Notes de cours de mathématiques de MPSI

Dorian Lesbre

2016 – 2017

Table des matières

Table des figures

Liste des tableaux

0 Une première équation différentielle

On cherche à résoudre une équation différentielle de type $y''+\omega^2 y = 0$, on cherche donc l'*ensemble* $\mathscr{S}$ des fonctions y deux fois dérivables de $\mathbb{R}$ dans $\mathbb{R}$ vérifiant cette relation. On cherche donc la forme *paramétrée* de $\mathscr{S}$, décrit sous forme *conditionnelle* comme :

$$\mathscr{S} = \left\{ y \in \mathrm{d}^2(\mathbb{R},\mathbb{R}) \ / \ \forall t \in \mathbb{R}, y''(t) + \omega^2 y = 0 \right\}$$

On procédera par condition nécessaire et suffisante (CNS), montrant que y est forcément de la forme $y(t) = A\cos(\omega t) + B\sin(\omega t)$. La condition suffisante est assez facile, la condition nécessaire se fait par l'étude de fonctions qui ne sont pas à connaitre.

Conclusion : on a l'égalité ensembliste suivante,

$$\mathscr{S} = \left\{ \begin{pmatrix} \mathbb{R} & \to & \mathbb{R} \\ t & \mapsto & A\cos(\omega t) + B\sin(\omega t) \end{pmatrix}, \ (A,B) \in \mathbb{R}^2 \right\}$$

1 Introduction à la combinatoire

1.1 Les coefficients du binôme

Définition : la fonction factorielle est définie sur $\mathbb{N}$ par :

$$\begin{cases} n! = n \times (n-1) \times \ldots \times 2 \times 1 = \prod_{i=1}^{n} i & \text{pour } n \geq 1 \\ 0! = 1 \text{ (produit vide)} \end{cases}$$

Si l'on cherche à lister *avec ordre* les éléments d'un ensemble de cardinal n, il y a $n!$ combinaisons possibles.

Définition : soit n et p deux entiers naturels, on définit l'entier $\begin{pmatrix} n \\ p \end{pmatrix}$ par :

$$\begin{pmatrix} n \\ p \end{pmatrix} = \frac{n \times (n-1) \times \ldots \times (n-p+1)}{p!} = \frac{\prod_{k=0}^{p-1}(n-k)}{p!}$$

il s'agit du nombre de façons p entiers *sans ordre* parmi n.

Propriétés : les coefficients du binôme vérifient :

$$\begin{pmatrix} n-1 \\ p-1 \end{pmatrix} + \begin{pmatrix} n-1 \\ p \end{pmatrix} = \begin{pmatrix} n \\ p \end{pmatrix} \qquad p\begin{pmatrix} n \\ p \end{pmatrix} = n\begin{pmatrix} n-1 \\ p-1 \end{pmatrix}$$

1.2 Le binôme de Newton

Soit N l'ensemble $[\![1, n]\!]$, $\mathscr{P}(N)$ l'ensemble de ses parties, $\mathscr{P}_k(N)$ l'ensemble de ses parties à k éléments, et $(a_1, \dots a_n)$, $(b_1, \dots b_n)$ deux listes de n réels, on a alors :

$$(a_1 + b_1)(a_2 + b_2) \dots (a_n + b_n) = \sum_{J \in \mathscr{P}(N)} \left(\prod_{i \in J} a_i \prod_{j \in N \setminus J} b_j \right)$$

Donc, en prenant $a = a_1 = \dots = a_n$ et $b = b_1 = \dots = b_n$:

$$(a+b)^n = \sum_{J \in \mathscr{P}(N)} \left(a^{\#J} b^{\#N \setminus J}\right) = \sum_{k=0}^{n} \left(\sum_{i \in \mathscr{P}_k(N)} a^k b^{n-k} \right)$$

$$\boxed{(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}}$$

2 Calcul algébrique et révisions de trigonométrie

2.1 Quelques sommes

Somme diverses : (démo par récurrence ou télescopage), soit $(a_1, \dots, a_n) \in \mathbb{C}^n$, soit $(u_n)_{n \in \mathbb{N}}$ une suite arithmétique, et $(s_n)_{n \in \mathbb{N}}$ une suite géométrique de raison ρ.

- $\displaystyle\sum_{i=0}^{n} (a_{i+1} - a_i) = a_n - a_0$
- $\displaystyle\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$
- $\displaystyle\sum_{k=p}^{q} u_k = (q - p + 1)\frac{u_q - u_p}{2}$
- $\displaystyle\sum_{k=p}^{q} s_k = \begin{cases} (q-p+1)s_p & \text{si } \rho = 1 \\ s_p \frac{1-\rho^{q-p+1}}{1-\rho} & \text{si } \rho \neq 1 \end{cases}$
- $\displaystyle\sum_{k=0}^{n} k = n\frac{n+1}{2}$
- $\displaystyle\sum_{k=0}^{n} k^3 = n^2\frac{(n+1)^2}{4}$

Factorisation de $a^n - b^n$: soit $(a, b) \in \mathbb{C}^2$ et $n \in \mathbb{N}$, on a alors

$$a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^{n-1-k} b^k$$

2.2 Un peu de trigonométrie

Équations et inéquations

$$\begin{aligned}\cos x = \cos\theta_0 &\Leftrightarrow x \equiv \theta_0\,[2\pi] \text{ ou } x \equiv -\theta_0\,[2\pi]\\ &\Leftrightarrow \exists k \in \mathbb{Z},\ x = \theta_0 + 2k\pi \text{ ou } x = -\theta_0 + 2k\pi\end{aligned}$$
$$\text{Ensemble solution } \boldsymbol{S = \{\theta_0 + 2k\pi, k \in \mathbb{Z}\} \cup \{-\theta_0 + 2k\pi, k \in \mathbb{Z}\}}$$

$$\begin{aligned}\sin x = \sin\theta_0 &\Leftrightarrow x \equiv \theta_0\,[2\pi] \text{ ou } x \equiv \pi - \theta_0\,[2\pi]\\ &\Leftrightarrow \exists k \in \mathbb{Z},\ x = \theta_0 + 2k\pi \text{ ou } x = \pi - \theta_0 + 2k\pi\end{aligned}$$
$$\text{Ensemble solution } \boldsymbol{S = \{\theta_0 + 2k\pi, k \in \mathbb{Z}\} \cup \{\pi - \theta_0 + 2k\pi, k \in \mathbb{Z}\}}$$

$$\tan x = \tan\theta_0 \Leftrightarrow \exists k \in \mathbb{Z}, x = \theta_0 + k\pi$$

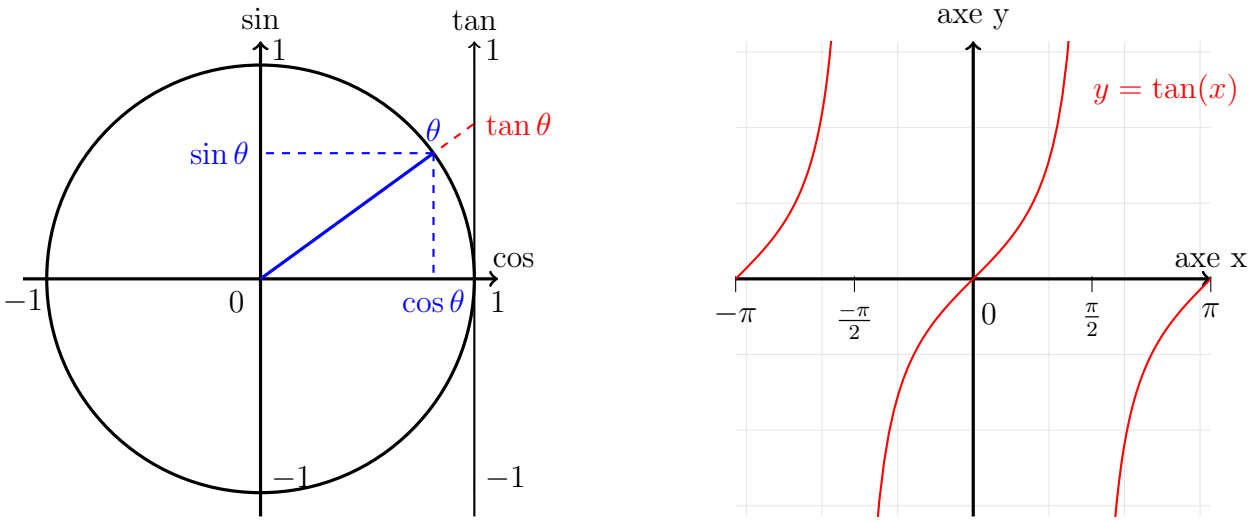

FIGURE 1 – Cercle trigonométrique et fonction tangente

3 Nombres Complexes

3.1 Opérations élémentaires

Soit z un nombre complexe. On définit ses **parties réelles Re(z)** et **imaginaire Im(z)** deux réels tels que $z = \mathrm{Re}(z) + i \times \mathrm{Im}(z)$. Les parties réelles et imaginaires vérifient. Les fonctions Im et Re sont $\mathbb{R}$-linéaires, donc compatible avec la somme et la multiplication par un réel, mais pas avec le produit : $\mathrm{Re}(z_1z_2) = \mathrm{Re}(z_1)\mathrm{Re}(z_2) - \mathrm{Im}(z_1)\mathrm{Im}(z_2)$ et $\mathrm{Im}(z_1z_2) = \mathrm{Re}(z_1)\mathrm{Im}(z_2) + \mathrm{Im}(z_1)\mathrm{Re}(z_2)$. L'unicité de ces parties donne l'équivalence

$$z_1 = z_2 \quad \Leftrightarrow \quad \mathrm{Re}(z_1) = \mathrm{Re}(z_2) \text{ et } \mathrm{Im}(z_1) = \mathrm{Im}(z_2)$$

On définit le **complexe conjugué** $\boldsymbol{\overline{z}} = \mathrm{Re}(z) - \mathrm{Im}(z)$. La conjugaison est compatible avec la somme, le produit, l'inverse, la division et la puissance entière. Le **module** du complexe z par $|z| = \sqrt{\mathrm{Re}^2(z) + \mathrm{Im}^2(z)}$. Le module n'est compatible qu'avec le produit et la puissance. On a les égalités suivantes, avec $z \in \mathbb{C}$:

- $|z|^2 = z\overline{z}$
- $\dfrac{1}{z} = \dfrac{\overline{z}}{|z|^2}$
- $\mathrm{Re}(z) = \dfrac{z + \overline{z}}{2}$
- $\mathrm{Im}(z) = \dfrac{z - \overline{z}}{2}$

On peut alors retrouver l'**inégalité triangulaire** à partir de ces définitions. On démontre d'abord l'identité remarquable $|z_1+z_2|^2 = |z_1|^2 + |z_2|^2 + 2\text{Re}(z_1 z_2)$:

$$\begin{aligned}|z_1+z_2|^2 &= (z_1+z_2)\overline{(z_1+z_2)} = (z_1+z_2)(\overline{z_1}+\overline{z_2} = z_1\overline{z_1} + z_2\overline{z_2} + z_1\overline{z_2} + z_2\overline{z_1} \\ &= |z_1|^2 + |z_2|^2 + z_1\overline{z_2} + \overline{z_1\overline{z_2}} = |z_1|^2 + |z_2|^2 + 2\text{Re}(z_1 z_2)\end{aligned}$$

Ce qui permet de démontrer l'inégalité triangulaire, son cas d'égalité et en déduire la deuxième inégalité triangulaire et l'inégalité triangulaire renversée :

- $\begin{cases} \boldsymbol{|z_1+z_2| \leqslant |z_1| + |z_2|} \\ |z_1+z_2| = |z_1| + |z_2| \end{cases} \Leftrightarrow \boldsymbol{\exists \lambda \in \mathbb{R}_+, z_1 = \lambda z_2}$ ou $\boldsymbol{z_2 = \lambda z_1}$
- $|z_1 - z_2| \leqslant |z_1| + |z_2|$
- $||z_1| - |z_2|| \leqslant |z_1 \pm z_2|$

Pour la démonstration, prendre l'identité remarquable et, pour majorer, exploiter le fait que $\text{Re}(z) \leqslant |\text{Re}(z)| \leqslant |z|$. Pour le cas d'égalité, on fera une démonstration par double implication.
$\boxed{\Rightarrow}$ on a $\text{Re}(z_1\overline{z_2}) = |z_1 z_2| \Rightarrow z_1\overline{z_2} \in \mathbb{R}_+$, On fait alors une disjonction de cas : immédiate si $z_2 = 0$, sinon on a $\overline{z_2} = \dfrac{1}{z_2}|z_2|^2$ donc $\dfrac{z_1}{z_2}|z_2|^2 \in \mathbb{R}_+$. On obtient alors $z_1 = \dfrac{z_1}{z_2}z_2 = \dfrac{z_1}{z_2}|z_2|^2 \dfrac{1}{|z_2|^2}z_2 = \lambda z_2$ avec $\lambda = \dfrac{z_1}{z_2}|z_2|^2 \dfrac{1}{|z_2|^2} \in \mathbb{R}_+$
$\boxed{\Leftarrow}$ on suppose l'existence de λ dans $\mathbb{R}_+$ et on raisonne par disjonction de cas $z_1 = \lambda z_2$ ou $z_2 = \lambda z_1$.
Finalement, on peut démontrer par récurrence finie l'inégalité triangulaire généralisée :

$$\boldsymbol{\left|\sum_{k=1}^{n} z_k\right| \leqslant \sum_{k=1}^{n} |z_k|}$$

3.2 Nombres complexes de module 1

On définit l'ensemble $\mathbb{U} = \{z \in \mathbb{C}, |z| = 1\}$. Il correspond donc sur le plan complexe au cercle trigonométrique. Il est stable par produit et inverse. Si $z \in \mathbb{U}$, alors $z^{-1} \in \mathbb{U}$ et $z^{-1} = \overline{z}$. On pose alors $e^{ix} = \cos(x) + i \times \sin(x)$ avec $x \in \mathbb{R}$ une paramétrisation de tout nombre de $\mathbb{U}$.
Formule de Moivre : $\forall x \in \mathbb{R}, \forall n \in \mathbb{N}, (\cos x + i \times \sin x)^n = \cos nx + i \times \sin nx$
Formule d'Euler : $\forall x \in \mathbb{R}, \cos x = \dfrac{e^{ix} + e^{-ix}}{2}$ et $\sin x = \dfrac{e^{ix} - e^{-ix}}{2}$
Factorisation d'une différence d'exponentielle :

$$e^{ix} + e^{iy} = e^{i\frac{x+y}{2}} \times 2\cos\left(\frac{x-y}{2}\right) \text{ et } e^{ix} - e^{iy} = e^{i\frac{x+y}{2}} \times 2i\sin\left(\frac{x-y}{2}\right)$$

La formule de Moivre permet de trouver les polynômes de Tchebychev. On part des relations $\cos nx = \text{Re}\left[(e^{ix})^n\right]$ et $\sin nx = \text{Im}\left[(e^{ix})^n\right]$, on replace $(e^{ix})^n$ par $(\cos x + i \times \sin x)^n$ puis on applique le binôme de Newton pour trouver les polynômes :

$$\cos nx = \sum_{\substack{k \in [\![0,\, n]\!] \\ k \equiv 0\ [2]}} \binom{n}{k} \left(\cos^2 x - 1\right)^{k/2} \cos^{n-k} x \quad \text{soit} \qquad T_n(X) = \sum_{\substack{k \in [\![0,\, n]\!] \\ k \equiv 0\ [2]}} \binom{n}{k} \left(X^2-1\right)^{k/2} X^{n-k}$$

$$\sin nx = \sin(x) \sum_{\substack{k \in [\![0,\, n]\!] \\ k \equiv 1\ [2]}} \binom{n}{k} \left(\cos^2 x - 1\right)^{\frac{k-1}{2}} \cos^{n-k} x \qquad U_n(X) = \sum_{\substack{k \in [\![0,\, n]\!] \\ k \equiv 1\ [2]}} \binom{n}{k} \left(X^2-1\right)^{\frac{k-1}{2}} X^{n-k}$$

Sommes d'exponentielle, et par identification, de sinus et de cosinus k-ièmes d'un x réel :

$$\sum_{k=0}^{n} e^{ikx} = e^{\frac{inx}{2}} \frac{\sin\left(\frac{n+1}{2}x\right)}{\sin\left(\frac{x}{2}\right)}$$

Soit z dans $\mathbb{C}^*$. Il existe un unique couple $(r, \theta) \in \mathbb{R}_+ \times \mathbb{R}$ tel que $\boldsymbol{z = re^{i\theta}}$. La démonstration se fait par CN puis CS, la condition nécessaire justifie l'unicité avec $r = |z|$ et $\theta \equiv \theta_0\ [2\pi]$, avec θ_0 un argument de z. La condition suffisante justifie l'existence.

3.3 Équations du second degré

On sait résoudre des équations du second degré $az^2+bz+c = 0$ dans $\mathbb{C}$ à coefficients complexes en trouvant un δ vérifiant $\delta^2 = b^2 - 4ac$. Les solutions, éventuellement doubles, sont alors de la forme $z_0 = \dfrac{-b \pm \delta}{2a}$.
La somme et le produit des racines d'un trinôme du second degré vérifient le système :
$\begin{cases} z_1 + z_2 = \frac{-b}{a} \\ z_1 z_2 = \frac{c}{a} \end{cases}$ (démonstration en développant $a(z - z_1)(z - z_2) = az^2 + bz + c$)

3.4 Racines n-ièmes de l'unité

On définit $\mathbb{U}_n$ l'ensemble des racines n-ièmes de l'unité. On a donc (démo par CNS)

$$\mathbb{U}_n = \{\omega \in \mathbb{C} \,/\, \omega^n = 1\} = \left\{e^{\frac{2ik\pi}{n}}, k \in [\![0,\ n-1]\!]\right\}$$

Cela permet d'aboutir à une factorisation plus complète de $a^n - b^n$ avec $b \neq 0$:

$$a^n - 1 = \prod_{k=0}^{n-1} \left(a - e^{\frac{2ik}{n}}\right) \qquad a^n - b^n = \prod_{k=0}^{n-1} \left(a - e^{\frac{2ik}{n}} b\right)$$

Et aux racines n-ièmes d'un complexe non nul z, si l'on connait une solution particulière z_p, alors $z^n = z_0 \Leftrightarrow z \in \{uz_p, u \in \mathbb{U}_n\}$. Démonstration : existence d'une solution particulière $z_p = |z|^{1/n} e^{i\theta/n}$, puis factorisation de $z^n - z_p^n$.

3.5 Exponentielle complexe

On définit l'exponentielle complexe par, pour tout z dans $\mathbb{C}$: $\boldsymbol{e^z = e^{\mathrm{Re}(z)} e^{i\mathrm{Im}(z)}}$. On a donc $\mathrm{Re}(e^z) = \cos(\mathrm{Im}(z))\, e^{\mathrm{Re}(z)}$ et $\mathrm{Im}(e^z) = \sin(\mathrm{Im}(z))\, e^{\mathrm{Re}(z)}$. De plus on a $|e^z| = e^{\mathrm{Re}(z)}$ et $\arg(e^z) = \mathrm{Im}(z)$. Soit $\alpha \in \mathbb{C}^*$ d'argument θ_0, on a les équivalences suivantes

$$\begin{aligned} e^z = |\alpha|\, e^{\theta_0} &\Leftrightarrow e^{\mathrm{Re}(z)} e^{i\mathrm{Im}(z)} = \alpha e^{\theta_0} \Leftrightarrow e^{\mathrm{Re}(z)} = |\alpha| \text{ et } \mathrm{Im}z \equiv \theta_0\ [2\pi] \\ &\Leftrightarrow \mathrm{Re}(z) = \ln|\alpha| \text{ et } \exists k \in \mathbb{Z}, \mathrm{Im}z = \theta_0 + 2k\pi \end{aligned}$$

De même, on a $e^{z_1} = e^{z_2} \Leftrightarrow \exists k \in \mathbb{Z}, z_1 = z_2 + 2ik\pi$

3.6 Interprétation géométrique

Soit A, B, C trois points u plan complexe d'affixes a, b et c. On a les conditions suivantes d'alignement et d'orthogonalité :

$$A,B,C \text{ alignés } \Leftrightarrow \frac{c-a}{b-a} \in \mathbb{R} \qquad \text{et} \qquad A,B,C \text{ rectangle en } A \Leftrightarrow \frac{c-a}{b-a} \in i\mathbb{R}$$

Examinons maintenant quelques transformations du plan complexe
— la symétrie d'axe $0 + \mathbb{R}u$, qui a pour écriture complexe $z \mapsto \overline{z}$
— la translation de vecteur $\overrightarrow{u}$ d'affixe b : $z \mapsto z + b$
— l'homothétie de centre $A(a)$ et de rapport λ : $(h_{A,\lambda})z \mapsto a + \lambda(z - a)$
— la rotation de centre $A(a)$ et d'angle θ : $(R_{A,\theta})z \mapsto a + e^{i\theta}(z - a)$
— la similitude directe d'écriture complexe $z \mapsto \alpha z + \beta$
C'est donc une translation si $\alpha = 0$, et sinon à la fois une homothétie et une rotation.

