}$ à l'aide de coefficients indéterminés.
5. On calcule ces coefficients indéterminés.

1.2.6 Quelques techniques de DES

Remarque. La technique des divisions euclidiennes successives est adaptée à la DES de fractions de la forme $\frac{P}{Q^m}$, où Q est irréductible.

Propriété. Soit $F \in \mathbb{K}(X)$ et soit $\alpha \in \mathbb{K}$ un pôle de F de multiplicité $m \in \mathbb{N}^*$. Alors le coefficient λ de l'élément simple $\frac{1}{(X - \alpha)^m}$ dans la DES de F vérifie $\lambda = [\widetilde{(X - \alpha)^m F}](\alpha)$.

Il faut savoir le démontrer.

Propriété. Soit $F \in \mathbb{K}(X)$ une fraction rationnelle admettant un pôle simple α .

Si $\frac{A}{S}$ est un représentant irréductible de F , alors le coefficient λ de l'élément simple $\frac{1}{X - \alpha}$ dans la DES de F vérifie $\lambda = \frac{\tilde{A}(\alpha)}{\tilde{S}'(\alpha)}$.

Il faut savoir le démontrer.

Généralisation : (hors programme) On suppose que $\text{car}(\mathbb{K}) = 0$.

Soit $F \in \mathbb{K}(X)$ dont $a \in \mathbb{K}$ est l'un des pôles, de multiplicité m . Si $\frac{A}{S}$ est un représentant irréductible de F , alors le coefficient λ de l'élément simple $\frac{1}{(X - a)^m}$ dans la DES de F vérifie $\lambda = \frac{m! \tilde{A}(\alpha)}{\widetilde{S^{(m)}}(\alpha)}$.

Utilisation d'un développement limité : Soit $F \in \mathbb{C}(X)$ et a un pôle de F de multiplicité m .

On peut écrire la DES de F sous la forme $F(X) = \sum_{i=1}^m \frac{\lambda_i}{(X - a)^i} + G(X)$. La fonction rationnelle

associée à G est continue en a , donc au voisinage de a , $(t - a)^m F(t) = \sum_{i=1}^m \lambda_i (t - a)^{m-i} + O((t - a)^m)$.

On peut donc calculer les λ_i en effectuant un développement limité de $(t - a)^m F(t)$ au voisinage de a puis en invoquant l'unicité du développement limité.

1.3 Application au calcul intégral

1.3.1 Primitives d'une fraction rationnelle

Si $F \in \mathbb{R}(X)$, pour calculer $\int F(t)dt$, on décompose F en éléments simples dans $\mathbb{R}(X)$.

On est ainsi ramené au problème du calcul des primitives des éléments simples de $\mathbb{R}(X)$:

Lorsque $F(X) = \frac{aX+b}{(X^2+cX+d)^\alpha}$, avec $\Delta = c^2 - 4d < 0$, on décompose le calcul de $\int F(t)dt$ en celui de $\int \frac{u'(t)}{u(t)^\alpha} dt$, où $u(t) = t^2 + ct + d$, et celui de $\int \frac{dt}{u(t)^\alpha}$.

Pour ce dernier, on écrit $X^2 + cX + d = (X + \frac{c}{2})^2 + d - \frac{c^2}{4} = (X - p)^2 + q^2$

et on se ramène au calcul de $\int \frac{dt}{(1+t^2)^\alpha}$, que l'on réalise en posant $t = \tan u$.

1.3.2 Fonctions rationnelles de sin et cos : hors programme

Pour calculer $\int R(\sin t, \cos t) dt$, où $R \in \mathbb{R}(X, Y)$:

Cas particulier. $\int \sin^p t \cos^q t dt$, avec p et q pairs. C'est le seul cas où on linéarise.

Cas général. On pose $u = \tan \frac{t}{2}$ pour se ramener à une primitive de fraction rationnelle.

Les règles de Bioche. Notons $f : t \mapsto R(\sin t, \cos t)$.

Si $f(-t)d(-t) = f(t)dt$, on posera $x = \cos t$ (On a $\cos(-t) = \cos t$),

Si $f(\pi - t)d(\pi - t) = f(t)dt$, on posera $x = \sin t$ (On a $\sin(\pi - t) = \sin t$),

Si $f(\pi + t)d(\pi + t) = f(t)dt$, on posera $x = \tan t$ (On a $\tan(\pi + t) = \tan t$).

Si deux des trois relations précédentes sont vérifiées, alors la troisième l'est aussi. On pose alors $x = \sin^2 t$ ou $x = \cos(2t)$.

1.3.3 Fonctions rationnelles en sh et ch : hors programme

Pour calculer $\int R(\sinh t, \cosh t) dt$, où $R \in \mathbb{R}(X, Y)$, on regarde quel procédé serait utilisé pour le calcul de $\int R(\sin t, \cos t) dt$ et on le transpose en trigonométrie hyperbolique.

Dans le cas général, on peut poser $x = e^t$.

2 Les matrices

2.1 Vocabulaire

Définition. Soit $(n, p) \in \mathbb{N}^{*2}$. On appelle **matrice** à n lignes et à p colonnes (à coefficients dans \mathbb{K}) toute famille de scalaires indexée par $\mathbb{N}_n \times \mathbb{N}_p$.

Si $M = (m_{i,j})_{(i,j) \in \mathbb{N}_n \times \mathbb{N}_p} = (m_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}}$, on représente M sous la forme suivante :

$$M = \begin{pmatrix} m_{1,1} & \cdots & m_{1,p} \\ \vdots & & \vdots \\ m_{n,1} & \cdots & m_{n,p} \end{pmatrix},$$

où le (i, j) ^{ème} coefficient est situé à l'intersection de la i ^{ème} ligne et de la j ^{ème} colonne.

Notation. L'ensemble des matrices à coefficients dans \mathbb{K} , à n lignes et p colonnes est noté $\mathcal{M}_{\mathbb{K}}(n, p)$ ou $\mathcal{M}_{n,p}(\mathbb{K})$. $\mathcal{M}_{\mathbb{K}}(n, n)$ est souvent noté $\mathcal{M}_{\mathbb{K}}(n)$ ou $\mathcal{M}_n(\mathbb{K})$.

Définitions :

- Une **matrice ligne** est une matrice ne possédant qu'une ligne.
- Une **matrice colonne** est une matrice ne possédant qu'une colonne.
- Une **matrice carrée** est une matrice possédant autant de lignes que de colonnes.
- $M = (m_{i,j}) \in \mathcal{M}_{\mathbb{K}}(n, p)$ est une **matrice triangulaire supérieure** si et seulement si $\forall (i, j) \in \mathbb{N}_n \times \mathbb{N}_p$ ($i > j \implies m_{i,j} = 0$).

- M est une **matrice triangulaire inférieure** si et seulement si $\forall (i, j) \in \mathbb{N}_n \times \mathbb{N}_p \ (i < j \implies m_{i,j} = 0)$.
- $M = (m_{i,j}) \in \mathcal{M}_{\mathbb{K}}(n, p)$ est une **matrice diagonale** si et seulement si $\forall (i, j) \in \mathbb{N}_n \times \mathbb{N}_p \ (i \neq j \implies m_{i,j} = 0)$. On note alors $M = \text{diag}(m_{1,1}, \dots, m_{n,n})$.
- Une matrice carrée et diagonale est dite **scalaire** lorsque tous ses coefficients diagonaux sont égaux. En particulier, lorsque tous ses coefficients diagonaux sont égaux à 1, on obtient la matrice identité, notée I_n .

Remarque. On identifiera \mathbb{K}^n avec $\mathcal{M}_{\mathbb{K}}(n, 1)$ (ensemble des matrices colonnes).

2.2 Opérations sur les matrices

Définition. On sait déjà que $\mathcal{M}_{\mathbb{K}}(n, p) = \mathbb{K}^{\mathbb{N}_n \times \mathbb{N}_p}$ est un \mathbb{K} -espace vectoriel. On dispose ainsi des lois d'addition et de multiplication par un scalaire.

Convention : Lorsque A est une matrice, on notera $A_{i,j}$ son coefficient de position (i, j) .

Définition du produit matriciel : Soit $(n, p, q) \in (\mathbb{N}^*)^3$. Soient $A \in \mathcal{M}_{\mathbb{K}}(n, p)$ et $B \in \mathcal{M}_{\mathbb{K}}(p, q)$. On appelle **produit des matrices** A et B la matrice $C \in \mathcal{M}_{\mathbb{K}}(n, q)$ définie par

$$[AB]_{i,j} = \sum_{k=1}^p A_{i,k} B_{k,j}.$$

Formule pour le produit de trois matrices : Soit $(n, m, l, p) \in (\mathbb{N}^*)^4$.

Soient $A \in \mathcal{M}_{\mathbb{K}}(n, m)$, $B \in \mathcal{M}_{\mathbb{K}}(m, l)$ et $C \in \mathcal{M}_{\mathbb{K}}(l, p)$: $[(AB)C]_{i,h} = [A(BC)]_{i,h} = \sum_{\substack{1 \leq j \leq m \\ 1 \leq k \leq l}} A_{i,j} B_{j,k} C_{k,h}.$

Il faut savoir le démontrer.

Propriété. La multiplication matricielle est associative.

Propriété. La multiplication matricielle est distributive par rapport à l'addition.

Propriété. Soit $A \in \mathcal{M}_{n,p}$, $B \in \mathcal{M}_{p,q}$ et $a \in \mathbb{K}$. Alors $a(AB) = (aA)B = A(aB)$.

Propriété. Pour tout $M \in \mathcal{M}_{\mathbb{K}}(n, p)$, $I_n M = M I_p = M$.

Propriété. Soit $n, p \in \mathbb{N}^*$ et $M \in \mathcal{M}_{\mathbb{K}}(n, p)$. Pour tout $X \in \mathbb{K}^p$, $MX \in \mathbb{K}^n$.

Si $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$, alors $\forall i \in \{1, \dots, n\}$, $[MX]_i = \sum_{j=1}^p M_{i,j} x_j$

et $MX = x_1 M_1 + \dots + x_p M_p$, en notant M_1, \dots, M_p les colonnes de M .

Il faut savoir le démontrer.

Propriété. Si $M \in \mathcal{M}_{\mathbb{K}}(n, p)$, la j -ème colonne de M est $M c_j$, où $c_j = (\delta_{i,j})_{1 \leq i \leq n} \in \mathbb{K}^p$.

Définition. Si $M \in \mathcal{M}_{\mathbb{K}}(n, p)$, $\begin{matrix} \tilde{M} : \mathbb{K}^p & \longrightarrow & \mathbb{K}^n \\ X & \longmapsto & MX \end{matrix}$ est une application linéaire que l'on appelle **l'application linéaire canoniquement associée à la matrice M** .

Propriété. $\begin{matrix} \mathcal{M}_{\mathbb{K}}(n, p) & \longrightarrow & L(\mathbb{K}^p, \mathbb{K}^n) \\ M & \longmapsto & \tilde{M} \end{matrix}$ est un isomorphisme d'espaces vectoriels.

Il faut savoir le démontrer.

Remarque. On identifie souvent M et \tilde{M} , auquel cas, pour tout $X \in \mathbb{K}^p$, $MX = M(X)$. Cela permet d'interpréter une matrice M comme une application linéaire.

Définition. Soit $M \in \mathcal{M}_{\mathbb{K}}(n, p)$: $\text{Ker}(M) \triangleq \{X \in \mathbb{K}^p / MX = 0\}$

et $\text{Im}(M) \triangleq \{MX / X \in \mathbb{K}^p\} = \text{Vect}\{\text{colonnes de } M\}$.

Corollaire. Soit $(M, M') \in \mathcal{M}_{\mathbb{K}}(n, p)$: $(\forall X \in \mathbb{K}^p \quad MX = M'X) \iff M = M'$.

2.3 L'algèbre des matrices carrées de taille $n \in \mathbb{N}^*$

Propriété. $(\mathcal{M}_n(\mathbb{K}), +, \cdot, \times)$ est une \mathbb{K} -algèbre, ni commutative ni intègre dès que $n \geq 2$.

Définition. $A \in \mathcal{M}_n(\mathbb{K})$ est nilpotente si et seulement si il existe $p \in \mathbb{N}^*$ tel que $A^p = 0$.

Propriété. $\begin{matrix} \mathcal{M}_{\mathbb{K}}(n) & \longrightarrow & L(\mathbb{K}^n) \\ M & \longmapsto & \tilde{M} \end{matrix}$ est un isomorphisme d'algèbres.

Il faut savoir le démontrer.

Corollaire. Soit $A \in \mathcal{M}_{\mathbb{K}}(n)$. A est inversible dans $\mathcal{M}_{\mathbb{K}}(n)$ si et seulement si \tilde{A} est inversible dans $L(\mathbb{K}^n)$ et dans ce cas, $\widetilde{M^{-1}} = \tilde{M}^{-1}$.

Corollaire. Soit $A \in \mathcal{M}_{\mathbb{K}}(n)$. A est inversible dans $\mathcal{M}_{\mathbb{K}}(n)$ si et seulement si, pour tout $X \in \mathbb{K}^n$, il existe un unique $Y \in \mathbb{K}^n$ tel que $AX = Y$.

Formule : Dans $\mathcal{M}_2(\mathbb{K})$, $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est inversible si et seulement si $\det(M) \triangleq ad - cb \neq 0$, et dans ce cas $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{\det(M)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Il faut savoir le démontrer.

Formule de Cramer : Soit $a, b, c, d, e, f \in \mathbb{K}^4$. Lorsque $\det = ad - cb \triangleq \begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0$,

$$\begin{cases} ax + by = e \\ cx + dy = f \end{cases} \iff x = \frac{\begin{vmatrix} e & b \\ f & d \end{vmatrix}}{\det} \wedge y = \frac{\begin{vmatrix} a & e \\ c & f \end{vmatrix}}{\det}.$$

Il faut savoir le démontrer.

Notation. $GL_n(\mathbb{K})$ = groupe des inversibles de $\mathcal{M}_n(\mathbb{K})$. On l'appelle le groupe linéaire de degré n .

Exemple. Un automorphisme intérieur de $\mathcal{M}_n(\mathbb{K})$ est un automorphisme sur $\mathcal{M}_n(\mathbb{K})$ de la forme $M \mapsto AMA^{-1}$ où $A \in GL_n(\mathbb{K})$.

Définition. Soit $M \in \mathcal{M}_n(\mathbb{K})$ et $\lambda \in \mathbb{K}$. On dit que λ est une valeur propre de M si et seulement si il existe $X \in \mathbb{C}^n$ avec $X \neq 0$ tel que $MX = \lambda X$. Dans ce cas, on dit que X est un vecteur propre de M pour la valeur propre λ .

Propriété. Les matrices diagonales de $\mathcal{M}_n(\mathbb{K})$ forment une sous-algèbre commutative de $\mathcal{M}_n(\mathbb{K})$.

Propriété. Pour tout $i \in \mathbb{N}_n$, on pose $c_i = (\delta_{i,j})_{1 \leq j \leq n} \in \mathbb{K}^n$ et $F_i = \text{Vect}(c_k)_{1 \leq k \leq i}$.

Si $M \in \mathcal{M}_n(\mathbb{K})$, M est triangulaire supérieure ssi, pour tout $j \in \{1, \dots, n\}$, F_j est stable par \tilde{M} .

Il faut savoir le démontrer.

Propriété. On suppose que $n \geq 2$.

- L'ensemble des matrices triangulaires supérieures (respectivement : inférieures) de $\mathcal{M}_n(\mathbb{K})$ est une sous-algèbre non commutative de $\mathcal{M}_n(\mathbb{K})$.
- Le produit d'une matrice triangulaire supérieure dont la diagonale est (a_1, \dots, a_n) par une matrice triangulaire supérieure dont la diagonale est (b_1, \dots, b_n) est une matrice triangulaire supérieure dont la diagonale est $(a_1 b_1, \dots, a_n b_n)$.

Il faut savoir le démontrer.

Semaine 29 (du 11 au 16 mai) : Résumé de cours

1 Les matrices (suite)

1.1 Transposée d'une matrice

Définition. Soit $A \in \mathcal{M}_{\mathbb{K}}(n, p)$. On appelle *transposée de la matrice* A et on note tA la matrice de $\mathcal{M}_{\mathbb{K}}(p, n)$ définie par $[{}^tA]_{i,j} = A_{j,i}$.

Propriété. Pour tout $A \in \mathcal{M}_{\mathbb{K}}(n, p)$, ${}^t({}^tA) = A$.

Propriété. L'application $\begin{array}{ccc} \mathcal{M}_{\mathbb{K}}(n, p) & \longrightarrow & \mathcal{M}_{\mathbb{K}}(p, n) \\ M & \longmapsto & {}^tM \end{array}$ est un isomorphisme d'espaces vectoriels.

Propriété. Soit $(A, B) \in \mathcal{M}_{\mathbb{K}}(n, p) \times \mathcal{M}_{\mathbb{K}}(p, q)$. Alors, ${}^t(AB) = {}^tB {}^tA$.

Il faut savoir le démontrer.

Corollaire. Si $A \in GL_n(\mathbb{K})$, ${}^tA \in GL_n(\mathbb{K})$ et $({}^tA)^{-1} = {}^t(A^{-1})$.

Définition. M est une *matrice symétrique* si et seulement si ${}^tM = M$.

M est une *matrice antisymétrique* si et seulement si ${}^tM = -M$.

Remarque. Lorsque $\text{car}(\mathbb{K}) \neq 2$, si $M \in \mathcal{M}_n(\mathbb{K})$ est antisymétrique, sa diagonale est nulle.

Notation. $\mathcal{S}_n(\mathbb{K})$ désigne l'ensemble des matrices symétriques d'ordre n .

$\mathcal{A}_n(\mathbb{K})$ désigne l'ensemble des matrices antisymétriques d'ordre n .

Propriété. $\mathcal{S}_n(\mathbb{K})$ et $\mathcal{A}_n(\mathbb{K})$ sont des sous-espaces vectoriels de $\mathcal{M}_n(\mathbb{K})$, mais ce ne sont pas des sous-algèbres. Cependant, elles sont stables par passage à l'inverse.

Il faut savoir le démontrer.

1.2 Différentes interprétations du produit matriciel

Au niveau des colonnes de la matrice de droite : Soit $A \in \mathcal{M}_{\mathbb{K}}(n, p)$. Si B_1, \dots, B_q sont des vecteurs colonnes de \mathbb{K}^p , $A \times \boxed{B_1} \boxed{B_2} \cdots \boxed{B_q} = \boxed{AB_1} \boxed{AB_2} \cdots \boxed{AB_q}$.

Au niveau des colonnes de la matrice de gauche :

— Si $M \in \mathcal{M}_{\mathbb{K}}(n, p)$ et $X \in \mathbb{K}^p$, MX est une combinaison linéaire des colonnes de M .

Plus précisément, si l'on note M_1, \dots, M_p les colonnes de M et $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$,

$$MX = x_1 M_1 + \cdots + x_p M_p.$$

— Soient $A \in \mathcal{M}_{\mathbb{K}}(n, p)$ et $B \in \mathcal{M}_{\mathbb{K}}(p, q)$. Les colonnes de AB sont des combinaisons linéaires des colonnes de A : en notant A_1, \dots, A_p les colonnes de A et $B = (b_{i,j})$, la $j^{\text{ème}}$ colonne de AB est égale à $b_{1,j}A_1 + \cdots + b_{p,j}A_p$.

Au niveau des lignes de la matrice de gauche : Soit $A \in \mathcal{M}_{\mathbb{K}}(n, p)$ et $B \in \mathcal{M}_{\mathbb{K}}(p, q)$. Notons

$${}_1A, \dots, {}_nA \text{ les lignes de } A. \text{ Alors } AB = \begin{pmatrix} \boxed{{}_1A} \\ \vdots \\ \boxed{{}_nA} \end{pmatrix} \times B = \begin{pmatrix} \boxed{{}_1AB} \\ \vdots \\ \boxed{{}_nAB} \end{pmatrix}.$$

Au niveau des lignes de la matrice de droite :

- Si $M \in \mathcal{M}_{\mathbb{K}}(n, p)$ et $X \in \mathcal{M}_{1,n}$, XM est une combinaison linéaire des lignes de M .
Plus précisément, si l'on note ${}_1M, \dots, {}_nM$ les lignes de M et $X = (x_1 \ \dots \ x_n)$,
 $XM = x_1 \times {}_1M + \dots + x_n \times {}_nM$.
- Soient $A \in \mathcal{M}_{\mathbb{K}}(n, p)$ et $B \in \mathcal{M}_{\mathbb{K}}(p, q)$. Les lignes de AB sont des combinaisons linéaires des lignes de B : en notant ${}_1B, \dots, {}_pB$ les lignes de B et $A = (a_{i,j})$, la $i^{\text{ème}}$ ligne de AB est égale à $a_{i,1} \times {}_1B + \dots + a_{i,p} \times {}_pB$.

1.3 Trace d'une matrice

Définition. La *trace de la matrice* $M \in \mathcal{M}_n(\mathbb{K})$ est $Tr(M) = \sum_{i=1}^n m_{i,i}$.

Propriété. La trace est une forme linéaire de $\mathcal{M}_n(\mathbb{K})$.

Propriété. Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et $B \in \mathcal{M}_{p,n}(\mathbb{K})$. Alors, $Tr(AB) = Tr(BA)$.

Il faut savoir le démontrer.

ATTENTION : Si $(A, B, C) \in \mathcal{M}_n(\mathbb{K})^3$, en général $Tr(ABC) \neq Tr(ACB)$.

Définition. Soit $A, B \in \mathcal{M}_n(\mathbb{K})$. On dit que A et B sont semblables si et seulement si il existe $P \in GL_n(\mathbb{K})$ telle que $B = PAP^{-1}$.

La relation de similitude ("être semblable à") est une relation d'équivalence sur $\mathcal{M}_n(\mathbb{K})$.

Définition. Une matrice de $\mathcal{M}_n(\mathbb{K})$ est diagonalisable (resp : trigonalisable) si et seulement si elle est semblable à une matrice diagonale (resp : triangulaire supérieure).

Propriété. Deux matrices semblables ont la même trace, mais la réciproque est fausse.

Il faut savoir le démontrer.

1.4 Matrices décomposées en blocs

1.4.1 Matrices extraites

Définition. Soit $n, p \in \mathbb{N}$ et soit I et J deux parties de \mathbb{N} telles que $|I| = n$ et $|J| = p$. Notons $0 \leq i_1 \leq i_2 \leq \dots \leq i_n$ les éléments de I et $0 \leq j_1 \leq i_2 \leq \dots \leq j_p$ les éléments de J .

Alors on convient d'identifier toute famille $(M_{i,j})_{(i,j) \in I \times J}$ de **scalaires** indexée par $I \times J$ avec la matrice $(M_{i_h, j_k})_{\substack{1 \leq h \leq n \\ 1 \leq k \leq p}} \in \mathcal{M}_{\mathbb{K}}(n, p)$.

Remarque. Lorsque I ou J est vide, $I \times J = \emptyset$ et $\mathbb{K}^{I \times J}$ possède un unique élément, que l'on appellera la matrice vide.

Définition. Soit $n, p \in \mathbb{N}^*$ et $M \in \mathcal{M}_{\mathbb{K}}(n, p)$. Une matrice extraite de M est une matrice de la forme $(M_{i,j})_{(i,j) \in I \times J}$, où $I \subset \mathbb{N}_n$ et $J \subset \mathbb{N}_p$.

1.4.2 Matrices blocs

Définition. Soient $(n_1, \dots, n_a) \in (\mathbb{N}^*)^a$ et $(p_1, \dots, p_b) \in (\mathbb{N}^*)^b$. On pose $n = \sum_{i=1}^a n_i$ et $p = \sum_{j=1}^b p_j$.

Pour tout $(i, j) \in \mathbb{N}_a \times \mathbb{N}_b$, considérons une matrice $M_{i,j} \in \mathcal{M}_{\mathbb{K}}(n_i, p_j)$. Alors la famille de ces matrices $M = (M_{i,j})_{\substack{1 \leq i \leq a \\ 1 \leq j \leq b}}$ peut être identifiée à une matrice possédant n lignes et p colonnes. On dit que M est une **matrice décomposée en blocs**, de dimensions (n_1, \dots, n_a) et (p_1, \dots, p_b) .

Définition. Avec ces notations, M est une **matrice triangulaire supérieure par blocs** si et seulement si, pour tout $(i, j) \in \mathbb{N}_a \times \mathbb{N}_b$ tel que $i > j$, $M_{i,j} = 0$.

De même on définit la notion de matrice triangulaire inférieure par blocs.

La matrice $M = (M_{i,j})_{\substack{1 \leq i \leq a \\ 1 \leq j \leq b}}$ est une **matrice diagonale par blocs** si et seulement si, pour tout $(i, j) \in \mathbb{N}_a \times \mathbb{N}_b$ tel que $i \neq j$, $M_{i,j} = 0$.

1.4.3 Opérations sur les matrices blocs

Combinaison linéaire de matrices décomposées en blocs : Soient $M = (M_{i,j})_{\substack{1 \leq i \leq a \\ 1 \leq j \leq b}}$ et $N = (N_{i,j})_{\substack{1 \leq i \leq a \\ 1 \leq j \leq b}}$ deux matrices décomposées en blocs selon les mêmes partitions $(I_i)_{1 \leq i \leq a}$ et $(J_j)_{1 \leq j \leq b}$ respectivement de \mathbb{N}_n et de \mathbb{N}_p . Alors, $\forall u \in \mathbb{K}$, $uM + N = (uM_{i,j} + N_{i,j})_{\substack{1 \leq i \leq a \\ 1 \leq j \leq b}}$.

Produit matriciel de deux matrices décomposées en blocs : soit $n, p, q \in \mathbb{N}^*$.

Soit $M = (M_{i,j})_{\substack{1 \leq i \leq a \\ 1 \leq j \leq b}}$ une matrice décomposée en blocs selon les partitions $(I_i)_{1 \leq i \leq a}$ et $(J_j)_{1 \leq j \leq b}$ respectivement de \mathbb{N}_n et de \mathbb{N}_p . Soit $N = (N_{j,k})_{\substack{1 \leq j \leq b \\ 1 \leq k \leq c}}$ une matrice décomposée en blocs selon la même partition $(J_j)_{1 \leq j \leq b}$ de \mathbb{N}_p et une partition $(K_k)_{1 \leq k \leq c}$ de \mathbb{N}_q .

Alors MN peut être vue comme une matrice décomposée en blocs selon les partitions $(I_i)_{1 \leq i \leq a}$ de

\mathbb{N}_n et $(K_k)_{1 \leq k \leq c}$ de \mathbb{N}_q et $MN = \left(\sum_{j=1}^b M_{i,j} N_{j,k} \right)_{\substack{1 \leq i \leq a \\ 1 \leq k \leq c}}$.

En résumé, le produit de deux matrices par blocs se comporte comme le produit matriciel usuel.

Application : Produit de matrices triangulaires (resp : diagonales) par blocs, puissances de telles matrices.

2 Familles de vecteurs

Notation. On fixe un \mathbb{K} -espace vectoriel E et un ensemble quelconque I (éventuellement infini).