4 Ensembles et applications

4.1 Les ensembles

Soit A et B deux ensembles. On définit les opérations :
— l'union $A \cup B = \{x/x \in A \text{ ou } x \in B\}$
— l'intersection $A \cap B = \{x/x \in A \text{ et } x \in B\}$
— la différence $A \setminus B = \{x/x \in A \text{ et } x \notin B\}$
— la différence symétrique $A\Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$
$A\Delta B = \{x/x \in A \text{ xor } x \in B\}$
Ces opérations, à l'exception de la différence sont associatives et commutatives.

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

La démonstration se fait par double inclusion, par tableau ou par diagramme de Wenn.

On note $\mathscr{P}(E)$ **l'ensemble des parties** de E. Si $A \in \mathscr{P}(E)$ on peut alors définir le complémentaire de A dans E par ${}^{C}A = C_E A = \overline{A} = \{x \in E/x \notin A\}$

On définit le **produit cartésien** d'un nombre fini $p \in \mathbb{N}^*$ d'ensemble $E_1 \times E_2 \times \ldots \times E_p$ comme l'ensemble des p-listes $(x_1, x_2, \ldots, x_p)$ avec $x_1 \in E_1, x_2 \in E_2, \ldots, x_p \in E_p$. Si les ensembles $E_1, E_2, \ldots, E_p$ sont finis, on a alors

$$\#(E_1 \times E_2 \times \ldots \times E_p) = \prod_{k=1}^{p} \#E_p$$

4.2 Fonctions

Une fonction est une correspondance entre les éléments d'un ensemble de départ A et d'arrivée B. Soit $\varphi : A \to B$ une fonction, et $\alpha \in A$, alors $\varphi(\alpha) \in B$ est l'image de α par φ. On définit le **graphe** de φ par $\{(a, \varphi(a)),\ a \in A\}$. On note B^A ou $\mathscr{F}(A, B)$ l'ensemble des fonctions de A vers B.

Soit A, B, C trois ensembles, $f \in B^A$ et $g \in C^B$ deux fonctions, on définit la **fonction composée** $g \circ f : \left\{ \begin{array}{ccc} A & \to & C \\ t & \mapsto & g(f(t)) \end{array} \right.$
La composition est associative : $h \circ (g \circ f) = (h \circ g) \circ f = h \circ g \circ f$.

Restriction et corestriction : On définit la restriction de f à A' comme la $f_{|A'} : A' \to B$ vérifiant, $\forall t \in A', f_{|A'}(t) = f(t)$ et $A' \subset A$. Inversement, on définit la corestriction $f^{|B'} : A \to B'$ de f à B' si $\forall t \in A, f(t) \in B'$ et $f^{|B'}(t) = f(t)$ et $B' \subset B$.

Prolongement : on appelle prolongement de f sur C toute fonction $g : C \to D$ vérifiant $A \subset C$, $B \subset D$, $\forall x \in A, g(x) = f(x)$.

Fonction indicatrice : la fonction indicatrice d'une partie A d'un ensemble E est définie par $\mathbb{1}_A : \left\{ \begin{array}{ccc} E & \to & \{0,1\} \\ e & \mapsto & \left| \begin{array}{l} 1 \text{ si } e \in A \\ 0 \text{ si } e \notin A \end{array} \right. \end{array} \right.$ Cette fonction vérifie les propriétés suivantes :

- $\forall e \in E, \mathbb{1}_E(e) = 1, \mathbb{1}_\emptyset(e) = 0$
- $\mathbb{1}_{A \cap B} = \mathbb{1}_A \times \mathbb{1}_B$
- $\mathbb{1}_{\overline{A}} = \mathbb{1}_E - \mathbb{1}_A$
- $A = B \Leftrightarrow \mathbb{1}_A = \mathbb{1}_B$
- $\mathbb{1}_{A \cup B} = \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_A \times \mathbb{1}_B$

4.3 Injectivité, surjectivité, bijectivité

Injectivité : une fonction $f : A \to B$ est dite injective si et seulement si,

$$\boldsymbol{\forall (a, b) \in A^2, f(a) = f(b) \Rightarrow a = b}$$

On a alors :

— f injective $\Leftrightarrow$ tout élément de B admet *au plus* un antécédent par la fonction f
— f injective $\Leftrightarrow \forall (x, y) \in A^2, x \neq y \Rightarrow f(x) \neq f(y)$
— $\left\{ \begin{array}{l} f \text{ injective} \\ g \text{ injective} \end{array} \right. \Rightarrow f \circ g$ injective

Surjectivité : $f : A \to B$ est dite surjective si et seulement si,

$$\boldsymbol{\forall b \in B, \exists a \in A, f(a) = b}$$

On a alors :

— f surjective $\Leftrightarrow$ tout élément de B admet *au moins* un antécédent par f

— $\left\{ \begin{array}{l} f \text{ surjective} \\ g \text{ surjective} \end{array} \right. \Rightarrow f \circ g$ surjective

Bijectivité : f est bijective si elle est à la fois surjective et injective. On a alors :

— f bijective $\Leftrightarrow$ tout élément de B admet *un unique* antécédent par f

— $\left\{ \begin{array}{l} f \text{ bijective} \\ g \text{ bijective} \end{array} \right. \Rightarrow f \circ g$ bijective

f étant bijective on peut définir une *bijection réciproque* f^{-1} par

$$f^{-1} : \left\{ \begin{array}{ccl} B & \to & A \\ t & \mapsto & \text{l'unique antécédent de } t \text{ par } f \end{array} \right.$$

Cette bijection réciproque vérifie $f^{-1} \circ f = \mathrm{id}_A$ et $f \circ f^{-1} = \mathrm{id}_B$. L'existence d'un telle réciproque est une CNS de bijectivité. Si f et g sont bijectives, alors $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

Itérée n-ième : On note φ^n l'itérée n-ième de φ. On a alors :

$$\varphi^0 = \mathrm{id} \qquad \varphi^1 = \varphi \qquad \varphi^2 = \varphi \circ \varphi \qquad \dots$$

Si φ est bijective, on a $\left(\varphi^2\right)^{-1} = \left(\varphi^{-1}\right)^2 = \varphi^{-2}$.

4.4 Image directe et réciproque

Image directe : Soit E, F deux ensembles, $f : E \to F$ et $A \in P(E)$. L'image directe de A par f est l'ensemble : $\boldsymbol{f(A) = \{f(x), x \in A\}}$ On a alors les propriétés suivantes (démonstration par double inclusion) :

- $f(\emptyset) = \emptyset$
- $f(A \cup B) = f(A) \cup f(B)$
- $(g \circ f)(A) = g(f(A))$
- $f(A \cap B) \subset f(A) \cap f(B)$

Image réciproque : soit $B \in F$. L'image réciproque de B par f est l'ensemble : $\boldsymbol{f^{-1}(B) = \{x / f(x) \in B\}}$ On a alors les propriétés suivantes (démonstration par double inclusion) :

- $f(f^{-1}(A)) \subset A$
- $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$
- $A \subset B \Rightarrow f^{-1}(A) \subset f^{-1}(B)$
- $(g \circ f)^{-1}(A) = g^{-1}(f^{-1}(A))$
- $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$
- $f^{-1}(F) = E$ et $f^{-1}(\emptyset) = \emptyset$

Si f est bijective, et B une partie de F, alors l'image directe de B par f^{-1} est égale à l'image réciproque de B par f.

4.5 Fonction indexée par un ensemble

Notation : soit I, E deux ensembles et $u \in E^I$ une fonction de I dans E. On note parfois $\boldsymbol{u = (u_i)_{i \in I}}$, on dit alors que u est une famille d'éléments de E indexée par I. L'exemple type est une suite de réels indexés par $\mathbb{N}$

Familles de parties d'un ensemble : on pose E et I deux ensembles et $(A_i)_{i \in I}$ une famille de partie de E, de sorte que $A \in P(E)^I$. On peut alors définir :

- $\bigcup_{i \in I} A_i = \{x \in E / \exists i \in I, x \in A_i\}$
- $\bigcap_{i \in I} A_i = \{x \in E / \forall i \in I, x \in A_i\}$

Cas particulier : soit $n \in \mathbb{N}^*$ et $u \in E^{[\![1,n]\!]}$ on notera $u = (u_1, u_2, \dots, u_n)$ de sorte que u est assimilé à un élément de E^n. On considère donc que $E^{[\![1,n]\!]} = E^n$
L'ensemble $E^\emptyset$ contient un seul élément, la famille vide : ()

5 Fonctions usuelles

5.1 Quelques énoncés d'analyse réelle

Soit I et J deux intervalles de $\mathbb{R}$, soit $f \in I^J$, on a alors :

1. si f est bijective et continue, alors sa fonction réciproque est continue
2. si I et J contiennent au moins deux éléments, et que f dérivable sur I est bijective, alors :

$$\boldsymbol{\forall y \in J, f^{-1} \text{ est dérivable en } y \Leftrightarrow f'\left(f^{-1}(y)\right) \neq 0}$$

Et on a, dans le cas où f^{-1} est dérivable : $\left(f^{-1}\right)'(y) = \dfrac{1}{f'\left(f^{-1}(y)\right)}$

3. si f est dérivable sur I, on a $\boldsymbol{f \text{ constante sur } I \Leftrightarrow \forall y \in I, f'(y) = 0}$
4. soit $f \in I^J$ dérivable et $g \in J^H$ dérivables, alors

$$\boldsymbol{\forall t \in I, (g \circ f)'(y) \Leftrightarrow f'(y) \times g'(f(y))}$$

5.2 Fonctions circulaires réciproques

Dérivation : Afin de dériver arccos et arcsin, on montre que

$$\forall t \in [-1;1] : \sqrt{1-t^2} = \cos(\arcsin(t)) = \sin(\arccos(t))$$

La démonstration est immédiate sur le cercle trigonométrique. On utilise alors le théorème de dérivation des bijections réciproques montrer les domaines de dérivabilités, puis calculer les dérivées.

	arcsin	arccos	arctan
Valeur	$\left(\sin_{\left\|\left[-\frac{\pi}{2};\frac{\pi}{2}\right]}^{\left\|[-1;1]}\right)$	$\left(\cos_{\left\|[0;\pi]}^{\left\|[-1;1]}\right)$	$\left(\tan_{\left\|\right]-\frac{\pi}{2};\frac{\pi}{2}\left[}\right)$
Ensemble de départ	$[-1;1]$	$[-1;1]$	$\mathbb{R}$
Ensemble d'arrivée	$\left[-\frac{\pi}{2};\frac{\pi}{2}\right]$	$[0;\pi]$	$\left]-\frac{\pi}{2};\frac{pi}{2}\right[$
Ensemble de dérivation	$]-1;1[$	$]-1;1[$	$\mathbb{R}$
Dérivée	$\dfrac{1}{\sqrt{1-t^2}}$	$\dfrac{-1}{\sqrt{1-t^2}}$	$\dfrac{1}{1+t^2}$

TABLE 1 – Récapitulatif de définitions de arcsin, arccos et arctan

Graphe : on admet que le graphe d'une bijection réciproque est le symétrique du graphe de la bijection par rapport à la première bissectrice (la droite $y = x$), on peut alors tracer l'allure du graphe des fonctions trigonométriques réciproques :

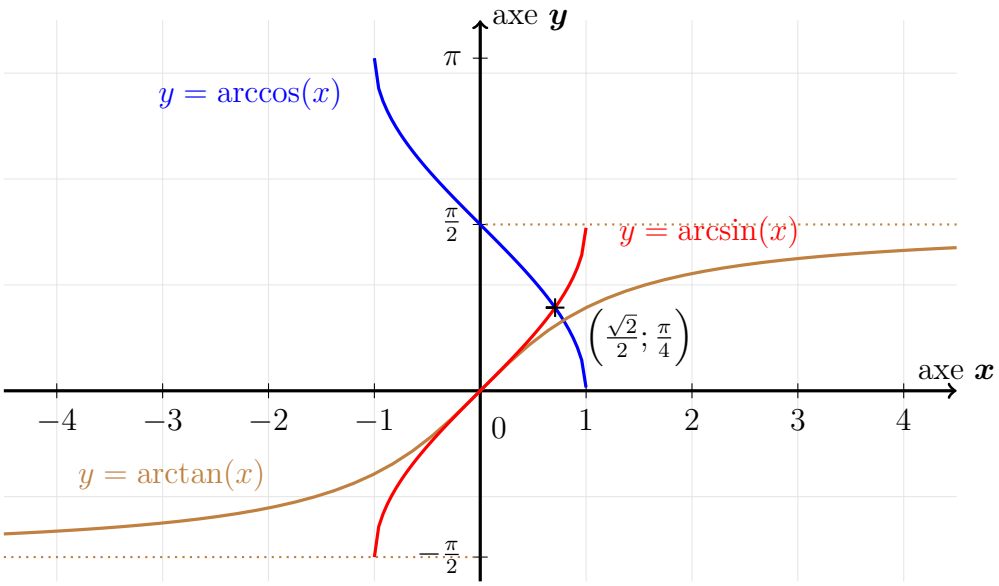

FIGURE 2 – Graphe des fonctions arccos, arcsin et arctan

Identités remarquables : on a les égalités suivantes.

- $\forall t \in [-1,1],\ \arccos(t) + \arcsin(t) = \dfrac{\pi}{2}$
- $\forall t \in \mathbb{R}^*,\ \arctan(t) + \arctan\left(\dfrac{1}{t}\right) = \left|\begin{array}{l} \frac{\pi}{2} \text{ si } t > 0 \\ -\frac{\pi}{2} \text{ si } t < 0 \end{array}\right.$
- $\forall t \in \mathbb{R},\ \arctan(t) \equiv \arg(1+it)\ [2\pi]$ (1)
- $\left\{\begin{array}{l} \forall t \in [-1;1], \arcsin(-t) = -\arcsin(t) \\ \forall t \in [-1;1], \arccos(-t) = \pi - \arccos(t) \\ \forall t \in \mathbb{R},\ \arctan(-t) = -\arctan(t) \end{array}\right.$

Les démonstrations se font en étudiant les fonctions associées, en remplaçant t par $\cos\theta$ ou $\sin\theta$, ou en composant par cos ou sin et exploitant leur injectivité. Pour la 1, on montre que $\sqrt{1+t}\,e^{i\arctan(t)} = 1+it$ en développant puis exploitant la relation $\frac{1}{cos^2 t} = 1 + tan^2 t$.

5.3 Autour de la fonction exponentielle

La fonction puissance : pour α dans $\mathbb{R}$, et t dans $]0,+\infty[$, on pose $\boldsymbol{t^\alpha = e^{\alpha \ln t}}$. Pour le cas ou t est nul, on a si $\alpha \neq 0$, $0^\alpha = 0$ et $0^0 = 1$.

Étude de $\boldsymbol{\alpha < 0}$: la fonction puissance $\varphi_\alpha(t) = t^\alpha$ est alors définie et dérivable sur $]0;\ +\infty[$. on a $\varphi'_a(t) = \alpha t^{\alpha-1}$. La fonction est alors strictement décroissante.

Étude de $\boldsymbol{\alpha \in]0;\ 1[}$: la fonction puissance $\varphi_\alpha(t)$: $\left\{ \begin{array}{ccc} \mathbb{R}_+ & \to & \mathbb{R} \\ t & \mapsto & \left| \begin{array}{l} e^{\alpha \ln t} \text{ si } t > 0 \\ 0 \text{ si } t = 0 \end{array} \right. \end{array} \right.$ est dérivable sur $]0;\ +\infty[$. on a $\varphi'_a(t) = \alpha t^{\alpha-1}$. La fonction est donc strictement croissante. Par ailleurs on a $\lim\limits_{t\to 0^+} \varphi_\alpha(t) = 0$. La fonction est donc continue en 0. En étudiant la dérivabilité en 0, on trouve que $\dfrac{\varphi_\alpha(t) - \varphi_\alpha(0)}{t} = t^{\alpha-1}$, donc comme $\alpha - 1 < 0$, on a un taux d'accroissement qui tend vers $+\infty$, la fonction n'est pas dérivable en 0.

Étude de $\boldsymbol{\alpha > 1}$: comme précédemment, la fonction est dérivable sur $\mathbb{R}_+^*$ et a pour dérivée $\alpha t^{\alpha-1} > 0$. Elle est donc strictement croissante. De plus elle est continue et dérivable en 0, où elle vaut 0 et sa dérivée est nulle.

Autres cas : si $\alpha = 1$ il s'agit de la fonction linéaire $f(x) = x$, et si $\alpha = 0$, c'est une fonction définie sur $\mathbb{R}_+$ constante égale à 1.

Bijectivité : si $\alpha \neq 0$, φ_α est bijective de $\mathbb{R}_+$ dans $\mathbb{R}_+$ (0 inclus si $\alpha > 0$, exclu sinon) et sa bijection réciproque est $\varphi_{\frac{1}{\alpha}}$.

Cas $\alpha < 0$

t	0		$+\infty$
$\varphi'_\alpha(t)$	‖	$+$	
φ_α	‖	$+\infty$ ↘	0

Cas $0 < \alpha < 1$

t	0		$+\infty$
$\varphi'_\alpha(t)$	‖	$+$	
φ_α	‖	0 ↗	$+\infty$

Cas $\alpha > 1$

t	0		$+\infty$
$\varphi'_\alpha(t)$	0	$+$	
φ_α	0	↗	$+\infty$

5.4 Comparaisons de fonctions usuelles

On a pour valeurs remarquables les limites suivantes :

- $\dfrac{\ln t}{t} \xrightarrow[t\to+\infty]{} 0$
- $t \cdot \ln t \xrightarrow[t\to 0^+]{} 0$
- $\dfrac{\ln^\beta t}{t^\alpha} \xrightarrow[t\to+\infty]{} 0$
- $t^\alpha \left|\ln t\right|^\beta \xrightarrow[t\to 0^+]{} 0$
- $\dfrac{t^\alpha}{e^{\beta t}} \xrightarrow[t\to+\infty]{} 0$

Les démonstrations se font en encadrant $0 \leqslant \ln t < \sqrt{t}$ pour la première, en remplaçant t par $\frac{1}{t}$ pour la deuxième et en passant au logarithme pour faire tomber les puissances pour les autres.

5.5 Fonctions trigonométriques hyperboliques

Pour tout t réel, on pose

$$\boldsymbol{\cosh(t) = \frac{e^t + e^{-t}}{2}} \qquad \boldsymbol{\sinh(t) = \frac{e^t - e^{-t}}{2}} \qquad \boldsymbol{\tanh(t) = \frac{\sinh(t)}{\cosh(t)} = \frac{e^t - e^{-t}}{e^t + e^{-t}}}$$

Ces trois fonctions sont dérivables sur $\mathbb{R}$ et ont pour dérivées respectives :

$$\cosh' = \sinh \qquad \sinh' = \cosh \qquad \tanh' = \frac{1}{\cosh^2} = 1 + \tanh^2$$

Finalement, on a comme propriété remarquable : $\forall x \in \mathbb{R}, \cosh^2(x) - \sinh^2(x) = 1$

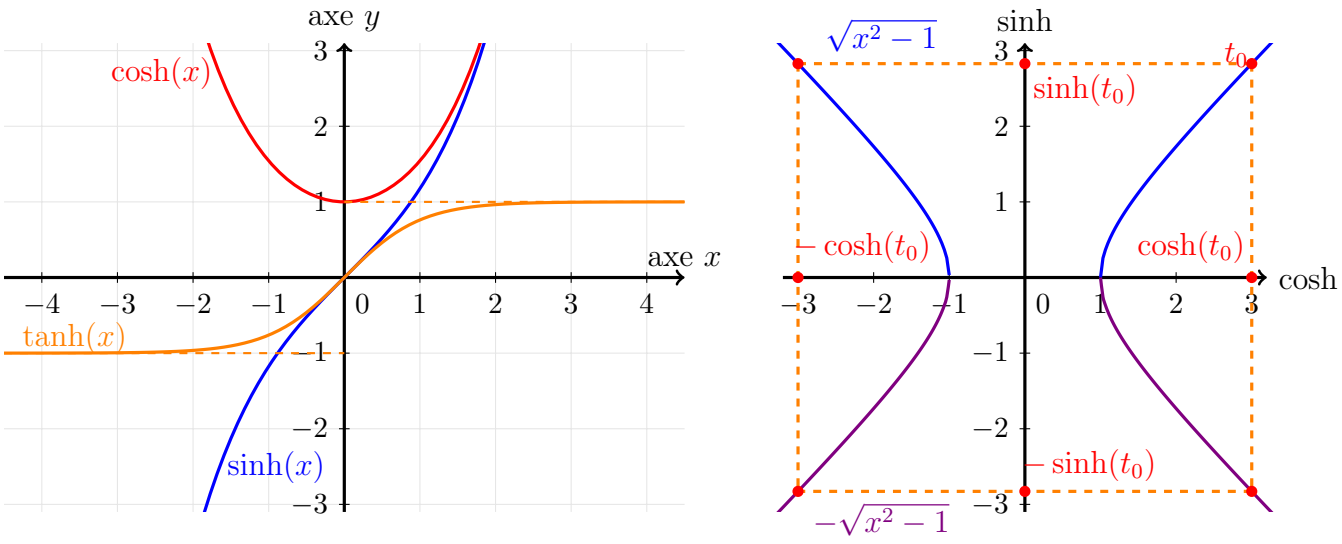

FIGURE 3 – Graphe de cosh, sinh, tanh et interprétation géométrique

6 Systèmes linéaires et sommes doubles

6.1 Systèmes linéaires

On appelle systèmes linéaires à n-équations et p-inconnues une équation de la forme :

$$(E) : \begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \ldots + a_{1,p}x_p = \lambda_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \ldots + a_{2,p}x_p = \lambda_2 \\ \vdots \\ a_{n,1}x_1 + a_{n,2}x_2 + \ldots + a_{n,p}x_p = \lambda_n \end{cases}$$

avec $(a_{i,j})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}}$ la famille des coefficients du système, $(\lambda_1, \lambda_2, \ldots, \lambda_p)$ la liste des seconds membres et $(x_1, x_2, \ldots, x_p)$ l'inconnue.

Méthode du pivot de Gauss : pour résoudre un tel système, on emploie la démarche suivant

1. Vérifier que le coefficient $a_{1,1}$ devant x_1 n'est pas nul. Si c'est le cas, inverser deux lignes ou deux inconnues.
2. Pour chaque ligne L_i de 2 à n, effectuer la transformation $\boldsymbol{L_i \leftarrow L_i - \frac{a_{i,1}}{a_{1,1}} L_1}$. Cette opération à pour effet de retirer la variable x_1 de toutes les lignes sauf la première
3. Répéter le processus avec le sous système obtenue jusqu'à ce que l'on soit à court d'inconnues (auquel cas on obtient des équations de compatibilité) ou d'équations (certaines inconnues sont alors des paramètres sans contraintes)

CNS de solutions : un système (E) admet des solutions si et seulement si toutes les équations de compatibilité sont vérifiées. Le sens direct de la démonstration est immédiat, pour la réciproque, il suffit de bien écrire le système après méthode de Gauss et prendre 0 pour les valeurs des paramètres.

6.2 Sommes doubles

Sommes sur un rectangle : soit $(n, p) \in \mathbb{N}^2$, R l'ensemble $[\![0,\ p]\!] \times [\![0,\ n]\!]$, et $(z_{i,j})_{(i,j) \in R}$ une famille de complexes dont on cherche la somme. On a les égalités :

$$\sum_{(i,j) \in R} z_{i,j} = \sum_{\substack{0 \leqslant i \leqslant n \\ 0 \leqslant j \leqslant p}} z_{i,j} = \sum_{i=0}^{n} \left(\sum_{j=0}^{p} z_{i,j} \right) = \sum_{j=0}^{p} \left(\sum_{i=0}^{n} z_{i,j} \right)$$

Sommes sur un triangle : soit $n \in \mathbb{N}$, on pose $T = \left\{(i,\, j) \in \mathbb{N}^2 / \; 0 \leqslant i \leqslant j \leqslant n\right\}$, et $(z_{i,\,j})_{(i,\,j)\in T}$ une famille de complexes dont on cherche la somme. On a les égalités : (sommes sur les colonnes, les lignes ou les diagonales.

$$\sum_{(i,\,j)\in T} z_{i,\,j} = \sum_{0\leqslant i\leqslant j\leqslant n} z_{i,\,j} = \sum_{i=0}^{n}\left(\sum_{j=i}^{p} z_{i,\,j}\right) = \sum_{j=0}^{n}\left(\sum_{i=j}^{n} z_{i,\,j}\right)$$

$$= \sum_{\substack{(i,\,j)\in T\\ d\,=\,j-i}} z_{i,\,j} = \sum_{\substack{0\leqslant i\leqslant j\leqslant n\\ j\,=\,d+i}} z_{i,\,j} = \sum_{\substack{0\leqslant i\leqslant d+i\leqslant n\\ 0\leqslant d\leqslant n}} z_{i,\,d+i} = \sum_{d=0}^{n}\left(\sum_{i=0}^{n-d} z_{i,\,j}\right)$$

7 Relations binaires

Soit E un ensemble, on nomme **relation binaire** $\mathcal{R}$ une partie de $E \times E$. Soit $(x,\, y) \in E^2$, on dit que x est en relation avec y noté $x\,\mathcal{R}\,y$ si et seulement si $(x,\, y) \in \mathcal{R}$. On a par exemple les relations suivantes :

- relation d'égalité : $x\,\mathcal{R}_{=}\,y \Leftrightarrow x = y$
- relation grossière : $x\,\mathcal{R}\,y \Leftrightarrow (x,\, y) \in E^2$
- supérieur (dans $\mathbb{R}$) : $x\mathcal{R}_{>}y \Leftrightarrow x > y$
- inclus (dans un ensemble de partie) : $A\mathcal{R}_{\subset}B \Leftrightarrow A \subset B, (A, B) \in E$
- congruence modulo α : $x\,\mathcal{R}_{\equiv\,[\alpha]}y \Leftrightarrow x \equiv y\;[\alpha]$

7.1 Relations d'équivalence

Définition : une relation binaire $\mathcal{R}$ sur E est qualifié d'équivalente si elle vérifie les propriétés suivantes :

- réflexivité : $\forall\, x \in E,\ \boldsymbol{x\,\mathcal{R}\,x}$
- symétrie : $\forall\,(x,\, y) \in E^2,\ \boldsymbol{x\,\mathcal{R}\,y \Rightarrow y\,\mathcal{R}\,x}$
- transitivité : $\forall\,(x,\, y,\, z) \in E^3,\ \begin{cases} \boldsymbol{x\,\mathcal{R}\,y} \\ \boldsymbol{y\,\mathcal{R}\,z} \end{cases} \boldsymbol{\Rightarrow x\,\mathcal{R}\,z}$

Des exemples précédents, l'égalité, la relation grossière et la congruence sont équivalentes.

Classe d'un élément : Soit $\mathcal{R}$ une relation équivalente sur E, soit $x \in E$ on définit la **classe** de x comme l'ensemble $\mathrm{Cl}(x) = \{t \in E / \; x\,\mathcal{R}\,T\}$. Elle peut aussi être notée $\overline{x}$, $\overline{x}^E$. De plus on appelle **ensemble quotient** l'ensemble ${}^{E}\!/_{x} = \{\mathrm{Cl}(t), t \in E\}$

Partition d'un ensemble : soit E un ensemble, et $P \in \mathscr{P}(E)$. On dit que P est une partition de E si :

- $\forall (A,\, B) \in P^2,\ \boldsymbol{A \neq B \ \Rightarrow\ A \cap B = \emptyset}$
- $\boldsymbol{\bigcup_{A\in P} A = E}$
- $\forall A \in P, \boldsymbol{A \neq \emptyset}$

On démontre par double inclusion que si $\mathcal{R}$ est une relation d'équivalence sur E, ${}^{E}/_{\mathcal{R}}$ est une partition de E. Réciproquement, pour toute partition P de E, on peut définir une relation d'équivalence $\mathcal{R}$ par $x \mathcal{R} y \Leftrightarrow \exists A \in P, (x, y) \in A^2$ vérifiant ${}^{E}/_{\mathcal{R}} = P$

7.2 Relations d'ordre

Soit E un ensemble, une relation binaire $\mathcal{R}$ sur E est qualifié de relation d'ordre si elle est :

— réflexive : $\forall x \in E,\ \boldsymbol{x \mathcal{R} x}$

— non-symétrique : $\forall (x, y) \in E^2, \begin{cases} \boldsymbol{x \mathcal{R} y} \\ \boldsymbol{y \mathcal{R} x} \end{cases} \Rightarrow \boldsymbol{x = y}$

— transitive : $\forall (x, y, z) \in E^3, \begin{cases} \boldsymbol{x \mathcal{R} y} \\ \boldsymbol{y \mathcal{R} z} \end{cases} \Rightarrow \boldsymbol{x \mathcal{R} z}$

Une relation d'ordre est dite totale si $\forall (x, y) \in E^2, x \mathcal{R} y$ ou $y \mathcal{R} x$. On dit alors que l'ensemble $(E, \mathcal{R}$ est (totalement) ordonné. On a par exemple la relation divisibilité sur $\mathbb{N}$, la relation d'inclusion qui sont des relations d'ordre et la relation $\geqslant$ qui est une relation d'ordre totale.

Éléments remarquables : soit $(E, \leqslant)$ un ensemble ordonné, et A une partie de E. On a les définitions suivantes :

— **majorant :** α de A vérifie $\forall t \in A, t \leqslant \alpha$

— **minorant :** β vérifie $\forall t \in A, \beta \leqslant t$

— **maximum :** $\max A$ vérifie $\begin{cases} \forall t \in A, t \leqslant \max A \\ \max A \in A \end{cases}$

— **minimum :** $\min A$ vérifie $\begin{cases} \forall t \in A, \min A \leqslant t \\ \min A \in A \end{cases}$

— **borne supérieure :** $\sup A$ vérifie $\begin{cases} \forall t \in A, t \leqslant \sup A \\ \forall \alpha \in \mathcal{M}_A, \sup A \leqslant \alpha \end{cases}$ avec $\mathcal{M}_A$ l'ensemble des majorants de A

— **borne inférieure :** $\inf A$ vérifie $\begin{cases} \forall t \in A, \inf A \leqslant t \\ \forall \beta \in m_A, \beta \leqslant \inf A \end{cases}$ avec m_A l'ensemble des minorants de A

Toute partie finie d'un ensemble totalement ordonnée admet un maximum et un minimum. La démonstration de l'unicité du maximum/minimum et borne supérieur et inférieur se fait en prenant deux candidats et montrant leur égalité.

Fonction monotone : soit $(E, \leqslant)$ et $(F, \preccurlyeq)$ deux ensembles ordonnés et $f : E \to F$ On a les définitions suivantes :

— $\boldsymbol{f}$ **croissante** $\Leftrightarrow \forall (a, b) \in E^2\ a \leqslant b \Rightarrow f(a) \preccurlyeq f(b)$

— $\boldsymbol{f}$ **décroissante** $\Leftrightarrow \forall (a, b) \in E^2\ a \leqslant b \Rightarrow f(b) \preccurlyeq f(a)$

— $\boldsymbol{f}$ **strictement monotone** $\Leftrightarrow \forall (a, b) \in E^2\ a \neq b \Rightarrow f(a) \neq f(b)$

On a de plus l'implication *f strictement monotone* $\Rightarrow$ *f injective*. (démonstration par contraposée)

8 Groupes, anneaux, corps

Une opération interne à un ensemble E est une fonction $* : E \times E \to E$. On note $a * b$ et non $*(b,\ a)$. On note $(E,\ *)$ l'ensemble E muni de la relation $*$.
Ex : $(\mathbb{N},\ +)$, $(\mathbb{Z},\ \times)$, $(A^A,\ \circ)$, $(\mathcal{M}_2(\mathbb{R}),\ \times)$

8.1 Groupes

Associativité : soit $(E,\ *)$ un ensemble muni d'une opération interne, on dit que $*$ **est associative** lorsque :

$$\boldsymbol{\forall (a,\ b,\ c) \in E^3,\ (a * b) * c = a * (b * c)}$$

Si $*$ est associative, on peut définir $e_1 * e_2 * \ldots * e_n$ en mettant les parenthèses où l'on souhaite et $e^n = \underbrace{e * e * \ldots * e}_{n \text{ fois}}$, l'itérée n-ième. (On peut appliquer les opérations usuelles sur les puissances), en faisant attention à la commutativité, on peut noter

$$e_1 * e_2 * \ldots * e_n = \overset{n}{\underset{i=1}{\ast}} e_i$$

Élément neutre : $(E,\ *)$ admet un unique élément neutre e si ce dernier vérifie $\forall x \in E \begin{cases} \boldsymbol{x * e = x} \\ \boldsymbol{e * x = x} \end{cases}$ (démonstration de l'unicité habituelle). Pour tout élément x de E, on définit $x^0 = e$

Inversibilité : on dit qu'un élément x est inversible ou symétrisable lorsque qu'il vérifie $\exists y \in E \begin{cases} \boldsymbol{x * y = e} \\ \boldsymbol{y * x = e} \end{cases}$. On appelle alors y l'inverse de x noté x^{-1}. Cet inverse est unique.
On note I l'ensemble des inversibles. On a alors :

- $e \in I \quad (e^{-1} = e)$
- $x \in I \Rightarrow x^{-1} \in I \quad ((x^{-1})^{-1} = x)$
- $(x,\ y) \in I \Rightarrow x * y \in I \quad ((x * y)^{-1} = y^{-1} * x^{-1})$

Définition : un groupe est un ensemble muni d'une relation interne associative qui possède un point fixe et dont tous les éléments sont inversibles.

Exemples de groupes : $(\mathbb{Z},\ +)$, $(\mathbb{C},\ +)$, $(\mathbb{Q}^*,\ \times)$ $(\mathbb{R}^*,\ \times)$, $(\mathscr{S}(A),\ \circ)$ sont des groupes commutatifs (sauf le dernier)

Groupes à partir d'autres groupes : soit $(G, *)$ un groupe, on munit $\mathscr{F}(I, G)$ de l'opération $\widetilde{*}$ suivante : $f\widetilde{*}g = \begin{cases} I \to G \\ b \mapsto f(a) * g(b) \end{cases}$. L'ensemble $(\mathscr{F}(I, G), \widetilde{*})$ est alors un groupe.
De même, si $(G_1, *)$ et $(G_2, \diamond)$ sont des groupes, alors $G_1 \times G_2$ muni de l'opération interne $\dagger$ définie par $(a, b) \dagger (c, d) = (a * c, b \diamond d)$ est un groupe.
À chaque fois montrer que c'est une opération interne vérifiant les axiomes du groupe.

8.2 Morphismes de groupe et sous-groupes

Morphisme : soit $(G_1, *)$ et $(G_2, \diamond)$ deux groupes, un morphisme de G_1 vers G_2 est une fonction φ vérifiant :

$$\boldsymbol{\forall (a, b) \in G_1^2,\ \varphi(a * b) = \varphi(a) \diamond \varphi(b)}$$

— Si $(G_1, *) = (G_2, \diamond)$, alors φ est un **endomorphisme**
— Si φ est bijective, c'est un **isomorphisme**
— φ est un **automorphisme** si elle est un endomorphisme bijectif

Morphismes et groupes : soit G_1, G_2, G_3 trois groupes, $\varphi : G_1 \to G_2$ et $\psi : G_2 \to G_3$ deux morphismes, alors $\boldsymbol{\psi \circ \varphi}$ est un **morphisme** de G_1 vers G_3.
Si $f : G_1 \to G_2$ est un isomorphisme, alors $\boldsymbol{f^{-1}} : G_2 \to G_1$ en est un **isomorphisme**.
Si φ est un morphisme, alors $\boldsymbol{\varphi(e_{G_1}) = e_{g_2}}$, $\boldsymbol{\varphi(x^{-1}) = (\varphi(x))^{-1}}$ (de même avec l'itérée n-ième en général). Démonstrations en vérifiant les axiomes.

Noyau et image : on définit le noyau et l'image d'un morphisme $\varphi : G_1 \to G_2$ par :
— **noyau : Ker(φ)** $\boldsymbol{\{g \in G_1 / \ \varphi(g) = e_{G_2}\}} = \varphi^{-1}(\{e_{G_2}\})$
— **image : Im(φ)** $\boldsymbol{\{\varphi(g),\ g \in G_1\}} = \varphi(G_1)$
On a l'équivalence $\boldsymbol{\varphi}$ **injective** $\boldsymbol{\Leftrightarrow \mathbf{Ker}(\varphi) = \{e_{G_1}\}}$

Sous-groupe : Soit $(G, \cdot)$ un groupe, on dit que H est un sous-groupe de G lorsque :

- $\boldsymbol{H \subset G}$
- $\boldsymbol{e_G \in H}$
- $\forall (a, b) \in H$, $\boldsymbol{a \cdot b \in H}$
- $\forall x \in H$, $\boldsymbol{x^{-1} \in H}$

$(H, \cdot)$ est alors un groupe

Morphismes et sous-groupes : soit G et G' deux groupes, de sous-groupes H et H', soit $\varphi : G \to G'$ un morphisme, alors :
— $\boldsymbol{\varphi(H)}$ est un **sous-groupe** de G' (en particulier $\mathrm{Im}(\varphi) = \varphi(G)$)
— $\boldsymbol{\varphi^{-1}(H')}$ est un **sous-groupe** de G (en particulier $\mathrm{Ker}(\varphi) = \varphi^{-1}(\{e_{G'}\})$)
Démo en vérifiant les axiomes d'un sous-groupe

Nouveaux sous-groupes : soit G un groupe, I un ensemble et $(H_i)_{i\in I}$ une famille de sous-groupes de G, alors $\bigcap_{i\in I} \boldsymbol{H_i}$ est un sous groupe.

Soit $B \subset G$, on pose $\xi = \{\text{sous-groupe de } G \text{ contenant } B\}$ alors on appelle sous-groupe engendré par B le plus petit sous-groupe contenant B noté $\mathbf{Gr(B)} = \bigcap_{H\in\xi} \boldsymbol{H}$

8.3 Anneaux et corps

Anneau : un ensemble A muni de **deux opérations internes** notés $+$ et $\times$ est un anneau si :

- $(A, +)$ est un **groupe commutatif**
- $\times$ est associative
- $\times$ admet un élément neutre
- $\forall (a, b, c, d) \in G^4, (a+b)\times(c+d) = ac + ad + bc + bd$

Les éléments neutres sont notés 0_A pour $+$ et 1_A pour $\times$

Ensemble des unités : soit $(A, +, \times)$ un anneau, on définit son ensemble des unités comme l'ensemble des inversibles de $\times$:

$$\mathcal{U}(a) = \left\{ t \in A / \exists a \in A \left\langle \begin{array}{l} t \times a = 1_A \\ a \times t = 1_A \end{array} \right. \right\}$$

Cet ensemble est un groupe

Corps : un corps est un anneau commutatif K tel que $1_K \neq 0_K$ et $\mathcal{U}(K) = K \setminus \{0_K\}$

Calcul algébrique sur les anneaux : on a les propriétés :

- $(-1_A)\times(-1_A) = 1_A$
- $\forall x \in A, \forall n \in \mathbb{Z}, (-x)^n = (-1)^n x^n$
- $\forall (x, y) \in A^2, \forall (n, p) \in \mathbb{Z}, (n\cdot x)\times(p\cdot y) = (np)\cdot(x\times y)$
- $\forall x \in A, \forall n \in \mathbb{Z}, (n\cdot 1_A)\times x = n\cdot x$
- $\forall x \in A, 0_A \times x = x \times 0_A = 0_A$

Démonstration à l'aide de $m_z : \left\{ \begin{array}{ccc} (A,+) & \to & (A,+) \\ t & \mapsto & z\times t \end{array} \right.$ et $M_z : \left\{ \begin{array}{ccc} (A,+) & \to & (A,+) \\ t & \mapsto & t\times z \end{array} \right.$, montrer que ce sont des morphismes puis appliquer les propriétés $(m_z(n\cdot t) = n\cdot m_z(t))$

Développements : On peut redémontrer les formules de développement bien connues :

- $\left(\sum_{k=1}^{n} a_k\right) \times \left(\sum_{k=1}^{p} b_k\right) = \sum_{\substack{1\leqslant k\leqslant n \\ 1\leqslant i\leqslant p}} (a_k \times b_i)$
- $\prod_{k=0}^{n}(a_k + b_k) = \sum_{J\in\mathscr{P}[\![1,n]\!]} \left(\prod_{i\in J} a_i \prod_{j\in[\![1,n]\!]\setminus J} b_j\right)$ (si $\times$ commute)
- $(a+b)^q = \sum_{k=0}^{n} \binom{n}{k} a^k b^{k-k}$ (si $ab = ba$)
- $(a-b)\sum_{k=0}^{n-1}(a^k b^{n-1-k}) = a^n - b^n = \sum_{k=0}^{n-1}(a^k b^{n-1-k})(a-b)$ (si $ab = ba$)

Sous-anneaux et sous-corps : soit $(A,\ +,\ \times)$ un anneau et $(K,\ +,\ \times)$ un corps.