2.1 Familles libres et génératrices

Définition. Soit $x = (x_i)_{i \in I}$ une famille de vecteurs de E .

x est libre ssi $\forall (\alpha_i)_{i \in I} \in \mathbb{K}^{(I)}$, $\left(\sum_{i \in I} \alpha_i x_i = 0 \implies (\forall i \in I \quad \alpha_i = 0) \right)$.

x est liée ssi $\exists (\alpha_i)_{i \in I} \in \mathbb{K}^{(I)} \setminus \{0\}$, $\sum_{i \in I} \alpha_i x_i = 0$.

x est génératrice dans E ssi $\forall x \in E$, $\exists (\alpha_i)_{i \in I} \in \mathbb{K}^{(I)}$, $\sum_{i \in I} \alpha_i x_i = x$.

x est une base de E si et seulement si elle est libre et génératrice dans E .

Définition. $x, y \in E$ sont **colinéaires** si et seulement si la famille (x, y) est liée.

Propriété. Soit $e = (e_i)_{i \in I}$ une famille de vecteurs de E . e est une base de E si et seulement si $\forall x \in E, \exists ! (\alpha_i)_{i \in I} \in \mathbb{K}^{(I)}, \sum_{i \in I} \alpha_i e_i = x$. Dans ce cas, pour $x \in E$, on appelle coordonnées de x dans

la base $(e_i)_{i \in I}$ l'unique famille presque nulle de scalaire $(\alpha_i)_{i \in I}$ telle que $x = \sum_{i \in I} \alpha_i e_i$.

2.2 Dimension d'un espace vectoriel

Définition. E est de dimension finie si et seulement si il possède une famille génératrice finie.

Lemme : Soit $n \in \mathbb{N}$ et $e_1, \dots, e_n \in E$.

Toute famille (x_1, \dots, x_{n+1}) de $n + 1$ vecteurs de $\text{Vect}(e_1, \dots, e_n)$ est liée.

Il faut savoir le démontrer.

Corollaire. Si (e_1, \dots, e_n) est une famille génératrice de E , alors toute famille libre de E est de cardinal inférieur ou égal à n .

Théorème de la base incomplète : Soient E un \mathbb{K} -espace vectoriel de dimension finie et $(e_i)_{i \in I}$ une famille génératrice de E . Soit $J \subset I$ tel que $(e_i)_{i \in J}$ est une famille libre.

Alors il existe un ensemble L avec $J \subset L \subset I$ tel que $(e_i)_{i \in L}$ est une base de E .

Il faut savoir le démontrer.

Propriété. Soit $(e_i)_{i \in I}$ une famille libre de vecteurs de E . Soit $e_j \in E$, où $j \notin I$.

La famille $(e_i)_{i \in I \cup \{j\}}$ est libre si et seulement si $e_j \notin \text{Vect}(e_i)_{i \in I}$.

Propriété.

Soient E un \mathbb{K} -espace vectoriel et $g = (e_i)_{i \in I}$ une famille génératrice de E .

On dit qu'une sous-famille libre $(e_i)_{i \in J}$ de g est maximale dans g si et seulement si pour tout $i_0 \in I \setminus J$, la famille $(e_i)_{i \in J \cup \{i_0\}}$ est liée.

Si $(e_i)_{i \in J}$ est libre maximale dans g , alors c'est une base de E .

Corollaire. Une famille libre de vecteurs de E est maximale si et seulement si en lui ajoutant un vecteur elle devient liée.

Toute famille libre maximale de vecteurs de E est une base de E .

Corollaire. Soit E un \mathbb{K} -espace vectoriel de dimension finie.

Toute famille libre de E peut être complétée en une base de E .

Définition. Soit E un \mathbb{K} -espace vectoriel de dimension finie.

E admet au moins une base. Toutes les bases de E sont finies et ont même cardinal. Ce cardinal est appelé la **dimension** de E et est noté $\dim(E)$ ou $\dim_{\mathbb{K}}(E)$.

Propriété. Soit E un \mathbb{K} -espace vectoriel de dimension finie égale à n et soit e une famille de E . e est une base de E si et seulement si e est libre et de cardinal n , ou encore si et seulement si e est génératrice et de cardinal n .

Il faut savoir le démontrer.

Propriété. Soit E un \mathbb{K} -espace vectoriel de dimension finie égale à n . Toute famille libre de E a au plus n éléments et toute famille génératrice de E a au moins n éléments.

Théorème. Soit E un \mathbb{K} -espace vectoriel de dimension quelconque.

Soit F et G deux sous-espaces vectoriels de E avec G de dimension finie et $F \subset G$.

Alors F est de dimension finie avec $\dim(F) \leq \dim(G)$.

De plus $[F = G \iff \dim(F) = \dim(G)]$.

Il faut savoir le démontrer.

2.3 Base canonique

Propriété. Soit $n \in \mathbb{N}^*$. \mathbb{K}^n est un \mathbb{K} -espace vectoriel de dimension n dont une base est $c = (c_1, \dots, c_n)$, où pour tout $i \in \{1, \dots, n\}$, $c_i = (\delta_{i,j})_{1 \leq j \leq n}$. c est la *base canonique* de \mathbb{K}^n . Les coordonnées de $x \in \mathbb{K}^n$ dans la base c sont les composantes de x .

Propriété. Soit I un ensemble quelconque. Pour tout $i \in I$, on note $c_i = (\delta_{i,j})_{j \in I}$. Ainsi $c = (c_i)_{i \in I}$ est une famille de $\mathbb{K}^{(I)}$. C'est une base de $\mathbb{K}^{(I)}$, appelée la *base canonique* de $\mathbb{K}^{(I)}$. De plus, pour tout $x = (\alpha_i)_{i \in I} \in \mathbb{K}^{(I)}$: les coordonnées de x sont ses composantes.

Corollaire. La base canonique de $\mathbb{K}[X]$ est la famille $(X^n)_{n \in \mathbb{N}}$. Soit $n \in \mathbb{N}$. $(1, X, \dots, X^n)$ est la base canonique de $\mathbb{K}_n[X]$: $\dim(\mathbb{K}_n[X]) = n + 1$.

Corollaire. La base canonique de $\mathcal{M}_{n,p}(\mathbb{K})$ est la famille des matrices élémentaires $(E_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}}$ définie par : Pour tout $i \in \{1, \dots, n\}$ et $j \in \{1, \dots, p\}$, $E_{i,j} = (\delta_{a,i} \delta_{b,j})_{\substack{1 \leq a \leq n \\ 1 \leq b \leq p}}$.

Pour tout $M \in \mathcal{M}_{n,p}(\mathbb{K})$, $M = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} M_{i,j} E_{i,j}$: $\dim(\mathcal{M}_{n,p}(\mathbb{K})) = np$.

Exercice. $E_{i,j} E_{h,k} = \delta_{j,h} E_{i,k}$.

Il faut savoir le démontrer.

2.4 Exemples

Propriété. Dans \mathbb{K}^2 , deux vecteurs $u = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}$ et $v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$ forment une base de \mathbb{K}^2 si et seulement si $u_1 v_2 - u_2 v_1 \stackrel{\Delta}{=} \det_c(u, v) \neq 0$.

Exercice. Soit $(P_n)_{n \in \mathbb{N}}$ une suite de polynômes de $\mathbb{K}[X]$. On suppose que cette suite de polynômes est étagée c'est-à-dire que, $\forall n \in \mathbb{N}$ $\deg(P_n) = n$.

Montrer que pour tout $N \in \mathbb{N}$, $(P_n)_{0 \leq n \leq N}$ est une base de $\mathbb{K}_N[X]$.

En déduire que $(P_n)_{n \in \mathbb{N}}$ est une base de $\mathbb{K}[X]$.

Il faut savoir le démontrer.

Exercice. Soit f un endomorphisme de E .

Montrer que f est une homothétie si et seulement si pour tout $u \in E$, $(u, f(u))$ est lié.

Il faut savoir le démontrer.

Propriété. Toute sur-famille d'une famille génératrice est génératrice.

Toute sous-famille d'une famille libre est libre.

Propriété. Une famille de vecteurs est libre si et seulement si toute sous-famille finie de cette famille est libre.

Théorème. $\dim(E_1 \times \dots \times E_n) = \dim(E_1) + \dots + \dim(E_n)$.

Il faut savoir le démontrer.

2.5 Application linéaire associée à une famille de vecteurs

Propriété. Soit $x = (x_i) \in E^I$. Notons
$$\Psi_x : \begin{array}{ccc} \mathbb{K}^{(I)} & \longrightarrow & E \\ (\alpha_i)_{i \in I} & \longmapsto & \sum_{i \in I} \alpha_i x_i \end{array}$$

Ψ_x est une application linéaire.

- x est une famille libre si et seulement si Ψ_x est injective.
- x est une famille génératrice si et seulement si Ψ_x est surjective.

- x est une base si et seulement si Ψ_x est un isomorphisme.

Ψ_x est appelée l'application linéaire associée à la famille de vecteurs x .

Il faut savoir le démontrer.

Propriété. Soit $x = (x_i)_{i \in I}$ une famille de vecteurs de E . x est libre si et seulement si, pour tout $y \in \text{Vect}(x)$, il existe une unique famille presque nulle de scalaires $(\alpha_i)_{i \in I}$ telle que $y = \sum_{i \in I} \alpha_i x_i$.

Propriété. Si $e = (e_i)_{i \in I}$ est une base de E , alors E est isomorphe à $\mathbb{K}^{(I)}$.

2.6 Image d'une famille par une application linéaire

Notation. Si $u \in L(E, F)$ et $x = (x_i)_{i \in I} \in E^I$, on notera $(u(x_i))_{i \in I} = u(x)$.

Propriété. Avec cette notation, $\Psi_{u(x)} = u \circ \Psi_x$.

Théorème.

- L'image d'une famille libre par une injection linéaire est une famille libre.
- L'image d'une famille génératrice par une surjection linéaire est génératrice.
- L'image d'une base par un isomorphisme est une base.

Il faut savoir le démontrer.

Théorème. Deux espaces de dimensions finies ont la même dimension si et seulement si ils sont isomorphes.

Il faut savoir le démontrer.

Propriété. Soit E et F deux espaces de dimensions finies et soit $f \in L(E, F)$.

Si f est injective, alors $\dim(E) \leq \dim(F)$.

Si f est surjective, alors $\dim(E) \geq \dim(F)$.

Propriété. Soient E et F deux \mathbb{K} -espaces vectoriels de dimensions quelconques. Soient $u \in L(E, F)$ et G un sous-espace vectoriel de E de dimension finie. Alors $u(G)$ est de dimension finie et $\dim(u(G)) \leq \dim(G)$, avec égalité lorsque u est injective.

Propriété. L'image d'une famille génératrice par une application linéaire u engendre $\text{Im}(u)$.

Propriété. L'image d'une famille liée par une application linéaire est liée.

Théorème.

On suppose que E est un \mathbb{K} -espace vectoriel admettant une base $e = (e_i)_{i \in I}$.

Soit $f = (f_i)_{i \in I}$ une famille quelconque de vecteurs d'un second \mathbb{K} -espace vectoriel F .

Il existe une unique application linéaire $u \in L(E, F)$ telle que, $\forall i \in I$ $u(e_i) = f_i$.

De plus, $(f_i)_{i \in I}$ est $\begin{cases} \text{libre} \\ \text{génératrice} \\ \text{une base} \end{cases}$ si et seulement si u est $\begin{cases} \text{injective} \\ \text{surjective} \\ \text{bijective} \end{cases}$.

Il faut savoir le démontrer.

Corollaire.

Soit E et F deux espaces vectoriels de dimensions finies et soit $u \in L(E, F)$.

Si $\dim(E) = \dim(F)$, alors u injective $\iff u$ surjective $\iff u$ bijective.

Exercice. Soit $u \in L(\mathbb{K}[X])$ tel que pour tout $P \in \mathbb{K}[X]$, $\deg(u(P)) = \deg(P)$. Montrer que u est un automorphisme sur $\mathbb{K}[X]$.

Il faut savoir le démontrer.

Propriété. Soit E un \mathbb{K} -espace vectoriel de dimension finie et $u \in L(E)$. Alors

u inversible dans $L(E)$ $\iff u$ inversible à droite dans $L(E)$
 $\iff u$ inversible à gauche dans $L(E)$.

Corollaire. Soit $A \in \mathcal{M}_n(\mathbb{K})$. Alors

$$\begin{aligned} A \text{ inversible dans } \mathcal{M}_n(\mathbb{K}) &\iff A \text{ inversible à droite dans } \mathcal{M}_n(\mathbb{K}) \\ &\iff A \text{ inversible à gauche dans } \mathcal{M}_n(\mathbb{K}). \end{aligned}$$

Exercice. Soit A une \mathbb{K} -algèbre et B une sous-algèbre de A de dimension finie. Soit $b \in B$. Montrer que si b est inversible dans A , alors $b^{-1} \in B$.

Il faut savoir le démontrer.

Propriété. Soit $A \in \mathcal{M}_n(\mathbb{K})$ une matrice triangulaire supérieure, dont la diagonale est notée (a_1, \dots, a_n) . Alors A est inversible si et seulement si pour tout $i \in \{1, \dots, n\}$, $a_i \neq 0$, et dans ce cas, A^{-1} est encore triangulaire supérieure et sa diagonale est $\left(\frac{1}{a_1}, \dots, \frac{1}{a_n}\right)$.

Propriété. Si E admet une base $(e_i)_{i \in I}$, alors $L(E, F)$ est isomorphe à F^I .

Il faut savoir le démontrer.

Théorème. $\dim(L(E, F)) = \dim(E) \times \dim(F)$.

2.7 Rang d'une famille de vecteurs

Définition. Soient E un espace vectoriel et x une famille de vecteurs de E .

Le rang de x est $\text{rg}(x) \triangleq \dim(\text{Vect}(x)) \in \mathbb{N} \cup \{+\infty\}$.

Propriété. Pour une famille x de vecteurs d'un \mathbb{K} -espace vectoriel E ,

- $\text{rg}(x) \leq \#(x)$. Lorsque $\text{rg}(x) < +\infty$, il y a égalité si et seulement si x est libre.
- $\text{rg}(x) \leq \dim(E)$. Lorsque $\text{rg}(x) < +\infty$, il y a égalité si et seulement si x est génératrice.

Propriété.

Soit $u \in L(E, F)$ et x une famille de vecteurs de E .

Alors $\text{rg}(u(x)) \leq \text{rg}(x)$, avec égalité lorsque $\text{rg}(x) < +\infty$ et u injective.

Il faut savoir le démontrer.

Propriété. Soit $(x_i)_{i \in I}$ une famille de vecteurs d'un \mathbb{K} -espace vectoriel E . Alors $\text{rg}(x_i)_{i \in I}$ n'est pas modifié si l'on échange l'ordre de deux vecteurs, si l'on multiplie l'un des vecteurs x_i par un scalaire non nul, ou bien si l'on ajoute à l'un des x_i une combinaison linéaire des autres x_j .

2.8 Matrice d'une application linéaire

Définition. Soient E et F deux \mathbb{K} -espaces vectoriels de dimensions respectives $p > 0$ et $n > 0$. Soient $e = (e_1, \dots, e_p)$ une base de E et $f = (f_1, \dots, f_n)$ une base de F . Si $u \in L(E, F)$, on appelle **matrice de l'application linéaire** u dans les bases e et f la matrice notée $\text{mat}(u, e, f) = (\alpha_{i,j}) \in \mathcal{M}_{\mathbb{K}}(n, p)$ définie par l'une des conditions équivalentes suivantes :

- pour tout $i \in \mathbb{N}_n$ et $j \in \mathbb{N}_p$, $\alpha_{i,j}$ est la $i^{\text{ème}}$ coordonnée du vecteur $u(e_j)$ dans la base f .
- pour tout $i \in \mathbb{N}_n$ et $j \in \mathbb{N}_p$, $[\text{mat}(u, e, f)]_{i,j} = f_i^*(u(e_j))$.
- $\text{mat}(u, e, f)$ est l'unique matrice $(\alpha_{i,j}) \in \mathcal{M}_{\mathbb{K}}(n, p)$ vérifiant : $\forall j \in \mathbb{N}_p \quad u(e_j) = \sum_{i=1}^n \alpha_{i,j} f_i$.
- $\text{mat}(u, e, f)$ est l'unique matrice dont la j -ème colonne, égale à $\Psi_f^{-1}(u(e_j))$, contient les coordonnées de $u(e_j)$ dans la base f .

Interprétation tabulaire : Avec les notations précédentes,

$$\text{mat}(u, e, f) = \begin{pmatrix} u(e_1) & \cdots & u(e_p) \\ m_{1,1} & \cdots & m_{1,p} \\ \vdots & & \vdots \\ m_{n,1} & \cdots & m_{n,p} \end{pmatrix} \begin{matrix} f_1 \\ \vdots \\ f_n \end{matrix}.$$

Notation. Lorsque $E = F$ et que l'on choisit $e = f$, on note $\text{mat}(u, e)$ au lieu de $\text{mat}(u, e, e)$.

Propriété. Pour tout $n, p \in \mathbb{N}^*$, pour tout $M \in \mathcal{M}_{\mathbb{K}}(n, p)$, $\boxed{\text{mat}(\tilde{M}, c, c') = M}$, en notant c et c' les bases canoniques de \mathbb{K}^p et de \mathbb{K}^n .

Remarque. Nous disposons maintenant de deux manières équivalentes de définir l'application linéaire canoniquement associée à une matrice $M \in \mathcal{M}_{\mathbb{K}}(n, p)$: c'est l'application $\tilde{M} : \mathbb{K}^p \rightarrow \mathbb{K}^n$ $X \mapsto \tilde{M}(X) = MX$, ou bien c'est l'unique application $\tilde{M} \in L(\mathbb{K}^p, \mathbb{K}^n)$ telle que $\text{mat}(\tilde{M}, c, c') = M$.

Propriété. Soient E et F deux \mathbb{K} -espaces vectoriels de dimensions respectives $p > 0$ et $n > 0$. Soient $e = (e_1, \dots, e_p)$ une base de E et $f = (f_1, \dots, f_n)$ une base de F .

L'application $L(E, F) \rightarrow \mathcal{M}_{\mathbb{K}}(n, p)$ $u \mapsto \text{mat}(u, e, f)$ est un isomorphisme d'espaces vectoriels.

Théorème. Soient E, F et G trois \mathbb{K} -espaces vectoriels de dimensions finies, munis de bases e, f et g . Soient $u \in L(E, F)$ et $v \in L(F, G)$. Alors, $\text{mat}(v \circ u, e, g) = \text{mat}(v, f, g) \times \text{mat}(u, e, f)$.

Il faut savoir le démontrer.

Propriété. Soient E et F deux \mathbb{K} -espaces vectoriels de dimensions respectives $p > 0$ et $n > 0$, munis des bases $e = (e_1, \dots, e_p)$ et $f = (f_1, \dots, f_n)$, et soit $u \in L(E, F)$.

On note M la matrice de u dans les bases e et f .

Soit $(x, y) \in E \times F$. On note X la matrice colonne des coordonnées de x dans la base e , et Y celle des coordonnées de y dans la base f . Alors,

$$\boxed{u(x) = y \iff MX = Y.}$$

Propriété. On reprend les notations précédentes. Lorsque $n = p$, u est un isomorphisme si et seulement si M est une matrice inversible et dans ce cas, $\text{mat}(u, e, f)^{-1} = \text{mat}(u^{-1}, f, e)$.

Propriété. Soit E un \mathbb{K} -espace vectoriel de dimension finie égale à n , muni d'une base e . L'application $L(E) \rightarrow \mathcal{M}_n(\mathbb{K})$ $u \mapsto \text{mat}(u, e)$ est un isomorphisme d'algèbres.

3 Les systèmes linéaires

3.1 Trois interprétations d'un système linéaire

Définition. Une équation linéaire à p inconnues scalaires est une équation de la forme

$(E) : \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_p x_p = b$, où $\alpha_1, \dots, \alpha_p, b \in \mathbb{K}$ sont des paramètres, et où $x_1, \dots, x_p \in \mathbb{K}$ sont les inconnues.

Notation. Fixons $(n, p) \in \mathbb{N}^{*2}$ et considérons un système linéaire à n équations et p inconnues, c'est-à-dire un système d'équations de la forme suivante :

$$(S) : \begin{cases} \alpha_{1,1}x_1 + \dots + \alpha_{1,p}x_p = b_1 \\ \vdots \\ \alpha_{i,1}x_1 + \dots + \alpha_{i,p}x_p = b_i \\ \vdots \\ \alpha_{n,1}x_1 + \dots + \alpha_{n,p}x_p = b_n \end{cases},$$

où, pour tout $(i, j) \in \{1, \dots, n\} \times \{1, \dots, p\}$, $\alpha_{i,j} \in \mathbb{K}$, pour tout $i \in \{1, \dots, n\}$, $b_i \in \mathbb{K}$, les p inconnues étant x_1, \dots, x_p , éléments de \mathbb{K} .

Le vecteur $\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ est appelé le second membre du système, ou bien le membre constant. Lorsqu'il est nul, on dit que le système est homogène.

Première interprétation. *Combinaison linéaire de vecteurs.*

Notons $C_1 = \begin{pmatrix} \alpha_{1,1} \\ \vdots \\ \alpha_{i,1} \\ \vdots \\ \alpha_{n,1} \end{pmatrix}$, $C_2 = \begin{pmatrix} \alpha_{1,2} \\ \vdots \\ \alpha_{i,2} \\ \vdots \\ \alpha_{n,2} \end{pmatrix}$, ..., $C_p = \begin{pmatrix} \alpha_{1,p} \\ \vdots \\ \alpha_{i,p} \\ \vdots \\ \alpha_{n,p} \end{pmatrix}$, et $B = \begin{pmatrix} b_1 \\ \vdots \\ b_i \\ \vdots \\ b_n \end{pmatrix}$. Il s'agit de $p+1$ vecteurs de \mathbb{K}^n . Alors $(S) \iff x_1 C_1 + x_2 C_2 + \dots + x_p C_p = B$.

Définition. On dit que (S) est **compatible** si et seulement s'il admet au moins une solution.

Propriété. (S) est compatible si et seulement si $B \in \text{Vect}(C_1, \dots, C_p)$.

Deuxième interprétation. *Matricielle.* Notons M la matrice de $\mathcal{M}_{n,p}(\mathbb{K})$ dont les colonnes sont

C_1, \dots, C_p , et $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$. Alors $(S) \iff MX = B$.

Définition. On dit que (S) est un **système de Cramer** si et seulement si $n = p$ et si M est inversible. Dans ce cas, (S) admet une unique solution.

Troisième interprétation. *A l'aide d'une application linéaire.*

Soient E et F des \mathbb{K} -espaces vectoriels de dimensions p et n munis de bases

$e = (e_1, \dots, e_p)$ et $f = (f_1, \dots, f_n)$. On note u l'unique application linéaire de $L(E, F)$ telle que $\text{mat}(u, e, f) = M$, x le vecteur de E dont les coordonnées dans e sont X et b le vecteur de F dont les coordonnées dans f sont B . Alors $(S) \iff u(x) = b$.

Définition. On dit que (S) est un **système homogène** si et seulement si $b = 0$.

Définition. Le système homogène associé à (S) est $(S_H) : u(x) = 0$.

Propriété. L'ensemble des solutions de (S_H) est $\text{Ker}(u)$.

C'est un sous-espace vectoriel de dimension $p - r$, où r désigne le rang de u (ou de M).

3.2 Les opérations élémentaires

Définition. On appelle manipulations ou opérations élémentaires sur les lignes d'une matrice, les applications de $\mathcal{M}_{\mathbb{K}}(n, p)$ dans $\mathcal{M}_{\mathbb{K}}(n, p)$ suivantes :

- 1) Ajouter à une ligne le multiple d'une autre, opération notée : $L_i \longleftarrow L_i + \lambda L_j$, où $i \neq j$ et $\lambda \in \mathbb{K}$. C'est une transvection.
- 2) Multiplier une ligne par un scalaire non nul, notée : $L_i \longleftarrow \alpha L_i$, où $\alpha \in \mathbb{K}^*$. C'est une affinité.
- 3) Permuter deux lignes, notée : $L_i \longleftrightarrow L_j$, où $i \neq j$. C'est une transposition.

On définirait de même les opérations sur les colonnes.

Propriété. Si $\sigma \in \mathcal{S}_n$, on note $P_\sigma = (\delta_{i, \sigma(j)}) \in \mathcal{M}_n(\mathbb{K})$. Alors $P_{\sigma\sigma'} = P_\sigma P_{\sigma'}$.

Il faut savoir le démontrer.

Propriété.

En notant $(E_{i,j})_{(i,j) \in \{1, \dots, n\}^2}$ la base canonique de $\mathcal{M}_n(\mathbb{K})$, si $\lambda \in \mathbb{K}^*$ et $(i, j) \in \{1, \dots, n\}^2$ avec $i \neq j$,

$$\begin{array}{ccc} L_i \leftarrow L_i + \lambda L_j : & \mathcal{M}_{\mathbb{K}}(n, p) & \longrightarrow \\ & M & \longmapsto \end{array} \quad \begin{array}{c} \mathcal{M}_{\mathbb{K}}(n, p) \\ (I_n + \lambda E_{i,j})M \end{array}$$

$$\begin{array}{ccc} L_i \leftarrow \lambda L_i : & \mathcal{M}_{\mathbb{K}}(n, p) & \longrightarrow \\ & M & \longmapsto \end{array} \quad \begin{array}{c} \mathcal{M}_{\mathbb{K}}(n, p) \\ (I_n + (\lambda - 1)E_{i,i})M \end{array}$$

$$\begin{array}{ccc} L_i \longleftrightarrow L_j : & \mathcal{M}_{\mathbb{K}}(n, p) & \longrightarrow \\ & M & \longmapsto \end{array} \quad \begin{array}{c} \mathcal{M}_{\mathbb{K}}(n, p) \\ P_{(i,j)}M \end{array}$$

De même, en notant $(E_{i,j})_{(i,j) \in \{1, \dots, p\}^2}$ la base canonique de $\mathcal{M}_p(\mathbb{K})$, si $\lambda \in \mathbb{K}^*$ et $(i, j) \in \{1, \dots, p\}^2$ avec $i \neq j$, alors

$$\begin{array}{ccc} C_i \leftarrow C_i + \lambda C_j : & \mathcal{M}_{\mathbb{K}}(n, p) & \longrightarrow \\ & M & \longmapsto \end{array} \quad \begin{array}{c} \mathcal{M}_{\mathbb{K}}(n, p) \\ M(I_p + \lambda E_{j,i}) \end{array}$$

$$\begin{array}{ccc} C_i \leftarrow \lambda C_i : & \mathcal{M}_{\mathbb{K}}(n, p) & \longrightarrow \\ & M & \longmapsto \end{array} \quad \begin{array}{c} \mathcal{M}_{\mathbb{K}}(n, p) \\ M(I_p + (\lambda - 1)E_{i,i}) \end{array} \quad .$$

$$\begin{array}{ccc} C_i \longleftrightarrow C_j : & \mathcal{M}_{\mathbb{K}}(n, p) & \longrightarrow \\ & M & \longmapsto \end{array} \quad \begin{array}{c} \mathcal{M}_{\mathbb{K}}(n, p) \\ MP_{(i,j)} \end{array}$$

Il faut savoir le démontrer.

Propriété. Si l'on effectue une série d'opérations élémentaires sur les lignes d'une matrice M , alors on a multiplié M à gauche par une certaine matrice inversible.

Si l'on effectue une série d'opérations élémentaires sur les colonnes d'une matrice M , alors on a multiplié M à droite par une certaine matrice inversible.

Notation. Soit $(S) : MX = B$ un système linéaire de matrice $M \in \mathcal{M}_{n,p}(\mathbb{K})$ et de vecteur constant $B \in \mathbb{K}^n$. On appellera matrice globale de (S) la matrice à n lignes et $p+1$ colonnes dont les p premières colonnes sont celles de M et dont la dernière colonne est égale à B .