B est un sous-anneau si :
— $\{0_A, 1_A\} \subset B \subset A$
— $\forall (x,y) \in B^2 : x+y \in B$ et $x \times y \in B$ et $-x \in B$

L est un sous-corps si :
— L est un sous-anneau
— $\forall x \in L, x \neq 0_K \Rightarrow x^{-1} \in L$

8.4 Zoologie des petits groupes

Éléments	Exemple	Cas général	Isomorphisme	commutatif
1	$A = (\{1\},\ \times)$	$G = (\{e\},\ \cdot)$	$\begin{cases} A \to G \\ g \mapsto 1 \end{cases}$	toujours
2	$A = (\{1,\ -1\},\ \times)$	$G = (\{e,\ a\},\ \cdot)$	$\begin{cases} A \to G \\ e \mapsto 1 \\ a \mapsto -1 \end{cases}$	toujours
3	$A = (\mathbb{U}_3,\ \times)$	$G = (\{e,\ a,\ b\},\ \cdot)$	$\begin{cases} A \to G \\ e \mapsto 1 \\ a \mapsto j \\ b \mapsto j^2 \end{cases}$	toujours
4	$A = (\mathbb{U}_4,\ \times)$	Seul $a^2 = e$	(faire la table)	oui
4	$A = (\mathbb{U}_2 \times U_2,\ \times)$	tout $x^2 = e$	idem	oui
5 (premier)	$A = (\mathbb{U}_5,\ \times)$	$G = (\{e,a,b,c,d\},\ \cdot)$	$G = \left\{a^k, k \in [\![0,\ \#G-1]\!]\right\}$	oui
6	$(\mathbb{U}_6,\ \times)$ commute, comme $(\mathbb{U}_2 \times \mathbb{U}_3,\ \times)$, mais pas $(\mathscr{S}_{[\![1,3]\!]},\ \circ)$			

Table 2 – Zoologie des petits groupes

9 Arithmétique

9.1 Axiomes de $\mathbb{N}$ et construction de $\mathbb{Z}$

Axiomes : on note $(\mathbb{N},\ \leqslant)$ l'ensemble ordonné qui est :
— Non-vide
— Non majoré

— toute partie non-vide admet un minimum
— toute partie non-vide majorée admet un maximum

On note $0 = \min(\mathbb{N})$, $1 = \min(\mathbb{N} \setminus \{0\})$, $\ldots$, $n+1 = \min(\mathbb{N} \setminus [\![0,\ n]\!])$

Définition de $\mathbb{Z}$: c'est le plus petit groupe contenant $\mathbb{N}$. Toute partie non-vide de $\mathbb{Z}$ qui admet un maximum/minimum et majorée/minorée.

Théorème de la division euclidienne : soit $(a,\ b) \in \mathbb{Z} \times \mathbb{N}^*$, il existe un *unique* couple $(q,\ r) \in \mathbb{Z}^2$ tel que : $\begin{cases} \boldsymbol{a = bq + r} \\ \boldsymbol{0 \leqslant r < b} \end{cases}$ De plus, on montre facilement que $q = \left\lfloor \dfrac{a}{b} \right\rfloor$

Unicité : prendre (q, r) et (q', r'), on a $(q - q')b = r - r'$...

Existence : $E = \left\{ a - qb, \middle| \begin{array}{l} q \in \mathbb{Z} \\ a - qb \geqslant 0 \end{array} \right\}$ est non vide (contient a ou $a - ab$), et donc admet un minimum r qui vérifie $0 \leqslant r < b$.

Raisonnement par récurrence : Les trois implications suivantes permettent de démontrer une propriété $P(n)$ dépendant de n par récurrence :

Classique : $\begin{cases} P(0)\ vraie \\ \forall n \in \mathbb{N},\ P(n) \Rightarrow P(n+1) \end{cases} \Rightarrow \forall n \in \mathbb{N}, P(n)\ vraie$

A deux pas : $\begin{cases} P(0)\ vraie \\ P(1)\ vraie \\ \forall n \in \mathbb{N},\ P(n) \text{ et } P(n+1) \Rightarrow P(n+2) \end{cases} \Rightarrow \forall n \in \mathbb{N}, P(n)\ vraie$

Forte : $\begin{cases} P(0)\ vraie \\ \forall n \in \mathbb{N}, \begin{cases} P(0) \\ \vdots \\ P(n) \end{cases} \Rightarrow P(n+1) \end{cases} \Rightarrow \forall n \in \mathbb{N}, P(n)\ vraie$

Démonstration par l'absurde : supposer un rang ou $P(n)$ est faux, considérer le minimum de l'ensemble $\{n \in \mathbb{N}, P(n) \text{ faux}\}$, ce n'est pas 0, et le rang précédent est vrai...

Décomposition en base $\boldsymbol{b}$: soit n un entier non-nul et $b \geqslant 2$. Il existe une unique liste $(c_1,\ \ldots,\ c_a) \in [\![0,\ b-1]\!]^a$ avec $a \in \mathbb{N}$ et $c_a \neq 0$ telle que :

$$\boldsymbol{n = \sum_{k=0}^{a} c_k b^k} \quad \text{on notera } n = \overline{c_a c_{a-1} \ldots c_2 c_1}^b$$

Existence par récurrence forte, initialisation pour tout $n \in [\![0,\ b-1]\!]$, puis faire la division euclidienne $n = bq + r$, comme $b < n$, il se décompose et r déjà compris entre 0 et $b - 1$.

Unicité : il existe un unique a tel que $b^a \leqslant n < b^{a+1}$. On effectue la division euclidienne $n = qb^a + r$, q est le chiffre c_a, réeffectuer la même opération avec le reste...

Sous-groupes de $(\mathbb{Z}, +)$ **:** pour tout $a \in \mathbb{Z}$, $a\mathbb{Z} = \{ak,\ k \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}, +)$ et tout sous-groupe H peut s'écrire sous la forme $a\mathbb{Z}$.
Démonstration en utilisant $\mathrm{Im}(h \to ah)$ pour la première et $a = \min(H \cap \mathbb{N}^*)$ (existant si $H \neq \{0\}$), puis une double inclusion pour la seconde (pour $x \in H$, on a $x = qa + r$ et par minimalité r forcément nul)

9.2 Nombres premiers et valuation p-adique

Notations : soit n un entier, $\mathcal{D}^+(n)$ l'ensemble de ces diviseurs positifs. n est premier si et seulement si $n \geqslant 2$ et $\mathcal{D}^+(n) = \{1,\ n\}$. On note $\mathcal{P}$ l'ensemble des nombres premiers. Si a divise b on notera $a \mid b$.

Lemme d'Euclide : pour tout $p \in \mathcal{P}$, et $(a,\ b) \in \mathbb{Z}$,

$$\boldsymbol{p \mid ab \Rightarrow p \mid a \text{ ou } p \mid b}$$

Démonstration intermédiaire : on pose $\delta = \min\{k \in \mathbb{N}^*, ak \in pN^*\}$, δ existe et $\delta \leqslant p$,
Montons que $\delta = p$: Il existe c tel que $pc = a\delta$ (1)
$\frac{a}{p} = \frac{c}{\delta}$. On effectue les divisions euclidiennes : $\begin{cases} a = q_1 c + r_1 & (0 \leqslant r_1 < c) \\ p = q_2 \delta + r_2 & (0 \leqslant r_2 < \delta) \end{cases}$ (2)
D'après (1) et (2), $q_2 c\delta + \underbrace{r_2 c}_{<\delta c} = q_1 c\delta + \underbrace{r_1 \delta}_{<\delta c}$

C'est une division euclidienne par δc, par unicité $r_2 c = r_1 \delta$ *i.e.* $\dfrac{r_2}{r_1} = \dfrac{c}{\delta} = \dfrac{a}{p}$.
On a $ar_2 = pr_1$, si $r_2 \neq 0$, alors $r_2 \in \{k \in \mathbb{N}^*, ak \in pN^*\}$ donc $r_2 > \delta$, ce qui est absurde : $r_2 = 0$, donc $p = q_2\delta + 0$, ce qui donne $\delta \in \mathcal{D}^+(p)$. Or $\mathcal{D}^+(p) = \{1,\ p\}$ et $1 \notin \{k \in \mathbb{N}^*, ak \in pN^*\}$ donc $\delta = p$
Démonstration : Cas $p \mid a$ immédiat, si $p \nmid a$, il existe c tel que $ab = pc$ ou $\frac{a}{p} = \frac{c}{b}$, on refait une division euclidienne $\begin{cases} c = q_3 a + r_3 & (0 \leqslant r_3 < a) \\ b = q_4 p + r_4 & (0 \leqslant r_4 < p) \end{cases}$ pour trouver $ar_4 = pr_3$.
Si $r_4 \neq 0$ alors $r_4 \geqslant \delta = p$ ce qui est absurde donc $r_4 = 0$, $b = q_4 p$ on a bien $p \mid b$

Construction de v_p : soit $(n,\ p) \in \mathbb{N} \times \mathcal{P}$ on note $E_p = \{\alpha \in \mathbb{N} / \ p^\alpha \mid n\}$. E_p est non vide (contient 0) et majoré (récurrence $p^{n+1} > n + 1$ et $p^a \mid n \Rightarrow p^a \leqslant n$) donc il admet un maximum. On définit la **valuation p-adique :**

$$\boldsymbol{v_p : \begin{cases} \mathbb{N}^* & \to & \mathbb{N} \\ n & \mapsto & \max\{\alpha \in \mathbb{N} / \ p^\alpha \mid n\} \end{cases}}$$

Cette fonction vérifie les propriétés :

- $\{\alpha \in \mathbb{N} / \ p^\alpha \mid n\} = [\![0,\ v_p(n)]\!]$
- $p^\alpha \mid n \Leftrightarrow \alpha \leqslant v_p(n) \Leftrightarrow v_p(p^\alpha) \leqslant v_p(n)$
- $\boldsymbol{v_p(a \times b) = v_p(a) + v_p(b)}$

Démonstration du point 3 : on sait que $p^{v_p(a)} \mid a$ donc $p^{v_p(a)+v_p(b)} \mid ab$ donc $v_p(a) + v_p(b) \leqslant v_p(ab)$, supposons $v_p(a) + v_p(b) < v_p(ab)$, alors $p^{v_p(a)}p^{v_p(b)}p \mid ab$.
Or $a = p^{v_p(a)}a'$ donc $p^{v_p(a)}p^{v_p(b)}p \mid p^{v_p(a)}a'p^{v_p(b)}b'$ soit $p \mid a'b'$ donc d'après le lemme d'Euclide $p \mid a$ ou $p \mid b$, ce qui est absurde par minimalité de $v_p(a)$

Premier facteur premier : soit n un entier, $l = \boldsymbol{\min \mathcal{D}^+(n) \setminus \{1\}}$ est premier. Existence facile, premier par minimalité (les diviseurs de l divisent n).

Décomposition en facteurs premiers : pour tout entier n non nul, on note $I_n = \{p \in \mathcal{P} / \ v_p(n) > 0\}$ un ensemble fini et

$$n = \prod_{p \in I_n} p^{v_p(n)} = \prod_{\boldsymbol{p \in \mathcal{P}}} \boldsymbol{p^{v_p(n)}}$$

Démonstration par récurrence forte : initialisation en 1 et 2, puis hérédité en exploitant $n = la$ avec l premier, on applique H.R. sur a, on a $n = l^{v_l(a)+1} \prod_{p \in \mathcal{P} \setminus \{l\}} p^{v_p(a)}$, de plus comme $v_p(n) = v_p(a) + v_p(l)$ on a $v_p(n) = v_p(a)$ et $v_l(n) = v_l(a) + 1$

Décomposition et divisibilité : $a \mid b \Leftrightarrow \forall p \in \mathcal{P},\ v_p(a) \leqslant v_p(b)$

9.3 PGCD et PPCM

PGCD : soit $(a,\ b) \in \mathbb{Z}^2$, on définit :

$$\boldsymbol{\text{pgcd}(a,\ b) = a \wedge b =} \left| \begin{array}{ll} \boldsymbol{\max(\mathcal{D}^+(a) \cap \mathcal{D}^+(b))} & \boldsymbol{si\ (a,\ b) \neq (0,\ 0)} \\ \boldsymbol{0} & \boldsymbol{si\ (a,\ b) = (0,\ 0)} \end{array} \right.$$

Si $(a,\ b) \in \mathbb{Z}^*$ alors $a \wedge b \in \mathbb{N}^*$ et

$$a \wedge b = \prod_{p \in \mathcal{P}} p^{\min\{v_p(|a|),\ v_p(|b|)\}} \quad car \quad \forall p \in \mathcal{P},\ v_p(a \wedge b) = \min\{v_p(|a|),\ v_p(|b|)\}$$

Démontrer l'existence du max, puis la décomposition par double inégalité en utilisation la propriété de divisibilité et des valuations p-adiques. Le pgcd vérifie les propriétés pour $(a,\ b,\ c,\ d) \in \mathbb{Z}^4$:

- $a \wedge b = b \wedge a \qquad (commutatif)$
- $a \wedge (b \wedge c) = (a \wedge b) \wedge c \ \ (associatif)$
- $0 \wedge b = |b|$
- $da \wedge db = |d|\,(a \wedge b)$

Démonstration en dissociant les cas ou l'un des termes est nul et en utilisant les valuations sinon

Généralisation : soit $k \geqslant 2$ et $(a_1, \ldots, a_k) \in \mathbb{Z}^k$ on peut définir $a_1 \wedge \ldots \wedge a_k$ et on a :
- $a_1 \wedge \ldots \wedge a_k = 0 \Leftrightarrow \forall i \in [\![1, k]\!], a_i = 0$
- si $a_i \neq 0$, $v_p(a_1 \wedge \ldots \wedge a_k) = \min\{a_1, \ldots, a_k\}$
- $a_1 \wedge \ldots \wedge a_k = \max\left(\bigcap_{i \in [\![1,k]\!]} \mathcal{D}^+(a_i)\right)$

Démonstration 1 par récurrence pour $\Rightarrow$ et par contraposée et commutativité pour $\Leftarrow$ du (1), par récurrence pour le (2) et par double inégalité pour (3)

Diviseur du PGCD : soit $b \in \mathbb{Z}$, $k \geqslant 2$ et $(a_1, \ldots, a_k) \in \mathbb{Z}^k$, on a l'équivalence :

$$\boldsymbol{|b| = \bigwedge_{i=1}^{k} a_i \Leftrightarrow \mathcal{D}(b) = \bigcap_{i=1}^{k} \mathcal{D}(a_i)}$$

Démonstration $\Rightarrow$ par double inclusion, ATTENTION aux valeurs absolues et cas $= 0$!

PPCM : soit $(a, b) \in \mathbb{Z}^2$, on définit :

$$\mathbf{ppcm}(a, b) = a \vee b = \left| \begin{array}{ll} \mathbf{min}(a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*) & \textbf{si } ab \neq 0 \\ 0 & \textbf{si } a = 0 \textbf{ ou } b = 0 \end{array} \right.$$

Si $(a, b) \in \mathbb{Z}^*$ alors $a \vee b \in \mathbb{N}^*$ et

$$a \vee b = \prod_{p \in \mathcal{P}} p^{\max\{v_p(|a|),\, v_p(|b|)\}} \quad car \quad \forall p \in \mathcal{P},\ v_p(a \vee b) = \max\{v_p(|a|),\ v_p(|b|)\}$$

On a des propriétés semblables au PGCD (commutativité, associativité, généralisation à k éléments, produit) qui se démontre de manière similaire, notamment :

$$|\mu| = \bigvee_{i=1}^{k} a_i \Leftrightarrow \mu\mathbb{Z} = \bigcap_{i=1}^{k} a_i\mathbb{Z} \cap \mathbb{N}^* \qquad \text{et} \qquad (a \wedge b)(a \vee b) = |ab|$$

Nombres premiers entre eux : $(a_1, \ldots, a_k)$ sont premiers entre eux
- dans leur ensemble si $\bigwedge_{i=0}^{k} a_k = 1$
- deux à deux si $\forall (i, j) \in [\![1, k]\!]^2, i \neq j \Rightarrow a_i \wedge a_k = 1$.

$(a_1, \ldots, a_k)$ sont premiers entre eux $\Leftrightarrow \bigcap_{i=1}^{k} \mathcal{D}^+(a_i) \subset \{1\}$
$\Leftrightarrow \boldsymbol{\forall p \in \mathcal{P}, \exists i \in [\![1, k]\!], v_p(a_i) = 0}$

Lemme de Gauss : soit $(a, b, c) \in \mathbb{Z}^2$ on a : $\left\{ \begin{array}{l} \boldsymbol{a \mid bc} \\ \boldsymbol{a \wedge b = 1} \end{array} \right. \boldsymbol{\Rightarrow a \mid c}$

Démo : étudier les cas ou l'un des nombres est nul, puis poser $p \in \mathcal{P}$ employer $v_p(|a|) = 0$ ou $v_p(|b|) = 0$ pour monter $a \mid c$

Diviseurs premiers distincts : soit $(a_1, \dots, a_k) \in Z^k$ des nombres premiers deux-à-deux distincts et $b \in \mathbb{Z}$, on a (démo employant les valuations p-adiques) :

$$\forall i \in [\![1,\ k]\!]\,, a_i \mid b \ \Rightarrow\ \prod_{i=1}^{k} a_i \ \middle|\ b$$

Formulaire : soit $(a, b, a_1, \dots, a_k) \in \mathbb{Z}^{k+2}$,

- $a \wedge b = 1 \Rightarrow a \vee b = |ab|$
- $a \wedge b = 1 \Rightarrow \boldsymbol{a^n \wedge b^p = 1}$
- $a \wedge b \neq 0 \Rightarrow \left(\dfrac{a}{a \wedge b}\right) \wedge \left(\dfrac{b}{a \wedge b}\right) = 1$
- $\forall i, a_i \wedge b = 1 \Rightarrow \left(\prod_{i=1}^{k} a_i\right) \wedge b = 1$
- a_i premier deux-à-deux $\Rightarrow \bigvee_{i=1}^{k} a_i = \prod_{i=1}^{k} |a_i|$
- $\delta = \bigwedge_{i=1}^{k} a_k$, alors $\bigwedge_{i=1}^{k} \dfrac{a_i}{\delta} = 1$

Toute se démontrent à l'aide des valuations p-adiques (cas $= 0$ et $|a|$)

PGCD et modulo : on démontre par double divisibilité (tout x divisant a et b divise $a \wedge b$) que $\forall (a,\ b,\ \lambda) \in \mathbb{Z}^3$, $\boldsymbol{(\lambda b + a) \wedge b = a \wedge b}$

Algorithme d'Euclide : soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$

Algorithme :

```
def pgcd(a, b):
    while b > 0:
        a, b = b, b % a
    return a
```

On définit la suite $(r_n)_{n\in\mathbb{N}}$ par :

$$\begin{cases} r_0 = a \\ r_1 = b \\ \forall n \geqslant 2, r_n = \left| \begin{array}{l} 0 \text{ si } r_{n-1} = 0 \\ \mathrm{mod}(r_{n-1},\ r_n) \text{sinon} \end{array} \right. \end{cases}$$

On a alors : $N = \boldsymbol{\min\{n \geqslant 1 / \ r_n = 0\}}$ existe et, pour tout $n \in [\![1,\ n]\!]\,, a \wedge b = r_{n-1} \wedge r_n$, en particulier $\boldsymbol{a \wedge b = r_{N-1}}$ et il existe $(u_n, v_n) \in \mathbb{Z}^2, r_n = au_n + bv_n$, notamment $\exists (u, v) \in \mathbb{Z}^2, \boldsymbol{au + bv = a \wedge b}$

Démonstration de l'existence par l'absurde, supposer qu'il n'existe pas et montrer qu'on obtient un reste négatif. La conservation du PGCD en montrant que $(r_n \wedge r_{n-1})_{n\in[\![1,\ N]\!]}$ est constante et l'existence par récurrence.

L'algorithme étendu permet de trouver $(u,\ v) \in \mathbb{Z}^2$ tels que $au + bv = a \wedge b$ en initialisant `u, v, w, x = 1, 0, 0, 1` puis à chaque itération en réaffectant les variables `u, v, w, x = w, x, u-w*a//b, v-x*a//b`

Caractérisation du PGCD : soit $(a,\ b) \in \mathbb{Z}^2$ et $d \in \mathbb{Z}$ on a les équivalences :

$$\begin{aligned} |d| = a \wedge b &\Leftrightarrow \left\{au + bv,\ (u,\ v) \in \mathbb{Z}^2\right\} = d\mathbb{Z} \\ &\Leftrightarrow \begin{cases} d \mid a \text{ et } d \mid b \\ \exists (u,\ v) \in \mathbb{Z}^2, au + bv = d \end{cases} \end{aligned}$$

Ces équivalences sont généralisables pour un PGCD entre k-nombres. Le théorème de Bézout et un cas particulier de la dernière.