Propriété. Soient $(S) : MX = B$ et $(S') : M'X = B'$. On suppose que l'on peut passer de la matrice globale de (S) à celle de (S') à l'aide d'une série d'opérations élémentaires portant uniquement sur les lignes. Alors ces deux systèmes sont équivalents.

Propriété. Soit $M \in \mathcal{M}_n(\mathbb{K})$. On suppose que l'on peut transformer, par des opérations élémentaires portant uniquement sur les lignes, la matrice blocs $\begin{bmatrix} M & I_n \end{bmatrix} \in \mathcal{M}_{\mathbb{K}}(n, 2n)$ en une matrice de la forme $\begin{bmatrix} I_n & N \end{bmatrix} \in \mathcal{M}_{\mathbb{K}}(n, 2n)$. Alors M est inversible et $M^{-1} = N$.

Il faut savoir le démontrer.

3.3 Méthode du pivot de Gauss

Notation. On souhaite résoudre le système $(S) : MX = B$ de n équations à p inconnues. La matrice globale du système sera notée $(a_{i,j}) \in \mathcal{M}_{\mathbb{K}}(n, p+1)$. Pour simplifier les notations, si on transforme $(a_{i,j})$ par des opérations élémentaires, le résultat sera encore noté $(a_{i,j})$.

But : Transformer $(a_{i,j})$ de sorte que : $\forall (i, j) \in \{1, \dots, n\} \times \{1, \dots, p\} \quad i > j \implies a_{i,j} = 0$.

Pour cela, si l'on suppose que les $r-1$ premières colonnes de $(a_{i,j})$ sont déjà bien formées :

Premier cas : $\forall i \in \{r, \dots, n\} \quad a_{i,r} = 0$: on passe à l'étape suivante.

Second cas : $\exists i_0 \in \{r, \dots, n\} \quad a_{i_0,r} \neq 0$: On dit que $a_{i_0,r}$ est le pivot de l'étape r .

On permute d'abord les lignes L_{i_0} et L_r . Ainsi $a_{r,r} \neq 0$. Ensuite on effectue la série d'opérations élémentaires : for i from $r+1$ to n do $L_i \leftarrow L_i - \frac{a_{i,r}}{a_{r,r}} L_r$ od.

Il faut être capable de présenter cet algorithme en détails.

Remarque. Comme on n'effectue que des opérations élémentaires sur les lignes, les lignes de la matrice finale du système engendrent le même espace vectoriel que les lignes de la matrice initiale. La

méthode du pivot permet donc de déterminer une base de l'espace vectoriel engendré par les lignes (ou les colonnes en opérant sur les colonnes) d'une matrice.

La méthode du pivot permet aussi de déterminer une base de l'image d'une application linéaire : On considère sa matrice dans des bases données et on détermine une base de ses vecteurs colonnes en appliquant la méthode du pivot au niveau des colonnes.

3.4 Méthode du pivot total

But : Transformer $(a_{i,j})$ de sorte qu'il existe $s \in \{0, \min(n, p)\}$ vérifiant

$$\forall (i, j) \in \mathbb{N}_s^2, i > j \implies a_{i,j} = 0, \forall r \in \mathbb{N}_s, a_{r,r} \neq 0 \text{ et } \forall (i, j) \in \{s+1, \dots, n\} \times \{1, \dots, p\}, a_{i,j} = 0.$$

La seule différence par rapport à l'algorithme précédent est qu'on accepte de choisir le pivot de l'étape r parmi les $a_{i,j}$ pour $(i, j) \in \{r, \dots, n\} \times \{r, \dots, p\}$. Notons $a_{i_0, j_0} \neq 0$ le pivot choisi. On échange C_r et C_{j_0} puis on applique les mêmes opérations élémentaires que dans l'algorithme précédent.

◇ À la fin de l'algorithme, le système est compatible si et seulement si $\forall i \in \{s+1, \dots, n\} \quad a_{i, p+1} = 0$: c'est un système d'équations de l'espace vectoriel engendré par les colonnes de (S) .

Si la matrice de (S) est celle d'une application linéaire u dans des bases e et f , ces conditions de compatibilité constituent un système d'équations de $Im(u)$ dans la base f .

Définition. Résoudre un système $(S) : MX = B$ à n équations et p inconnues, c'est déterminer une partie I de $\{1, \dots, p\}$ et une famille $(b_{i,j})_{(i,j) \in (\{1, \dots, p\} \setminus I) \times I}$ telles que :

$$\forall i \in \{1, \dots, p\} \setminus I, x_i = c_i + \sum_{j \in I} b_{i,j} x_j. \text{ Les } (x_j)_{j \in I} \text{ sont les inconnues principales et les } (x_i)_{i \in \{1, \dots, p\} \setminus I}$$

sont les inconnues secondaires. En résumé, résoudre un système, c'est exprimer les inconnues secondaires en fonction des inconnues principales.

3.5 Méthode de Gauss-Jordan, lorsque le système est de Cramer

But : Transformer la matrice globale en une matrice dont les n premières colonnes correspondent à la matrice I_n , en utilisant uniquement des opérations élémentaires sur les lignes.

Pour cela, comme pour le pivot partiel, à l'étape r , on choisit un pivot $a_{i_0, r} \neq 0$ où $r \leq i_0 \leq n$, ce qui est possible car le système est de Cramer, puis on effectue : $L_{i_0} \longleftrightarrow L_r$,

$$\forall i \in \{1, \dots, n\} \setminus \{r\}, L_i \longleftarrow L_i - \frac{a_{i,r}}{a_{r,r}} L_r \text{ et } L_r \longleftarrow \frac{1}{a_{r,r}} L_r.$$

Il faut être capable de présenter cet algorithme en détails.

Corollaire. Une matrice de $\mathcal{M}_n(\mathbb{K})$ est inversible si et seulement si elle est le produit de matrices de transvections, d'affinités et de transpositions.

Semaine 30 (du 18 au 20 mai) : Résumé de cours

Somme de sous-espaces vectoriels

Notation. \mathbb{K} désigne un corps quelconque et E désigne un \mathbb{K} -espace vectoriel.

1 Sommes et sommes directes

Définition. Si $E_i = \text{sev de } E$, $E_1 + \cdots + E_k = \text{Vect} \left(\bigcup_{i=1}^k E_i \right)$.

Propriété. $E_1 + \cdots + E_k = \left\{ \sum_{i=1}^k x_i \mid \forall i \in \{1, \dots, k\} \quad x_i \in E_i \right\}$.

Définition. $\sum_{i=1}^k E_i$ est *directe*, et alors notée $\bigoplus_{1 \leq i \leq k} E_i$, si et seulement si

$$\forall (x_1, \dots, x_k) \in E_1 \times \cdots \times E_k \quad \left(\sum_{i=1}^k x_i = 0 \implies (\forall i \in \{1, \dots, k\} \quad x_i = 0) \right),$$

ce qui est équivalent à : $\forall x \in \sum_{i=1}^k E_i$, $\exists! (x_1, \dots, x_k) \in E_1 \times \cdots \times E_k \quad x = \sum_{i=1}^k x_i$.

2 Supplémentaires d'un sous-espace vectoriel

Propriété. $F + G$ est directe si et seulement si $F \cap G = \{0\}$.

Propriété. Si $x \notin F$, F et $\mathbb{K}x$ sont en somme directe.
Deux droites vectorielles distinctes sont en somme directe.

Définition. Deux sous-espaces vectoriels F et G de E sont *supplémentaires* (dans E) si et seulement si $E = F \oplus G$, i.e $E = F + G$ et $F \cap G = \{0\}$, i.e $\forall x \in E$, $\exists! (x_1, x_2) \in F \times G$, $x = x_1 + x_2$.

Propriété. Soient E un \mathbb{K} -espace vectoriel de dimension finie et F un sous-espace vectoriel de E . F admet au moins un supplémentaire, et pour tout supplémentaire G de F , $\dim(F) + \dim(G) = \dim(E)$.

Remarque. En dimension quelconque, tout sous-espace vectoriel de E possède au moins un supplémentaire, si l'on accepte l'axiome du choix.

Propriété. $\mathcal{M}_n(\mathbb{K}) = \mathcal{S}_n(\mathbb{K}) \oplus \mathcal{A}_n(\mathbb{K}) : \forall M \in \mathcal{M}_n(\mathbb{K}), \quad M = \frac{1}{2}(M + {}^t M) + \frac{1}{2}(M - {}^t M)$.

De plus $\dim(\mathcal{S}_n(\mathbb{K})) = \frac{n(n+1)}{2}$ et $\dim(\mathcal{A}_n(\mathbb{K})) = \frac{n(n-1)}{2}$.

Il faut savoir le démontrer.

3 Rang d'une application linéaire

Théorème. Soit $u \in L(E, F)$.

Si H est un supplémentaire de $\text{Ker}(u)$ dans E , alors $u|_H^{\text{Im}(u)}$ est un isomorphisme.

Il faut savoir le démontrer.

Définition. $\text{rg}(u) = \dim(\text{Im}(u)) \in \mathbb{N} \cup \{+\infty\}$: il s'agit du rang de l'application linéaire u .

Propriété. Si e est une base de E et $u \in L(E, F)$, alors $\text{rg}(u) = \text{rg}(u(e))$.

Formule du rang. Soit $u \in L(E, F)$ avec E de dimension finie.

Alors $\text{rg}(u)$ est fini et $\boxed{\dim(\text{Im}(u)) + \dim(\text{Ker}(u)) = \dim(E)}$.

Propriété. Si $u \in L(E, F)$, alors $\text{rg}(u) \leq \min(\dim(E), \dim(F))$. De plus, lorsque E est de dimension finie, $\text{rg}(u) = \dim(E)$ si et seulement si u est injective et lorsque F est de dimension finie, $\text{rg}(u) = \dim(F)$ si et seulement si u est surjective.

Théorème. $\text{rg}(v \circ u) \leq \inf(\text{rg}(u), \text{rg}(v))$.

On ne modifie par le rang d'une application linéaire en la composant avec un isomorphisme (à sa gauche ou à sa droite).

Définition. Si $M \in \mathcal{M}_{\mathbb{K}}(n, p)$, le rang de M est $\text{rg}(M) \triangleq \text{rg}(\tilde{M}) = \dim(\text{Im}(M))$.

Le rang d'une matrice est aussi le rang de la famille de ses vecteurs colonnes.

Propriété. $\text{rg}(\text{mat}(u, e, f)) = \text{rg}(u)$.

Il faut savoir le démontrer.

Propriété. $M \in \mathcal{M}_n(\mathbb{K})$ est inversible si et seulement si $\text{rg}(M) = n$.

Propriété. Soit $(A, B) \in \mathcal{M}_{\mathbb{K}}(n, p) \times \mathcal{M}_{\mathbb{K}}(p, q)$. Alors, $\text{rg}(AB) \leq \min(\text{rg}(A), \text{rg}(B))$.

On ne modifie pas le rang d'une matrice en la multipliant par une matrice inversible.

4 Propriétés des sommes directes

4.1 Un moyen de définir une application linéaire

Théorème. Soit $(E_i)_{1 \leq i \leq k}$ une famille de k sous-espaces vectoriels de E telle que $E = \bigoplus_{1 \leq i \leq k} E_i$. Soit

F un \mathbb{K} -espace vectoriel et, pour tout $i \in \{1, \dots, k\}$, soit u_i une application linéaire de E_i dans F .

Il existe une unique application linéaire u de E dans F telle que, pour tout $i \in \{1, \dots, k\}$, la restriction de u à E_i est égale à u_i . Ainsi, pour définir une application linéaire u de E dans F , il suffit de préciser ses restrictions aux sous-espaces vectoriels E_i .

4.2 Formules dimensionnelles

Propriété. $\dim\left(\sum_{i=1}^k E_i\right) \leq \sum_{i=1}^k \dim(E_i)$, $\boxed{\text{avec égalité si et seulement si la somme est directe}}$.

Il faut savoir le démontrer.

Remarque. Ainsi, lorsque E est de dimension finie, si F et G sont deux sous-espaces vectoriels de E , ils sont supplémentaires dans E si et seulement si $E = F + G$ et $\dim(E) = \dim(F) + \dim(G)$.

Formule de Grassmann : $\dim(F + G) = \dim(F) + \dim(G) - \dim(F \cap G)$.

Il faut savoir le démontrer.

4.3 Associativité des sommes directes

Propriété. Associativité d'une somme directe. Si $(I_i)_{1 \leq i \leq p}$ est une partition de $\{1, \dots, k\}$, alors E_1, \dots, E_k forment une somme directe si et seulement si $\forall i \in \{1, \dots, p\}$, $(E_j)_{j \in I_i}$ forment une somme directe et $\left(\bigoplus_{j \in I_i} E_j\right)_{i \in \{1, \dots, p\}}$ forment une somme directe.

Théorème. Soient k un entier supérieur ou égal à 2, et $(E_i)_{1 \leq i \leq k}$ une famille de k sous-espaces vectoriels de E . E_1, \dots, E_k sont en somme directe si et seulement si $\forall i \in \{2, \dots, k\} \quad E_i \cap \sum_{j=1}^{i-1} E_j = \{0\}$.

Il faut savoir le démontrer.

4.4 Base adaptée à une décomposition en somme directe

Théorème. Soit E un \mathbb{K} -espace vectoriel muni d'une base $(e_i)_{i \in I}$. Soit $(I_k)_{1 \leq k \leq n}$ une partition de I . Pour tout $k \in \{1, \dots, n\}$, on pose $E_k = \text{Vect}(e_i)_{i \in I_k}$. Alors $E = \bigoplus_{k=1}^n E_k$.

Théorème réciproque. Soit $(E_k)_{1 \leq k \leq n}$ une famille de sous-espaces vectoriels d'un \mathbb{K} -espace vectoriel E tels que $E = \bigoplus_{k=1}^n E_k$. Pour tout $k \in \{1, \dots, n\}$, on suppose que E_k admet une base b_k . Alors la concaténation des bases $(b_k)_{1 \leq k \leq n}$, notée b , est une base de E . On dit que b est une **base adaptée à la décomposition en somme directe** $E = \bigoplus_{k=1}^n E_k$.

Définition. Lorsque F est un sous-espace vectoriel de E , on appelle **base de E adaptée à F** toute base obtenue en complétant une base de F .

5 Les projecteurs

Définition. $p \in L(E)$ est un **projecteur** si et seulement si $p^2 = p$.

Propriété. Soient F et G deux sous-espaces vectoriels supplémentaires de E . Pour $x \in E$, on note $(p(x), q(x))$ l'unique couple de $F \times G$ tel que $x = p(x) + q(x)$. p et q sont des projecteurs. p est appelé le projecteur sur F parallèlement à G , et q le **projecteur associé** à p . On vérifie que $p + q = Id_E$ et $pq = qp = 0$.

Il faut savoir le démontrer.

Propriété réciproque. Soit p un projecteur de E . Alors p est le projecteur sur $\text{Im}(p)$ parallèlement à $\text{Ker}(p)$. La décomposition de $x \in E$ selon la somme directe $E = \text{Im}(p) \oplus \text{Ker}(p)$ est $x = p(x) + (x - p(x))$, avec $p(x) \in F = \text{Im}(p)$ et $x - p(x) \in G = \text{Ker}(p)$.

Pour tout $x \in E$, $\boxed{x = p(x) \iff x \in F} : F = \text{Ker}(Id_E - p)$.

Il faut savoir le démontrer.

Définition. $s \in L(E)$ est une **symétrie** si et seulement si $s^2 = Id_E$.

Propriété. Soient F et G deux sous-espaces vectoriels supplémentaires de E . L'unique application s de E dans E telle que, pour tout $f, g \in F \times G$, $s(f+g) = f-g$ est une symétrie, appelée symétrie par rapport à F parallèlement à G . Si l'on note p le projecteur sur F parallèlement à G , et q le projecteur associé à p , alors $s = p - q = 2p - Id_E$.

Propriété réciproque. On suppose que $\text{car}(\mathbb{K}) \neq 2$.

Pour toute symétrie s de E , il existe deux sous-espaces vectoriels supplémentaires F et G tels que s est la symétrie par rapport à F parallèlement à G . Il s'agit de $F = \text{Ker}(Id_E - s)$ et de $G = \text{Ker}(Id_E + s)$.

6 Sous-espaces propres

Notation. On fixe un \mathbb{K} -espace vectoriel E et $u \in L(E)$.

Définition. $\lambda \in \mathbb{K}$ est une **valeur propre** de u si et seulement s'il existe un vecteur x *non nul* de E tel que $u(x) = \lambda x$. Dans ce cas, tout vecteur y *non nul* tel que $u(y) = \lambda y$ est appelé un **vecteur propre** de u associé à la valeur propre λ .

De plus, toujours lorsque λ est une valeur propre de u , $\text{Ker}(\lambda Id_E - u)$ est appelé le **sous-espace propre** de u associé à la valeur propre λ . Il est noté E_λ , ou E_λ^u en cas d'ambiguïté.

Remarque. Si λ est une valeur propre de u , l'ensemble des vecteurs propres de u pour la valeur propre λ est $E_\lambda \setminus \{0\}$.

Remarque. Même lorsque λ n'est pas une valeur propre de u , on note parfois $E_\lambda = \text{Ker}(\lambda Id_E - u)$, mais dans ce cas, $E_\lambda = \{0\}$.

Définition. Soient $n \in \mathbb{N}^*$ et $M \in \mathcal{M}_n(\mathbb{K})$: Les **éléments propres** de M (c'est-à-dire les valeurs propres, les vecteurs propres et les sous-espaces propres) sont les éléments propres de l'endomorphisme canoniquement associé à M .

Propriété.

$\lambda \in \mathbb{K}$ est une valeur propre de u si et seulement si $\lambda Id_E - u$ n'est pas injective.

En particulier, u est injectif si et seulement si 0 n'est pas une valeur propre de u .

Définition. On appelle **spectre** de u l'ensemble des valeurs propres de u . Il est noté $Sp(u)$.

Théorème.

La somme d'un nombre fini de sous-espaces propres de u est toujours directe.

Il faut savoir le démontrer.

Corollaire. Si $(x_i)_{i \in I}$ est une famille de vecteurs propres de u associés à des valeurs propres deux à deux distinctes, alors cette famille est libre.

Exemple. Supposons que $E \neq \{0\}$.

Soient F et G deux sous-espaces vectoriels supplémentaires non nuls dans E .

- Si u est une homothétie de rapport λ , où $\lambda \in \mathbb{K}$, $Sp(u) = \{\lambda\}$ et $E_\lambda = E$.
- Si u est le projecteur sur F parallèlement à G , $Sp(u) = \{0, 1\}$, $E_1 = F$ et $E_0 = G$.
- Si u est la symétrie par rapport à F parallèlement à G , $Sp(u) = \{1, -1\}$, $E_1 = F$ et $E_{-1} = G$.

Propriété.

Si $v \in L(E)$ commute avec u , les sous-espaces propres de u sont stables par v .

Il faut savoir le démontrer.

7 Changement de base

Notation. On fixe un \mathbb{K} -espace vectoriel E de dimension finie égale à $n \in \mathbb{N}^*$.

Propriété. Soit $e = (e_1, \dots, e_n)$ une base de E et $f = (f_j)_{1 \leq j \leq n} \in E^n$ une famille de n vecteurs de E . Pour tout $j \in \mathbb{N}_n$, on pose $p_{i,j} = e_i^*(f_j)$: c'est la $i^{\text{ème}}$ coordonnée dans la base e du $j^{\text{ème}}$ vecteur de la famille f . Alors f est une base si et seulement si la matrice $P = (p_{i,j})$ est inversible. Dans ce cas, P est noté P_e^f (ou bien $P_{e \rightarrow f}$) et on dit que $P_e^f = (p_{i,j})$ est la **matrice de passage** de la base e vers la base f .

Interprétation tabulaire : Avec les notations précédentes,

$$P_e^f = \begin{pmatrix} f_1 & \cdots & f_n \\ p_{1,1} & \cdots & p_{1,n} \\ \vdots & & \vdots \\ p_{n,1} & \cdots & p_{n,n} \end{pmatrix} \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}.$$

Remarque. Si $f = (f_j)_{1 \leq j \leq p}$ est une famille de p vecteurs de E , on pose $\text{mat}_e^f \triangleq (e_i^*(f_j))_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} \in \mathcal{M}_{n,p}(\mathbb{K})$. Alors $\text{rg}(\text{mat}_e^f) = \text{rg}(f)$.

Propriété. Soit e une base de E :

Pour toute matrice P inversible d'ordre n , il existe une unique base f de E telle que $P = P_e^f$.

Propriété. Soit e et e' deux bases de E . Alors $P_e^{e'} = \text{mat}(Id_E, e', e) = \text{mat}(Id_E)_e^{e'}$.

Il faut savoir le démontrer.

Formule de changement de base pour les vecteurs :

Soit e et e' deux bases de E . Soit $x \in E$. On pose $X \triangleq \text{mat}(x)_e$ le vecteur colonne des coordonnées de x dans la base e . De même on pose $X' = \text{mat}(x)_{e'}$.

Alors, $\boxed{X = P_e^{e'} X'}$, ou encore $\text{mat}(x)_e = P_e^{e'} \text{mat}(x)_{e'}$.

Il faut savoir le démontrer.

Formule. Si e, e' et e'' sont trois bases de E , $\boxed{P_e^{e''} = P_e^{e'} P_{e'}^{e''} \text{ et } (P_e^{e'})^{-1} = P_{e'}^e}$.

Formule de changement de bases pour les applications linéaires :

Soient E et F deux \mathbb{K} -espaces vectoriels de dimensions finies.

On suppose que e et e' sont deux bases de E et que f et f' sont deux bases de F .

Soit $u \in L(E, F)$. Notons $M = \text{mat}(u)_f^e$, $M' = \text{mat}(u)_{f'}^{e'}$, $P = P_e^{e'}$ et $Q = Q_f^{f'}$.

Alors, $\boxed{M' = Q^{-1} M P}$ c'est-à-dire $\boxed{\text{mat}(u)_{f'}^{e'} = P_{f'}^f \times \text{mat}(u)_f^e \times P_e^{e'}}$.

Il faut savoir le démontrer.

Formule de changement de bases pour les endomorphismes :

Soit E un \mathbb{K} -espace vectoriel de dimension finie et $u \in L(E)$. On suppose que e et e' sont deux bases de E . Notons $M = \text{mat}(u, e)$, $M' = \text{mat}(u, e')$ et $P = P_e^{e'}$. Alors, $\boxed{M' = P^{-1} M P}$.

Semaine 31 (du 25 au 30 mai) : Résumé de cours

Notation. \mathbb{K} désigne un corps quelconque.

1 Diagonalisation et trigonalisation

Définition. Soit E un \mathbb{K} -espace vectoriel de dimension $n \in \mathbb{N}^*$ et $u \in L(E)$.

On dit que u est **diagonalisable** si et seulement si il vérifie l'une des propriétés suivantes :

i) Il existe une base e de E telle que $\text{mat}(u, e)$ est diagonale.

ii) Il existe une base de E constituée de vecteurs propres de u .

iii) $E = \bigoplus_{\lambda \in \text{Sp}_{\mathbb{K}}(u)} E_{\lambda}^u$.

iv) $n = \sum_{\lambda \in \text{Sp}_{\mathbb{K}}(u)} \dim(E_{\lambda}^u)$.

Il faut savoir le démontrer.

Propriété. les homothéties, les projecteurs et les symétries sont diagonalisables.

Définition. Soit $M \in \mathcal{M}_n(\mathbb{K})$. On dit que M est diagonalisable si et seulement si son endomorphisme canoniquement associé est diagonalisable.

Propriété. $M \in \mathcal{M}_n(\mathbb{K})$ est diagonalisable si et seulement si il existe $P \in GL_n(\mathbb{K})$ telle que $P^{-1}MP$ est une matrice diagonale.

Il faut savoir le démontrer.

Définition. Soit $M \in \mathcal{M}_n(\mathbb{K})$ une matrice diagonalisable. “diagonaliser” M , c’est déterminer une matrice diagonale D et une matrice inversible P telles que $M = PDP^{-1}$.

Définition. Un endomorphisme u est **trigonalisable** si et seulement s’il existe une base dans laquelle la matrice de u est triangulaire supérieure.

Définition. $M \in \mathcal{M}_n(\mathbb{K})$ est trigonalisable si et seulement si l’endomorphisme canoniquement associé à M est trigonalisable, c’est-à-dire si et seulement si il existe $P \in GL_n(\mathbb{K})$ telle que $P^{-1}MP$ est triangulaire supérieure.

Définition. Soit $M \in \mathcal{M}_n(\mathbb{K})$. “**Trigonaliser**” M , c’est déterminer si M est trigonalisable, et dans ce cas, c’est calculer $P \in GL_n(\mathbb{K})$ et T triangulaire supérieure telles que $M = PTP^{-1}$.

2 Trace d'un endomorphisme

Définition.

Soit E un \mathbb{K} -espace vectoriel de dimension finie. La quantité $\text{Tr}(\text{mat}(u, e))$ ne dépend pas du choix de la base e de E . On la note $\text{Tr}(u)$. C’est la trace de l’endomorphisme u .

Propriété. Si $u, v \in L(E)$, alors $\text{Tr}(uv) = \text{Tr}(vu)$.

Propriété. Soit E un \mathbb{K} -espace vectoriel de dimension finie.

Si p est un projecteur de E , alors $\text{Tr}(p) = \text{rg}(p)$.

Il faut savoir le démontrer.

3 Matrices équivalentes et matrices semblables

3.1 Matrices équivalentes

Définition. Deux matrices M et M' de $\mathcal{M}_{\mathbb{K}}(n, p)$ sont *équivalentes* si et seulement s'il existe $P \in GL_p(\mathbb{K})$ et $Q \in GL_n(\mathbb{K})$ telles que $M' = QMP^{-1}$.

On définit ainsi une relation d'équivalence sur $\mathcal{M}_{\mathbb{K}}(n, p)$.

Propriété. Deux matrices sont équivalentes si et seulement si elles représentent une même application linéaire dans des bases différentes, autant pour la base de départ que pour la base d'arrivée.

Propriété. Deux matrices sont équivalentes si et seulement si il est possible de transformer l'une en l'autre par une succession d'opérations élémentaires portant sur les lignes ou sur les colonnes.

Il faut savoir le démontrer.

Théorème. Soient E et F deux \mathbb{K} -espaces vectoriels de dimensions respectives $p > 0$ et $n > 0$, et soit $u \in L(E, F)$. Notons r le rang de u . Il existe une base e de E et une base f de F telles que $\text{mat}(u, e, f)$ admet la décomposition en blocs suivante : $\text{mat}(u, e, f) = \begin{pmatrix} I_r & 0_{r, p-r} \\ 0_{n-r, r} & 0_{n-r, p-r} \end{pmatrix} \triangleq J_{n, p, r}$.

Il faut savoir le démontrer.

Propriété. Si $M \in \mathcal{M}_{\mathbb{K}}(n, p)$, M est équivalente à $J_{n, p, r}$, où r désigne le rang de M .

Corollaire. Deux matrices sont équivalentes si et seulement si elles ont le même rang.

Il faut savoir le démontrer.

3.2 Propriétés du rang d'une matrice

Propriété. Pour toute matrice $M \in \mathcal{M}_{\mathbb{K}}(n, p)$, $\text{rg}(M) = \text{rg}({}^t M)$.

On en déduit que le rang de M est aussi le rang de la famille de ses vecteurs lignes.

Il faut savoir le démontrer.

Propriété. Si l'on effectue une série de manipulations élémentaires sur une matrice, on ne modifie pas le rang de cette matrice.

Remarque. Pour déterminer le rang d'une matrice, une méthode consiste donc à transformer cette matrice en une matrice dont on connaît le rang par une succession d'opérations élémentaires portant sur les lignes ou sur les colonnes. On peut en particulier utiliser l'algorithme du pivot.

Propriété. Le rang d'une matrice est égal au nombre d'étapes dans la méthode du pivot global.

Propriété. Soit $M \in \mathcal{M}_{\mathbb{K}}(n, p)$. Si P est une matrice extraite de M , alors $\text{rg}(P) \leq \text{rg}(M)$.

Propriété. Soit $A \in \mathcal{M}_{\mathbb{K}}(n, p)$ une matrice non nulle.

$\text{rg}(A)$ est égal à la taille maximale des matrices inversibles extraites de A .

Il faut savoir le démontrer.

3.3 Matrices semblables

Définition. Deux matrices carrées M et M' dans $\mathcal{M}_n(\mathbb{K})$ sont **semblables** si et seulement s'il existe $P \in GL_n(\mathbb{K})$ tel que $M' = PMP^{-1}$. On définit ainsi une seconde relation d'équivalence sur $\mathcal{M}_n(\mathbb{K})$, appelée relation de similitude.

Propriété. Deux matrices sont semblables si et seulement si elles représentent un même endomorphisme dans des bases différentes, en imposant de prendre une même base au départ et à l'arrivée.

Propriété. Soient $(M, M') \in \mathcal{M}_n(\mathbb{K})^2$ et $P \in GL_n(\mathbb{K})$ tels que $M' = PMP^{-1}$. Alors, pour tout $n \in \mathbb{N}$, $M'^n = PM^nP^{-1}$ et pour tout $Q \in \mathbb{K}[X]$, $Q(M') = PQ(M)P^{-1}$. Si M' et M sont inversibles, pour tout $n \in \mathbb{Z}$, $M'^n = PM^nP^{-1}$.

4 Les hyperplans

Dans tout ce chapitre, on fixe un \mathbb{K} -espace vectoriel E , où \mathbb{K} est un corps.

4.1 En dimension quelconque

Définition. Soit H un sous-espace vectoriel de E . On dit que H est un hyperplan si et seulement si il existe une droite vectorielle D telle que $H \oplus D = E$.

Propriété. Soit H un hyperplan et D une droite non incluse dans H . Alors $H \oplus D = E$.

Il faut savoir le démontrer.

Propriété. Soit H une partie de E . H est un hyperplan de E si et seulement si il est le noyau d'une forme linéaire non nulle. De plus, si $H = \text{Ker}(\varphi) = \text{Ker}(\psi)$, alors φ et ψ sont colinéaires.

Il faut savoir le démontrer.

Définition. Soient H un hyperplan de E et $\varphi \in L(E, \mathbb{K}) \setminus \{0\}$ tel que $H = \text{Ker}(\varphi)$.

Alors $x \in H \iff [(\varphi) : \varphi(x) = 0]$. On dit que (φ) est **équation de H** .

4.2 En dimension finie

Notation. On suppose que E est un espace de dimension finie notée n , avec $n > 0$.

Si $e = (e_1, \dots, e_n)$ est une base de E , pour tout $i \in \{1, \dots, n\}$, on note e_i^* l'application qui associe à tout vecteur x de E sa $i^{\text{ème}}$ coordonnée dans la base e .

Propriété. Avec les notations précédentes, la famille $e^* = (e_i^*)_{1 \leq i \leq n}$ est une base de $L(E, \mathbb{K}) = E^*$, que l'on appelle la base duale de e .

Il faut savoir le démontrer.

Remarque. Les hyperplans de E sont les sous-espaces vectoriels de E de dimension $n - 1$.

Définition. Soit $e = (e_1, \dots, e_n)$ une base de E et H un hyperplan de E .

Si $H = \text{Ker}(\psi)$, où $\psi \in E^*$, en notant $\psi = \sum_{i=1}^n \alpha_i e_i^*$, l'équation de l'hyperplan H devient

$$x = \sum_{i=1}^n x_i e_i \in H \iff \sum_{i=1}^n \alpha_i x_i = 0 : \text{c'est une équation cartésienne de } H.$$

Exemple. Dans un plan vectoriel rapporté à une base (\vec{i}, \vec{j}) , une droite vectorielle D a une équation cartésienne de la forme : $\vec{v} = x\vec{i} + y\vec{j} \in D \iff ax + by = 0$, où $(a, b) \in \mathbb{R}^2 \setminus \{0\}$.

Exemple. Dans un espace vectoriel de dimension 3 rapporté à une base $(\vec{i}, \vec{j}, \vec{k})$, un plan vectoriel P a une équation cartésienne de la forme : $\vec{v} = x\vec{i} + y\vec{j} + z\vec{k} \in P \iff ax + by + cz = 0$, où $(a, b, c) \in \mathbb{R}^3 \setminus \{0\}$.

4.3 Les hyperplans affines

Notation. Soit \mathcal{E} un espace affine de direction E . On fixe un point $O \in \mathcal{E}$.

Définition. Un hyperplan affine est un sous-espace affine dirigé par un hyperplan de E .

Propriété. Soit \mathcal{H} une partie de \mathcal{E} . \mathcal{H} est un hyperplan affine de \mathcal{E} si et seulement si il existe $\varphi \in L(E, \mathbb{K}) \setminus \{0\}$ et $a \in \mathbb{K}$ tel que, pour tout $M \in \mathcal{E}$, $[M \in \mathcal{H} \iff \varphi(\overrightarrow{OM}) = a]$.

Dans ce cas, la condition $\varphi(\overrightarrow{OM}) = a$ est appelée une équation de \mathcal{H} .

De plus, la direction de \mathcal{H} est l'hyperplan $\text{Ker}(\varphi)$, d'équation $\varphi(x) = 0$ en l'inconnue $x \in E$.

Il faut savoir le démontrer.

Remarque. Dans le cas particulier où $\mathcal{E} = E$ et où $O = \vec{0}$, l'équation devient $\varphi(M) = a$, donc les hyperplans affines de E sont exactement les $\varphi^{-1}(\{a\})$, avec $\varphi \in L(E, \mathbb{K}) \setminus \{0\}$ et $a \in \mathbb{K}$.

Propriété. Supposons que E est de dimension finie égale à $n \in \mathbb{N}^*$ et que E est muni d'une base $e = (e_1, \dots, e_n)$, dont la base duale est notée $e^* = (e_1^*, \dots, e_n^*)$. Soit \mathcal{H} un hyperplan affine de \mathcal{E} , dont une équation est $\Psi(\overrightarrow{OM}) = a$. Notons $(\alpha_1, \dots, \alpha_n)$ les coordonnées de Ψ dans e^* . Si M a pour

coordonnées (x_1, \dots, x_n) dans le **repère affine** (O, e) , alors $M \in \mathcal{H} \iff \sum_{i=1}^n \alpha_i x_i = a$.

C'est la forme générale d'une équation cartésienne d'hyperplan affine en dimension n .

4.4 Application aux systèmes linéaires

Notation. On fixe $(n, p) \in \mathbb{N}^{*2}$ et on considère un système linéaire de n équations à p inconnues de la forme : $\forall i \in \mathbb{N}_n, \sum_{j=1}^p \alpha_{i,j} x_j = b_i$, où, pour tout i, j , $\alpha_{i,j} \in \mathbb{K}$, pour tout i , $b_i \in \mathbb{K}$, les p inconnues étant x_1, \dots, x_p , éléments de \mathbb{K} .

Propriété. Notons M la matrice de (S) . Ainsi $(S) \iff MX = B$, où $B = (b_i) \in \mathbb{K}^n$.

Si (S) est compatible, l'ensemble des solutions de (S) est un sous-espace affine de \mathbb{K}^p dimension $p - r$, où r désigne le rang de M et dont la direction est $\text{Ker}(M)$.

Propriété. Soient E et F des \mathbb{K} -espaces vectoriels de dimensions p et n munis de bases $e = (e_1, \dots, e_p)$ et $f = (f_1, \dots, f_n)$. On note u l'unique application linéaire de $L(E, F)$ telle que $\text{mat}(u, e, f) = M$, x le vecteur de E dont les coordonnées dans e sont X et b le vecteur de F dont les coordonnées dans f sont B . Alors $(S) \iff u(x) = b$. Avec ces notations, l'ensemble des solutions de (S) est soit vide, soit un sous-espace affine de E de direction $\text{Ker}(u)$.

Quatrième interprétation d'un système linéaire : *A l'aide de formes linéaires.*

Notons $e^* = (e_1^*, \dots, e_p^*)$ la base duale de e . Pour tout $i \in \{1, \dots, n\}$, posons $l_i = \sum_{j=1}^p \alpha_{i,j} e_j^*$.

Les l_i sont des formes linéaires telles que $(S) \iff [\forall i \in \{1, \dots, n\} \ l_i(x) = b_i]$.

L'ensemble des solutions de (S) est $\bigcap_{i=1}^n l_i^{-1}(\{b_i\})$. C'est une intersection d'hyperplans affines.

Propriété. Si E est un \mathbb{K} -espace vectoriel de dimension p , l'intersection de r hyperplans vectoriels de E est un sous-espace vectoriel de dimension supérieure à $p - r$.

Réciproquement tout sous-espace vectoriel de E de dimension $p - r$ où $r \geq 1$ est une intersection de r hyperplans de E , donc est caractérisé par un système de r équations linéaires.

Il faut savoir le démontrer.

Propriété. Tout sous-espace affine de \mathcal{E} peut être caractérisé par un système d'équations linéaires. Tout sous-espace affine différent de \mathcal{E} est une intersection d'un nombre fini d'hyperplans affines.

5 Déterminants

Notation. \mathbb{K} désigne un corps quelconque.

5.1 Applications multilinéaires

Définition. Soient $p \in \mathbb{N}^*$ et (E_1, \dots, E_p) une famille de p \mathbb{K} -espaces vectoriels.

Soient F un \mathbb{K} -espace vectoriel et f une application de $E_1 \times \dots \times E_p$ dans F .

f est une **application p -linéaire** si et seulement si, pour tout $j \in \mathbb{N}_p$

et pour tout $(a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_p) \in E_1 \times \dots \times E_{j-1} \times E_{j+1} \times \dots \times E_p$,

l'application $\begin{matrix} E_j & \longrightarrow & F \\ x_j & \longmapsto & f(a_1, \dots, a_{j-1}, x_j, a_{j+1}, \dots, a_p) \end{matrix}$ est linéaire.

Définition. Une **application bilinéaire** est une application 2-linéaire.

Notation.

— $L_p(E_1, \dots, E_p; F)$ désigne l'ensemble des applications p -linéaires de $E_1 \times \dots \times E_p$ dans F .

C'est un sous-espace vectoriel de $\mathcal{F}(E_1 \times \dots \times E_p, F)$.

— On note $L_p(E, F) = L_p(\underbrace{E, \dots, E}_{p \text{ fois}}; F)$ et $L_p(E) = L_p(E, \mathbb{K})$.

Les éléments de $L_p(E)$ sont appelés des **formes p -linéaires** sur E .

Notation. On fixe $p \in \mathbb{N}^*$ et deux \mathbb{K} -espaces vectoriels E et F .

Propriété. Soit u_1, \dots, u_p p applications linéaires de E dans \mathbb{K} .

$$u : E^p \longrightarrow \mathbb{K}$$

Alors l'application $(x_1, \dots, x_p) \longmapsto \prod_{i=1}^p u_i(x_i)$ est une forme p -linéaire.

Définition. Soient $\sigma \in \mathcal{S}_p$ et $f \in L_p(E, F)$. On note $\sigma(f) :$

$$\begin{matrix} E^p & \longrightarrow & F \\ (x_1, \dots, x_p) & \longmapsto & f(x_{\sigma(1)}, \dots, x_{\sigma(p)}) \end{matrix}$$

Définition. Soit $f \in L_p(E, F)$. f est une application p -linéaire symétrique (resp : antisymétrique) si et seulement si pour tout $\sigma \in \mathcal{S}_p$, $\sigma(f) = f$ (resp : $\sigma(f) = \varepsilon(\sigma)f$, où $\varepsilon(\sigma)$ désigne la signature de la permutation σ).

Propriété. Soit $f \in L_p(E, F)$.

f est symétrique si et seulement si pour toute transposition τ de \mathcal{S}_p , $\tau(f) = f$.

f est antisymétrique si et seulement si pour toute transposition τ de \mathcal{S}_p , $\tau(f) = -f$.

Il faut savoir le démontrer.

Définition. Soit $f \in L_p(E, F)$. f est une **application p -linéaire alternée** si et seulement si elle annule tout p -uplet de vecteurs de E contenant au moins deux vecteurs égaux.

Propriété. Soit $f \in L_p(E, F)$.

Si f est alternée, alors elle est antisymétrique.

Lorsque $\text{car}(\mathbb{K}) \neq 2$, alternée \iff antisymétrique.

Il faut savoir le démontrer.

Propriété. $f \in L_p(E, F)$ est alternée si et seulement si pour tout $(x_1, \dots, x_p) \in E^p$, $f(x_1, \dots, x_p)$ ne varie pas lorsque l'on ajoute à l'un des x_i une combinaison linéaire des autres x_j , ou encore si et seulement si l'image par f de toute famille liée de vecteurs est nulle.

Corollaire. Si E est de dimension $n \in \mathbb{N}^*$ et si $p > n$, toute forme p -linéaire alternée sur E est nulle.

5.2 Les trois notions de déterminants

Au sein de ce paragraphe, E désignera un \mathbb{K} -espace vectoriel de dimension finie égale à n , avec $n > 0$.

5.2.1 Volume

Supposons temporairement que $\mathbb{K} = \mathbb{R}$. Pour tout $x = (x_1, \dots, x_n) \in E^n$, on note H_x l'hyperparallélépipède $H_x = \{\sum_{i=1}^n t_i x_i \mid t_1, \dots, t_n \in [0, 1]\}$.

Si vol est une application de E^n dans \mathbb{R} telle que, pour tout $x \in E^n$, $|\text{vol}(x)|$ représente le volume de H_x et le signe de $\text{vol}(x)$ représente l'orientation du n -uplet x , alors en imposant des contraintes raisonnables aux notions de volume et d'orientation, l'application vol est nécessairement une forme n -linéaire alternée.

5.2.2 Déterminant d'un système de n vecteurs

Notation. On note $A_n(E)$ l'ensemble des formes n -linéaires alternées.

Définition. Soit $e = (e_1, \dots, e_n)$ une base de E et $x = (x_1, \dots, x_n) \in E^n$.

Le **déterminant de x** dans la base e est le scalaire $\det_e(x_1, \dots, x_n) \triangleq \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \prod_{j=1}^n e_{\sigma(j)}^*(e_j)$.

Théorème. Soit e une base de E . Si f est une forme n -linéaire alternée sur E , alors $f = f(e) \det_e$.

Il faut savoir le démontrer.

Propriété. $\det_e(x_1, \dots, x_n) = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \prod_{j=1}^n e_{\sigma(j)}^*(e_j) = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \prod_{j=1}^n e_j^*(x_{\sigma(j)})$.

Il faut savoir le démontrer.

Propriété. \det_e est une forme n -linéaire alternée telle que $\det_e(e) = 1$.

Il faut savoir le démontrer.

Propriété. $A_n(E)$ est une droite vectorielle dirigée par \det_e .

Remarque. $\det_e(x)$ est donc la seule définition raisonnable du volume algébrique de H_x , si l'on choisit l'unité de volume de sorte que le volume de H_e soit égal à 1.

5.2.3 Déterminant d'une matrice

Définition. Le déterminant de $M \in \mathcal{M}_n(\mathbb{K})$ est le déterminant des vecteurs colonnes de M dans la base canonique de \mathbb{K}^n .

Représentation tabulaire. Si $M = (\alpha_{i,j}) \in \mathcal{M}_n(\mathbb{K})$. On note $\det(M) = \begin{vmatrix} \alpha_{1,1} & \cdots & \alpha_{1,n} \\ \vdots & & \vdots \\ \alpha_{n,1} & \cdots & \alpha_{n,n} \end{vmatrix}$.

Propriété. $\det(M) = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \prod_{j=1}^n M_{j,\sigma(j)} = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \prod_{j=1}^n M_{\sigma(j),j} = \det({}^t M)$.

Ainsi $\det(M)$ est aussi le déterminant des vecteurs lignes de M dans la base canonique de \mathbb{K}^n .

Formule de Sarrus :

$$\begin{vmatrix} p_{1,1} & p_{1,2} & p_{1,3} \\ p_{2,1} & p_{2,2} & p_{2,3} \\ p_{3,1} & p_{3,2} & p_{3,3} \end{vmatrix} = p_{1,1}p_{2,2}p_{3,3} + p_{2,1}p_{3,2}p_{1,3} + p_{3,1}p_{1,2}p_{2,3} - p_{1,3}p_{2,2}p_{3,1} - p_{2,3}p_{3,2}p_{1,1} - p_{3,3}p_{1,2}p_{2,1}.$$

5.2.4 Déterminant d'un endomorphisme

Définition. Soit $u \in L(E)$. Le *déterminant de l'endomorphisme* u est l'unique scalaire, noté $\det(u)$, vérifiant $\forall f \in A_n(E) \quad \forall x \in E^n \quad f(u(x)) = (\det(u))f(x)$.

Il faut savoir le démontrer.

Propriété. Soient e une base de E et $u \in L(E)$.

Pour tout $(x_1, \dots, x_n) \in E^n$, $\boxed{\det_e(u(x_1), \dots, u(x_n)) = \det(u)\det_e(x_1, \dots, x_n)}$.

En particulier, $\det(u) = \det_e(u(e_1), \dots, u(e_n))$.

Propriété. Pour toute base e de E et pour tout $u \in L(E)$, $\det(u) = \det(\text{Mat}(u, e))$.

Semaine 32 (du 1er au 5 juin) : Résumé de cours

1 Déterminants (suite et fin)

1.1 Propriétés du déterminant

Notation. On fixe $n \in \mathbb{N}^*$, E un \mathbb{K} -espace vectoriel de dimension n et e une base de E .

Propriété. \det_e est n -linéaire alternée, donc antisymétrique. $\det_e(e) = 1$.

$\det_e(x_1, \dots, x_n)$ n'est pas modifié si l'on ajoute à l'un des x_i une combinaison linéaire des autres x_j .

Propriété. Le déterminant d'une matrice M de $\mathcal{M}_n(\mathbb{K})$ est modifié en :

- $\det(M)$ pour une opération élémentaire du type $L_i \leftarrow L_i + \lambda L_j$ ou $C_i \leftarrow C_i + \lambda C_j$;
- $\alpha \det(M)$ pour une opération élémentaire du type $L_i \leftarrow \alpha L_i$ ou $C_i \leftarrow \alpha C_i$;
- $-\det M$ pour un échange entre deux lignes ou deux colonnes.

ATTENTION : En général, $\det(\alpha M + N) \neq \alpha \det(M) + \det(N)$.

Méthode : Pour calculer le déterminant d'une matrice, on tente de modifier la matrice par des manipulations élémentaires, afin de se ramener à une matrice dont on connaît le rang ou le déterminant.

Propriété. $\det(\text{Id}_E) = 1$, $\det(I_n) = 1$.

Pour tout $\lambda \in \mathbb{K}$ et $u \in L(E)$, $\det(\lambda u) = \lambda^n \det(u)$.

Pour tout $\lambda \in \mathbb{K}$ et $A \in \mathcal{M}_n(\mathbb{K})$, $\det(\lambda A) = \lambda^n \det(A)$.

Théorème. Si $f, g \in L(E)$, alors $\boxed{\det(fg) = \det(f) \times \det(g)}$.

Pour tout $A, B \in \mathcal{M}_n(\mathbb{K})$, $\det(AB) = \det(A)\det(B)$.

Il faut savoir le démontrer.

Formule de changement de base : Soient e et e' deux bases de E , et soit x une famille de n vecteurs de E . Alors, $\boxed{\det_{e'}(x) = \det_{e'}(e) \det_e(x)}$.

Théorème. $\boxed{x \text{ est une base si et seulement si } \det_e(x) \neq 0.}$

Il faut savoir le démontrer.

Corollaire. Soit $u \in L(E)$ et $A \in \mathcal{M}_n(\mathbb{K})$.

$u \in GL(E)$ si et seulement si $\det(u) \neq 0$ et dans ce cas, $\det(u^{-1}) = \frac{1}{\det(u)}$.

$A \in GL_n(\mathbb{K})$ si et seulement si $\det(A) \neq 0$ et dans ce cas, $\det(A^{-1}) = \frac{1}{\det(A)}$.

Remarque. \det est donc un morphisme du groupe $GL(E)$ vers (\mathbb{K}^*, \times) .

Son noyau est un sous-groupe (distingué) de $GL(E)$, noté $SL(E)$.

C'est le groupe spécial linéaire de E : $SL(E) = \{u \in L(E) \mid \det(u) = 1\}$.

En particulier de $SL_n(\mathbb{K}) = \{M \in \mathcal{M}_n(\mathbb{K}) \mid \det(M) = 1\}$: c'est le groupe spécial linéaire de degré n .

Propriété. Deux matrices carrées semblables ont le même déterminant.

1.2 Calcul des déterminants

Définition. Soit $M = (m_{i,j}) \in \mathcal{M}_n(\mathbb{K})$. Pour tout $(i, j) \in \mathbb{N}_n^2$, notons ${}_{i,j}M$ la matrice extraite de M en ôtant la $i^{\text{ème}}$ ligne et la $j^{\text{ème}}$ colonne. La quantité $\det({}_{i,j}M)$ s'appelle le $(i, j)^{\text{ème}}$ **mineur** de M . La quantité $C_{i,j} = (-1)^{i+j} \det({}_{i,j}M)$ s'appelle le $(i, j)^{\text{ème}}$ **cofacteur** de M .

Théorème. Pour tout $j \in \mathbb{N}_n$,

$$\det(M) = \sum_{i=1}^n m_{i,j} C_{i,j} : \text{c'est le développement de } \det(M) \text{ selon sa } j^{\text{ème}} \text{ colonne.}$$

Pour tout $i \in \mathbb{N}_n$, $\det(M) = \sum_{j=1}^n m_{i,j} C_{i,j} : \text{c'est le développement de } \det(M) \text{ selon sa } i^{\text{ème}} \text{ ligne.}$

Il faut savoir le démontrer.

Définition. On appelle **comatrice** de M la matrice $(C_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$ des cofacteurs de M .

On la notera $Com(M)$ ou bien $Cof(M)$.

La transposée de la comatrice s'appelle la **matrice complémentaire** de M .

Théorème. $\forall M \in \mathcal{M}_n(\mathbb{K}) \quad M^t Cof(M) = {}^t Cof(M) M = \det(M) I_n$.

Il faut savoir le démontrer.

Corollaire. Lorsque M est inversible, $M^{-1} = \frac{1}{\det(M)} {}^t Cof(M)$.

Théorème. Soit $M = (M_{i,j})_{\substack{1 \leq i \leq a \\ 1 \leq j \leq a}}$ une matrice décomposée en blocs, où, pour tout $i, j \in \mathbb{N}_a$,

$M_{i,j} \in \mathcal{M}_{n_i, n_j}(\mathbb{K})$. Si M est triangulaire supérieure (ou inférieure) par blocs, $\det(M) = \prod_{i=1}^a \det(M_{i,i})$.

Il faut savoir le démontrer.

Corollaire. Le déterminant d'une matrice triangulaire supérieure ou inférieure est égal au produit de ses éléments diagonaux.

1.3 Formules de Cramer

Propriété. Considérons un système linéaire de Cramer $(S) : MX = B$, où $M \in GL_n(\mathbb{K})$, $B \in \mathbb{K}^n$,

dont l'unique solution est notée $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n$. Alors, pour tout $j \in \{1, \dots, n\}$, $x_j = \frac{\det({}_j M)}{\det(M)}$

où ${}_j M$ est la matrice dont les colonnes sont celles de M , sauf la $j^{\text{ème}}$ qui est égale à B .

Il faut savoir le démontrer.

1.4 Exemples de déterminants.

1.4.1 Déterminant de Vandermonde

Définition. Soient $n \in \mathbb{N}$ et $(a_0, \dots, a_n) \in \mathbb{K}^{n+1}$.

La **matrice de Vandermonde** est $\mathcal{V}(a_0, \dots, a_n) = (a_{i-1}^{j-1}) \in \mathcal{M}_{n+1}(\mathbb{K})$,

et le **déterminant de Vandermonde** est $V(a_0, \dots, a_n) = \det(\mathcal{V}(a_0, \dots, a_n))$.

Propriété. $V(a_0, \dots, a_n) = \prod_{0 \leq i < j \leq n} (a_j - a_i)$.

Il faut savoir le démontrer.

1.4.2 Déterminants tridiagonaux

Définition. Soient n un entier supérieur ou égal à 2 et $M = (m_{i,j}) \in \mathcal{M}_n(\mathbb{K})$. M est tridiagonale si et seulement si, pour tout $(i, j) \in \mathbb{N}_n^2$, $|i - j| \geq 2 \implies m_{i,j} = 0$.

Propriété. Soit $M = (m_{i,j}) \in \mathcal{M}_n(\mathbb{K})$ une matrice tridiagonale. Pour tout $k \in \mathbb{N}_n$, notons M_k la matrice extraite de M en ne retenant que ses k premières colonnes et ses k premières lignes. Alors la suite $(\det(M_k))_{1 \leq k \leq n}$ vérifie une relation de récurrence linéaire d'ordre 2.

1.4.3 Déterminants circulants

Définition. Une matrice $M \in \mathcal{M}_n(\mathbb{K})$ est circulante si et seulement si on passe de l'une de ses lignes à la suivante selon une permutation circulaire des coefficients vers la droite.

Méthode : Pour des matrices circulantes simples, on peut commencer par remplacer la première ligne par la somme de toutes les lignes. La première ligne devient alors colinéaire à $(1, 1, \dots, 1)$. On peut ensuite effectuer des différences de colonnes pour placer des 0 sur la première ligne.

2 Produits scalaires

2.1 Définition d'un produit scalaire

Notation. E est un \mathbb{R} -espace vectoriel.

Définition. $\varphi \in L_2(E)$ est définie si et seulement si $\forall x \in E \setminus \{0\}$, $\varphi(x, x) \neq 0$.

Définition. $\varphi \in L_2(E)$ est positive si et seulement si $\forall x \in E$, $\varphi(x, x) \geq 0$.

Définition. Un **produit scalaire** est une forme bilinéaire symétrique définie positive, c'est-à-dire une application $\varphi : E^2 \rightarrow \mathbb{R}$ telle que, pour tout $x, y, z \in E$ et $\lambda \in \mathbb{R}$,

- $\varphi(x, y) = \varphi(y, x)$;
- $\varphi(\lambda x + y, z) = \lambda \varphi(x, z) + \varphi(y, z)$;
- $x \neq 0 \implies \varphi(x, x) > 0$.

Un **espace préhilbertien réel** est un couple (E, φ) , où E est un \mathbb{R} -espace vectoriel et où φ est un produit scalaire sur E .

2.2 Exemples

◇ Si $e = (e_i)_{i \in I}$ est une base de E , $\left(\sum_{i \in I} x_i e_i, \sum_{i \in I} y_i e_i \right) \mapsto \sum_{i \in I} x_i y_i$ est un p.s sur E .