Les démonstrations se font en utilisant $|d| = a \wedge b \Leftrightarrow \mathcal{D}(d) = \mathcal{D}(a) \cap \mathcal{D}(b)$

9.4 Congruences, infinité de $\mathcal{P}$ et autres

On dit que $\boldsymbol{a \equiv b\,[n]}$ lorsque $\boldsymbol{n \mid (a-b)}$ donc qu'il existe $\lambda \in \mathbb{Z}, a = b + \lambda n$. Si a et b sont congrus modulo n alors :

- $\lambda a \equiv \lambda b\,[n]$
- $a^p \equiv b^p\,[n]$
- $a + c \equiv b + d\,[n]$
- $ac \equiv bd\,[n]$

Utiliser l'identité de Bernoulli pour les puissances et introduire $+bc-bc$ pour le produit

Petit théorème de Fermat : soit $p \in \mathcal{P}$ et $n \in \mathbb{Z}$,

$$\boldsymbol{n^p \equiv n\,[p]} \qquad \text{et si } p \nmid n,\ n^{p-1} \equiv 1\,[p]$$

Démonstration par récurrence : $n^p = ((n-1)+1)^p = (n-1)^p \sum_{k=1}^{n-1} \binom{p}{k} (n-1)^k + 1$,

on a $(n-1)^p + 1 \equiv n\,[p]$ et on montre que comme $k! \binom{p}{k} = p(p-1)\dots(p+1-k)$

passage à v_p pour montrer que $p \left| \binom{p}{k} \right.$

Infinité de $\mathcal{P}$: elle se démontre par l'absurde (qui divise $\prod p + 1$) ou à partir de la suite de Fermat $F_n = 2^{2^n} + 1$ de nombre tous premiers entre eux.

Forme irréductible d'un rationnel : soit $x \in \mathbb{Q}$, il existe un unique couple $(a,\ b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $x = \dfrac{a}{b}$ et $a \wedge b = 1$

L'unicité se fait en montrant l'égalité de deux dénominateurs, l'existence en partant de la définition d'un rationnel puis divisant par le PGCD.

Points $(x,\ y)$ entiers sur une droite : $ax + by = c$ passe par des couples d'entiers si et seulement si $c \in (a \wedge b)\mathbb{Z}$, résolution en trouvant une solution particulière puis Gauss dans l'équation sans second membre.

10 Ensembles finis

10.1 Ensembles finis

Lemme des tiroirs : $\forall n \in \mathbb{N}^*, \forall f : [\![1,\ n]\!] \to [\![1,\ n-1]\!]$, f non injective

Démonstration par récurrence : aucune injection de $\{1\} \to \emptyset$ puis au rang n, si n n'admet pas d'antécédent, restreindre et corestreindre pour se ramener à l'HR, sinon supposer f injective, et a l'antécédent de n, poser $f_{|\llbracket 1, n+1\rrbracket \setminus \{a\}}^{|\llbracket 1, n-1\rrbracket}$ et montrer une contradiction avec l'hypothèse de récurrence

Soit $\forall f : \llbracket 1, \alpha\rrbracket \to \llbracket 1, \beta\rrbracket$, cette propriété permet de montrer les implications :

— f injective $\Rightarrow a \leqslant b$

— f surjective $\Rightarrow a \geqslant b$

— f bijective $\Rightarrow a = b$

Ensembles finis : un ensemble E est fini s'il existe $n \in \mathbb{N}$ et $\varphi : \llbracket 1, n\rrbracket \to E$ tel que φ soit bijective
Un tel n est unique, on dit que c'est le *cardinal* de E (noté $\#E$ ou $\text{card}(E)$)

On peut aussi démontrer que deux ensembles finis en bijection ont le même cardinal.

Partie d'un ensemble fini : soit E non vide, alors $\exists e \in E$ et $\#(E \setminus \{e\}) = \#E - 1$ (construire la bijection) et, plus généralement,

$$\forall a \in \mathscr{P}(E), \left| \begin{array}{l} A \text{ est un ensemble fini} \\ \#A \leqslant \#E \\ A \subsetneq E \Leftrightarrow \#A < \#E \end{array} \right.$$

Fonctions et ensembles finis : on a les implications, pour $f : A \to B$,

— f surjective et A fini $\Rightarrow \left\{ \begin{array}{l} B \text{ fini et } \#B \leqslant \#A \\ \#B = \#A \Leftrightarrow f \text{ bijective} \end{array} \right.$

— f injective et B fini $\Rightarrow \left\{ \begin{array}{l} A \text{ fini et } \#A \leqslant \#B \\ \#A = \#B \Leftrightarrow f \text{ bijective} \end{array} \right.$

— $\#A = \#B$, alors f injective $\Leftrightarrow f$ bijective $\Leftrightarrow f$ surjective

Démonstration en (co)restreignant pour trouver une bijection d'une partie de A vers une partie de B

10.2 Un peu de dénombrement

Réunion d'ensemble finis : soit I un ensemble d'index finis et $(E_i)_{i\in I}$ une famille d'ensembles finis disjoints deux-à-deux. On a :

$$\bigcup_{i\in I} E_i \text{ fini et } \# \left(\bigcup_{i\in I} E_i \right) = \sum_{i\in I} (\#E_i)$$

La propriété est similaire pour des ensembles non disjoints, mais on majore seulement le cardinal ($\#(A \cup B) = \#A + \#B - \#(A \cap B)$)

Démonstration par récurrence, initialisation à partir des bijections $\varphi_1 : [\![1,\ \#A]\!] \to A$ et $\varphi_1 : [\![1,\ \#B]\!] \to B$, construire $f : \left\{ \begin{array}{ccc} [\![1,\ \#A+\#B]\!] & \to & A \cup B \\ t & \mapsto & \left| \begin{array}{ll} \varphi_1(t) & \text{si } t \leqslant \#A \\ \varphi_2(t-\#A) & \text{si } t \geqslant \#A+1 \end{array} \right. \end{array} \right.$ bijective puis conclure. Procéder de même pour l'hérédité. Pour les groupes non-distincts : $A \cup B = (A \cap \overline{B}) \cup (A \cap B) \cup (\overline{A} \cap B)$

Produit cartésien : soit $(E_i)_{i \in [\![1,\ n]\!]}$ une famille d'ensembles finis, alors $E_1 \times \ldots \times E_n$ est fini et de cardinal $\prod_{k=1}^{n} (\#E_k)$

Démo par récurrence, en utilisant $A \times B = \bigcup_{a \in A} (\{a\} \times B)$

Ensemble des fonctions : soit A et B finis, alors B^A est fini et $\#\left(B^A\right) = (\#B)^{\#A}$.

Démonstration en posant $n = \#A$, et $\varphi : [\![1,\ n]\!] \to A$ bijective, puis en posant G : $\left\{ \begin{array}{ccc} B^A & \to & B^n \\ f & \mapsto & (f(\varphi(1)), \ldots, f(\varphi(n))) \end{array} \right.$ bijective, $G^{-1} : \left\{ \begin{array}{ccc} B^n & \to & B^A \\ (b_1, \ldots, b_n) & \mapsto & \left\{ \begin{array}{ccc} A & \to & B \\ a & \mapsto & b_{\varphi^{-1}(a)} \end{array} \right. \end{array} \right.$

Listes disjointes d'un ensemble : soit E fini de cardinal n, soit $p \in \mathbb{N}$. on pose $A = \{(e_1,\ \ldots,\ e_p) \in E^p /\ (e_1,\ \ldots,\ e_p)$ disjoint 2 à 2$\}$. On a A fini et $\#A = n(n-1)\ldots(n-p+1)$

La démonstration se fait par récurrence sur p, initialisation à $p = 0$, $A = \{()\}$, puis hérédité en posant $A = \bigcup_{(x_1,\ldots,x_{p-1}) \in \widetilde{A}} \{(x_1, \ldots, x_{p-1}, e), e \in E \setminus \{s_1,\ \ldots,\ x_{p-1}\}\}$ puis employant l'HR sur $\widetilde{A}$ et l'union finie disjointe d'ensemble finis

Injections d'un ensemble fini : soit $\mathrm{Inj}(E,\ F)$ l'ensemble des injections de E vers F, $\mathrm{Inj}(E,\ F)$ est fini et $\#\mathrm{Inj}(E,\ F) = n(n-1)\ldots(n-p+1)$

Démonstration en mettant les bijections en lien avec les $\#E$-listes de F et employant le résultat précédent

Parties d'un ensemble : soit E fini de cardinal n et $\mathscr{P}_p(E)$ l'ensemble des parties de E de cardinal p. On a $\#\mathscr{P}_p(E) = \dfrac{n(n-1)\ldots(n-p+1)}{p!} = \left(\begin{array}{c} n \\ p \end{array} \right)$

Démonstration en posant $G : \left\{ \begin{array}{ccc} \mathrm{Inj}([\![1,\ p]\!],\ E) & \to & \mathscr{P}_p(E) \\ \varphi & \mapsto & \{\varphi(1),\ \ldots,\ \varphi(p)\} \end{array} \right.$, puis en posant $A \in \mathscr{P}_p(E)$ et calculant $G^{-1}(\{A\})$, qui correspond à $\mathrm{Inj}([\![1,\ p]\!],\ A)$. Donc comme $\mathrm{Inj}([\![1,\ p]\!],\ E) = \bigcup_{A \in \mathscr{P}_p(E))} G^{-1}(\{A\})$, on utilise la réunion finie d'ensemble finis disjoints pour trouver le cardinal de l'ensemble d'index

Cela permet également de montrer que $\#\mathscr{P}(E) = 2^n$ avec le binôme de Newton

11 Autour des réels

11.1 Bornes supérieure et inférieure dans $\mathbb{R}$

Axiome : toute partie non-vide majorée de $\mathbb{R}$ admet une borne sup. Cela permet de démontrer que toute partie non-vide minorée de $\mathbb{R}$ admet une borne inf, en prenant pour candidat sup m_A, on a bien $\forall x \in m_A$, sup $m_A \geqslant x$ et comme $\forall t \in A, \forall x \in m_A, t \geqslant x$ t majore m_A, donc $t \geqslant$ sup m_A.

Intervalles : soit $I \in \mathscr{P}(\mathbb{R})$, I est un **intervalle** de $\mathbb{R}$ si et seulement si $\boldsymbol{\forall (x,\, y) \in I^2,\, x < y \Rightarrow [x,\, y] \in I}$.

On peut alors classifier les intervalles en 4 catégories :
- non-majoré et non-minoré : $\mathbb{R}$
- majoré et non minoré : $]-\infty,\, \beta]$ ou $]-\infty,\, \beta[$
- non-majoré et minoré : $[\alpha,\, +\infty[$ ou $]\alpha,\, +\infty[$
- majoré et minoré : $\emptyset$ ou $\{\alpha\}$ ou $[\alpha,\, \beta]$ avec bornes ouvertes ou fermées

Démonstration par étude de cas et en montrant que $]-\infty,\, \beta[\subset I \subset]-\infty,\, \beta]$

11.2 Fonction partie entière

Définition : soit $x \in \mathbb{R}$, et $E_x = \{p \in \mathbb{Z} / \, p \leqslant x\}$, on note alors $\boldsymbol{\lfloor x \rfloor = \min E_x}$

Démonstration de l'existence par dissociation de cas : E_x non-vide si $x \geqslant 0$, alors on montre que sup E_x est entier par l'absurde (sinon deux entiers entre sup $E_x - \frac{1}{2}$ et sup E_x), puis si $E_x < 0$, alors $\lfloor -x \rfloor - 1 < x$...

Caractéristiques : soit $p \in \mathbb{Z}$, on a les propriétés :

$$p = \lfloor x \rfloor \Leftrightarrow p \leqslant x < p+1 \Leftrightarrow x - 1 < p \leqslant x \qquad \lfloor x + p \rfloor = \lfloor x \rfloor + p$$

Approximation décimale : soit $t \in \mathbb{R}$, on peut encadrer t par :

$$\boldsymbol{\frac{\lfloor 10^n t \rfloor}{10^n} \leqslant t < \frac{\lfloor 10^n t \rfloor + 1}{10^n}} \qquad \text{à } 10^{-n} \text{ près}$$

Densité dans $\mathbb{R}$: On dit qu'un ensemble $A \in \mathscr{P}(\mathbb{R})$ est **dense** dans $\mathbb{R}$ si, pour tout $a < b$ réel, $\boldsymbol{\exists x \in A, x \in]a,\, b[}$. Notamment, $\mathbb{Q}$, $\mathbb{D}$ et $\mathbb{R} \setminus \mathbb{Q}$ sont denses.

Démonstration de la densité de $\mathbb{Q}$ en posant $[\alpha, \beta] \subset]a, b[$ puis multipliant par $k \in \mathbb{N}^*, k(\beta - \alpha) > 1$ pour trouver un entier $p = \lfloor \beta \rfloor$. $\frac{p}{k} \in]a, b[$. Pour les irrationnels, utiliser le fait qu'il y ait un rationnel dans $]a + \sqrt{2}, b + \sqrt{2}[$

12 Suites numériques

12.1 Suites convergentes

Convergence vers ℓ : on dit que $(x_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ converge vers $\ell \in \mathbb{K}$ lorsque :

$$\boldsymbol{\forall \varepsilon > 0,\ \exists n_0 \in \mathbb{N},\ \forall n > n_0,\ |x_n - \ell| < \varepsilon}$$

On note alors $(x_n)_{n\in\mathbb{N}} \to \ell$ ou $x_n \xrightarrow[n\to+\infty]{} l$
On dit que (x_n) *converge* s'il existe un tel ℓ. La limite est *unique*

Convergence vers 0 : soit $(x_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ et $\ell \in \mathbb{K}$. On a

$$x_n \xrightarrow[n\to+\infty]{} \ell \quad \Leftrightarrow \quad (x_n - \ell) \xrightarrow[n\to+\infty]{} 0 \quad \Leftrightarrow \quad |x_n - \ell| \xrightarrow[n\to+\infty]{} 0$$

Encadrement : $\begin{cases} \forall n \in \mathbb{N},\ |x_n| < |y_n| \\ y_n \xrightarrow[n\to+\infty]{} 0 \end{cases} \Rightarrow x_n \xrightarrow[n\to+\infty]{} 0$ (démo epsilonesque)

Combinaison linéaire de suite : soit (x_n) et (y_n) deux suites de $\mathbb{K}^{\mathbb{N}}$ et $(\lambda, \mu) \in \mathbb{K}^2$. On a alors (démonstration epsilonesque) :

$$\begin{cases} \boldsymbol{(x_n) \to L} \\ \boldsymbol{(y_n) \to L'} \end{cases} \boldsymbol{\Rightarrow (\lambda x_n + \mu y_n) \longrightarrow \lambda L + \mu L'}$$

Suites associées : soit $(z_n) \in \mathbb{C}^{\mathbb{N}}$, $\boldsymbol{(z_n)}$ **converge** $\boldsymbol{\Leftrightarrow}$ $\boldsymbol{(\mathrm{Re}(z_n))}$ **et** $\boldsymbol{(\mathrm{Im}(z_n))}$ **convergent**. Si (z_n) converge alors on a (démonstration par encadrement)

- $(\overline{z_n})$ converge et $\lim \overline{z_n} = \overline{\lim z_n}$
- $(|z_n|)$ converge et $\lim |z_n| = |\lim z_n|$
- $(\mathrm{Re}(z_n))$ converge et $\lim \mathrm{Re}(z_n) = \mathrm{Re}(\lim z_n)$
- $(\mathrm{Im}(z_n))$ converge et $\lim \mathrm{Im}(z_n) = \mathrm{Im}(\lim z_n)$

Convergence et parité : soit $(x_n) \in \mathbb{K}^{\mathbb{N}}$, (x_n) converge $\Leftrightarrow$ $(x_{2p})_{p\in\mathbb{N}}$ et $(x_{2p+1})_{p\in\mathbb{N}}$ convergent vers la même limite (démonstration par epsilon)

Caractérisation séquentielle : soit $A \in \mathscr{P}(\mathbb{R}) \setminus \{\emptyset\}$ et $\lambda \in \mathbb{R}$:

si A majorée alors : $\boldsymbol{\lambda = \sup A} \quad \Leftrightarrow \quad \begin{cases} \boldsymbol{\lambda \text{ majore } A} \\ \boldsymbol{\exists (x_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}},\ x_n \xrightarrow[n\to+\infty]{} \lambda} \end{cases}$

si A minorée alors : $\boldsymbol{\lambda = \inf A} \quad \Leftrightarrow \quad \begin{cases} \boldsymbol{\lambda \text{ minore } A} \\ \boldsymbol{\exists (x_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}},\ x_n \xrightarrow[n\to+\infty]{} \lambda} \end{cases}$

Démo par double implication. $\Rightarrow$ construire la suite à partir du x_n existant vérifiant $\lambda \geqslant x_n > \frac{1}{10^n}$. $\Leftarrow$ montrer que λ est le meilleur majorant par l'absurde.

Limite et densité : soit $A \subset \mathbb{R}$, on a l'équivalence :

$$\boldsymbol{A \text{ est dense dans } \mathbb{R} \Leftrightarrow \forall x \in \mathbb{R}, \exists (\alpha_n) \in A^{\mathbb{N}},\ \alpha_n \to x}$$

Démonstration : $\Rightarrow$ construire la suite $\alpha_n \in \left]x - \frac{1}{10^n}, x + \frac{1}{10^n}\right[\cap A$, $\Rightarrow$ trouver l'élément de $A \cap]a, b[$ à partir de la suite convergeant vers $\frac{a+b}{2}$

Convergence en 0 : soit (x_n) une suite qui tend vers 0 en (y_n) une suite bornée. On a alors $(x_n \times y_n) \xrightarrow[n \to \infty]{} 0$

Démonstration par epsilon : $|y_n| \leqslant M$, donc $|x_n y_n| \leqslant \varepsilon M$

Convergence et bornes : une suite (x_n) convergente vers Lest bornée, si sa limite $(x_n) \neq 0, \exists n_0 \in \mathbb{N}, \forall n \geqslant n_0, |x_n| \geqslant \frac{1}{2}|L|$
Démonstration : $|x_n| = |(x_n - L) + L| \leqslant \varepsilon + |L|$, soit $M = \max\{|x_0|, \ldots, |x_{n-1}|, \varepsilon + |L|\}$, c'est un majorant de (x_n) De plus, si $L \neq 0$, alors on peut prendre $\varepsilon = \frac{1}{2}|L|$ et donc il existe $n_0 \in \mathbb{N}, \forall n \geqslant n_0, |x_n| \geqslant |L| - |x_n - L| = \frac{1}{2}|L|$

Produit et quotient : soit $(x_n) \longrightarrow L$ et $(y_n) \longrightarrow L'$, on a :

$$\boldsymbol{(x_n y_n) \longrightarrow LL'} \qquad \boldsymbol{\left(\frac{x_n}{y_n}\right) \longrightarrow \frac{L}{L'}}$$

Démo : pour le produit, considérer $|x_n y_n - LL'| = |x_n y_n + x_n L' - x_n L' - LL'| = |x_n(y_n - L') + L'(x_n - L)|$
Pour le quotient, on a $\left|\frac{1}{y_n} - \frac{1}{L'}\right| = \left|\frac{L' - y_n}{y_n L'}\right|$

Limites connues : on a notamment (z^n) converge si $|z| < 1$ ou $z = 1$.

Démonstration en minorant $|z|^n = ((|z| - 1) + 1)^n \geqslant 1 + n(|z| - 1)$ pour le cas $|z| > 1$, en minorant de même $\left|\frac{1}{z}\right|$ si $|z| < 1$ et en raisonnant pas $CN\ CS$ si $|z| = 1$

12.2 Suites réelles convergentes

Suites monotones : soit $(x_n) \in \mathbb{R}^{\mathbb{N}}$, on a :

$$\begin{cases} (x_n) \text{ croissante ou décroissante} \\ (x_n) \text{ majorée ou minorée à partir de } n_0 \end{cases} \Rightarrow \begin{cases} (x_n) \text{ converge} \\ \forall n \geqslant n_0, x_n \leqslant \lim(x_n) \text{ ou } x_n \geqslant \lim(x_n) \end{cases}$$

Démonstration : prendre $L = \sup\{x_n, n \in \mathbb{N}\}$, cet borne existe et pour $\varepsilon > 0$, $L - \varepsilon$ ne majore pas l'ensemble, donc il existe $n \in \mathbb{N}, |x_n - L| < \varepsilon$, or (x_n) est croissante...

Suites adjacentes : soit $\big((x_n),\ (y_n)\big) \in \big(\mathbb{R}^{\mathbb{N}}\big)^2$, on a :

$$\begin{cases} (x_n) \text{ décroissante et } (y_n) \text{ croissante} \\ (x_n - y_n) \longrightarrow 0 \end{cases} \Rightarrow \begin{cases} (x_n) \text{ et } (y_n) \text{ convergent} \\ \lim(x_n) = \lim(y_n) \end{cases}$$

On montre d'abord que $x_n - y_n > 0$ car elle est décroissante $(x_{n+1} - y_{n+1} - x_n + y_n) < 0$, donc on a $x_0 \geqslant x_n \geqslant y_n \geqslant y_0$, ce qui permet de montrer leur convergence. Pour l'égalité on a $(x_n) = (x_n - y_n) + (y_n)$...