$\varphi : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$

◇ $((\alpha_1, \dots, \alpha_n), (\beta_1, \dots, \beta_n)) \mapsto \sum_{i=1}^n \alpha_i \beta_i$ est le produit scalaire canonique de \mathbb{R}^n .

Alors, pour tout $X, Y \in \mathbb{R}^n$, $\varphi(X, Y) = {}^tXY$.

◇ En posant $\varphi(f, g) = \int_a^b f(t)g(t)dt$, φ est un produit scalaire sur $\mathcal{C}([a, b], \mathbb{R})$.

Il faut savoir le démontrer.

Exercice. Montrer que $(M, N) \mapsto \text{Tr}({}^tMN)$ est un produit scalaire sur $\mathcal{M}_n(\mathbb{R})$.

Il faut savoir le démontrer.

Notation. ◇ Pour $p \in \mathbb{R}_+^*$, $l^p = \{(u_n) \in \mathbb{R}^\mathbb{N} / \sum |u_n|^p < \infty\}$.

◇ Notons l^∞ l'ensemble des suites bornées de réels.

Propriété. l^1 , l^2 et l^∞ sont des sous-espaces vectoriels de $\mathbb{R}^{\mathbb{N}}$.

De plus si (a_n) et (b_n) sont dans l^2 , alors (a_nb_n) est un élément de l^1 .

Propriété. Pour tout $(u_n), (v_n) \in l^2$, on pose $((u_n)|(v_n)) = \sum_{n \in \mathbb{N}} u_nv_n$.

l^2 muni de $(\cdot|\cdot)$ est un espace préhilbertien.

2.3 Identités remarquables

Notation. E est un espace préhilbertien réel. Son produit scalaire sera noté $(\cdot|\cdot)$.

Définition. Pour tout $x \in E$, la norme de x est $\|x\| = \sqrt{(x|x)}$.

Formule. Pour tout $((x, y), \alpha) \in E^2 \times \mathbb{R}$,

$\ \alpha x\ $	$= \alpha \ x\ ,$
$\ x + y\ ^2$	$= \ x\ ^2 + \ y\ ^2 + 2(x y),$
$\ x - y\ ^2$	$= \ x\ ^2 + \ y\ ^2 - 2(x y),$
$\ x + y\ ^2 - \ x - y\ ^2$	$= 4(x y),$
$\ x + y\ ^2 + \ x - y\ ^2$	$= 2(\ x\ ^2 + \ y\ ^2).$

La dernière formule est la **formule du parallélogramme** ou **formule de la médiane**.

Les seconde, troisième et quatrième formules sont des **formules de polarisation**.

Théorème de Pythagore : $(x|y) = 0 \iff \|x + y\|^2 = \|x\|^2 + \|y\|^2$.

2.4 Inégalités de Cauchy-Schwarz et de Minkowski

Inégalité de Cauchy-Schwarz : $\forall (x, y) \in E^2 \quad |(x|y)| \leq \|x\| \|y\|,$

avec égalité si et seulement si x et y sont colinéaires.

Il faut savoir le démontrer.

Inégalité de Minkowski, ou inégalité triangulaire : $\forall (x, y) \in E^2 \quad \|x + y\| \leq \|x\| + \|y\|,$

avec égalité ssi x et y sont positivement colinéaires, i.e $y = 0$ ou il existe $k \in \mathbb{R}_+$ tel que $x = ky$.

Il faut savoir le démontrer.

Théorème. La norme associée au produit scalaire d'un espace préhilbertien est bien une norme.

3 Espaces vectoriels normés de dimensions finies

Notation. \mathbb{K} désigne \mathbb{R} ou \mathbb{C} .

Propriété. Suites à valeurs dans un espace de dimension finie. On suppose que E est un \mathbb{K} -espace vectoriel de dimension finie, muni d'une base $e = (e_1, \dots, e_q)$. Soit (x_n) une suite de vecteurs

de E . Pour tout $n \in \mathbb{N}$, on note $x_n = \sum_{i=1}^q x_{i,n} e_i$. Alors, la suite (x_n) converge dans E si et seulement

si, pour tout $i \in \mathbb{N}_q$, la suite $(x_{i,n})$ converge dans \mathbb{K} , et, dans ce cas, $\lim_{n \rightarrow +\infty} x_n = \sum_{i=1}^q \left(\lim_{n \rightarrow +\infty} x_{i,n} \right) e_i$.

Propriété. Limite d'une application à valeurs dans un espace de dimension finie. Supposons que F est un \mathbb{K} -espace vectoriel de dimension finie dont une base est (e_1, \dots, e_q) et notons $f: E \rightarrow F$

$$x \mapsto f(x) = \sum_{i=1}^q f_i(x) e_i. \text{ Soient } A \text{ une partie de } \mathcal{D}_f, a \in \overline{A} \text{ et } l = \sum_{i=1}^q l_i e_i \in F.$$

Alors, $f(x) \xrightarrow[x \in A]{x \rightarrow a} l$ si et seulement si pour tout $i \in \mathbb{N}_q$, $f_i(x) \xrightarrow[x \in A]{x \rightarrow a} l_i$.

Propriété. Continuité en un point d'une application à valeurs dans un espace de dimension finie. Supposons que F est un \mathbb{K} -espace vectoriel de dimension finie dont une base est (e_1, \dots, e_q)

$$f : E \longrightarrow F$$

et notons $x \longmapsto f(x) = \sum_{i=1}^q f_i(x)e_i$. Soit $a \in \mathcal{D}_f$.

Alors, f est continue en a si et seulement si pour tout $i \in \mathbb{N}_q$, f_i est continue en a .

Théorème.

Les parties compactes d'un espace vectoriel de dimension finie sont exactement ses fermés bornés.

Théorème de Bolzano-Weierstrass.

De toute suite bornée de vecteurs d'un \mathbb{K} -espace vectoriel de dimension finie, on peut extraire une sous-suite convergente.

Théorème. Tout \mathbb{K} -espace vectoriel de dimension finie est complet.

Propriété. Soit G un \mathbb{K} -espace vectoriel normé de dimension finie ou infinie. Tout sous-espace vectoriel de G de dimension finie est fermé.

Il faut savoir le démontrer.

Théorème.

Sur un \mathbb{K} -espace vectoriel de dimension finie, toutes les normes sont équivalentes.

Théorème. Toute application linéaire dont l'ensemble de départ est de dimension finie est continue.

Il faut savoir le démontrer.

Théorème. Une application p -linéaire est toujours continue lorsqu'elle est définie sur le produit cartésien de p \mathbb{K} -espaces vectoriels *de dimensions finies*.

Propriété. Les applications polynomiales de \mathbb{K}^n dans \mathbb{K} , dépendant de n variables, sont continues. Si E est un \mathbb{K} -espace vectoriel de dimension finie et si e est une base de E , lorsque $f : E \longrightarrow \mathbb{K}$ est telle que $f(x)$ dépend polynomialement des coordonnées du vecteur x dans la base e , alors f est continue.

4 Orthogonalité

Notation. E est un espace préhilbertien. Son produit scalaire est noté $\langle \cdot, \cdot \rangle$.

4.1 Orthogonalité en dimension quelconque

Définition. Soit $(x, y) \in E^2$. x et y sont orthogonaux ssi $\langle x, y \rangle = 0$. On note $x \perp y$.

Définition. Si $A \subset E$, $A^\perp = \{x \in E / \forall y \in A \quad x \perp y\}$: l'orthogonal de A est l'ensemble des vecteurs de E qui sont orthogonaux à tous les vecteurs de A .

Exemple. Si $a \in E \setminus \{0\}$, a^\perp est un hyperplan.

Propriété. Soit A une partie de E . Alors A^\perp est un sous-espace vectoriel de E .

Définition. Soient A et B deux parties de E . On dit qu'elles sont orthogonales si et seulement si tout vecteur de A est orthogonal à tout vecteur de B : $A \perp B \iff [\forall (a, b) \in A \times B, \quad a \perp b]$.

Propriété. Soient A et B deux parties de E . $A \perp B \iff A \subset B^\perp \iff B \subset A^\perp$.

Propriété. $A \subseteq B \implies B^\perp \subseteq A^\perp$, $(A \cup B)^\perp = A^\perp \cap B^\perp$, $A^\perp = (\text{Vect}(A))^\perp$ et $A \subseteq (A^\perp)^\perp$.

Il faut savoir le démontrer.

Remarque. Si F et G sont deux sous-espaces vectoriels, $(F + G)^\perp = F^\perp \cap G^\perp$, mais en général, $(F \cap G)^\perp \neq F^\perp + G^\perp$ et $F^{\perp\perp} \neq F$.

Semaine 33 (du 8 au 12 juin) : Résumé de cours

Espaces préhilbertiens

1 Orthogonalité

1.1 Orthogonalité en dimension quelconque (suite)

Propriété. $\{0\}^\perp = E$ et $E^\perp = \{0\}$.

Définition. $(x_i)_{i \in I} \in E^I$ est orthogonale si et seulement si : $\forall (i, j) \in I^2, (i \neq j \implies x_i \perp x_j)$. Elle est orthonormale si et seulement si : $\forall (i, j) \in I^2, \langle x_i, x_j \rangle = \delta_{i,j}$.

Relation de Pythagore : Si (x_1, \dots, x_n) une famille orthogonale de vecteurs de E ,

$$\left\| \sum_{i=1}^n x_i \right\|^2 = \sum_{i=1}^n \|x_i\|^2. \text{ Lorsque } n \geq 3, \text{ la réciproque est fausse.}$$

Propriété. Une famille orthogonale sans vecteur nul est libre. En particulier, une famille orthonormale est toujours libre.

Propriété. Supposons que E admet une base orthonormée notée $(e_i)_{i \in I}$.

Si $x = \sum_{i \in I} \alpha_i e_i \in E$ et $y = \sum_{i \in I} \beta_i e_i \in E$, alors

$$\langle x, y \rangle = \sum_{i \in I} \alpha_i \beta_i, \|x\|^2 = \sum_{i \in I} \alpha_i^2 \text{ et } x = \sum_{i \in I} \langle e_i, x \rangle e_i.$$

Propriété. Supposons que E est muni d'une base $e = (e_i)_{i \in I}$.

Alors il existe un unique produit scalaire sur E pour lequel e est une base orthonormée.

Propriété. Soient $n \in \mathbb{N}^*$ et $(E_i)_{1 \leq i \leq n}$ une famille de n sous-espaces vectoriels de E deux à deux

orthogonaux. Alors ils forment une somme directe que l'on note $E_1 \overset{\perp}{\oplus} \dots \overset{\perp}{\oplus} E_n = \overset{\perp}{\bigoplus}_{1 \leq i \leq n} E_i$.

Définition. Soient F et G deux sous-espaces vectoriels de E .

G est un **supplémentaire orthogonal** de F si et seulement si $E = F \overset{\perp}{\oplus} G$.

Propriété. Soit F un sous-espace vectoriel de E . F admet au plus un supplémentaire orthogonal.

Il s'agit de F^\perp . Il est cependant possible que $F \overset{\perp}{\oplus} F^\perp \neq E$.

Il faut savoir le démontrer.

1.2 En dimension finie

Propriété. Si E est de dimension finie, l'application $\begin{matrix} E & \longrightarrow & L(E, \mathbb{R}) \\ x & \longmapsto & \langle x, . \rangle \end{matrix}$ est un isomorphisme.

Théorème. On ne suppose pas que E est de dimension finie. Si F est un sous-espace vectoriel de dimension finie de E , alors F^\perp est l'unique supplémentaire orthogonal de F . De plus $F = (F^\perp)^\perp$.

Il faut savoir le démontrer.

Définition. Un espace euclidien est un espace préhilbertien de dimension finie.

Hypothèse : jusqu'à la fin du paragraphe, E est supposé euclidien de dimension $n > 0$.

Propriété. Si F et G sont deux sous-espaces vectoriels de E , alors $(F \cap G)^\perp = F^\perp + G^\perp$.

Propriété. Si F est un sous-espace vectoriel de E , alors $\dim(F^\perp) = \dim E - \dim F$.

Propriété. Soit e une base orthonormée de E . Soient $x, y \in E$ dont les coordonnées dans la base e sont données sous forme de vecteurs colonnes notés X et Y . Alors $\langle x, y \rangle = {}^t Y X = {}^t X Y$.

Remarque. Si e est une base orthonormée de E , pour tout $u \in L(E)$, pour tout $i, j \in \mathbb{N}_n$, $[\text{mat}(u, e)]_{i,j} = \langle e_i, u(e_j) \rangle$.

La fin de ce paragraphe est hors programme.

Définition. La matrice du produit scalaire dans la base e est égale à

$$\text{mat}(\langle ., . \rangle, e) = (\langle e_i, e_j \rangle)_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} \in \mathcal{M}_n(\mathbb{R}).$$

Propriété. e est orthogonale si et seulement si $\text{mat}(\langle ., . \rangle, e)$ est diagonale.
 e est orthonormée si et seulement si $\text{mat}(\langle ., . \rangle, e) = I_n$.

Formule. Soit e une base quelconque de E . On note Ω la matrice de $\langle ., . \rangle$ dans la base e . Soient x et y deux vecteurs de E , dont les coordonnées dans e sont données sous la forme des vecteurs colonnes X et Y de \mathbb{R}^n . Alors

$$\langle x, y \rangle = {}^t X \Omega Y = {}^t Y \Omega X = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} x_i y_j \omega_{i,j}.$$

Il faut savoir le démontrer.

Définition. Soit E un \mathbb{K} -espace vectoriel de dimension finie, muni d'une base $e = (e_1, \dots, e_n)$ et soit φ une forme bilinéaire sur E .

La matrice de φ dans la base e est $\text{mat}(\varphi, e) = (\varphi(e_i, e_j))_{1 \leq i, j \leq n} \in \mathcal{M}_n(\mathbb{K})$.

Pour tout $x, y \in E$, en posant $X = \text{mat}_e(x)$ et $Y = \text{mat}_e(y)$, $\varphi(x, y) = {}^t X \Omega Y$.

φ est symétrique si et seulement si $\Omega \in S_n(\mathbb{K})$.

1.3 Distance d'un vecteur à un sous-espace vectoriel

Définition. Soit F un sous-espace vectoriel de E tel que $F \oplus F^\perp = E$. La **projection orthogonale** sur F est la projection sur F parallèlement à F^\perp . Dans ce chapitre, elle est notée p_F .

Remarque. Pour tout $x \in E$, $x - p_F(x) = p_{F^\perp}(x) \in F^\perp$.

Formule. Soit F un sous-espace vectoriel de dimension finie de E , muni d'une base orthonormée

$$e = (e_1, \dots, e_n). \text{ Alors, pour tout } x \in E, \quad p_F(x) = \sum_{i=1}^n \langle e_i, x \rangle e_i.$$

Il faut savoir le démontrer.

Théorème de la projection orthogonale :

Soient $a \in E$ et F un sous-espace vectoriel de dimension finie de E . Alors, $d(a, F) = d(a, p_F(a))$.

Pour tout $y \in F \setminus \{p_F(a)\}$, $d(a, y) > d(a, F)$. $\|a\|^2 = \|p_F(a)\|^2 + d(a, F)^2$.

Si (e_1, \dots, e_n) est une base **orthonormée** de F , $\|a\|^2 \geq \sum_{i=1}^n \langle e_i, a \rangle^2$: inégalité de Bessel.

Il faut savoir le démontrer.

Propriété. Soit $a \in E \setminus \{0\}$. On pose $H = a^\perp$. H est un hyperplan dont a est un vecteur **normal**.

Pour tout $x \in E$, $p_H(x) = x - \frac{\langle x, a \rangle}{\|a\|^2} a$ et, en notant s_H la symétrie orthogonale par rapport à H ,

$$s_H(x) = x - 2 \frac{\langle x, a \rangle}{\|a\|^2} a.$$

Propriété. On suppose que E est de dimension finie $n \geq 1$. Soit \mathcal{H} un hyperplan affine de E , passant par un point A et dirigé par l'hyperplan vectoriel H : Si \vec{n} est un vecteur non nul de H^\perp , on dit que

\vec{n} est un vecteur normal à \mathcal{H} . Dans ce cas, pour tout $M \in E$ $d(M, \mathcal{H}) = \frac{|\langle \vec{n}, \overrightarrow{AM} \rangle|}{\|\vec{n}\|}$.

Si \mathcal{H} a pour équation cartésienne $\sum_{i=1}^n \alpha_i x_i = c$ dans un repère orthonormé, pour tout $M \in E$,

$$d(M, \mathcal{H}) = \frac{|\sum_{i=1}^n \alpha_i x_i - c|}{\sqrt{\sum_{i=1}^n \alpha_i^2}}, \text{ où } (x_1, \dots, x_n) \text{ sont les coordonnées de } M \text{ dans le repère.}$$

Il faut savoir le démontrer.

1.4 Procédé d'orthonormalisation de Gram-Schmidt

Théorème. Orthonormalisation de Gram-Schmidt.

Soient $n \in \mathbb{N}^*$ et $(x_k)_{k \in \{1, \dots, n\}}$ une famille **libre** de vecteurs de E . Alors il existe une unique famille orthonormale de vecteurs $(e_k)_{k \in \{1, \dots, n\}}$ telle que, pour tout $k \in \{1, \dots, n\}$,

- i) $e_k \in \text{Vect}(x_1, \dots, x_k)$
- ii) et $\langle e_k, x_k \rangle \in \mathbb{R}_+^*$.

De plus, la famille $(e_k)_{k \in \{1, \dots, n\}}$ est définie par $e_k = \frac{E_k}{\|E_k\|}$, où $E_k = x_k - \sum_{i=1}^{k-1} \langle e_i, x_k \rangle e_i$.

Il faut savoir le démontrer.

Interprétation matricielle du procédé de Gram-Schmidt.

Soient $n \in \mathbb{N}^*$ et $x = (x_k)_{k \in \{1, \dots, n\}}$ une base de E .

Alors il existe une unique base orthonormée $e = (e_1, \dots, e_n)$ de E telle que la matrice de passage de e vers x est triangulaire supérieure, ses coefficients diagonaux étant de plus strictement positifs.

Il faut savoir le démontrer.

Propriété. Si E est euclidien, il admet au moins une base orthonormée.

Toute une famille orthonormale de E peut être complétée en une base orthonormale de E .

Théorème. Orthonormalisation de Gram-Schmidt pour une famille infinie

Soient $(x_k)_{k \in \mathbb{N}^*}$ une famille **libre** de vecteurs de E . Alors il existe une unique famille orthonormale de vecteurs $(e_k)_{k \in \mathbb{N}^*}$ telle que, pour tout $k \in \mathbb{N}^*$,

- i) $e_k \in \text{Vect}(x_1, \dots, x_k)$
- ii) et $\langle e_k, x_k \rangle \in \mathbb{R}_+^*$.

De plus, la famille $(e_k)_{k \in \mathbb{N}^*}$ est définie par : $e_k = \frac{E_k}{\|E_k\|}$, où $E_k = x_k - \sum_{i=1}^{k-1} \langle e_i, x_k \rangle e_i$.

2 Endomorphismes d'un espace euclidien E

2.1 Endomorphismes symétriques

Définition. $u \in L(E)$ est symétrique ssi $\forall (x, y) \in E^2, \langle u(x), y \rangle = \langle x, u(y) \rangle$.

Propriété. Soient e une base **orthonormée** de E et $u \in L(E)$.

Alors u est symétrique si et seulement si $\text{mat}(u, e)$ est symétrique.

Il faut savoir le démontrer.

Notation. $S(E)$ est l'ensemble des endomorphismes symétriques de E .

C'est un sous-espace vectoriel de $L(E)$.

Propriété. Une projection est un endomorphisme symétrique ssi c'est une projection orthogonale.

Il faut savoir le démontrer.

Propriété. Une symétrie est un endomorphisme symétrique ssi c'est une symétrie orthogonale.

Propriété. Si $u \in S(E)$ et si F est un sous-espace vectoriel stable par u , alors F^\perp est stable par u .

Vous verrez en seconde année le

Théorème spectral : Si $u \in S(E)$, il existe au moins une base orthonormée de vecteurs propres de u . On dit que u est diagonalisable en base orthonormée.

2.2 Groupe orthogonal.

2.2.1 Caractérisations d'un automorphisme orthogonal.

Définition. Soit $u \in L(E)$. On dit que u est un **automorphisme orthogonal** ou une **isométrie vectorielle** si et seulement si l'une des propriétés suivantes est vérifiée.

- conservation du produit scalaire : $\forall x, y \in E, \langle u(x), u(y) \rangle = \langle x, y \rangle$;
- conservation de la norme : $\forall x \in E, \|u(x)\| = \|x\|$.
- si e est une base orthonormée de E , en posant $M = \text{mat}(u, e)$,
 M inversible et $M^{-1} = {}^t M$.

Il faut savoir le démontrer.

Notation. On note $O(E)$ l'ensemble des automorphismes orthogonaux de E .

Propriété. $O(E)$ est un sous-groupe de $(GL(E), \circ)$. On l'appelle le **groupe orthogonal** de E .

Propriété. Si $u \in O(E)$, $Sp_{\mathbb{R}}(u) \subset \{1, -1\}$.

Propriété. Soit $u \in O(E)$. Si F est un sous-espace vectoriel stable par u , F^\perp est stable par u .

2.2.2 Les rotations.

Propriété. Si $u \in O(E)$, alors $\det(u) \in \{-1, 1\}$, mais la réciproque est fausse.

Définition. Soit $u \in O(E)$. On dit que u est une **rotation** si et seulement si $\det(u) = 1$.

u est une **isométrie vectorielle indirecte** ou négative si et seulement si $\det(u) = -1$.

Propriété. L'ensemble des rotations de E , noté $SO(E)$, est un sous-groupe de $O(E)$, appelé **groupe spécial orthogonal**. L'ensemble des isométries indirectes de E est noté $O^-(E) = O(E) \setminus SO(E)$. Il n'a pas de structure particulière.

2.2.3 Les symétries orthogonales

Propriété. La symétrie par rapport à F parallèlement à G (où $F \oplus G = E$) est un automorphisme orthogonal si et seulement si c'est une symétrie orthogonale (ie : $G = F^\perp$).

Propriété. Soit F un sous-espace vectoriel de E . Notons s la symétrie orthogonale par rapport à F . $s \in SO(E)$ si et seulement si $\dim(E) - \dim(F)$ est paire.

En particulier, si F est un hyperplan, $s \in O^-(E)$ et, dans ce cas, s est appelée une **réflexion**, et si $\dim(F) = \dim(E) - 2$, s est une rotation, et dans ce cas, s est appelée un **retournement**.

Définition. On dit que deux sous-espaces vectoriels F et G de E sont perpendiculaires lorsque F^\perp et G^\perp sont orthogonaux, c'est-à-dire lorsque $G^\perp \subset F$.

2.2.4 Matrices orthogonales.

Propriété. Soit $M \in \mathcal{M}_n(\mathbb{R})$. C'est une **matrice orthogonale** si et seulement si l'une des propriétés suivantes est vérifiée.

- ${}^tMM = I_n$;
- $M^tM = I_n$;
- M est inversible et $M^{-1} = {}^tM$.

Propriété. L'ensemble des matrices orthogonales est un sous-groupe de $GL_n(\mathbb{R})$ appelé le **groupe orthogonal de degré n** et noté $O(n)$.

Propriété. Pour tout $M \in O(n)$, $\det(M) \in \{-1, 1\}$.

Définition. Les matrices orthogonales de déterminant égal à 1 sont appelées les **matrices de rotations**. Les matrices orthogonales de déterminant égal à -1 sont appelées les matrices orthogonales gauches ou indirectes. L'ensemble des matrices de rotations est un sous-groupe de $O(n)$, appelé **groupe spécial orthogonal de degré n** et noté $SO(n)$. L'ensemble des matrices orthogonales indirectes est noté $O^-(n) = O(n) \setminus SO(n)$. Il n'a pas de structure particulière.

Propriété. $M \in O(n)$ si et seulement si la famille de ses vecteurs colonnes (ou de ses vecteurs lignes) est orthonormale dans \mathbb{R}^n muni de son produit scalaire canonique.

Il faut savoir le démontrer.

Propriété. Soient e une base orthonormée de E et e' une base quelconque de E .

e' est orthonormée si et seulement si la matrice de passage de e à e' est orthogonale.

Propriété. Soient $u \in L(E)$ et e une base orthonormée de E .

Les propriétés suivantes sont équivalentes.

- $u \in O(E)$;
- $\text{mat}(u, e) \in O(n)$;
- $u(e)$ est une base orthonormée.

Propriété. (Hors programme) Dans une matrice orthogonale droite, chaque coefficient est égal à son cofacteur. Dans une matrice orthogonale gauche, chaque coefficient est l'opposé de son cofacteur.

Propriété. Si $M \in S_n(\mathbb{R})$, il existe $P \in O(n)$ et D diagonale telles que $M = PDP^{-1} = PD^tP$.

2.2.5 Orientation d'un espace vectoriel réel.

Dans ce paragraphe, E est un \mathbb{R} -espace vectoriel de dimension finie $n > 0$, pour le moment non muni d'une structure euclidienne.

Notation. \mathcal{B} étant l'ensemble des bases de E , on convient que $\forall (e, e') \in \mathcal{B}^2$, $e\mathcal{R}e' \iff \det(P_e^{e'}) > 0$.

Propriété. \mathcal{R} est une relation d'équivalence sur \mathcal{B} .

\mathcal{B}/\mathcal{R} est formé de deux éléments qui sont appelés les **orientations** de E .

“Orienter E ”, c’est choisir l’une de ces deux orientations qui devient l’ensemble des **bases directes**.

Hypothèse : jusqu’à la fin de ce chapitre, on suppose que E est un espace euclidien orienté de dimension $n > 0$.

Définition. Soit D une droite vectorielle incluse dans E que l’on oriente en choisissant un vecteur unitaire $\vec{k} \in D$. “Orienter l’hyperplan D^\perp par le vecteur \vec{k} de D ”, c’est choisir comme orientation de D^\perp l’ensemble des bases (e_1, \dots, e_{n-1}) de D^\perp telles que $(e_1, \dots, e_{n-1}, \vec{k})$ est une base directe de E .

Propriété. Soient e et e' deux bases orthonormées de E . On suppose que e est directe. Alors e' est directe si et seulement si $P_e^{e'} \in SO(n)$.

Propriété. Soient $u \in L(E)$ et e une base orthonormée directe de E .

Les propriétés suivantes sont équivalentes.

- $u \in SO(E)$;
- $\text{mat}(u, e) \in SO(n)$;
- $u(e)$ est une base orthonormée directe.

2.2.6 Produit mixte.

Dans tout ce paragraphe, E désigne un espace euclidien **orienté** de dimension $n > 0$.

Définition. Soit $(x_1, \dots, x_n) \in E^n$. Le **produit mixte** de (x_1, \dots, x_n) est $\det_e(x_1, \dots, x_n)$, où e est une base orthonormée directe quelconque de E . Il est noté $\det(x_1, \dots, x_n)$ ou encore $[x_1, \dots, x_n]$.

Remarque.

Si on change l’orientation de l’espace E , le produit mixte est changé en son opposé.

Propriété.

On suppose que $n = 2$. L’aire d’un parallélogramme $ABCD$ vaut $|\det(\overrightarrow{AB}, \overrightarrow{AD})|$.

Propriété. On suppose que $n = 3$. Le volume d’un parallélépipède dont les côtés correspondent aux vecteurs u, v , et w vaut $|\det(u, v, w)|$.

3 Géométrie plane

Notation. E est un plan euclidien orienté dont (\vec{i}, \vec{j}) est une base orthonormée.

Pour tout $\alpha \in \mathbb{R}$, on notera $u_\alpha = \cos(\alpha)\vec{i} + \sin(\alpha)\vec{j}$.

3.1 Le groupe orthogonal de degré 2

Propriété.

$$SO(2) = \left\{ R_\theta = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} / \theta \in \mathbb{R} \right\}. O^-(2) = \left\{ S_\theta = \begin{pmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{pmatrix} / \theta \in \mathbb{R} \right\}.$$

Il faut savoir le démontrer.

Propriété. En identifiant \mathbb{R}^2 avec le plan complexe \mathbb{C} ,

- l’endomorphisme r_θ canoniquement associé à R_θ est la similitude directe $z \mapsto e^{i\theta}z$, c’est-à-dire la rotation de centre 0 et d’angle θ ;
- l’endomorphisme s_θ canoniquement associé à S_θ est la similitude indirecte $z \mapsto e^{i\theta}\bar{z}$, c’est-à-dire la réflexion par rapport à la droite $\mathbb{R}e^{i\frac{\theta}{2}}$.

Formule. Pour tout $(\theta, \alpha) \in \mathbb{R}^2$, $R_\theta \begin{pmatrix} \cos \alpha \\ \sin \alpha \end{pmatrix} = \begin{pmatrix} \cos(\theta + \alpha) \\ \sin(\theta + \alpha) \end{pmatrix}$ et $S_\theta \begin{pmatrix} \cos \alpha \\ \sin \alpha \end{pmatrix} = \begin{pmatrix} \cos(\theta - \alpha) \\ \sin(\theta - \alpha) \end{pmatrix}$.

Formules : $R_\theta R_\varphi = R_{\theta+\varphi}$, $R_\theta S_\varphi = S_{\theta+\varphi}$, $S_\theta S_\varphi = R_{\theta-\varphi}$, $S_\theta R_\varphi = S_{\theta-\varphi}$.

Il faut savoir le démontrer.

Formule. Pour tout $(\theta, \varphi) \in \mathbb{R}^2$, $S_\theta^{-1} = S_\theta$ et $S_\alpha^{-1} R_\theta S_\alpha = R_{-\theta}$.

Propriété. L'application $\begin{matrix} (\mathbb{R}, +) & \longrightarrow & (SO(2), \times) \\ \theta & \longmapsto & R_\theta \end{matrix}$ est un morphisme surjectif de groupes. On en déduit que $(SO(2), \times)$ est un groupe commutatif.

Propriété. L'application $R_\theta \mapsto e^{i\theta}$ est un isomorphisme entre les groupes $(SO(2), \times)$ et \mathbb{U} .

3.2 Les isométries vectorielles du plan

Propriété. Soient $s \in O^-(E)$. Il existe $\theta \in \mathbb{R}$ tel que $mat(s, e) = S_\theta$. s est la réflexion par rapport à la droite vectorielle $\mathbb{R}u_{\frac{\theta}{2}}$. Ainsi, les éléments de $O^-(E)$ sont les réflexions de E .

Définition. On suppose que E est orienté. Soit $r \in SO(E)$. La matrice R_θ de r dans une base orthonormée directe de E ne dépend pas du choix de cette base. θ est appelé l'angle de la rotation r , déterminé à 2π près. Si on change d'orientation, cette mesure est changée en son opposé.

3.3 Un résultat sur les similitudes (hors programme)

Propriété. Soit E un espace euclidien et $f : E \longrightarrow E$ une **application** telle que $f(0) = 0$ et pour tout $x, y \in E$, $\|f(x) - f(y)\| = \|x - y\|$. Alors f est un automorphisme orthogonal.

Il faut savoir le démontrer.

Corollaire. Une application $f : \mathbb{C} \longrightarrow \mathbb{C}$ est une similitude si et seulement si il existe $\lambda \in \mathbb{R}_+^*$ tel que : $\forall z, z' \in \mathbb{C}$, $|f(z) - f(z')| = \lambda|z - z'|$.

Semaine 34 (du 15 au 20 juin) : Résumé de cours

Espaces préhilbertiens (fin)

1 Géométrie plane (suite)

1.1 Angles

Notation. E désigne un plan euclidien orienté.

Définition. Soient x et y deux vecteurs non nuls de E . L'angle orienté des vecteurs x et y est l'angle de l'unique rotation qui transforme $\frac{x}{\|x\|}$ en $\frac{y}{\|y\|}$. $\cos(\widehat{x, y}) = \frac{\langle x, y \rangle}{\|x\|\|y\|}$ et $\sin(\widehat{x, y}) = \frac{\det(x, y)}{\|x\|\|y\|}$.

Propriété. Les x_i désignant des vecteurs non nuls de E , on a les formules suivantes :

- ◇ Relation de Chasles : $\widehat{(x_1, x_2)} + \widehat{(x_2, x_3)} = \widehat{(x_1, x_3)}$.
- ◇ $\widehat{(x_2, x_1)} = -\widehat{(x_1, x_2)}$.
- ◇ $\widehat{(x_1, x_2)} = 0 \iff \mathbb{R}_+x_1 = \mathbb{R}_+x_2$ et $\widehat{(x_1, x_2)} = \pi \iff \mathbb{R}_+x_1 = \mathbb{R}_-x_2$.
- ◇ Si r est une rotation, $\widehat{(r(x_1), r(x_2))} = \widehat{(x_1, x_2)}$.
- ◇ Si s est une réflexion, $\widehat{(s(x_1), s(x_2))} = -\widehat{(x_1, x_2)}$.

Définition. E est un espace préhilbertien quelconque. L'angle non orienté ou écart angulaire des vecteurs $x, y \in E$ est $\widehat{(x, y)} = \arccos\left(\frac{\langle x, y \rangle}{\|x\|\|y\|}\right) \in [0, \pi]$.

- Lorsque $\widehat{(x, y)} \in]0, \frac{\pi}{2}[$, cet angle est dit aigu ;
- Lorsque $\widehat{(x, y)} \in]\frac{\pi}{2}, \pi[$, cet angle est dit obtus ;
- Lorsque $\widehat{(x, y)} = \frac{\pi}{2}$ (i.e lorsque $x \perp y$), on dit que c'est un angle droit ;
- Lorsque $\widehat{(x, y)} \in \{0, \pi\}$, on dit que c'est un angle plat :

1.2 Les droites affines du plan usuel

On se place dans un plan affine \mathcal{E} euclidien orienté.

Propriété. Les droites affines de \mathcal{E} ont pour équation : $ux + vy + w = 0$, où $(u, v) \neq 0$.

Le vecteur de coordonnées (u, v) est orthogonal à la droite.

Les droites non parallèles à \vec{j} admettent une équation de la forme $y = px + q$, p étant appelé la pente de la droite.

Propriété. La droite passant par le point de coordonnées (x_0, y_0) et orthogonale au vecteur (u, v) a pour équation $u(x - x_0) + v(y - y_0) = 0$.

Propriété. La droite passant par le point de coordonnées (x_0, y_0) et dirigée par le vecteur (u, v) a pour équation $-v(x - x_0) + u(y - y_0) = 0 = \begin{vmatrix} u & x - x_0 \\ v & y - y_0 \end{vmatrix}$.

Propriété. La droite passant par les points (supposés distincts) de coordonnées (x_0, y_0) et (x_1, y_1) a pour équation $\begin{vmatrix} x - x_0 & x_1 - x_0 \\ y - y_0 & y_1 - y_0 \end{vmatrix} = 0$.

2 Géométrie dans l'espace

E est un espace euclidien orienté de dimension 3 et \mathcal{E} est un espace affine de direction E . On dit que \mathcal{E} est l'espace usuel. On fixe un repère de \mathcal{E} , noté $R = (O, e)$, où e une base orthonormée directe de E , notée $e = (\vec{i}, \vec{j}, \vec{k})$ ou $e = (e_1, e_2, e_3)$ selon les cas.

2.1 Le produit vectoriel (hors programme).

Définition. Si $a, b \in E$, $a \wedge b$ est l'unique vecteur de E tel que $\boxed{\forall x \in E \det(a, b, x) = \langle a \wedge b, x \rangle}$.

Il faut savoir le démontrer.

Propriété. L'application $(a, b) \mapsto a \wedge b$ est bilinéaire et antisymétrique.

Propriété. Soit $(a, b) \in E^2$. (a, b) est un système lié si et seulement si $a \wedge b = 0$.

Il faut savoir le démontrer.

Propriété. Soit a et b deux vecteurs indépendants entre eux.

Alors $a \wedge b$ est un vecteur orthogonal à a et b tel que $(a, b, a \wedge b)$ est une base directe de l'espace. De plus $\|a \wedge b\| = \|a\| \|b\| \sin \phi$, où ϕ est l'angle non orienté entre a et b .

Formule. *Identité de Lagrange* : Pour tout $(a, b) \in E^2$, $\langle a, b \rangle^2 + \|a \wedge b\|^2 = \|a\|^2 \|b\|^2$.

Propriété. $e_1 \wedge e_2 = e_3 \quad e_2 \wedge e_3 = e_1 \quad e_3 \wedge e_1 = e_2$.

Formule. Si $a = \begin{vmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{vmatrix}_e$ et $b = \begin{vmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \end{vmatrix}_e$ alors $a \wedge b = \begin{vmatrix} \alpha_2 \beta_3 - \alpha_3 \beta_2 \\ \alpha_3 \beta_1 - \alpha_1 \beta_3 \\ \alpha_1 \beta_2 - \alpha_2 \beta_1 \end{vmatrix}_e$.

Il faut savoir le démontrer.

2.2 Equation d'un plan

Propriété. Les plans affines de \mathcal{E} ont pour équation : $ux + vy + wz + t = 0$, où $(u, v, w) \neq 0$.

Le vecteur de coordonnées (u, v, w) est orthogonal (on dit aussi normal) au plan.

La direction du plan est le plan vectoriel d'équation $ux + vy + wz = 0$.

Propriété. Deux plans de \mathcal{E} d'équations $ux + vy + wz + t = 0$ et $u'x + v'y + w'z + t' = 0$ sont parallèles si et seulement si les vecteurs normaux de coordonnées (u, v, w) et (u', v', w') sont colinéaires, donc si

et seulement si $\begin{vmatrix} u \\ v \\ w \end{vmatrix}_e \wedge \begin{vmatrix} u' \\ v' \\ w' \end{vmatrix}_e = 0$.

Propriété. Le plan passant par le point de coordonnées (x_0, y_0, z_0) et orthogonal au vecteur (u, v, w) a pour équation $u(x - x_0) + v(y - y_0) + w(z - z_0) = 0$.

Propriété. Le plan passant par le point de coordonnées (x_0, y_0, z_0) et dirigé par deux vecteurs indépendants de coordonnées (u, v, w) et (u', v', w') a pour équation cartésienne $\begin{vmatrix} x - x_0 & u & u' \\ y - y_0 & v & v' \\ z - z_0 & w & w' \end{vmatrix} = 0$.

2.3 Système d'équations d'une droite

Propriété. Une droite affine de \mathcal{E} admet un système d'équations de la forme :

$$\begin{cases} ux + vy + wz + t = 0 \\ u'x + v'y + w'z + t' = 0 \end{cases}, \text{ où } ux + vy + wz + t = 0 \text{ et } u'x + v'y + w'z + t' = 0 \text{ sont les équations}$$

de deux plans affines non parallèles. Cette droite est dirigée par le vecteur ${}_e \begin{vmatrix} u \\ v \\ w \end{vmatrix} \wedge {}_e \begin{vmatrix} u' \\ v' \\ w' \end{vmatrix}$.

2.4 Le groupe orthogonal en dimension 3

Théorème. Réduction des matrices orthogonales :

On suppose ici que E est un espace euclidien de dimension $n \geq 1$.

Si $u \in O(E)$, il existe une base orthonormale \mathcal{B} de E telle que

$$\text{mat}(u, \mathcal{B}) = \begin{pmatrix} I_{k_1} & 0 & \dots & \dots & 0 \\ 0 & -I_{k_2} & 0 & \dots & 0 \\ 0 & 0 & \tau_1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & \tau_p \end{pmatrix}$$

où $\tau_i = \begin{pmatrix} \cos \theta_i & -\sin \theta_i \\ \sin \theta_i & \cos \theta_i \end{pmatrix}$ avec $\sin \theta_i \neq 0$ et $k_1 + k_2 + 2p = n$.

Notation. Soient ω un vecteur non nul de E et $\theta \in \mathbb{R}$. On désigne par $r(\omega, \theta)$ l'unique rotation de E qui laisse invariant ω et qui induit sur le plan ω^\perp , orienté selon le vecteur ω , la rotation d'angle θ .

Propriété. Soient ω un vecteur non nul de E et $\theta \in \mathbb{R}$. Il existe une base orthonormée directe e de

E telle que $\text{mat}(r(\omega, \theta), e) = \begin{pmatrix} \cos \theta & -\sin \theta & 0 \\ \sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Plus précisément, on peut choisir $e = (i, j, k)$ où

(i, j) est une base orthonormée directe du plan ω^\perp , orienté selon le vecteur ω et où $k = \frac{\omega}{\|\omega\|}$.

Théorème. Si $r \in SO(E)$, il existe $\omega \in E \setminus \{0\}$ et $\theta \in \mathbb{R}$ tels que $r = r(\omega, \theta)$.

Remarque. Si $r \in SO(E)$, on obtient ω tel que $r = r(\omega, \theta)$, en étudiant l'équation $r(x) = x$, c'est-à-dire en recherchant les vecteurs propres pour la valeur propre 1. De plus, $\boxed{\text{Tr}(r) = 1 + 2 \cos \theta}$.

Remarque. Soit $u \in O^-(E)$. $\det(-u) = (-1)^3 \det(u) = 1$, donc $-u \in SO(E)$.

Ainsi, on peut décrire géométriquement une isométrie indirecte, en déterminant $\omega \in E \setminus \{0\}$ et $\theta \in \mathbb{R}$ tels que $u = -r(\omega, \theta)$.

Ensembles dénombrables et familles sommables

3 Ensembles dénombrables

Définition. Un ensemble est dénombrable si et seulement s'il est en bijection avec \mathbb{N} .

Propriété. Toute partie infinie de \mathbb{N} est dénombrable.

Propriété. On dit qu'un ensemble est au plus dénombrable si et seulement si il est fini ou dénombrable. Un ensemble est au plus dénombrable si et seulement s'il est en bijection avec une partie de \mathbb{N} .

Lemme technique : Un ensemble I est fini ou dénombrable si et seulement s'il existe une suite croissante $(J_n)_{n \in \mathbb{N}}$ de parties finies de I dont la réunion est égale à I .

Dans ce cas, on dira que $(J_n)_{n \in \mathbb{N}}$ est une suite adaptée à I .

Corollaire. \mathbb{Z} , $\mathbb{N} \times \mathbb{N}$ et \mathbb{Q} sont dénombrables.

Exercice. Montrer que $\mathbb{Q}[X]$ est dénombrable.

Solution. À connaître.

Propriété. Une réunion au plus dénombrable d'ensembles au plus dénombrables est au plus dénombrable.

Il faut savoir le démontrer.

Propriété. Un produit cartésien fini d'ensembles dénombrables est dénombrable.

Propriété. \mathbb{R} n'est pas dénombrable.

Il faut savoir le démontrer.

Propriété. Hors programme : $\mathcal{P}(\mathbb{N})$ n'est pas dénombrable.

4 Familles sommables de réels positifs

Notation. Pour tout ce paragraphe, on fixe un ensemble I .

On fixe également une famille $u = (u_i)_{i \in I} \in \mathbb{R}_+^I$ de réels positifs indexée par I .

Définition. On pose
$$\sum_{i \in I} u_i = \sup_{\substack{J \in \mathcal{P}(I) \\ J \text{ finie}}} \sum_{i \in J} u_i \in \mathbb{R}_+ \cup \{+\infty\}.$$

Définition. La famille u est sommable si et seulement si $\sum_{i \in I} u_i < +\infty$, c'est-à-dire si et seulement si il existe $M \geq 0$ tel que, pour toute partie finie J de I , $\sum_{i \in J} u_i \leq M$.

Propriété. Si $(u_i)_{i \in I}$ est sommable, alors $\{i \in I / u_i \neq 0\}$ est au plus dénombrable.

Remarque. Pour toute la suite, I est supposé au plus dénombrable.

Propriété. Soient $v = (v_i)_{i \in I}$ et $w = (w_i)_{i \in I}$ deux familles de réels positifs telles que, pour tout $i \in I$, $v_i \leq w_i$. Si w est sommable, alors v est également sommable et
$$\sum_{i \in I} v_i \leq \sum_{i \in I} w_i$$

Propriété. Lorsque $v = (v_i)_{i \in I}$ et $w = (w_i)_{i \in I}$ sont deux familles de réels positifs telles que, pour tout $i \in I$ $v_i \leq w_i$, on peut toujours écrire que, dans $[0, +\infty]$,
$$\sum_{i \in I} v_i \leq \sum_{i \in I} w_i.$$

Propriété. Soit $(J_n)_{n \in \mathbb{N}}$ une suite adaptée à I . Les propriétés suivantes sont équivalentes :

- $(u_i)_{i \in I}$ est sommable.
- La suite $\left(\sum_{i \in J_n} u_i\right)_{n \in \mathbb{N}}$ est majorée.
- La suite $\left(\sum_{i \in J_n} u_i\right)_{n \in \mathbb{N}}$ est convergente dans \mathbb{R}_+ .

De plus, dans ce cas, $\sum_{i \in I} u_i = \sup_{n \in \mathbb{N}} \sum_{i \in J_n} u_i = \lim_{n \rightarrow +\infty} \sum_{i \in J_n} u_i$.

Il faut savoir le démontrer.

Propriété. Lorsque $I = \mathbb{N}$, $(u_n) \in \mathbb{R}_+^{\mathbb{N}}$ est sommable si et seulement si $\sum u_n$ est convergente et dans ce cas, $\sum_{n \in \mathbb{N}} u_n = \sum_{n=0}^{+\infty} u_n$.

Théorème. Supposons que I est dénombrable et soit φ une bijection de \mathbb{N} dans I .

$(u_i)_{i \in I}$ est sommable si et seulement si $\sum u_{\varphi(n)}$ est convergente et dans ce cas, $\sum_{i \in I} u_i = \sum_{n=0}^{+\infty} u_{\varphi(n)}$.

Propriété de linéarité : Si $(v_i)_{i \in I}$ et $(w_i)_{i \in I}$ sont deux familles sommables de réels positifs, alors pour tout $\alpha \in \mathbb{R}_+$, $(\alpha v_i + w_i)_{i \in I}$ est sommable. Dans ce cas, $\sum_{i \in I} (\alpha v_i + w_i) = \alpha \sum_{i \in I} v_i + \sum_{i \in I} w_i$.

Il faut savoir le démontrer.

Convention : Soit $(u_i)_{i \in I}$ une famille d'éléments de $\mathbb{R}_+ \cup \{+\infty\}$.

S'il existe $i_0 \in I$ tel que $u_{i_0} = +\infty$, on convient que $\sum_{i \in I} u_i = +\infty$.

Convention : lorsqu'on travaille dans $\mathbb{R}_+ \cup \{+\infty\}$, on utilise la convention $0 \times (+\infty) = 0$.

On convient aussi, mais c'est plus universel, que pour tout $x \in \mathbb{R}_+^*$, $x \times (+\infty) = +\infty$.

Propriété. Soit $(v_i)_{i \in I}$ et $(w_i)_{i \in I}$ deux familles d'éléments de $\mathbb{R}_+ \cup \{+\infty\}$ et soit $\alpha \in \mathbb{R}_+ \cup \{+\infty\}$.

Alors, dans tous les cas, $\sum_{i \in I} (\alpha v_i + w_i) = \alpha \sum_{i \in I} v_i + \sum_{i \in I} w_i$.

5 Familles sommables de complexes

Notation. I désigne un ensemble au plus dénombrable et $(J_n)_{n \in \mathbb{N}}$ est une suite adaptée à I .

On fixe une famille $u = (u_i)_{i \in I}$ de complexes.

Définition. $(u_i)_{i \in I}$ est sommable si et seulement si la famille $(|u_i|)_{i \in I}$ est sommable dans \mathbb{R}_+ .

Ainsi, $(u_i)_{i \in I}$ est sommable si et seulement si $\sum_{i \in I} |u_i| < +\infty$.

Propriété. Supposons que tous les u_i sont réels. On pose $u_i^+ = \max(u_i, 0)$ et $u_i^- = \max(-u_i, 0)$. : $u_i = u_i^+ - u_i^-$ et $|u_i| = u_i^+ + u_i^-$. $(u_i)_{i \in I}$ est sommable si et seulement si $(u_i^+)_{i \in I}$ et $(u_i^-)_{i \in I}$ sont sommables. Dans ce cas, on pose $\sum_{i \in I} u_i = \sum_{i \in I} u_i^+ - \sum_{i \in I} u_i^-$.

Propriété. Supposons que les u_i sont complexes. Alors $\operatorname{Re}(u) = (\operatorname{Re}(u_k))_{k \in I}$ et $\operatorname{Im}(u) = (\operatorname{Im}(u_k))_{k \in I}$ sont à valeurs dans \mathbb{R} . u est sommable si et seulement si $\operatorname{Re}(u)$ et $\operatorname{Im}(u)$ sont sommables et dans ce cas, on convient que $\sum_{k \in I} u_k = \sum_{k \in I} \operatorname{Re}(u_k) + i \sum_{k \in I} \operatorname{Im}(u_k)$,

Propriété. $\forall (u_i)_{i \in I} \in \mathbb{C}^I$, $\sum_{i \in I} u_i = \lim_{n \rightarrow +\infty} \sum_{j \in J_n} u_j$.

Il faut savoir le démontrer.

Inégalité triangulaire : si u est sommable, alors $|\sum_{i \in I} u_i| \leq \sum_{i \in I} |u_i|$.

Propriété. Lorsque $I = \mathbb{N}$, une suite $(u_n)_{n \in \mathbb{N}}$ est sommable si et seulement si la série $\sum u_n$ est absolument convergente. Dans ce cas, $\sum_{n \in \mathbb{N}} u_n = \sum_{n=0}^{+\infty} u_n$.

Propriété. Lorsque $I = \mathbb{Z}$, $(u_n)_{n \in \mathbb{Z}}$ est sommable si et seulement si les séries $\sum_{n \geq 0} u_n$ et $\sum_{n \geq 0} u_{-n}$ sont absolument convergentes et dans ce cas $\sum_{n \in \mathbb{Z}} u_n = \sum_{n=1}^{+\infty} u_{-n} + \sum_{n=0}^{+\infty} u_n$.

6 Propriétés des familles sommables

Notation. I désigne un ensemble au plus dénombrable et $(J_n)_{n \in \mathbb{N}}$ est une suite adaptée à I .

6.1 Linéarité

Propriété de linéarité : soit $a = (a_i)_{i \in I}$ et $b = (b_i)_{i \in I}$ deux familles sommables de complexes et soit $\alpha \in \mathbb{C}$. Alors la famille $\alpha a + b = (\alpha a_i + b_i)_{i \in I}$ est sommable et $\sum_{i \in I} (\alpha a_i + b_i) = \alpha \sum_{i \in I} a_i + \sum_{i \in I} b_i$.

Il faut savoir le démontrer.

Propriété. Soit $(u_i)_{i \in I} \in \mathbb{R}_+^I$ et $(v_i)_{i \in I} \in \mathbb{C}^I$. Si pour tout $i \in I$, $|v_i| \leq u_i$ et si (u_i) est sommable, alors (v_i) est sommable et $|\sum_{i \in I} v_i| \leq \sum_{i \in I} u_i$.

Notation. $l^\infty(I, \mathbb{K})$ est l'ensemble des familles $(u_i)_{i \in I}$ bornées de réels, et pour $p \in [1, +\infty[$, $l^p(I, \mathbb{K}) = \left\{ (u_i)_{i \in I} / \sum_{i \in I} |u_i|^p < +\infty \right\}$.

Propriété. $l^1(I, \mathbb{K})$, $l^2(I, \mathbb{K})$ et $l^\infty(I, \mathbb{K})$ sont des sous-espaces vectoriels de \mathbb{K}^I . De plus si (a_i) et (b_i) sont dans $l^2(I, \mathbb{K})$, alors $(a_i b_i)$ est un élément de $l^1(I, \mathbb{K})$.

Propriété. Pour tout $(u_i), (v_i) \in l^2(I, \mathbb{R})$, on pose $((u_i)|(v_i)) = \sum_{i \in I} u_i v_i$.

$l^2(I, \mathbb{R})$ muni de $(.|.)$ est un espace préhilbertien.

Propriété.

- En posant $\|(u_i)_{i \in I}\|_\infty = \sup_{i \in I} |u_i|$, $(l^\infty(I), \mathbb{K})$ est un espace vectoriel normé ;
- En posant $\|(u_i)_{i \in I}\|_1 = \sum_{i \in I} |u_i|$, $(l^1(I), \mathbb{K})$ est un espace vectoriel normé ;
- En posant $\|(u_i)_{i \in I}\|_2 = \sqrt{\sum_{i \in I} |u_i|^2}$, $(l^2(I), \mathbb{K})$ est un espace vectoriel normé.

6.2 Commutativité

Propriété. Commutativité de la somme d'une famille sommable.

Soient $(u_i)_{i \in I}$ une famille sommable de complexes et φ une bijection de I dans I .

Alors $(u_{\varphi(i)})_{i \in I}$ est aussi sommable et $\sum_{i \in I} u_{\varphi(i)} = \sum_{i \in I} u_i$.

Il faut savoir le démontrer.

Propriété. (Hors programme) Soient $(u_i)_{i \in I}$ une famille sommable de complexes et φ une bijection de K dans I . Alors $(u_{\varphi(k)})_{k \in K}$ est aussi sommable et $\sum_{k \in K} u_{\varphi(k)} = \sum_{i \in I} u_i$.

Remarque. Lorsque $(u_i)_{i \in I} \in \mathbb{R}_+^I$, pour toute bijection d'un ensemble K dans I , $\sum_{k \in K} u_{\varphi(k)} = \sum_{i \in I} u_i$.

Théorème. Sommation par paquets pour des familles de réels positifs.

Soit $(I_q)_{q \in \mathbb{N}}$ une partition de I (on accepte que certains I_q soient vides).

On suppose que $u = (u_i)_{i \in I} \in \mathbb{R}_+^I$. Alors u est sommable si et seulement si

- ◇ pour tout $q \in \mathbb{N}$, la famille $(u_i)_{i \in I_q}$ est sommable et
- ◇ la suite $\left(\sum_{i \in I_q} u_i \right)_{q \in \mathbb{N}}$ est sommable.

Dans ce cas, $\sum_{i \in I} u_i = \sum_{q \in \mathbb{N}} \sum_{i \in I_q} u_i$.

Remarque. En cas de non sommabilité, on a encore : $\sum_{i \in I} u_i = \sum_{q \in \mathbb{N}} \sum_{i \in I_q} u_i = +\infty$.

Ainsi, on peut énoncer le théorème sous une forme plus concise :

si $(I_q)_{q \in \mathbb{N}}$ est une partition de I et si $(u_i)_{i \in I} \in \mathbb{R}_+^I$, alors $\sum_{i \in I} u_i = \sum_{q \in \mathbb{N}} \sum_{i \in I_q} u_i$.

Corollaire. Intersion de sommations pour des suites doubles de réels positifs (Fubini).

Soit $(u_{p,q})_{(p,q) \in \mathbb{N}^2} \in \mathbb{R}_+^{\mathbb{N}^2}$. Les propriétés suivantes sont équivalentes.