Théorème d'encadrement : soit $\big((x_n),\ (y_n),\ (z_n)\big) \in \big(\mathbb{R}^{\mathbb{N}}\big)^3$, on a :

$$\begin{cases} (x_n) \text{ et } (z_n) \text{ convergent} \\ \lim(x_n) = \lim(z_n) \\ \exists n_0 \in \mathbb{N}, \forall n \geqslant n_0,\ x_n \leqslant y_n \leqslant z_n \end{cases} \Rightarrow \begin{cases} (y_n) \text{ converge} \\ \lim(y_n) = \lim(x_n) = \lim(z_n) \end{cases}$$

Démonstration : on a $0 \leqslant (y_n - x_n) \leqslant (z_n - y_n)$ donc $(y_n - x_n) \longrightarrow 0$ or $(y_n) = (y_n - x_n) + (x_n)$

Limite et intervalle : soit $(x_n) \longrightarrow L$, et $(a,\ b) \in \mathbb{R}, a < L < b$, il existe alors $n_0 \in \mathbb{N}, \forall n \geqslant n_0, x_n \in]a,\ b[$. Démonstration par epsilon immédiate

Limites et comparaison : soit $(x_n) \longrightarrow L$ et $(y_n) \longrightarrow L'$. On suppose qu'à partir d'un rang n_0, $x_n \geqslant y_n$, alors $L \geqslant L'$

Démonstration par l'absurde, si $L' > L$, il existe un $x_{n_1} < L + \frac{1}{3}|L' - L|$ et $y_{n_2} > L' - \frac{1}{3}|L' - L|$, donc $y_{\max(n_1,\, n_2)} > x_{\max(n_1,\, n_2)}$

12.3 De l'ordre dans le chaos

Extraction : une fonction $\varphi : \mathbb{N} \to \mathbb{N}$ est une extraction si elle est strictement croissante. Soit (x_n) une suite, on peut définir la suite extraite $(y_p)_{p\in\mathbb{N}} = (x_{\varphi(p)})_{p\in\mathbb{N}}$. Si $(x_n) \to L$ alors $(y_p) \to L$

Théorème de Bolzano-Weierstrass : soit $(x_n) \in \mathbb{K}^{\mathbb{N}}$ une suite *bornée*. Il existe $L \in \mathbb{K}$ et $\varphi \in \mathscr{F}(\mathbb{N},\, \mathbb{N})$ une extraction telle que $\boldsymbol{(x_{\varphi(p)})_{p\in\mathbb{N}} \longrightarrow L}$

Dans le cas réel construire les suites (a_n) et (b_n) avec a_0 un minorant et b_0 un majorant, puis $c_n = \frac{a_n + b_n}{2}$. On a $E = \{n \in \mathbb{N} / \ a_n \leqslant x_n \leqslant b_n\}$ infini donc l'un des ensembles $\{n \in \mathbb{N} / \ a_n \leqslant x_n \leqslant c_n\}$ ou $\{n \in \mathbb{N} / \ c_n \leqslant x_n \leqslant b_n\}$ l'est également, définir les termes du rang $n+1$ comme ceux encadrant l'ensemble infini. Les suites (a_n) et (b_n) ainsi construites sont adjacentes. Construire une extraction à partir de $\min E$ à chaque rang, puis montrer la convergence de la suite extraite par encadrement entre (a_n) et (b_n).
Dans le cas complexe, séparer les suites $(\mathrm{Re}(x_n))$ et $(\mathrm{Im}(x_n))$

Divergence : si (x_n) admet deux telles valeurs d'adhérence distinctes, alors (x_n) diverge

12.4 Suites définies par récurrence

Suite arithmétiquo-géométrique : soit $(a, b) \in \mathbb{K}^2$ et $(x_n) \in \mathbb{K}^{\mathbb{N}}$ une suite vérifiant : $\forall n \in \mathbb{N}, x_{n+1} = ax_n + b$, si $a \neq 1$, alors $\boldsymbol{x_n = \frac{b}{1-a} + a^n \left(x_0 - \frac{b}{1-a}\right)}$. Démonstration en posant $z = \frac{b}{1-a}$, on a $z = az + b$ donc $(x_{n+1} - z) = a(x_n - z)$...

Suites linéaires du second ordre : soit $(a, b) \in \mathbb{K}$ et $(x_n) \in \mathbb{K}^{\mathbb{N}}$ une suite vérifiant $\forall n \in \mathbb{N}, x_{n+2} = ax_{n+1} + bx_n$. On définit l'équation caractéristique (E_c) par $z^2 = az + b$.

- **Cas 1 :** deux solutions r_1 et r_2, alors il existe $(\alpha,\ \beta) \in \mathbb{K}^2$ tel que pour tout $n \in \mathbb{N}, \boldsymbol{x_n = \alpha r_1^n + \beta r_2^n}$
- **Cas 2 :** une solution double r, alors il existe $(\alpha,\ \beta) \in \mathbb{K}^2$ tel que pour tout $n \in \mathbb{N}, \boldsymbol{x_n = \alpha r^n + \beta n r^n}$
- **Cas 3 :** aucune solution (suite réelle), et solution complexe de la forme $\rho e^{i\theta}$ alors il existe $(\alpha,\ \beta)$ßK^2 tel que $\forall n \in \mathbb{N}, \boldsymbol{x_n = \alpha \rho^n \cos(n\theta) + \beta \rho^n \sin(n\theta)}$

Démonstration : considérer λ un racine non nulle, et μ l'autre racine, et $(y_n) = \left(\frac{x_n}{\lambda^n}\right)$, on a $y_{n+2} = y_{n+1} + \frac{\mu}{\lambda}(y_{n+1} - y_n)$, donc $(y_{n+1} - y_n$ est géométrique. En sommant les termes on trouve $y_n - y_0 = (y_1 - y_0) \sum_{k=0} n - 1 \left(\frac{\mu}{\lambda}\right)^k$, dissocier les cas $\lambda = \mu$ et $\lambda \neq \mu$

Récurrence de la forme $u_{n+1} = f(u_n)$: il faut impérativement vérifier la bonne définition en trouvant une partie $A \subset \mathbb{R}$ vérifiant $u_0 \in A$ et $f(A) \subset A$. Pour déterminer les propriétés vérifiées par la suite, faire un dessin.

12.5 Divergence vers $\pm\infty$

DÉFINITION : soit $(x_n) \in \mathbb{R}^{\mathbb{N}}$, on dit que :
- $(x_n) \longrightarrow +\infty$ lorsque $\forall\, A \in \mathbb{R},\ \exists\, n_0 \in \mathbb{N},\ \forall\, n \geqslant n_0,\ \ x_n > A$
- $(x_n) \longrightarrow -\infty$ lorsque $\forall\, B \in \mathbb{R},\ \exists\, n_0 \in \mathbb{N},\ \forall\, n \geqslant n_0,\ \ x_n < B$

On notera $\overline{\mathbb{R}}$ l'ensemble $\mathbb{R} \cup \{-\infty,\ +\infty\}$

Monotonie : Une suite croissante et non-majorée ou décroissante et non-minorée tend respectivement vers $+\infty$ ou $-\infty$. Démonstration assez immédiate

Croissance comparée : soit (x_n) et (y_n) deux suites, on a les implications :

$$\begin{cases} (x_n) \longrightarrow +\infty \\ x_n \leqslant y_n \end{cases} \Rightarrow (y_n) \longrightarrow +\infty \qquad \begin{cases} (x_n) \longrightarrow - + \infty \\ x_n \geqslant y_n \end{cases} \Rightarrow (y_n) \longrightarrow -\infty$$

Démonstration epsilonesque

Équivalent de Bolzano-Weierstrass : soit $(x_n) \in \mathbb{R}^{\mathbb{N}}$,
- (x_n) non majorée $\Rightarrow \exists \varphi \in \mathscr{F}(\mathbb{N}, \mathbb{N})$ une extraction, $\left(x_{\varphi(p)}\right)_{p \in p} \longrightarrow +\infty$

— (x_n) non minorée $\Rightarrow \exists \varphi \in \mathscr{F}(\mathbb{N}, \mathbb{N})$ une extraction, $\left(x_{\varphi(p)}\right)_{p \in p} \longrightarrow -\infty$
Construire l'extraction par récurrence vérifiant $\varphi(n+1) > \varphi(n)$ et $x_{\varphi(n+1)} > n+1$

Opération	$+\infty + (x \in \mathbb{R}$ ou $+\infty)$	$-\infty + (x \in \mathbb{R}$ ou $-\infty)$	$+\infty \times (x \in \mathbb{R}_+^*$ ou $+\infty)$
Limite	$+\infty$	$-\infty$	$+\infty$
Opération	$-\infty \times (x \in \mathbb{R}_-^*$ ou $-\infty)$	$-1 \times (+\infty)$	$\frac{1}{+\infty}$
Limite	$+\infty$	$-\infty$	0^+
Formes indéterminés	$0 \times \infty$ 1^∞	$\frac{\infty}{\infty}$ $\frac{0}{0}$	$\infty - \infty$ 0^0

Table 3 – Théorèmes d'opération sur les limites

13 Espaces vectoriels

13.1 Espaces vectoriels et opérations

Définition : un ensemble $(E, +, \cdot)$ est un $\mathbb{K}$-*espace vectoriel* si :

1. $(E, +)$ est un *groupe commutatif*
2. $\cdot$ est une fonction de $\mathbb{K} \times E \to E$ vérifiant :
   (a) $\forall (\lambda, \mu, x) \in \mathbb{K}^2 \times E, (\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$
   (b) $\forall (\lambda, x, y) \in \mathbb{K} \times E^2, \lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$
   (c) $\forall (\lambda, \mu, x) \in \mathbb{K}^2 \times E, \lambda \cdot (\mu \cdot x) = (\lambda \times \mu) \cdot x$
   (d) $\forall x \in E, 1_{\mathbb{K}} \cdot x = x$

Les éléments de E sont alors appelés *vecteurs*, ceux de F *scalaires*, et on nomme vecteur nul l'élément 0_E.

Exemples : Les ensembles suivants sont des $\mathbb{K}$-espaces vectoriels : En particulier, $(\mathbb{K}, +, \times)$ est un $\mathbb{K}$-espace vectoriel et tout $\mathbb{C}$-espace vectoriel est un $\mathbb{R}$-espace vectoriel
Démonstration en vérifiant les axiomes.

Ensemble	Loi +	Fonction $\cdot$	Vecteur Nul
$\mathbb{K}^n$	$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$	$\lambda \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{pmatrix}$	$\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$
$E_1 \times \ldots \times E_p$ E_i un $\mathbb{K}$ev	$\begin{pmatrix} e_1 \\ \vdots \\ e_p \end{pmatrix} + \begin{pmatrix} u_1 \\ \vdots \\ u_p \end{pmatrix} = \begin{pmatrix} e_1 + u_1 \\ \vdots \\ e_p + u_p \end{pmatrix}$	$\lambda \cdot \begin{pmatrix} e_1 \\ \vdots \\ e_p \end{pmatrix} = \begin{pmatrix} \lambda \cdot e_1 \\ \vdots \\ \lambda \cdot e_p \end{pmatrix}$	$\begin{pmatrix} 0_{E_1} \\ \vdots \\ 0_{E_p} \end{pmatrix}$
$\mathscr{F}(A, E)$ E un $\mathbb{K}$ev	$f_1 + f_2 = \left\{ \begin{array}{ccc} A & \to & E \\ t & \mapsto & f_1(t) + f_2(t) \end{array} \right.$	$\lambda \cdot f_1 = \left\{ \begin{array}{ccc} A & \to & E \\ t & \mapsto & \lambda \cdot f_1(t) \end{array} \right.$	$\left\{ \begin{array}{ccc} A & \to & E \\ t & \mapsto & 0_E \end{array} \right.$

Table 4 – Exemples de $\mathbb{K}$-espaces vectoriels

Combinaison linéaire : Soit E un $\mathbb{K}$-espace vectoriel, A un ensemble, et $(e_i)_{i\in A}$ une famille de vecteurs. Soit $x \in E$, on dit que x est une combinaison linéaire de $(e_i)_{i\in A}$ lorsqu'il existe $B \subset A$ finie et $(\lambda_i)_{i\in B} \in \mathbb{K}^B$ telle que : $\boldsymbol{x = \sum_{i\in B} \lambda_i \cdot e_i}$.

On note $\mathrm{Vect}\big((e_i)_{i\in A}\big)$ l'ensemble des combinaisons linéaires de $(e_i)_{i\in A}$, aussi appelée espace vectoriels engendré par $(e_i)_{i\in A}$

Si $A = \mathbb{N}$ on a $\mathrm{Vect}\big((e_i)_{i\in\mathbb{N}}\big) = \bigcup_{p\in\mathbb{N}} \mathrm{Vect}\big((e_i)_{i\leqslant p}\big)$
Réunion croissante $\mathrm{Vect}\big((e_i)_{i\leqslant p}\big) \subset \mathrm{Vect}\big((e_i)_{i\leqslant p+1}\big)$

Si A infini, on peut sommer sur une famille presque vide, *i.e* une famille dont un nombre fini d'éléments est non-nul, on note l'ensemble de familles presque vide note $\mathbb{K}^{(A)}$. Ainsi on a $\varphi : \begin{cases} \mathbb{K}^{(A)} & \to \mathrm{Vect}\big((e_i)_{i\in A}\big) \\ (\lambda_i)_{i\in A} & \mapsto \sum_{i\in A} \lambda_i \cdot e_i \end{cases}$ bien définie et surjective.

Opérations usuelles : soit $(x,\, y) \in E$ et $(\lambda,\, \mu) \in \mathbb{K}$, on a :

- $\boldsymbol{\lambda \cdot x = 0_E \Leftrightarrow \lambda = 0_{\mathbb{K}}}$ ou $\boldsymbol{x = 0_E}$
- $(\lambda - \mu)\cdot x = \lambda \cdot x - \mu \cdot x$
- $nx = (n\, 1_{\mathbb{K}}) \cdot x$
- $-x = (-1_{\mathbb{K}}) \cdot x$
- $\lambda \cdot (x - y) = \lambda \cdot x - \lambda \cdot y$

Démonstration en utilisant les morphismes de groupe $\varphi_1 : \begin{cases} \mathbb{K} & \to E \\ t & \mapsto t \cdot x \end{cases}$ et $\varphi_2 : \begin{cases} E & \to E \\ e & \mapsto \lambda \cdot e \end{cases}$

13.2 Sous-espaces vectoriels

Définition : soit $(E,\, +,\, \cdot)$ un $\mathbb{K}$-espace vectoriel, on dit que F est un sous-espace vectoriel de E lorsque :

1. $F \subset E$
2. $0_E \in F$
3. $\forall (x,\, y) \in F^2, x + y \in F$
4. $\forall (\lambda,\, x) \in \mathbb{K} \times F, \lambda \cdot x \in F$

Un tel sous-espace vectoriel $(F,\, +,\, \cdot)$ est un $\mathbb{K}$-espace vectoriel

Démonstration en vérifiant que $(F,\, +)$ est un sous-groupe de $(E,\, +)$ (inversion), puis les axiomes de $\cdot$

Intersection de sous-espaces : soit $F_1, \ldots, F_p$ des sous-espaces vectoriels de E. On a alors $\bigcap_{i=0}^{p} F_i$ est un sous-espace vectoriel de E

Somme d'un nombre fini de sous-espaces : soit $F_1, \ldots, F_p$ des sous-espaces vectoriels de E. On pose :

$$F_1 + \ldots + F_p = \sum_{i=0}^{p} F_i = \left\{ e_1 + \ldots + e_p,\ (e_1, \ldots, e_p) \in F_1 \times \ldots \times F_p \right\}$$

Cet ensemble somme est un sous-espace vectoriel de E, contient tous les ensembles F_i. Tout sous-espace vectoriel G contenant tous les ensemble F_i contient l'ensemble somme

Démonstration par vérification d'axiome, puis posant $x \in F_i = 0_E + \ldots + 0_E + x + 0_E + \ldots + 0_E$... la somme est inclus dans G, car G stable par $+$

Somme directe : on dit que les espaces $F_1, \ldots, F_p$ sont en *somme directe* si $\boldsymbol{\varphi}$: $\begin{cases} \boldsymbol{F_1 \times \ldots \times F_p} & \to & \boldsymbol{E} \\ \boldsymbol{(e_1, \ldots, e_p)} & \mapsto & \boldsymbol{e_1 + \ldots + e_p} \end{cases}$ est **injective**. Autrement dit si

$$\boldsymbol{\forall x \in \sum_{i=1}^{p} F_i,\ \exists! (e_i, \ldots, e_p) \in F_1 \times \ldots \times F_p, x = \sum_{i=0}^{p} F_i}$$

On note alors $F_1 \oplus \ldots \oplus F_p$ ou $\bigoplus_{i=0}^{p} F_i$

$F_1, \ldots, F_p$ sont en somme directe $\Leftrightarrow \forall (e_1, \ldots, e_p) \in F_1 \times \ldots \times F_p, \sum_{i=1}^{p} e_i = 0 \Rightarrow (e_1, \ldots, e_p) = (0, \ldots, 0)$. $\Rightarrow$ évident, pour le $\Leftarrow$, montrer l'injectivité de φ...

Associativité : soit F_1, F_2, F_3 trois sous espaces vectoriels de E, on a $(F_1 + F_2) + F_3 = F_1 + (F_2 + F_3) = F_1 + F_2 + F_3$ et l'équivalence

$$\boldsymbol{F_1 \oplus F_2 \oplus F_3 \text{ existe}} \Leftrightarrow \begin{cases} \boldsymbol{F_1 \oplus F_2 \text{ existe}} \\ \boldsymbol{(F_1 \oplus F_2) \oplus F_3 \text{ existe}} \end{cases}$$

On a alors $F_1 \oplus F_2 \oplus F_3 = (F_1 \oplus F_2) \oplus F_3$. Démonstration de l'associativité immédiate. Pour $\Leftrightarrow$, utiliser la caractérisation en somme nulle.

Intersection : on a $\boldsymbol{F \oplus G \text{ existe}} \Leftrightarrow \boldsymbol{F \cap G \subset \{0_E\}} \Leftrightarrow F \cap G = \{0_E\}$

$i \Rightarrow ii$ et $ii \Rightarrow iii$ facile, utiliser la caractérisation $= 0$ pour $iii \Rightarrow i$

Supplémentaire : on dit que F et G sont supplémentaires dans E si $E = F \oplus G$

Combinaison linéaire : soit $A \subset E$ un sous-espace vectoriel, on définit $\text{Vect}(A) = \text{Vect}\big((a)_{a \in A}$ on a $\boldsymbol{\text{Vect}\big((a_i)_{i \in A}\big) \subset A}$ est un **sous-espace vectoriel** de E et A.

$\subset$ immédiate par stabilité de A par $+$, puis vérification d'axiomes

Concaténation : soit $\mathcal{F} = (e_1, \ldots, e_m)$ et $\mathcal{G} = (u_1, \ldots, u_p)$ deux familles de vecteurs, on note $\mathcal{F} \vee \mathcal{G} = (e_1, \ldots, e_p, u_1, \ldots, u_p)$ la concaténation de deux familles. On a :

$$\text{Vect}(\mathcal{F} \vee \mathcal{G}) = \text{Vect}(\mathcal{F}) + \text{Vect}(\mathcal{G})$$

13.3 Applications linéaires

Définition : soit E et F deux $\mathbb{K}$-espaces vectoriels, et $u : E \to F$. u est une application si $\forall (x, y, \lambda) \in E^2 \times \mathbb{K}$:

$$\boldsymbol{u(x+y) = u(x) + u(y)} \qquad \text{et} \qquad \boldsymbol{u(\lambda \cdot x) = \lambda \cdot u(x)}$$

Une application linéaire est appelée *isomorphisme* si elle est bijective, *endomorphisme* si elle est définie de E vers E, et *automorphisme* si les deux.
On note $\mathscr{L}(E, F)$ l'ensemble des applications linéaires de E vers F, $\mathscr{L}(E)$ celui des endomorphismes et $\text{Gl}(E)$ celui des automorphismes.