- ◇ La famille $(u_{p,q})_{(p,q) \in \mathbb{N}^2}$ est sommable.
- ◇ Pour tout $q \in \mathbb{N}$, $(u_{p,q})_{p \in \mathbb{N}}$ est sommable et la suite $\left(\sum_{p \in \mathbb{N}} u_{p,q} \right)_{q \in \mathbb{N}}$ est sommable.
- ◇ Pour tout $p \in \mathbb{N}$, $(u_{p,q})_{q \in \mathbb{N}}$ est sommable et la suite $\left(\sum_{q \in \mathbb{N}} u_{p,q} \right)_{p \in \mathbb{N}}$ est sommable.

Dans ce cas, on dit que $(u_{p,q})_{(p,q) \in \mathbb{N}^2}$ est une suite double sommable et on dispose des égalités suivantes.

$$\sum_{(p,q) \in \mathbb{N}^2} u_{p,q} = \sum_{q=0}^{+\infty} \left(\sum_{p=0}^{+\infty} u_{p,q} \right) = \sum_{p=0}^{+\infty} \left(\sum_{q=0}^{+\infty} u_{p,q} \right).$$

Remarque. Comme précédemment, si l'on accepte de travailler dans $\mathbb{R}_+ \cup \{+\infty\}$, on peut énoncer ce théorème sous la forme suivante :

Pour tout $(u_{p,q})_{(p,q) \in \mathbb{N}^2} \in \mathbb{R}_+^{\mathbb{N}^2}$, $\sum_{(p,q) \in \mathbb{N}^2} u_{p,q} = \sum_{q=0}^{+\infty} \left(\sum_{p=0}^{+\infty} u_{p,q} \right) = \sum_{p=0}^{+\infty} \left(\sum_{q=0}^{+\infty} u_{p,q} \right)$.

Théorème. Sommation par paquets pour des familles de complexes.

Soit $(I_q)_{q \in \mathbb{N}}$ une partition de I et $(u_i)_{i \in I}$ une famille sommable de complexes. Alors, pour tout $q \in \mathbb{N}$, $(u_i)_{i \in I_q}$ est sommable, et $\left(\sum_{i \in I_q} u_i \right)_{q \in \mathbb{N}}$ est sommable. De plus, $\boxed{\sum_{i \in I} u_i = \sum_{q \in \mathbb{N}} \sum_{i \in I_q} u_i}$.

Corollaire. Interversion de sommations pour des suites doubles de complexes.

Soit $(u_{p,q})_{(p,q) \in \mathbb{N}^2} \in \mathbb{C}^{\mathbb{N}^2}$ une suite double sommable de complexes. Pour tout $q_0 \in \mathbb{N}$, (u_{p,q_0}) est sommable, pour tout $p_0 \in \mathbb{N}$, $(u_{p_0,q})$ est sommable, et les suites $\left(\sum_{p \in \mathbb{N}} u_{p,q} \right)_{q \in \mathbb{N}}$ et $\left(\sum_{q \in \mathbb{N}} u_{p,q} \right)_{p \in \mathbb{N}}$ sont sommables. De plus $\sum_{(p,q) \in \mathbb{N}^2} u_{p,q} = \sum_{q=0}^{+\infty} \left(\sum_{p=0}^{+\infty} u_{p,q} \right) = \sum_{p=0}^{+\infty} \left(\sum_{q=0}^{+\infty} u_{p,q} \right)$.

Exemple. Soient $\sum a_n$ et $\sum b_n$ deux séries absolument convergentes de complexes. Alors la famille $(a_p b_q)_{(p,q) \in \mathbb{N}^2}$ est une suite double sommable et $\sum_{(p,q) \in \mathbb{N}^2} a_p b_q = \left(\sum_{p \in \mathbb{N}} a_p \right) \left(\sum_{q \in \mathbb{N}} b_q \right)$.

Il faut savoir le démontrer.

Définition. Produit de Cauchy de deux séries. Soient $\sum u_n$ et $\sum v_n$ deux séries de complexes.

Pour tout $n \in \mathbb{N}$, on pose $w_n = \sum_{p+q=n} u_p v_q = \sum_{p=0}^n u_p v_{n-p}$.

La série $\sum w_n$ est appelée le produit de Cauchy des deux séries $\sum u_n$ et $\sum v_n$.

Propriété. Le produit de Cauchy de deux séries **absolument** convergentes est absolument convergent.

Si $\sum u_n$ et $\sum v_n$ sont absolument convergentes, alors $\sum_{n=0}^{+\infty} w_n = \left(\sum_{n=0}^{+\infty} u_n \right) \left(\sum_{n=0}^{+\infty} v_n \right)$.

Il faut savoir le démontrer.

Semaine 35 (du 22 au 27 juin) : Résumé de cours

Les probabilités (début)

1 Espaces probabilisés

Définition. On appelle tribu, ou σ -algèbre sur un ensemble Ω tout ensemble \mathcal{F} de parties de Ω vérifiant : $\Omega \in \mathcal{F}$, \mathcal{F} est stable par passage au complémentaire (si $F \in \mathcal{F}$ alors $\Omega \setminus F \in \mathcal{F}$) et \mathcal{F} est stable par réunion dénombrable (si $(F_n)_{n \in \mathbb{N}} \in \mathcal{F}^{\mathbb{N}}$, alors $\bigcup_{n \in \mathbb{N}} F_n \in \mathcal{F}$).

Vocabulaire spécifique aux probabilités : Avec les notations précédentes,

- ◇ Ω s'appelle l'univers.
- ◇ Les éléments de \mathcal{F} s'appellent les **événements**.
- ◇ Si $\{\omega\} \in \mathcal{F}$, on dit que c'est un **événement élémentaire**.
- ◇ \emptyset est l'événement impossible.
- ◇ Si A est un événement, $\Omega \setminus A$ est l'événement contraire de A .
- ◇ Si A et B sont deux événements, $A \cap B$ est l'événement “ A et B ”, $A \cup B$ est l'événement “ A ou B ”. Lorsque $A \cap B = \emptyset$, les deux événements A et B sont dits incompatibles.

Définition. Soit \mathcal{F} une tribu sur un univers Ω . On appelle système complet d'événements toute famille $(A_i)_{i \in I}$ (où I est fini ou dénombrable) d'événements 2 à 2 disjoints dont la réunion vaut Ω .

Définition. Si \mathcal{F} est une tribu sur un univers Ω , on dit que (Ω, \mathcal{F}) est un espace probabilisable.

Définition. Soit (Ω, \mathcal{F}) un espace probabilisable. On dit que P est une probabilité sur (Ω, \mathcal{F}) si et seulement si P est une application de \mathcal{F} dans $[0, 1]$ telle que $P(\Omega) = 1$ et pour toute suite $(F_n)_{n \in \mathbb{N}}$

d'événements de \mathcal{F} deux à deux disjoints, $P\left(\bigcup_{n=0}^{\infty} F_n\right) = \sum_{n=0}^{\infty} P(F_n)$.

Dans ce cas, le triplet (Ω, \mathcal{F}, P) est appelé un espace probabilisé.

Propriété. Avec les notations précédentes, pour $F, G, H, F_n \in \mathcal{F}$ on a :

- ◇ $P(\emptyset) = 0$,
- ◇ Si F_0, \dots, F_p sont $p+1$ événements deux à deux disjoints, où $p \geq 1$,

alors $P\left(\bigcup_{n=0}^p F_n\right) = \sum_{n=0}^p P(F_n)$.

- ◇ $P(\overline{F}) = 1 - P(F)$ (où \overline{F} désigne $\Omega \setminus F$),
- ◇ si $G \subset H$, $P(H \setminus G) = P(H) - P(G)$.
- ◇ si $G \subset H$, $P(G) \leq P(H)$ (on dit que P est croissante),
- ◇ $P(G \cup H) = P(G) + P(H) - P(G \cap H)$,
- ◇ **Inégalité de Boole :** $P\left(\bigcup_{n=0}^{\infty} F_n\right) \leq \sum_{n=0}^{\infty} P(F_n)$.

Il faut savoir le démontrer.

Notation. On notera souvent $P(G, H) \triangleq P(G \cap H)$.

Propriété : Probabilité sur un univers dénombrable. Lorsque Ω est fini ou dénombrable, on prendra toujours $\mathcal{F} = \mathcal{P}(\Omega)$. Dans ce cas, pour se donner une probabilité P sur (Ω, \mathcal{F}) , il faut et il suffit de donner une famille sommable $(p_\omega)_{\omega \in \Omega}$ de réels positifs telle que $\sum_{\omega \in \Omega} p_\omega = 1$. On définit alors

$$P \text{ par : pour tout } F \in \mathcal{F}, P(F) = \sum_{\omega \in F} p_\omega.$$

Définition. Supposons que Ω est de cardinal fini. On dit que P est la probabilité uniforme lorsque tous les événements élémentaires sont équiprobables. Dans ce cas, avec les notations de la propriété précédente, pour tout $\omega \in \Omega$, $p_\omega = \frac{1}{\text{Card}(\Omega)}$, et pour tout $F \in \mathcal{F}$, $P(F) = \frac{\text{Card}(F)}{\text{Card}(\Omega)}$.

Propriété de continuité : dans un espace probabilisé (Ω, \mathcal{F}, P) ,

si (F_n) est une suite croissante d'événements, $P\left(\bigcup_{n=0}^{\infty} F_n\right) = \lim_{n \rightarrow +\infty} P(F_n)$.

Si (F_n) est une suite décroissante d'événements, $P\left(\bigcap_{n=0}^{\infty} F_n\right) = \lim_{n \rightarrow +\infty} P(F_n)$.

Il faut savoir le démontrer.

Définition. On dit que l'événement F est négligeable si et seulement si $P(F) = 0$.

On dit que l'événement F est presque sûr si et seulement si $P(F) = 1$.

Si \mathcal{Q} est une propriété dépendant de $\omega \in \Omega$, lorsque $\{\omega \in \Omega / \mathcal{Q}(\omega)\}$ est un événement presque sûr, on dit que " $\mathcal{Q}(\omega)$ presque sûrement".

Propriété. Une réunion finie ou dénombrable d'événements négligeables est négligeable.

Une intersection finie ou dénombrable d'événements presque sûrs est presque sûre.

2 Probabilité conditionnelle et indépendance

Définition. Si $P(G) > 0$, $P(H|G) \triangleq \frac{P(H \cap G)}{P(G)}$: c'est la probabilité conditionnelle de H sachant que G est réalisé. L'application $H \mapsto P(H|G)$ est une probabilité sur Ω , notée P_G .

$$\text{Ainsi, } P(H|G) = P_G(H) = \frac{P(H \cap G)}{P(G)}.$$

Formule des probabilités composées :

si G_1, \dots, G_k sont k événements tels que $P(G_1 \cap \dots \cap G_{k-1}) > 0$, alors

$$P\left(\bigcap_{i=1}^k G_i\right) = P(G_1) \times P(G_2|G_1) \times P(G_3|G_1 \cap G_2) \times \dots \times P(G_k|G_1 \cap \dots \cap G_{k-1}).$$

Formule des probabilités totales : si $(G_i)_{i \in I}$ est un système complet d'événements, où I est fini ou dénombrable, et si pour tout $i \in I$, $P(G_i) > 0$, alors $P(G) = \sum_{i \in I} P(G|G_i)P(G_i)$.

Formule de Bayes : Si $P(G) \in]0, 1[$ et $P(H) > 0$, alors
$$P(G|H) = \frac{P(H|G)P(G)}{P(H|G)P(G) + P(H|\bar{G})P(\bar{G})}$$

Si $(G_i)_{i \in I}$ est un système complet d'événements avec pour tout $i \in I$, $P(G_i) > 0$, et si $P(H) > 0$,

$$\text{alors } P(G_i|H) = \frac{P(H|G_i)P(G_i)}{\sum_{j \in I} P(H|G_j)P(G_j)}.$$

Il faut savoir le démontrer.

Définition. H et G sont indépendants si et seulement si $P(G \cap H) = P(G)P(H)$.

Propriété. Si H et G sont indépendants, alors H et \overline{G} sont aussi indépendants.

Remarque. Un événement A est indépendant de lui-même si et seulement si $P(A) \in \{0, 1\}$.

Définition. I étant un ensemble quelconque, les événements de la famille $(G_i)_{i \in I}$ sont mutuellement indépendants si et seulement si pour toute partie finie J de I , $P\left(\bigcap_{i \in J} G_i\right) = \prod_{i \in J} P(G_i)$.

Remarque. “mutuellement indépendants” \implies “2 à 2 indépendants”, mais la réciproque est fausse.

Propriété. Soit $(G_i)_{i \in I}$ une famille d'événements mutuellement indépendants. Si l'on remplace certains G_i par leur conjugué $\overline{G_i}$, alors c'est encore une famille d'événements mutuellement indépendants.

3 Variables aléatoires discrètes

Définition. Soit (Ω, \mathcal{F}, P) un espace de probabilité. Une variable aléatoire à valeurs dans un ensemble E muni d'une tribu \mathcal{E} est une fonction $X : \Omega \longrightarrow E$ telle que, pour tout $A \in \mathcal{E}$, $X^{-1}(A) \in \mathcal{F}$. On note souvent “ $X \in A$ ” au lieu de $X^{-1}(A)$.

Remarque. Lorsque $E = \mathbb{R}$, on dit que X est une variable aléatoire réelle. Lorsque $E = \mathbb{N}$, on dit que X est une variable aléatoire entière.

Propriété. Avec les notations précédentes, si l'on pose, pour tout $A \in \mathcal{E}$, $P_X(A) = P(X \in A)$, alors P_X est une probabilité sur (E, \mathcal{E}) que l'on appelle la loi de X .

Définition. Si B est un événement de Ω , la loi de X conditionnée par B désigne l'application $A \longmapsto P(X \in A | B) = \frac{P((X \in A) \cap B)}{P(B)}$, de \mathcal{E} dans $[0, 1]$. C'est encore une probabilité sur (E, \mathcal{E}) .

Définition. On dit qu'une variable aléatoire X est discrète si et seulement si $X(\Omega)$ est fini ou dénombrable et si $\mathcal{E} = \mathcal{P}(E)$.

Remarque. Le programme de MP ne prévoit que l'étude des variables aléatoires discrètes, ce que nous supposons donc dorénavant.

Propriété. Soit (Ω, \mathcal{F}, P) un espace de probabilité et X une application de Ω dans un ensemble quelconque E . X est une variable aléatoire discrète si et seulement si $X(\Omega)$ est fini ou dénombrable et si, pour tout $d \in X(\Omega)$, $X^{-1}(\{d\}) \in \mathcal{F}$.

Dans ce cas, la loi de X est entièrement déterminée par la famille $(P(X = d))_{d \in X(\Omega)}$.

Remarque. Toute variable aléatoire entière est discrète.

Définition. Soit X une variable aléatoire discrète de Ω dans E et f une application de E dans un ensemble F . Alors $Y = f(X) \triangleq f \circ X$ est une nouvelle variable aléatoire discrète dont la loi est donnée

par : $\forall y \in F, P_Y(y) = P(X \in f^{-1}(\{y\})) = \sum_{\substack{x \in X(\Omega) \\ f(x) = y}} P_X(x)$.

Il faut savoir le démontrer.

Définition. Soit X une variable aléatoire de Ω dans un ensemble E de cardinal fini. On dit que X suit une loi uniforme (souvent notée \mathcal{U}) si et seulement si P_X est la probabilité uniforme, c'est-à-dire si et seulement si pour tout $k \in E$, $P(X = k) = \frac{1}{\text{Card}(E)}$.

Définition. On fixe une variable aléatoire X à valeurs dans \mathbb{N} . Les lois classiques au programme sont les suivantes :

- Loi de dirac, lorsqu'il existe $n_0 \in \mathbb{N}$ tel que $P(X = n_0) = 1$ et $P(X = n) = 0$ pour tout $n \neq n_0$. On dit alors que X est une variable aléatoire déterministe, ou bien constante.
- **Loi de Bernoulli** de paramètre $p \in [0, 1]$, notée $\mathcal{B}(p)$:

$$P(X = 1) = p \text{ et } P(X = 0) = 1 - p.$$
C'est le cas lorsque X représente le succès ($X = 1$) ou l'échec ($X = 0$) d'une épreuve.
- **Loi binomiale** de paramètres $n \in \mathbb{N}^*$ et $p \in [0, 1]$, notée $\mathcal{B}(n, p)$:
Pour tout $k \in \{0, \dots, n\}$,
$$P(X = k) = \binom{n}{k} p^k (1 - p)^{n-k}$$
 (et $P(X = m) = 0$ pour $m \notin \{0, \dots, n\}$). C'est le cas lorsque X désigne le nombre de succès parmi une suite de n épreuves indépendantes de loi de Bernoulli de paramètre p .
- **Loi géométrique** de paramètre $p \in]0, 1[$, notée $\mathcal{G}(p)$:
Pour tout $n \in \mathbb{N}^*$,
$$P(X = n) = (1 - p)^{n-1} p$$
 (et $P(X = 0) = 0$).
C'est le cas lorsque X représente l'instant du premier succès lors d'une suite d'épreuves indépendantes de loi de Bernoulli de paramètre p .
- **Loi de Poisson** de paramètre $\lambda \in \mathbb{R}_+^*$, notée $\mathcal{P}(\lambda)$: pour tout $n \in \mathbb{N}$,
$$P(X = n) = e^{-\lambda} \frac{\lambda^n}{n!}.$$

Notation. On utilisera la notation $X \sim \mathcal{L}$ pour indiquer que la variable aléatoire X suit la loi \mathcal{L} et la notation $X \sim Y$ pour indiquer que les deux variables aléatoires suivent la même loi.

Propriété. X est une variable aléatoire à valeurs dans $\{0, 1\}$ si et seulement si il existe un événement A tel que $X = 1_A$. Dans ce cas, on a $X = 1_A \sim \mathcal{B}(p)$ où $p = P(A)$.

Semaine 36 (du 29 juin au 3 juillet) : Résumé de cours

Les probabilités (fin)

1 Variables aléatoires discrètes (suite)

Définition. Si X est une variable aléatoire réelle, l'application $x \mapsto P(X \leq x)$ est la fonction de répartition de X .

Définition. Hors programme : Convergence en loi :

Soit $(X_k)_{k \in \mathbb{N}}$ une suite de variables aléatoires réelles et X une autre variable aléatoire réelle. On dit que X_k converge en loi vers X lorsque k tend vers $+\infty$ si et seulement si pour tout $x \in \mathbb{R}$ tel que $P(X = x) = 0$, $P(X_k \leq x) \xrightarrow[k \rightarrow +\infty]{} P(X \leq x)$. on note alors $X_k \xrightarrow[k \rightarrow +\infty]{\mathcal{L}} X$.

Propriété. Soit $(X_k)_{k \in \mathbb{N}}$ une suite de variables aléatoires entières et X une autre variable aléatoire entière. $X_k \xrightarrow[k \rightarrow +\infty]{\mathcal{L}} X \iff [\forall n \in \mathbb{N}, P(X_k = n) \xrightarrow[k \rightarrow +\infty]{} P(X = n)]$.

Propriété. Pour les variables aléatoires entières, les lois géométriques sont les seules lois sans mémoire. Plus précisément, si X est une variable aléatoire à valeurs dans \mathbb{N}^* , elle est sans mémoire, c'est-à-dire qu'elle vérifie pour tout $(n, k) \in \mathbb{N}^2$ $P(X > n + k | X > n) = P(X > k)$, si et seulement si il existe $p \in]0, 1[$ tel que $X \sim \mathcal{G}(p)$.

Il faut savoir le démontrer.

2 Variables aléatoires indépendantes

2.1 Lois conjointes et lois marginales

Définition. Soit $n \in \mathbb{N}^*$. Si X_1, \dots, X_n est une suite de n variables aléatoires discrète de Ω dans des ensemble E_i , alors, en posant pour tout $\omega \in \Omega$, $X(\omega) = (X_1(\omega), \dots, X_n(\omega))$, on définit une variable aléatoire discrète $X \triangleq (X_1, \dots, X_n)$ de Ω dans $E_1 \times \dots \times E_n$.

On dit que la loi de X est la loi conjointe des variables aléatoires X_1, \dots, X_n .

Pour tout $i \in \{1, \dots, n\}$, la loi de X_i est appelée la i ème loi marginale de X .

Exemple. Soit $X = (X_1, X_2)$ un couple de variables aléatoires entières. On note $(p_{1,k}) = (P(X_1 = k))$ la première loi marginale de X et $(p_{2,k}) = (P(X_2 = k))$ la seconde loi marginale.

On note également $c_{h,k} = P(X = (h, k))$ la loi conjointe. Alors $p_{1,k} = \sum_{h \in \mathbb{N}} c_{k,h}$ et $p_{2,k} = \sum_{h \in \mathbb{N}} c_{h,k}$.

Définition. Soit $X = (X_1, X_2)$ un couple de variables aléatoires discrètes. Pour tout $h \in X_2(\Omega)$ tel que $P(X_2 = h) > 0$, la loi conditionnelle de X_1 sachant que $X_2 = h$ désigne la probabilité $A \mapsto P(X_1 \in A | X_2 = h)$ (définie sur $\mathcal{P}(X_1(\Omega))$). Elle est caractérisée par la suite des

$(P(X_1 = k|X_2 = h))_{k \in \mathbb{N}}$. On définit de même la loi conditionnelle de X_2 sachant que $X_1 = k$.

Exemple. Avec les notations de l'exemple précédent, $P(X_1 = k|X_2 = h) = \frac{c_{k,h}}{p_{2,h}}$.

2.2 Indépendance

Définition. Soit $X = (X_1, \dots, X_n)$ un n -uplet de variables discrètes. Elles sont mutuellement indépendantes si et seulement si pour tout $k = (k_1, \dots, k_n) \in \prod_{i=1}^n X_i(\Omega)$, $P(X = k) = \prod_{i=1}^n P(X_i = k_i)$.

Propriété. X_1, \dots, X_n sont indépendantes si et seulement si pour toute famille K_1, \dots, K_n de parties de $X_1(\Omega), \dots, X_n(\Omega)$, $P(X_1 \in K_1, \dots, X_n \in K_n) = \prod_{i=1}^n P(X_i \in K_i)$.

Remarque. Si X_1, \dots, X_n sont des variables aléatoires mutuellement indépendantes, alors elles sont 2 à 2 indépendantes, mais la réciproque est fausse.

Définition. Si $(X_i)_{i \in I}$ est une famille de variables aléatoires discrètes, avec I de cardinal infini, on dit que ces variables aléatoires sont mutuellement indépendantes si et seulement si pour toute partie finie J incluse dans I , les variables aléatoires X_j pour $j \in J$ sont mutuellement indépendantes.

Propriété. Soit X et Y deux variables aléatoires discrètes indépendantes de Ω dans E et F respectivement. Soit $f : E \rightarrow E'$ et $g : F \rightarrow F'$ deux fonctions. Alors $f(X)$ et $g(Y)$ sont encore deux variables aléatoires discrètes indépendantes.

Il faut savoir le démontrer.

Remarque. On peut généraliser l'énoncé et la démonstration au cas suivant : Si $(X_i)_{i \in I}$ est une famille de variables aléatoires mutuellement indépendantes, alors pour toute famille de fonctions $(f_i)_{i \in I}$ correctement définies, $(f_i(X_i))_{i \in I}$ est encore une famille de variables aléatoires mutuellement indépendantes.

Corollaire. Soit $X_1, \dots, X_m, Y_1, \dots, Y_n$ des variables aléatoires discrètes mutuellement indépendantes. Alors pour toutes fonctions f et g correctement définies, les variables aléatoires $f(X_1, \dots, X_m)$ et $g(Y_1, \dots, Y_n)$ sont indépendantes.

Remarque. Là encore, on peut généraliser ...

Propriété. Soit X_1, \dots, X_m des variables aléatoires entières mutuellement indépendantes. On suppose qu'il existe $p \in [0, 1]$ tel que, pour tout $i \in \{1, \dots, m\}$, $X_i \sim \mathcal{B}(n_i, p)$, où $n_i \in \mathbb{N}^*$ (p ne dépend pas de i). Alors $X_1 + \dots + X_m \sim \mathcal{B}(n_1 + \dots + n_m, p)$.

Il faut savoir le démontrer.

Remarque. On en déduit que le nombre de succès parmi une suite de m épreuves indépendantes de loi de Bernoulli de paramètre p suit une loi binomiale de paramètres m et p .

Exercice. Soit X_1, \dots, X_m des variables aléatoires entières mutuellement indépendantes telles que chaque X_i suit une loi de Poisson de paramètre $\lambda_i > 0$. Montrer que $X = X_1 + \dots + X_n$ suit une loi de Poisson de paramètre $\lambda = \lambda_1 + \dots + \lambda_m$.

Il faut savoir le démontrer.

Propriété. Soit $(p_n) \in]0, 1[^\mathbb{N}$ telle que $np_n \xrightarrow{n \rightarrow +\infty} \lambda \in \mathbb{R}_+^*$. Soit (X_n) une suite de variables aléatoires telle que $X_n \sim \mathcal{B}(n, p_n)$. Alors X_n converge en loi vers la loi de Poisson de paramètre λ .

Il faut savoir le démontrer.

Remarque. Vue la démonstration, l'approximation de la loi de X_n par une loi de Poisson est d'autant plus valable que $k \ll n$ et $\lambda \ll n$.

Application : Dans une file d'attente, supposons que le nombre moyen d'individus arrivant entre les temps 0 et 1 vaut $\lambda > 0$. On note N la variable aléatoire égale au nombre d'individus arrivant dans la file d'attente entre les temps 0 et 1. On suppose que, pour n suffisamment grand, au plus un individu arrive entre les temps $\frac{i-1}{n}$ et $\frac{i}{n}$ (c'est l'hypothèse des événements rares). Alors N suit une loi de Poisson de paramètre λ .

Définition. Une loi discrète sur un ensemble E est la donnée d'une probabilité sur E muni de sa tribu pleine $\mathcal{P}(E)$ telle que $A = \{x \in E / P(x) > 0\}$ est fini ou dénombrable et telle que $\sum_{x \in A} P(x) = 1$.

Théorème. Soit $(E_n)_{n \in \mathbb{N}}$ une suite d'ensembles et pour tout $n \in \mathbb{N}$, soit \mathcal{L}_n une loi discrète sur E_n . Alors il existe un espace probabilisé (Ω, \mathcal{F}, P) et une suite (X_n) de variables aléatoires mutuellement indépendantes telle que, pour tout $n \in \mathbb{N}$, $X_n \sim \mathcal{L}_n$.

Remarque. Ce théorème prouve l'existence d'une suite $(X_n)_{n \geq 1}$ de variables aléatoires indépendantes telles que pour tout $n \in \mathbb{N}^*$, $X_n \sim \mathcal{B}(p)$, où $p \in]0, 1[$ ne dépend pas de n . Cette suite modélise une succession infinie d'épreuves indépendantes qui ont toutes la même probabilité de succès, égale à p . Notons X la variable aléatoire égale à l'instant du premier succès : $X(\omega) = \min\{k \in \mathbb{N}^* / X_k(\omega) = 1\}$. Alors $X \sim \mathcal{G}(p)$.

3 Espérance et variance

3.1 L'espérance

Définition. Soit X est une variable aléatoire discrète à valeurs réelles.

◇ Si X est à valeurs dans \mathbb{R}_+ , $E(X) \triangleq \sum_{d \in X(\Omega)} d \cdot P(X = d) \in \mathbb{R}_+ \cup \{+\infty\}$.

◇ Sinon, on dit que X est d'espérance finie si et seulement si $(d \cdot P(X = d))_{d \in X(\Omega)}$ est sommable, et dans ce cas, $E(X) \triangleq \sum_{d \in X(\Omega)} d \cdot P(X = d)$.

Remarque. $E(X)$ ne dépend que de la loi de X .

Propriété. Si Ω est fini ou dénombrable, alors $E(X) = \sum_{\omega \in \Omega} X(\omega) P(\{\omega\})$.

Propriété. Si A est un événement de l'espace probabilisé (Ω, \mathcal{F}, P) , alors $\boxed{P(A) = E(1_A)}$, où 1_A désigne la fonction caractéristique de la partie A de Ω .

Définition. Une variable aléatoire réelle est dite centrée si et seulement si $E(X) = 0$.

Exercice. Montrer qu'une variable aléatoire réelle et positive est centrée si et seulement si elle est nulle presque sûrement.

Il faut savoir le démontrer.

Théorème de transfert : Soit $X : \Omega \rightarrow E$ une variable aléatoire discrète et $g : E \rightarrow \mathbb{R}$ une application. $g(X)$ est d'espérance finie si et seulement si la famille $(g(d) \cdot P(X = d))_{d \in X(\Omega)}$ est sommable, et dans ce cas,

$$\boxed{E(g(X)) = \sum_{d \in X(\Omega)} g(d) P(X = d)}.$$

Il faut savoir le démontrer lorsque $X(\Omega)$ est fini.

Linéarité de l'espérance :

On note $L^1(\Omega, P)$ l'ensemble des variables aléatoires discrètes de Ω dans \mathbb{R} d'espérance finie.

$L^1(\Omega, P)$ est un espace vectoriel et pour tout $X, Y \in L^1(\Omega, P)$, $E(\alpha X + \beta Y) = \alpha E(X) + \beta E(Y)$.

Il faut savoir le démontrer.

Propriété. Si $X \in L^1(\Omega, P)$, pour tout $a, b \in \mathbb{R}$, $aX + b \in L^1(\Omega, P)$ et $E(aX + b) = aE(X) + b$.

Propriété. Soit $X \in L^1(\Omega, P)$. Si X est presque sûrement constante égale à c , alors $E(X) = c$.
 X est presque sûrement constante si et seulement si X est presque sûrement égale à son espérance.

Propriété. $X \geq 0 \implies E(X) \geq 0$.

Propriété. Croissance de l'espérance : $X \leq Y \implies E(X) \leq E(Y)$.

Propriété. Inégalité triangulaire : Pour tout $X \in L^1(\Omega, P)$, $|E(X)| \leq E(|X|)$.

Propriété de comparaison : Soit X et Y deux variables aléatoires réelles telles que $|X| \leq Y$ et Y est d'espérance finie. Alors X est aussi d'espérance finie.

Formule. Inégalité de Markov : Si $X \geq 0$ et $a > 0$, alors $P(X \geq a) \leq \frac{E(X)}{a}$.

Il faut savoir le démontrer.

Théorème. Si X_1, \dots, X_k sont k variables aléatoires discrètes réelles d'espérances finies et **mutuellement indépendantes**, alors $X_1 \times \dots \times X_k$ est d'espérance finie et $E(X_1 \times \dots \times X_k) = E(X_1) \times \dots \times E(X_k)$. La réciproque est fausse.

À savoir démontrer lorsque les $X_i(\Omega)$ sont finis.

3.2 La variance

Définition. Soit $k \in \mathbb{N}^*$ et X une variable aléatoire réelle. Si X^k est d'espérance finie, on dit que $E(X^k)$ est le moment d'ordre k de X .

Notation. On note $L^2(\Omega, P)$ l'ensemble des variables aléatoires X discrètes à valeurs réelles possédant un moment d'ordre 2, définies sur l'espace probabilisé (Ω, \mathcal{F}, P) .

Lemme : Si $X_1, X_2 \in L^2(\Omega, P)$, alors $X_1 X_2 \in L^1(\Omega, P)$.

Corollaire. $L^2(\Omega, P)$ est un sous-espace vectoriel de $L^1(\Omega, P)$.

Définition. Si $X_1, X_2 \in L^2(\Omega, P)$, la covariance est $Cov(X_1, X_2) = E[(X_1 - E(X_1))(X_2 - E(X_2))]$.

Propriété. Cov est une forme bilinéaire symétrique positive sur $L^2(\Omega, P)$, mais ce n'est pas un produit scalaire.

Définition. Si $X \in L^2(\Omega, P)$, la variance de X est $Var(X) = E[(X - E(X))^2]$.
L'écart type de X est $\sigma(X) = \sqrt{Var(X)}$.

Remarque. $Var(X) = 0$ si et seulement si X est presque sûrement constante.

Définition. X est réduite si et seulement si $X \in L^2(\Omega, P)$ et $Var(X) = 1$.

Propriété. Formule de Koenig-Huygens : Si $X \in L^2(\Omega, P)$, $Var(X) = E(X^2) - E(X)^2$.

Si $X_1, X_2 \in L^2(\Omega, P)$, alors $Cov(X_1, X_2) = E(X_1 X_2) - E(X_1)E(X_2)$: donc, si deux variables aléatoires de $L^2(\Omega, P)$ sont indépendantes, elles sont orthogonales au sens de Cov (la réciproque est fausse).

Propriété. Pour $a, b \in \mathbb{R}$ et $X \in L^2(\Omega, P)$, $Var(aX + b) = a^2 Var(X)$.

Propriété. Si $X \in L^2(\Omega, P)$ avec $\sigma(X) \neq 0$, alors $\frac{X - E(X)}{\sigma(X)}$ est centrée et réduite.

Propriété.

◇ Si $X_1, X_2 \in L^2(\Omega, P)$, $Var(X_1 + X_2) = Var(X_1) + Var(X_2) + 2Cov(X_1, X_2)$.

◇ Si $X_1, \dots, X_k \in L^2(\Omega, P)$, $Var(X_1 + \dots + X_k) = \sum_{i=1}^k Var(X_i) + 2 \sum_{1 \leq i < j \leq k} Cov(X_i, X_j)$.

◇ Si X_1, \dots, X_k sont k variables aléatoires de $L^2(\Omega, P)$ que l'on suppose **deux à deux indépendantes**, alors $Var(X_1 + \dots + X_k) = Var(X_1) + \dots + Var(X_k)$.

Il faut savoir le démontrer.

Propriété. Inégalité de Cauchy-Schwarz : pour tout $X, Y \in L^2(\Omega, P)$, $E(XY)^2 \leq E(X^2)E(Y^2)$, avec égalité ssi il existe $\alpha, \beta \in \mathbb{R}$ tel que $(\alpha, \beta) \neq (0, 0)$ et $\alpha X + \beta Y$ est presque sûrement nulle.
pour tout $X, Y \in L^2(\Omega, P)$, $Cov(X, Y)^2 \leq Var(X)Var(Y)$, avec égalité ssi il existe $\alpha, \beta \in \mathbb{R}$ tel que $(\alpha, \beta) \neq (0, 0)$ et $\alpha X + \beta Y$ est presque sûrement constante.

Définition. (hors programme) : Soient $X, Y \in L^2(\Omega, P)$ telles que $Var(X)Var(Y) > 0$. Le coefficient de corrélation linéaire entre X et Y est $Corr(X, Y) \triangleq \frac{Cov(X, Y)}{\sigma(X)\sigma(Y)}$.

Propriété. $Corr(X, Y) \in [-1, 1]$.

Propriété. $|Corr(X, Y)| = 1$ si et seulement si il existe $(a, b) \in \mathbb{R}^2$ tel que $P(Y = aX + b) = 1$.

Remarque. $Corr(X, Y)$ indique dans quelle mesure Y dépend **linéairement** de X , mais $Corr(X, Y)$ ne mesure pas les dépendances non linéaires (on peut avoir par exemple $Corr(X, X^2) = 0$).

Formule. Espérance et variance pour les lois au programme.

◇ **Loi de Bernoulli** de paramètre $p \in [0, 1]$: $P(X = 1) = p$ et $P(X = 0) = 1 - p$.

$$\boxed{E(X) = p \text{ et } Var(X) = p(1 - p)}.$$

◇ **Loi binomiale** de paramètres $n \in \mathbb{N}^*$ et $p \in [0, 1]$: Pour tout $k \in \{0, \dots, n\}$, $P(X = k) = \binom{n}{k} p^k (1 - p)^{n-k}$ (et $P(X = m) = 0$ pour $m \notin \{0, \dots, n\}$).

$$\boxed{E(X) = np \text{ et } Var(X) = np(1 - p)}.$$

◇ **Loi géométrique** de paramètre $p \in]0, 1[$: Pour tout $n \in \mathbb{N}^*$, $P(X = n) = (1 - p)^{n-1}p$ (et $P(X = 0) = 0$). $\boxed{E(X) = \frac{1}{p} \text{ et } Var(X) = \frac{1 - p}{p^2}}.$

◇ **Loi de Poisson** de paramètre $\lambda \in \mathbb{R}_+^*$:

pour tout $n \in \mathbb{N}$, $P(X = n) = e^{-\lambda} \frac{\lambda^n}{n!}$. $E(X) = \lambda = Var(X)$.

Il faut savoir le démontrer.

4 Propriétés de convergence

Formule. Inégalité de Bienaymé-Tchebychev : Soit X une variable aléatoire réelle. Alors, pour

$$\text{tout } \varepsilon > 0, \quad \boxed{P(|X - E(X)| \geq \varepsilon) \leq \frac{Var(X)}{\varepsilon^2}}.$$

Il faut savoir le démontrer.

Définition. (hors programme) Soit $(X_n)_{n \in \mathbb{N}}$ une suite de variables aléatoires et soit X une variable aléatoire. X_n converge vers X en probabilité ssi pour tout $\varepsilon > 0$, $P(|X_n - X| \geq \varepsilon) \xrightarrow[n \rightarrow +\infty]{} 0$.

Théorème. Loi faible des grands nombres :

Soit (X_n) une suite de variables aléatoires dans $L^2(\Omega, P)$ que l'on suppose toutes de même loi et deux à deux indépendantes. Posons $\mu = E(X_n)$, qui est indépendante de n . Alors $\frac{X_1 + \dots + X_n}{n}$ converge en probabilité vers la variable aléatoire constante égale à μ .

Il faut savoir le démontrer.

Théorie de l'intégration

Notation. $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$, $a, b \in \mathbb{R}$ avec $a < b$, E est un Banach, i.e un \mathbb{K} -espace vectoriel normé complet, f est une application de $[a, b]$ dans E .

5 Intégration des applications en escalier

5.1 Les applications en escalier

Définition. On appelle subdivision de $[a, b]$ toute famille finie $(a_i)_{0 \leq i \leq n}$ de réels telle que $a = a_0 < a_1 < \dots < a_n = b$.

Notation. On notera \mathcal{S} l'ensemble des subdivisions de $[a, b]$.

Exemple. $\left(a + i \frac{b-a}{n}\right)_{0 \leq i \leq n} \in \mathcal{S}$. On dit que c'est une subdivision uniforme.

Définition. Le pas de $\sigma = (a_i)_{0 \leq i \leq n} \in \mathcal{S}$ est $\delta(\sigma) = \max_{1 \leq i \leq n} (a_i - a_{i-1})$.

Notation. Le support de la subdivision σ est l'ensemble $A(\sigma) \triangleq \{a_i / 0 \leq i \leq n\}$.

Propriété. Notons $\mathcal{P}_f([a, b])$ l'ensemble des parties finies de $[a, b]$ contenant a et b .

L'application
$$\begin{array}{ccc} A : \mathcal{S} & \longrightarrow & \mathcal{P}_f([a, b]) \\ \sigma & \longmapsto & A(\sigma) \end{array}$$
 est bijective.

Définition. $\sigma \in \mathcal{S}$ est plus fine que $\sigma' \in \mathcal{S}$ ssi $A(\sigma) \supseteq A(\sigma')$. Dans ce cas, on note $\sigma' \preceq \sigma$.

Propriété. \preceq est une relation d'ordre partiel.

Définition. Si $\sigma, \sigma' \in \mathcal{S}$, on pose $\sigma \cup \sigma' \triangleq A^{-1}(A(\sigma) \cup A(\sigma'))$: c'est l'unique subdivision de $[a, b]$ dont le support est la réunion des supports de σ et de σ' . C'est $\sup\{\sigma, \sigma'\}$.

Définition. f est une application en escalier sur $[a, b]$ si et seulement s'il existe une subdivision $(a_i)_{0 \leq i \leq n}$ de $[a, b]$ telle que, pour tout $i \in \mathbb{N}_n$, f est constante sur l'intervalle $]a_{i-1}, a_i[$.

Définition. Si f est en escalier et $\sigma = (a_i)_{0 \leq i \leq n} \in \mathcal{S}$, σ est une subdivision adaptée à f si et seulement si, pour tout $i \in \mathbb{N}_n$, f est constante sur l'intervalle $]a_{i-1}, a_i[$.

Propriété. Les applications en escalier de $[a, b]$ sont bornées.

Propriété. Soit f une application en escalier et σ une subdivision de $[a, b]$ adaptée à f . Alors toute subdivision plus fine que σ est aussi adaptée à f .

5.2 Intégrale d'une application en escalier

Définition. Soit f une application en escalier et $\sigma = (a_i)_{0 \leq i \leq n}$ une subdivision adaptée à f . Pour tout $i \in \mathbb{N}_n$, notons λ_i la valeur constante de f sur $]a_{i-1}, a_i[$. On pose

$$\int_a^b f(t) dt = \sum_{i=1}^n (a_i - a_{i-1}) \lambda_i.$$

Cette quantité est indépendante du choix de σ parmi les subdivisions adaptées à f .

Il faut savoir le démontrer.

Remarque. Lorsque $E = \mathbb{R}$, $\int_a^b f$ représente une somme d'aires de rectangles, affectées d'un signe négatif lorsque $\lambda_i < 0$, donc $\int_a^b f$ est l'aire algébrique de la surface située entre le graphe de f et l'axe des abscisses.

Propriété. Supposons que f est en escalier et soit g une application de $[a, b]$ dans E qui ne diffère de f qu'en un nombre fini de points de $[a, b]$. Alors g en escalier et $\int_a^b g = \int_a^b f$.

Théorème. Notons $\mathcal{E}([a, b], E)$ l'ensemble des applications en escalier de $[a, b]$ dans E . C'est un \mathbb{K} -espace vectoriel et l'application $\begin{array}{ccc} \mathcal{E}([a, b], E) & \longrightarrow & E \\ f & \longmapsto & \int_a^b f \end{array}$ est linéaire.

Il faut savoir le démontrer.

Propriété. Soient F un second \mathbb{K} -espace vectoriel de dimension finie et $u \in L(E, F)$.

Si f est en escalier, $u \circ f$ est en escalier et $\int_a^b u \circ f = u \left(\int_a^b f \right)$.

Propriété. Si f est une application en escalier à valeurs dans \mathbb{R}_+ , $\int_a^b f \geq 0$.

Corollaire. Si $f, g \in \mathcal{E}([a, b], E)$, alors $[\forall t \in [a, b], f(t) \leq g(t)] \implies \int_a^b f \leq \int_a^b g$.

Inégalité triangulaire : Pour tout $f \in \mathcal{E}([a, b], E)$, $\left\| \int_a^b f(t) dt \right\| \leq \int_a^b \|f(t)\| dt$.

Relation de Chasles : Soit $f \in \mathcal{E}([a, b], E)$ et $c \in]a, b[$.

Alors $f|_{[a, c]}$ et $f|_{[c, b]}$ sont des applications en escalier et $\int_a^b f = \int_a^c f + \int_c^b f$.

6 Les applications réglées (hors programme)

6.1 Définition

Définition. On dit que $f : [a, b] \longrightarrow E$ est réglée si et seulement si c'est la limite uniforme d'une suite d'applications en escalier, c'est-à-dire si et seulement si il existe une suite $(f_n) \in \mathcal{E}([a, b], E)^{\mathbb{N}}$ telle que $\sup_{x \in [a, b]} \|f_n(t) - f(t)\| \xrightarrow{n \rightarrow +\infty} 0$. On note $\mathcal{R}([a, b], E)$ l'ensemble des applications réglées.

Propriété. $\mathcal{R}([a, b], E)$ est l'adhérence de $\mathcal{E}([a, b], E)$ dans $(\mathcal{B}([a, b], E), \|\cdot\|_{\infty})$.

6.2 Les applications continues par morceaux

Propriété. $C([a, b], E) \subset \mathcal{R}([a, b], E)$: toute application continue est réglée.

Il faut savoir le démontrer.

Définition. $f : [a, b] \longrightarrow E$ est continue par morceaux si et seulement si il existe une subdivision $\sigma = (a_i)_{0 \leq i \leq n}$ de $[a, b]$ telle que, pour tout $i \in \mathbb{N}_n$, $f|_{]a_{i-1}, a_i[}$ est prolongeable par continuité sur $[a_{i-1}, a_i]$, ce qui est équivalent à f est continue sur $[a, b] \setminus \{a_0, \dots, a_n\}$ et f admet en chaque a_i une limite à droite (sauf en b) et une limite à gauche (sauf en a). Dans ce cas, on dit que la subdivision σ est adaptée à f .

Définition. Si I est un intervalle quelconque de \mathbb{R} , $f : I \longrightarrow E$ est continue par morceaux si et seulement si toutes ses restrictions aux segments inclus dans I sont continues par morceaux.

Propriété. Les applications continues par morceaux de $[a, b]$ dans E sont réglées.

Théorème. (Hors programme) Une application de $[a, b]$ dans E est réglée si et seulement si elle admet en tout point de $[a, b]$ une limite à droite (sauf en b) et une limite à gauche (sauf en a).

Corollaire. Les applications monotones de $[a, b]$ dans \mathbb{R} sont réglées.

Corollaire. Le produit de deux applications réglées est réglé.

7 Intégration des applications réglées

7.1 Construction

Définition. Soit $f : [a, b] \rightarrow E$ une application réglée.

Il existe $(f_n)_{n \in \mathbb{N}} \in \mathcal{E}([a, b], E)^{\mathbb{N}}$ telle que $f_n \xrightarrow{\|\cdot\|_{\infty}} f$. On pose $\int_a^b f(t) dt = \lim_{n \rightarrow +\infty} \left(\int_a^b f_n(t) dt \right)$.

Il faut savoir le démontrer.

Remarque. Seule la construction de l'intégrale sur $[a, b]$ d'une application continue par morceaux est au programme.

7.2 Propriétés

Théorème. $\mathcal{R}([a, b], E)$ est un \mathbb{K} -espace vectoriel et $\begin{array}{ccc} \mathcal{R}([a, b], E) & \longrightarrow & E \\ f & \longmapsto & \int_a^b f \end{array}$ est linéaire.

Il faut savoir le démontrer.

Propriété. Soit F un second \mathbb{K} -espace vectoriel de Banach et $u \in L(E, F)$ que l'on suppose continue.

Si $f \in \mathcal{R}([a, b], E)$, alors $u \circ f \in \mathcal{R}([a, b], F)$ et $\int_a^b u \circ f = u \left(\int_a^b f \right)$.

Il faut savoir le démontrer.

Propriété. On suppose que E est de dimension finie et que $e = (e_1, \dots, e_p)$ est une base de E . Soit $f \in \mathcal{R}([a, b], E)$. Notons f_1, \dots, f_p les applications coordonnées de f , de sorte que, pour tout $t \in [a, b]$, $f(t) = \sum_{j=1}^n f_j(t) e_j$. Alors f_1, \dots, f_p sont réglées et $\int_a^b f(t) dt = \sum_{j=1}^n \left(\int_a^b f_j(t) dt \right) e_j$.

Remarque. Réciproquement, si f_1, \dots, f_p sont réglées, alors f est aussi réglée.

Propriété. Supposons que $E = \prod_{i=1}^p E_i$, où pour tout $i \in \mathbb{N}_p$, E_i est un espace de Banach. Soit $f \in \mathcal{R}([a, b], E)$. Notons f_1, \dots, f_p les applications composantes de f , de sorte que, pour tout $t \in [a, b]$, $f(t) = (f_1(t), \dots, f_p(t))$. Alors f_1, \dots, f_p sont réglées et $\int_a^b f = \left(\int_a^b f_i \right)_{1 \leq i \leq p}$.

Remarque. Réciproquement, si f_1, \dots, f_p sont réglées, alors f est aussi réglée.

Inégalité triangulaire : Pour tout $f \in \mathcal{R}([a, b], E)$, $\left\| \int_a^b f(t) dt \right\| \leq \int_a^b \|f(t)\| dt$.

Propriété. Si f est une application réglée à valeurs dans \mathbb{R}_+ , $\int_a^b f \geq 0$.

Corollaire. Si $f, g \in \mathcal{R}([a, b], E)$, alors $[\forall t \in [a, b], f(t) \leq g(t)] \implies \int_a^b f \leq \int_a^b g$: l'intégrale est croissante.

Exemple. Si f est réglée, $\left\| \int_a^b f(t) dt \right\| \leq (b-a) \sup_{t \in [a, b]} \|f(t)\|$.

Propriété. Soit f une application réglée (resp : continue par morceaux) de $[a, b]$ dans E . Si g est une application de $[a, b]$ dans E qui ne diffère de f qu'en un nombre fini de points de $[a, b]$, alors g est réglée (resp : continue par morceaux) et $\int_a^b f = \int_a^b g$.

Relation de Chasles : soit $f \in \mathcal{R}([a, b], E)$ et $c \in]a, b[$.

Alors $f|_{[a, c]}$ et $f|_{[c, b]}$ sont réglées et $\int_a^b f = \int_a^c f + \int_c^b f$.

Convention : Si f est une application définie en $\alpha \in \mathbb{R}$, on convient $\int_\alpha^\alpha f = 0$.

Convention : Si $f : [a, b] \rightarrow E$ est réglée, on convient que $\int_b^a f = - \int_a^b f$.

Propriété. La relation de Chasles se généralise au cas d'une application f réglée sur l'intervalle $[\min(a, b, c), \max(a, b, c)]$, les réels (a, b, c) étant quelconques.

Remarque. Avec ces conventions, les égalités établies dans ce paragraphe restent valables, mais ce n'est pas le cas des inégalités.

8 Sommes de Riemann

Notation. On fixe une application f de $[a, b]$ dans E .

Définition. On appelle subdivision pointée de $[a, b]$ tout couple (σ, ξ) , où $\sigma = (a_i)_{0 \leq i \leq n}$ est une subdivision de $[a, b]$ et où $\xi = (\xi_i)_{1 \leq i \leq n}$ vérifie $\forall i \in \mathbb{N}_n \quad \xi_i \in [a_{i-1}, a_i]$.

Notation. Notons \mathcal{S}' l'ensemble des subdivisions pointées de $[a, b]$. Si $(\sigma, \xi) = ((a_i), (\xi_i)) \in \mathcal{S}'$, on notera $f_{\sigma, \xi}$ l'application en escalier définie par $\forall i \in \mathbb{N}_n \quad \forall x \in]a_{i-1}, a_i[\quad f(x) = f(\xi_i)$,

Définition. Soit $(\sigma, \xi) = ((a_i)_{0 \leq i \leq n}, (\xi_i)_{1 \leq i \leq n}) \in \mathcal{S}'$. On appelle somme de Riemann associée à f et à (σ, ξ) la quantité $S(f, \sigma, \xi) = \int_a^b f_{\sigma, \xi} = \sum_{i=1}^n (a_i - a_{i-1}) f(\xi_i)$.

Théorème. Si f est une application réglée de $[a, b]$ dans E ,

$$\forall \varepsilon \in \mathbb{R}_+^* \quad \exists \alpha \in \mathbb{R}_+^* \quad \forall (\sigma, \xi) \in \mathcal{S}' \quad (\delta(\sigma) \leq \alpha \implies \|S(f, \sigma, \xi) - \int_a^b f\| \leq \varepsilon).$$

À savoir démontrer lorsque f est continue.

Corollaire. Soit $(\sigma_n, \xi_n)_{n \in \mathbb{N}} \in \mathcal{S}'^{\mathbb{N}}$ une suite de subdivisions pointées dont le pas tend vers 0. Alors, si f est réglée, la suite des sommes de Riemann associée à f et à (σ_n, ξ_n) converge vers $\int_a^b f$. Plus

précisément, en notant, pour tout $n \in \mathbb{N}$, $\sigma_n = (a_{i,n})_{0 \leq i \leq \varphi(n)}$ et $\xi_n = (\xi_{i,n})_{1 \leq i \leq \varphi(n)}$, si f est réglée et si $\max_{1 \leq i \leq \varphi(n)} (a_{i,n} - a_{i-1,n}) \xrightarrow{n \rightarrow +\infty} 0$,

$$\text{alors } \sum_{i=1}^{\varphi(n)} (a_{i,n} - a_{i-1,n}) f(\xi_{i,n}) \xrightarrow{n \rightarrow +\infty} \int_a^b f.$$

Cas particulier : si f est continue par morceaux, $\frac{b-a}{n} \sum_{i=1}^n f(a + i \frac{b-a}{n}) \xrightarrow{n \rightarrow +\infty} \int_a^b f$.

9 Primitives

Notation. Conformément au programme officiel, on se limite au cas où E est un \mathbb{K} -espace vectoriel de dimension finie. On sait alors qu'il est complet, donc c'est bien un espace de Banach.

On fixe un intervalle I de \mathbb{R} d'intérieur non vide et une application $f : I \longrightarrow E$.

Définition. $g : I \longrightarrow E$ est une primitive de f si et seulement si g est dérivable sur I et $g' = f$.

Propriété. Si f admet une primitive g_0 sur I , alors g est une primitive de f si et seulement si il existe $k \in E$ tel que $\forall x \in I \quad g(x) = g_0(x) + k$.

Propriété. On suppose que f est réglée sur I (c'est-à-dire que les restrictions de f aux intervalles compacts inclus dans I sont réglées). Soit $a \in I$. Alors $x \longmapsto \int_a^x f(t) dt$ est continue sur I .

Théorème fondamental de l'analyse : On suppose que f est continue sur I . Soit $a \in I$.

Alors
$$\boxed{\begin{array}{lcl} F : & I & \longrightarrow E \\ x & \longmapsto & \int_a^x f(t) dt \end{array} \text{ est l'unique primitive de } f \text{ s'annulant en } a.}$$

Il faut savoir le démontrer.

Corollaire. Soient $(a, b) \in \mathbb{R}^2$ avec $a \neq b$ et f une application continue de $[a, b]$ dans E . Si F est une primitive de f , alors $\int_a^b f(t) dt = F(b) - F(a) \stackrel{\text{notation}}{=} [F(t)]_a^b$.

Corollaire. Si f est une application de classe C^1 sur $[a, b]$, $\int_a^b f'(t) dt = f(b) - f(a)$.

Théorème. Soit f une application de $[a, b]$ dans \mathbb{R} .

Si f est **continue**, positive et si $\int_a^b f = 0$, alors f est identiquement nulle sur $[a, b]$.

Il faut savoir le démontrer.

Définition. Si $f : [a, b] \longrightarrow E$ est réglée, la valeur moyenne de f est $\frac{1}{b-a} \int_a^b f(t) dt$.

Propriété. Si $f : [a, b] \longrightarrow \mathbb{R}$ est une application continue, f atteint sa valeur moyenne : il existe $c \in]a, b[$ tel que $f(c) = \frac{1}{b-a} \int_a^b f(t) dt$.