$0_{\mathscr{L}(E,F)} \in \mathscr{L}(E, F)$, $\text{id}_E \in \text{Gl}(E)$ et $\lambda \cdot \text{id}_E \in \mathscr{L}(E)$ et $\text{Gl}(E)$ si $\lambda \neq 0$

Sous-espaces vectoriels : soit E et E' deux $\mathbb{K}$-espaces vectoriels, F et F' deux sous-espaces vectoriels respectifs et $u : E \to E'$ une fonction linéaire. On a :

- $u(0_E) = 0_{E'}$
- $u(F)$ est un s-e v de E'
- $u^{-1}(F')$ est un s-e v de E
- on pose $\text{Im}(u) = u(E)$
- on pose $\text{Ker}(u) = u^{-1}(\{0_{E'}\})$
- u injective $\Leftrightarrow \text{Ker}(u) = \{0_E\}$

Fonction et combinaison linéaire : soit $u \in \mathscr{L}(E, E')$ et $(x_i)_{i \in I} \in E^I$, on a pour $(\lambda_i)_{i \in I} \in \mathbb{K}^{(I)}$, $u\left(\sum_{i \in I} \lambda_i x_i\right)$ existe et vaut $\sum_{i \in I} \lambda_i u(x_i)$. On en déduit :

$$\boldsymbol{\text{Vect}\Big[u\big((x_i)_{i \in I}\big)\Big] = u\Big[\text{Vect}\big((x_i)_{i \in I}\big)\Big]}$$

Opérations usuelles : soit $(u, v) \in \mathscr{L}(E, E')^2$, on a $\lambda \cdot u + \mu \cdot v \in \mathscr{L}(E, E')$.
Soit $w \in \mathscr{L}(E', E'')$, on a $u \circ w \in \mathscr{L}(E, E'')^2$
Soit $(a_1, a_2) \in \mathscr{L}(E, E')^2, (b_1, b_2) \in \mathscr{L}(E', E'')^2$, on a

$$(\mu_1 \cdot b_1 + \mu_2 \cdot b_2) \circ (\lambda_1 \cdot a_1 + \lambda_2 \cdot a_2) =$$
$$(\mu_1\lambda_1) \cdot (b_1 \circ a_1) + (\mu_1\lambda_2) \cdot (b_1 \circ a_2) + (\mu_2\lambda_1) \cdot (b_2 \circ a_1) + (\mu_2\lambda_2) \cdot (b_2 \circ a_2)$$

Structures algébriques : soit E et E' deux $\mathbb{K}$-espaces vectoriels.

- $(\mathscr{L}(E, E'), +, \cdot)$ est un $\mathbb{K}$-espace vectoriel (sev de $(E')^E$)
- $(\mathscr{L}(E), +, \circ)$ est l'anneau des endomorphismes de E
- $(\text{Gl}(E), \circ)$ est un groupe (sous groupe de $(\mathscr{S}_E, \circ)$)

Projecteurs et symétries : soit F et G tel que $E = F \oplus G$, on a alors $\forall x \in E, \exists!(x_F, x_G) \in F \times G, x = x_F + x_G$. on définit :

— le projecteur sur F, parallèlement à G : $p_{F,G} : \begin{pmatrix} E & \to & E \\ x & \mapsto & x_F \end{pmatrix}$

— la symétrie sur F, parallèlement à G : $s_{F,G} : \begin{pmatrix} E & \to & E \\ x & \mapsto & x_F - x_G \end{pmatrix}$

Propriétés : les symétries et projecteurs sont des fonction linéaires vérifiant :

- $p_{F,G} + p_{G,F} = \mathrm{id}_E$
- $p_{F,G}^2 = p_{F,G}$
- $\mathrm{Im}(p_{F,G}) = \mathrm{Ker}(\mathrm{id}_E - p_{F,G}) = F$
- $\mathrm{Ker}(s_{F,G} + \mathrm{id}_E) = G$
- $s_{F,G} = p_{F,G} - p_{G,F}$
- $s_{F,G}^2 = \mathrm{id}_E$
- $\mathrm{Ker}(s_{F,G} - \mathrm{id}_E) = F$

Démonstration en employant l'unicité de la décomposition dans $F \oplus G$.

Définition algébrique : soit $p \in \mathscr{L}(E)$ tel que $\boldsymbol{p^2 = p}$, alors, :

$$\mathbf{Ker(id_E - p) \oplus Ker(p) = E} \quad \text{et} \quad \boldsymbol{p = p_{\mathbf{Ker(id_E - p), Ker(p)}}}$$

$\mathrm{id}_E - p$ est aussi un projecteur associé à p, $\mathrm{Im}(p) = \mathrm{Ker}(\mathrm{id}_E - p)$ et $p \circ (\mathrm{id}_E - p) = (\mathrm{id}_E - p) \circ p = 0_{\mathscr{L}(E)}$.
Soit $s \in \mathscr{L}(E)$ tel que $\boldsymbol{s^2 = \mathrm{id}_E}$, alors :

$$\mathbf{Ker(s - id_E) \oplus Ker(s + id_E) = E} \quad \text{et} \quad \boldsymbol{s = s_{\mathbf{Ker(s - id_E), Ker(s + id_E)}}}$$

Montrer $\oplus$ par intersection incluse dans $\{0\}$, puis l'inclusion en décomposant dans F et G.

Hyperplan et forme linéaire : une forme linéaire est un élément de $\mathscr{L}(E, \mathbb{K})$. Soit $H \subset E$, on dit que H est un *hyperplan* de E lorsqu'il existe $\varphi \in \mathscr{L}(E, \mathbb{K})$ tel que $\varphi \neq 0_{\mathscr{L}(E,\mathbb{K})}$ et $H = \mathrm{Ker}(\varphi)$

Caractérisation d'un hyperplan : soit H un hyperplan et $e \in E \setminus H$, on a

$$\boldsymbol{H \oplus \mathbf{Vect}(e) = E}$$

Réciproquement, s'il existe $e \in E$ tel que $H \oplus \mathrm{Vect}(e) = E$, H est un hyperplan.

.

Démonstration : employer $H \cap \mathrm{Vect}(e) \subset \{0\}$, puis $x \in E = y + \lambda \cdot e$ avec $\lambda = \frac{\varphi(x)}{\varphi(e)}$...
Pour la réciproque, construire $\varphi : y + \lambda \cdot e \mapsto \lambda$

Construction sous contrainte : soit E un $\mathbb{K}$-espace vectoriel et $F_1, \dots, F_p$ des sous-espaces vectoriels tel que $E = \bigoplus_{i=1}^{p} F_i$, soit $u_1, \dots, u_p \in \mathscr{L}(F_1, E') \times \dots \times \mathscr{L}(F_p, E')$, il existe un *unique* $u \in \mathscr{L}(E, E')$ tel que $\forall i \in [\![1, p]\!], \boldsymbol{\forall e \in F_i, u(e) = u_i(e)}$

Unicité en décomposant $x \in e$ dans $\bigoplus_{i=1}^{p} F_i$, puis exploitant la propriété caractéristique. Existence en posant p_i le projecteur de F_i parallèlement à $\bigoplus_{\substack{j=1 \\ j\neq i}}^{p} F_j$, puis posant $u = \begin{pmatrix} E & \to & E' \\ x & \mapsto & \sum_{i=1}^{p} u_i(p_i(x)) \end{pmatrix}$, vérifier bonne def et linéarité, puis la propriété caractéristique

14 Limites et continuité

14.1 Continuité et théorème globaux

Continuité : soit $f : A \to \mathbb{R}$, et $a \in I$, f est continue en a lorsque :

$$\boldsymbol{\forall \epsilon > 0, \exists \eta \in \mathbb{R}, \forall t \in I, |t - a| \leqslant \eta \Rightarrow |f(t) - f(a)| \leqslant \epsilon}$$

f est continue sur A si f est continue en tout point de A.
On note $\mathscr{C}(A, \mathbb{R})$ l'ensemble des fonctions continues de A dans $\mathbb{R}$

Composition : soit $(x_n) \in I^{\mathbb{N}}$ une suite et $F : I \to \mathbb{R}$, on a :

$$\begin{cases} (x_n) \longrightarrow \ell \\ f \text{ continue en } \ell \end{cases} \Rightarrow \big(f(x_n)\big) \longrightarrow f(\ell)$$

Démonstration par ε, il existe $\eta > 0$ tel que... donc $\exists n_0, |x_n - \ell| < \eta$

Théorème des valeurs intermédiaires : soit $f : I \to \mathbb{R}$ continue et $(a, b) \in I^2$ tel que $f(a) < f(b)$, alors

$$\boldsymbol{\forall c \in]f(a), f(b)[, \exists \alpha \in]\min(a,b), \max(a,b)[, f(\alpha) = c}$$

Cas $a < b$, poser $E = \{x \in I, f(x) \leqslant c\}$, et considérant sa borne sup α. $f(\alpha) \leqslant f(c)$ par caractérisation séquentielle, $\alpha \neq b$, et en considérant la suite $t_n = \alpha + \frac{1}{2^n}(b - \alpha)$, on a $(t_n) \to \alpha$, et $f(t_n) > c$ donc $f(\alpha) \geqslant c$. Procéder de même pour $b < a$

TVI version ensembliste : soit $f : I \to \mathbb{R}$ continue, alors $f(I)$ est un intervalle

Démo immédiate, soit $(a, b) \in f(I), a < b, \forall c \in]a, b[, c \in f(I)$ d'après le TVI.

Fonction continue non-nulle : soit $f \in \mathscr{C}(I,\ \mathbb{R})$ telle que $\forall t \in I, f(t) \neq 0$, on a $f(I) \subset \mathbb{R}_+^*$ ou $f(I) \subset \mathbb{R}_-^*$.

Théorème de la borne atteinte : soit $f \in \mathscr{C}\big([a,b],\mathbb{R}\big)$, on a alors
- f admet un maximum et un minimum
- $f\big([a,b]\big)$ est un segment

Mq f est minorée par l'absurde (sinon contient (x_n) t.q. $\big(f(x_n)\big) < -n$, d'après Bolzano-Weierstrass, $(x_{\varphi(p)}) \to \ell \in [a,b]$, donc $f(\ell) = -\infty$), $f([a,b])$ admet donc une borne inf, par caractérisation séquentielle, $\exists (t_n)$ t.q. $f(t_n) \to \inf([a,b])$, or t_n bornée donc $(t_{\phi(p)}) \to L$, d'où $\inf([a,b]) = f(L)$.
On démontre de même le maximum M et on conclut $f([a,b]) = [m,M]$

Injectivité, continuité et monotonie : soit $f \in \mathscr{C}(I,\ \mathbb{R})$ tel que f soit injective, alors, f est *strictement monotone.*

Prendre $(a,b) \in I$, $a<b$, cas $f(a)<f(b)$, prendre $(c,d) \in I$, $c<d$ puis poser la fonction $\phi : \begin{pmatrix} [0,1] & \to & \mathbb{R} \\ t & \mapsto & f\big(a+t(c-a)\big) - f\big(b+t(d-b)\big) \end{pmatrix}$. ϕ est continue et bien définie ($a+t(c-a) \in I$), de plus $a+t(c-a) < b+t(d-b)$, donc ϕ ne s'annule jamais. Donc ϕ et de signe constant strict, or $\phi(0)<0$ donc $f(c)<f(d)$.

Bijectivité et continuité : soit $f \in \mathscr{C}(I,J)$, $f^{-1} \in \mathscr{C}(J,I)$

Si f croissante, poser $\varepsilon > 0$, puis $\eta = \min(z - f^{-1}\big(z-\varepsilon\big),\ f^{-1}(z+\varepsilon) - z\big)$ puis $t \in [\eta - z, \eta + z]$...

Caractérisation séquentielle : soit $f : \mathscr{C}(A,\ \mathbb{K})$ et $a \in A$,

$$\boldsymbol{f \text{ est continue en } a \ \Rightarrow\ \forall (t_n) \in A^{\mathbb{N}},\ \big[(t_n) \longrightarrow a \Rightarrow f(t_n) \longrightarrow f(a)\big]}$$

Utiliser la contraposée ($\exists (t_n) \in A^{\mathbb{N}}, (t_n) \to a, f(t_n) \not\to f(a) \Rightarrow f$ non continue).
On en déduit les théorèmes d'opération (f et g sont continues) :

- $\mathscr{C}(A,\ B)$ est un sev de B^A
- $\forall x \in A, f(x) \neq 0 \Rightarrow \dfrac{1}{f} \in \mathscr{C}(A,\ \mathbb{R})$
- $\big(\mathrm{Re}(f),\ \mathrm{Im}(f),\ |f|\ \big) \in \mathscr{C}(A,\ \mathbb{R})^3$
- $f \times G \in \mathscr{C}(A,\ B)$
- $f \circ g \in \mathscr{C}(A,\ C)$

14.2 Étude locale

Définition : soit $f \in \mathscr{C}(I,\mathbb{C})$, $g \in \mathscr{C}(I,\mathbb{R})$, $\ell \in \mathbb{K}$

Les limites en a^+, a^-, $a^{\neq}$ ne sont définies que a n'est pas la borne sup / inf de I

En un point	$f(t) \xrightarrow[t\to a]{} \ell$	$\forall \varepsilon > 0 \quad \exists \eta > 0, \quad \forall t \in I,$	$\lvert t-a\rvert < \eta \Rightarrow \lvert f(t)-\ell\rvert < \varepsilon$
	$g(t) \xrightarrow[t\to a]{} -\infty$	$\forall A \in \mathbb{R}, \exists \eta > 0, \quad \forall t \in I,$	$\lvert t-a\rvert < \eta \Rightarrow f(t) \geqslant A$
En l'infini	$f(t) \xrightarrow[t\to -\infty]{} \ell$	$\forall \varepsilon > 0, \quad \exists M \in \mathbb{R}, \forall t \in I,$	$t \geqslant M \Rightarrow \lvert f(t)-\ell\rvert < \varepsilon$
	$f(t) \xrightarrow[t\to -\infty]{} -\infty$	$\forall A \in \mathbb{R}, \exists M \in \mathbb{R}, \forall t \in I,$	$t \geqslant M \Rightarrow f(t) \geqslant A$
Latérale	$f(t) \xrightarrow[t\to a^-]{} \ell$	$\forall \varepsilon > 0, \quad \exists \eta > 0, \quad \forall t \in I \cap]-\infty, a[,$	$\lvert t-a\rvert \leqslant \eta \Rightarrow \lvert f(t)-\ell\rvert < \varepsilon$
	$f(t) \xrightarrow[t\to a^+]{} \ell$	$\forall \varepsilon > 0, \quad \exists \eta > 0, \quad \forall t \in I \cap]a, +\infty[,$	$\lvert t-a\rvert \leqslant \eta \Rightarrow \lvert f(t)-\ell\rvert < \varepsilon$
Épointée	$f(t) \xrightarrow[t\to a^{\neq}]{} \ell$	$\forall \varepsilon > 0, \quad \exists \eta > 0, \quad \forall t \in I \setminus \{a\},$	$\lvert t-a\rvert \leqslant \eta \Rightarrow \lvert f(t)-\ell\rvert < \varepsilon$

TABLE 5 – Définitions des limites d'une fonction

Limite latérales et continuité : si $f(t) \xrightarrow[t\to a^-]{} f(a)$ et $f(t) \xrightarrow[t\to a^+]{} f(a)$, alors f est continue en a

Démonstration par ε

Unicité de la limite : soit $(a, \ell, \ell') \in \overline{\mathbb{R}}^3$, si $f(t) \xrightarrow[t\to a]{} \ell$ et $f(t) \xrightarrow[t\to a]{} \ell'$, alors $\ell = \ell'$

Montrer que $\forall \varepsilon > 0, |\ell - \ell'| < \varepsilon$

Théorèmes d'opérations : on retrouve ceux des limites de suite (TABLE 3), on les démontre par caractérisation séquentielle

Prolongement par continuité : soit f défini sur I, et a une des bornes de I telle que $a \notin I$, si f admet une limite $\ell \in \mathbb{K}$ en a, on peut définir $\phi : \begin{cases} I \cup \{a\} & \to & \mathbb{K} \\ t & \mapsto & \left| \begin{array}{l} t \text{ si } t \neq a \\ \ell \text{ si } t = a \end{array} \right. \end{cases}$.

ϕ est alors continue en a

THÉORÈME DE LA LIMITE MONOTONE : soit $(a, b) \in \overline{\mathbb{R}}^2$ et $f :]a, b[\to \mathbb{R}$ une fonction monotone. Il existe $(\ell, \ell') \in \overline{\mathbb{R}}^2$ tel que $f(t) \xrightarrow[t\to a^+]{} \ell$ et $f(t) \xrightarrow[t\to b^-]{} \ell'$

Démonstration dans un cas particulier (ex croissante et majorée en prenant sup $f(]a, b[)$.

Image d'une fonction monotone : soit $f : I \to \mathbb{R}$ monotone, $f(I)$ est alors un intervalle dont les bornes sont les limites de f aux bornes de I. Remarque : si f est croissante sur $\mathbb{R}$ alors pour tout $a \in \mathbb{R}$, la limite de f en a^+ ou a^- et est un réel.

Démonstration au cas par cas

Encadrement local : soit $f : I \to \mathbb{R}$, $(\ell, a, b) \in \overline{\mathbb{R}}^3$. Soit $\gamma \in \overline{\mathbb{R}}$ on a :

— $f(t) \xrightarrow[t\to\gamma]{} \ell$ et $a < \ell < b \Rightarrow a < f(t) < b$ au voisinage de γ

— $g(t) \leqslant f(t) \leqslant h(t)$ au voisinage de γ et $\lim\limits_{t\to\gamma} g(t) = \lim\limits_{t\to\gamma} h(t) = \ell \Rightarrow f(t) \xrightarrow[t\to\gamma]{} \ell$
— $f(t) = g(t)$ au voisinage de γ et $\lim\limits_{t\to\gamma} g(t) = \ell \Rightarrow f(t) \xrightarrow[t\to\gamma]{} \ell$
— $f(t) \leqslant g(t)$ au voisinage de γ, $\lim\limits_{t\to\gamma} f(t) = \ell_1$ $\lim\limits_{t\to\gamma} g(t) = \ell_2 \Rightarrow \ell_1 \leqslant \ell_2$

15 Calcul asymptotique

15.1 Relations o, O et $\sim$

Définition soit $\alpha \in \overline{\mathbb{R}}$ et f et g deux fonctions définies au voisinage de α :
— f **négligeable** devant g, noté $\boldsymbol{f(t) = \underset{t\to\alpha}{o}(g(t))}$ lorsque $\boldsymbol{\dfrac{f(t)}{g(t)} \xrightarrow[g\to\alpha]{} 0}$
— f **dominée** par g, noté $\boldsymbol{f(t) = \underset{t\to\alpha}{O}(g(t))}$ lorsque $\boldsymbol{\left|\dfrac{f(t)}{g(t)}\right|}$ est **borné**
— f **équivalente** à g, noté $\boldsymbol{f(t) \underset{t\to\alpha}{\sim} g(t)}$ lorsque $\boldsymbol{\dfrac{f(t)}{g(t)} \xrightarrow[g\to\alpha]{} 1}$

Exemple : $2x^4 + 6x^2 + 3 \underset{x\to\infty}{\sim} 2x^4$, $\dfrac{1}{2^n} = \underset{n\to\infty}{o}\dfrac{1}{n}$

Propriétés de l'équivalence : $\sim$ est une relation d'équivalence vérifiant :

- $f(t) \underset{t\to\alpha}{\sim} g(t) \quad \Leftrightarrow f(t) - g(t) = \underset{t\to\alpha}{o}(g(t))$
- $f(t) \xrightarrow[t\to\alpha]{} \ell \quad \Leftrightarrow f(t) - \ell = \underset{t\to\alpha}{o}(1)$
  $\Leftrightarrow f(t) \underset{t\to\alpha}{\sim} \ell$ (si $\ell \neq 0$)

Démonstration par opération sur les limites

Fonctions équivalentes : soit f et g deux fonctions équivalentes en α, alors f et g sont de *même signe strict* au voisinage de α. Si $f(t) \xrightarrow[t\to\alpha]{} \ell$, alors $g(t) \xrightarrow[t\to\alpha]{} \ell$.
Démonstration par opération sur les limites

Changement de variable : soit $\varphi(t) \xrightarrow[t\to\beta]{} \alpha$ et f et g deux fonctions. On a :
— $f(x) = \underset{x\to\alpha}{o}(g(x)) \Rightarrow f(\varphi(t)) = \underset{t\to\beta}{o}(g(\varphi(t)))$
— $f(x) = \underset{x\to\alpha}{O}(g(x)) \Rightarrow f(\varphi(t)) = \underset{t\to\beta}{O}(g(\varphi(t)))$
— $f(x) \underset{x\to\alpha}{\sim} g(x) \Rightarrow f(\varphi(t)) \underset{t\to\beta}{\sim} g(\varphi(t))$

Opérations licites : Ces relations sont transitives, compatibles avec une combinaison linéaire pour o et O, et avec le produit (cf. poly)

15.2 Calcul asymptotique

Règle d'or : présenter si possible les termes du plus grand au plus petit

Formule de Stirling : on a l'équivalence : $\boldsymbol{n! \underset{n\to+\infty}{\sim} (ne^{-1})^n\sqrt{2\pi n}}$.

On en déduit que $\ln(n!) = n\ln(n) - n + \frac{1}{2}\ln(n) + \ln\left(\sqrt{2\pi}\right) + o(1)$, et donc un équivalent simple de $ln(n!)$, $n\ln(n)$. On peut aussi déterminer l'équivalent simple de l'erreur : $\ln(n!) - n\ln(n) = -n + o(n)$

16 Dimension finie

16.1 Autour des familles de vecteurs

Famille libre : Une famille $(e_i)_{i\in I} \in E^I$ est libre si toute combinaison linéaire de cette famille nulle est triviale, donc si :

$$\forall (\boldsymbol{\lambda_i})_{i\in I} \in \mathbb{K}^{(I)},\ \sum_{i\in I} \boldsymbol{\lambda_i \cdot e_i = 0_E} \ \Rightarrow\ \forall \boldsymbol{j \in I, \lambda j = 0_{\mathbb{K}}}$$

Famille liée : une famille est liée si elle est non-libre, donc si :

$$\exists (\boldsymbol{\lambda_i})_{i\in I} \in \mathbb{K}^{(I)},\ \sum_{i\in I} \boldsymbol{\lambda_i \cdot e_i = 0_E} \text{ et } \boldsymbol{\exists j \in I, \lambda j \neq 0_{\mathbb{K}}}$$

Héritage : une sous-famille d'une famille libre est libre, une sur-famille d'une famille liée est liée. Plus généralement, soit $a \in E^I$ et $e \in E$. On pose $a' = a \vee (e)$. On a les équivalences :

$$\boldsymbol{a' \text{ est libre}} \ \Leftrightarrow\ \begin{cases} \boldsymbol{a \text{ est libre}} \\ \boldsymbol{e \notin \mathrm{Vect}(a)} \end{cases} \qquad \boldsymbol{a' \text{ est lié}} \ \Leftrightarrow\ \boldsymbol{a \text{ est liée}} \text{ ou } \boldsymbol{e \in \mathrm{Vect}(a)}$$

Pour la 2 : $\Leftarrow$ triviale, $\Rightarrow$ considérer le cas $\lambda_e \neq 0$, alors a non liée et $e = \ldots$

Liberté et somme directe : sois $(a^{(1)}, \ldots, a^{(n)}) \in E^n$. On suppose que $a^{(1)} \vee \ldots \vee a^{(n)}$ est libre. Alors $\mathrm{Vect}\left(a^{(1)}\right) \oplus \ldots \oplus \mathrm{Vect}\left(a^{(n)}\right)$ *existe.*
Réciproquement, si on considère $(F_1, \ldots, F_n)$ des sous-espaces vectoriels de E en somme directe, et $(a^{(1)}, \ldots, a^{(n)})$ des familles libre de $F_1 \times \ldots \times F_n$, $a^{(1)} \vee \ldots \vee a^{(n)}$ est libre.

Liberté et sous-familles : soit $(e_i)_{i\in I} \in E^I$ on a : (démo avec les familles presque nulle)

$$\boldsymbol{(e_i)_{i\in I} \text{ est libre } \Leftrightarrow \text{Toute sous-famille finie de } (e_i)_{i\in I} \text{ est libre.}}$$

Colinéarité : Soit $(x, y) \in E^2$. x et y *sont colinéaires* lorsque $x \in \text{Vect}(y)$ ou $y \in \text{Vect}(x)$.
x *est colinéaire à* y lorsque $x \in \text{Vect}(y)$

Lemme Fondamental de la Dimension Finie : soit $n \in \mathbb{N}$, $(x_1, \dots, x_n) \in E^n$ et $(y_1, \dots, y_{n+1}) \in \text{Vect}\big((x_1, \dots, x_n)\big)^{n+1}$. On a $(y_1, \dots, y_{n+1})$ est **liée**

Démo par récurrence, initialisé à $n = 0$, tout $y_1 \in \text{Vect}(\{\}) = \{0_E\}$ est lié.
Hérédité : écrire $y_i = \underbrace{z_i}_{\in \text{Vect}(x_1, \dots x_{n-1})} + \lambda_n x_n$, puis si $\lambda_1 \neq 0$, $y_i - \frac{\lambda_i}{\lambda_1} y_1 \in \text{Vect}(x_1, \dots x_{n-1})$, donc $y_i - \frac{\lambda_i}{\lambda_1} y_1$ lié...

Famille génératrice et base : soit $(e_i)_{i \in I} \in E^I$, on dit que (e_i) est *génératrice* lorsque $\boldsymbol{\text{Vect}\big((e_i)\big) = E}$.
(e_i) est une *base* si elle est *libre* et *génératrice*

Famille et coordonnées : pour $(a_i) \in E^I$, on pose $\boldsymbol{\varphi_{(a_i)}} : \begin{cases} \mathbb{K}^{(I)} & \to & \boldsymbol{E} \\ \boldsymbol{(\lambda_i)} & \mapsto & \boldsymbol{\sum_{i \in I} \lambda_i a_i} \end{cases}$. On a les équivalences :

$$\begin{aligned} \boldsymbol{\varphi} \textbf{ injective} &\Leftrightarrow \boldsymbol{(a_i)} \textbf{ libre} \\ \boldsymbol{\varphi} \textbf{ surjective} &\Leftrightarrow \boldsymbol{(a_i)} \textbf{ génératrice} \\ \boldsymbol{\varphi} \textbf{ bijective} &\Leftrightarrow \boldsymbol{(a_i)} \textbf{ est une base} \end{aligned}$$

Base et somme directe : soit $(F_1, \dots, F_n)$ des SEV de E vérifiant $F_1 \oplus \dots \oplus F_n = E$, soit $(b_1, \dots, b_n)$ des bases de $F_1, \dots, F_n$, alors $b_1 \vee \dots \vee b_n$ est une base de E

16.2 Dimension finie

Définition : un $\mathbb{K}$-espace vectoriel E est de dimension finie lorsqu'il existe une famille génératrice finie de E.

Dimension et bases : si E est un $\mathbb{K}$-espace vectoriel fini, et (b_1, b_2) deux bases de E, alors b_1 et b_2 contiennent un nombre fini de vecteurs et $\boldsymbol{\#b_1 = \#b_2}$.
De plus, il existe une base b de E, construite à partir d'une famille libre maximale

Démo en utilisant le lemme de la dimension finie et la définition. Pour l'existence, on pose $L = \{\#a,\ a \text{ famille libre de } E\}$, L majoré, inclus dans $\mathbb{N}$ d'après le lemme, et contient $0 = \#()$. Donc il existe b, $\#b = \max L$. Pour tout $x \in E$, $b \vee (x)$ non libre donc...

Dimension : soit E un $\mathbb{K}$-ev, il existe b une base de E. On pose $\boldsymbol{\dim E = \#b}$

Dimension finie et sous espaces : soit F un sev de E, si E est de dimension finie, on a : $\begin{cases} \boldsymbol{F} \textbf{ fini et } \boldsymbol{\dim F \leqslant \dim E} \\ \boldsymbol{\dim F = \dim E \Rightarrow F = E} \end{cases}$
Démonstration : poser $L = \{\#a, a \text{ famille libre de } F\}$. L majoré par $\dim E$, inclus dans $\mathbb{N}$ et non vide, il existe b libre, $\#b = \max L$, une base. Si $\#b = \dim E$, alors on montre que $\text{Vect}(b) \supset E$

Dimension et somme : soit F et G deux sev de E. On a si F et G en somme directe, $\dim(F \oplus G) = \dim F + \dim G$, et dans le cas général, $\boldsymbol{\dim(F+G) = \dim F + \dim G - \dim(F \cap G)}$
Le cas $\oplus$ découle de la concaténation des bases. Pour le général, il existe H sev $(F \cap G) \oplus H = G$, on a alors $F + G = F \oplus H$ d'où l'égalité sur les cardinaux...

Dimension et supplémentaires : soit F et G deux sev de E, on a :

$$\boldsymbol{F \oplus G = E} \Leftrightarrow \begin{cases} \boldsymbol{F \cap G = \{0_E\}} \\ \boldsymbol{\dim F + \dim G = \dim E} \end{cases} \Leftrightarrow \begin{cases} \boldsymbol{F + G = E} \\ \boldsymbol{\dim F + \dim G = \dim E} \end{cases}$$

Démo : si $\dim(F \cap G) = 0_{\mathbb{N}}$, alors $F + G = E$, si $F + G = E$, alors $\dim(F \cap G) = 0_{\mathbb{N}}$

Dimensions : une droite vectorielle est un sev de dimension 1, un plan de dimension 2, et un hyperplan de dimension $\dim E - 1$

Théorème de la base incomplète : soit $a \in E^I$ un famille libre, et g une famille génératrice de E. *il existe* g' une sous-famille de g telle que $\boldsymbol{a \vee g'}$ **soit une base de** $\boldsymbol{E}$

Démo en posant $L = \{\#\widetilde{g}, \widetilde{g} \subset g \text{ et } \widetilde{g} \text{ libre}\}$, L admet un maximum...

Existence d'un supplémentaire : soit F un sev de E, il *existe* un sev G, $\boldsymbol{F \oplus G = E}$. Poser b une base de F, il existe e une sous-famille de E, $b \vee e$ est une base

Caractérisation des bases : soit E un $\mathbb{K}$-ev de dimension finie et a une famille finie de vecteurs, on a :

$$\boldsymbol{a} \textbf{ est une base } \Leftrightarrow \boldsymbol{\#a = \dim E} \text{ et } \boldsymbol{a} \textbf{ libre } \Leftrightarrow \boldsymbol{\#a = \dim E} \text{ et } \boldsymbol{a} \textbf{ génératrice}$$

Démo : si a libre il existe e, $a \vee e$ est une base... Si a génératrice, () libre donc il existe a' dans a, $a' \vee a$ est une base. Conclure avec les cardinaux.

16.3 Applications linéaires et dimension finie

Construction sous contrainte : soit E et E' deux $\mathbb{K}$-ev, soit $b = (e_i)$ une base de E et $c = (e'_i) \in E'^I$.

$$\boldsymbol{\exists! u \in \mathscr{L}(E, E'),\ \forall i \in I,\ u(e_i) = e'_i}$$

Démo : poser $\varphi_b = \begin{pmatrix} \mathbb{K}^{(I)} & \to & E \\ (\lambda_i) & \mapsto & \sum_{i\in I} \lambda_i e_i \end{pmatrix}$ et φ_c, puis montrer que $u = \varphi_c \circ \varphi_b^{-1}$.

u bijective $\Leftrightarrow$ c est une base injective $\Leftrightarrow$ libre surjective $\Leftrightarrow$ génératrice

Bijectivité et dimension finie : soit E et E' deux $\mathbb{K}$-ev de dimension finie, soit $u \in \mathscr{L}(E, E')$. On a :

$$u \text{ bijective } \Leftrightarrow u \text{ injective } \Leftrightarrow u \text{ surjective}$$

Il existe $b = (e_1, \ldots, e_{\dim E})$ une base de E, considérer $(u(e_1), \ldots, u(e_{\dim E})$

Isomorphie : soit E un $\mathbb{K}$-ev de dimension finie, on a :

$$\boldsymbol{\left[E' \text{ fini et } \dim E' = \dim E\right] \Leftrightarrow E \text{ isomorphique à } E'}$$

$\Rightarrow$, poser deux bases b et c, $\Leftarrow$ $(f(b_1), \ldots, f(b_n))$ est une base de E'

Produit cartésien et somme : soit $E_1, \ldots, E_p$ des $\mathbb{K}$-ev de dimension finie, le produit $E_1 \times \ldots \times E_p$ est de dimension finie et $\boldsymbol{\dim(E_1 \times \ldots \times E_p) = \sum_{i=1}^{p} \dim E_i}$.
Soit $F_1, \ldots, F_p$ des sevs, $\sum F_i$ fini et $\boldsymbol{dim\left(\sum F_i\right) \leqslant \sum \dim F_i}$. Finalement, on a

$$dim\left(\sum F_i\right) = \sum \dim F_i \Leftrightarrow F_1 \oplus \ldots \oplus F_p \text{ existe}$$

Démo, par récurrence, base $= \left((b_1^{(1)}, 0_{E_2}, \ldots, 0_{E_p}), \ldots (0_{E_1}, \ldots, 0_{E_{p-1}}, b_p^{(p)})\right)$. Pour (2), concaténer les bases... La (3) $\Rightarrow$ vrai car $\varphi : \begin{cases} \prod F_i & \to & \sum F_1 \\ e_1, \ldots, e_i & \mapsto & e_1 + \ldots + e_i \end{cases}$ est injective car surjective entre deux sev de même dimension

Rang : soit $u \in \mathscr{L}(E, E')$, on dit que $\boldsymbol{u}$ est de **rang fini** lorsque $\boldsymbol{\mathrm{Im}(u)}$ est de **dimension finie**. On pose alors $\boldsymbol{\mathrm{rg}(u) = \dim(\mathrm{Im}(u))}$
Soit a une famille de e, on définit $\boldsymbol{\mathrm{rg}(a) = \dim(\mathrm{Vect}(a))}$

Composition : soit $F \xrightarrow{\psi} E \xrightarrow{u} E' \xrightarrow{\varphi} F'$ avec ψ et ϕ bijective. On a $\boldsymbol{\mathrm{rg}(u \circ \psi) = \mathrm{rg}(\varphi \circ u) = \mathrm{rg}(u)}$.
En effet, $u(\psi(F)) = u(E)$ et $\widetilde{\varphi} : \mathrm{Im}(u) \to \varphi(\mathrm{Im}(u))$ linéaire et bijective...

Famille finie et rang : on a $\mathrm{rg}(e_1, \ldots, e_p) \leqslant p$ et

$$\mathrm{rg}(e_1, \ldots, e_p) = p \Leftrightarrow (e_1, \ldots, e_p) \text{ libre}$$

Rang et supplémentaire : soit $u \in \mathscr{L}(E, E')$, s'il existe F un sev tel que $\mathrm{Ker}(u) \oplus F = E$, alors $\widetilde{u} : \left\{ \begin{array}{ccc} F & \to & \mathrm{Im}(u) \\ e & \mapsto & u(e) \end{array} \right.$ est un isomorphisme.

Théorème du rang : soit E de dimension finie et $u \in \mathscr{L}(E, E')$, on a $\boldsymbol{\mathrm{rg}(u)}$ **existe** et

$$\boldsymbol{\mathrm{rg}(u) + \mathrm{Ker}(u) = \dim E}$$

Démo : $\mathrm{Im}(u)$ isomorphique à F tel que $F \oplus \mathrm{Ker}(u) = E$

Rang et composée : (HP) soit $E \xrightarrow{v} E' \xrightarrow{u} E''$. On a $\left\{ \begin{array}{l} \mathrm{rg}(u \circ v) \leqslant \mathrm{rg}(u) \\ \mathrm{rg}(u \circ v) \leqslant \mathrm{rg}(v) \end{array} \right.$

En effet, $\mathrm{Im}(u \circ v) \subset \mathrm{Im}(u)$ et $\mathrm{Ker}(v) \subset \mathrm{Ker}(u \circ v)$...

Dimension d'hyperplans : soit $H_1, \ldots, H_n$ des hyperplans de E, $\boldsymbol{\dim(H_1 \cap \ldots \cap H_n) \geqslant \dim E - n}$

Il existe φ_i t.q. $\mathrm{Ker}(\varphi_i) = H_i$. Poser $u : \left\{ \begin{array}{ccc} E & \to & \mathbb{K}^n \\ e & \mapsto & (\varphi_1(e), \ldots, \varphi_n(e)) \end{array} \right.$, $\mathrm{Ker}(u) = \bigcap H_i$, $\mathrm{Im}(u) \subset \mathbb{K}^n$ donc...

Caractérisation d'automorphismes : soit E de dimension finie et $u \in \mathscr{L}(E)$, les propositions suivantes sont équivalentes :

(i) $u \in \mathrm{Gl}(E)$ (iii) $\mathrm{rg}(u) = \dim E$ (iv) $\exists w \in \mathscr{L}(E), u \circ w = \mathrm{id}_E$

(ii) $\mathrm{Ker}(u) = \{0_E\}$ (v) $\exists v \in \mathscr{L}(E), v \circ u = \mathrm{id}_E$

Forme coordonnée dans une base : il existe $b = (e_1, \ldots, e_n)$ une base de E, soit $j \in [\![1, n]\!]$ on pose $e_j^* \in \mathscr{L}(E, \mathbb{K})$ l'unique forme linéaire telle que

$$\boldsymbol{\forall i \in [\![1, n]\!], i \neq j \Rightarrow e_j^*(e_i) = 0_{\mathbb{K}}} \quad \text{et} \quad \boldsymbol{e_j^*(e_j) = 1_{\mathbb{K}}}$$

C'est la j-ième forme coordonnée dans la base b, on a $\boldsymbol{\forall x \in e, x = \sum_{i=1}^n e_i^*(x) \cdot e_i}$

Forme linéaire : $\forall \varphi \in \mathscr{L}(E, \mathbb{K})$, $\boldsymbol{\varphi = \sum_{i=1}^n \varphi(e_i) \cdot e_i^*}$. On appelle $\mathscr{L}(E, \mathbb{K})$ le **dual** de E. $(e_1^*, \ldots, e_n^*)$ est une base duale (base de $\mathscr{L}(E, \mathbb{K})$)

Démonstration : $\varphi(x) = \varphi\big(\sum_{i=1}^n e_i^*(x) \cdot e_i\big) = ...$, pour la base, montrer la liberté en évaluant en e_i

Sous-espaces et intersection d'hyperplans : soit E de dimension fini $n \geqslant 2$ et F un sev strict de E de dimension $p \leqslant n - 1$, il existe $H_1, \ldots, H_{n-p}$ des hyperplans tels que $\boldsymbol{F = H_1 \cap \ldots \cap H_{n-p}}$.

Poser $(e_1, \ldots, e_p)$ une base de F, la compléter, considérer $\mathrm{Ker}(e_{p+1}^*), \ldots, \mathrm{Ker}(e_n^*)$

Équations d'hyperplans : soit $x \in E$, on pose $x_i = e_i^*(x)$.

— H est un hyperplan si et seulement s'il existe $(\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n \backslash \{(0_\mathbb{K}, \dots, 0_\mathbb{K})\}$, tel que $\boldsymbol{x \in H \Leftrightarrow \lambda_1 x_1 + \dots + \lambda_n x_n = 0_\mathbb{K}}$

— soit $(\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n \backslash \{(0_\mathbb{K}, \dots, 0_\mathbb{K})\}$, et $(\mu_1, \dots, \mu_n) \in \mathbb{K}^n \backslash \{(0_\mathbb{K}, \dots, 0_\mathbb{K})\}$. On a $\boldsymbol{H_1 = H_2 \Leftrightarrow \exists \alpha \neq 0_\mathbb{K} (\lambda_1, \dots, \lambda_n) = \alpha(\mu_1, \dots, \mu_n)}$

Démo : poser la forme linéaire φ, $\lambda_i = \varphi(e_i)$..., de même dans l'autre sens.

17 Matrices

17.1 Matrices et dimension finie

On note $\mathcal{M}_{n,\,p}(\mathbb{K})$ l'ensemble des matrices à n-ligne et p-colonnes, et $\mathcal{M}_n(\mathbb{K})$ l'ensemble des matrices carrées.

Matrice de coordonnées : soit E un $\mathbb{K}-ev$ de dimension finie n, soit $b = (e_1, \dots, e_n)$ une base de E. Pour $x \in E$, on pose : $\mathcal{M}_b(x) = \begin{bmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{bmatrix} \in \mathcal{M}_{n,1}(\mathbb{K})$ avec $\lambda_i = e_i^*(x)$.

Pour une famille de vecteurs $a = (x_1, \dots, x_p)$, on pose $\mathcal{M}_b(a) = \begin{bmatrix} \lambda_{1,1} & \cdots & \lambda_{1,p} \\ \vdots & \ddots & \vdots \\ \lambda_{n,1} & \cdots & \lambda_{n,p} \end{bmatrix} \in \mathcal{M}_{n,p}(\mathbb{K})$. avec $\lambda_{i,j} = e_i^*(x_j)$. Une famille admet une unique matrice de coordonnée, et réciproquement

Matrice d'une forme linéaire : soit $u \in \mathscr{L}(E, E')$, $b = (e_1, \dots, e_n)$ une base de E et $b' = (e'_1, \dots, e'_p)$ une base de E'. On définit : $\mathcal{M}_{b,b'}(u) = \begin{bmatrix} \lambda_{1,1} & \cdots & \lambda_{1,p} \\ \vdots & \ddots & \vdots \\ \lambda_{n,1} & \cdots & \lambda_{n,p} \end{bmatrix} \in \mathcal{M}_{p,n}(\mathbb{K})$ vérifiant $\forall i \in [\![1,\, n]\!]\,, u(e_i) = \sum_{j=1}^{p} \lambda_{i,j} e'_j$. $\left\{ \begin{array}{ccc} \mathscr{L}(E,E') & \to & \mathcal{M}_{p,n}(\mathbb{K}) \\ u & \mapsto & \mathcal{M}_{b,b'}(u) \end{array} \right.$ est bijective.

Une 1ère réduction : $(n, p, r) \in \mathbb{N}^3, r \leqslant n, p$. On pose $J_{n,p,r} = \begin{pmatrix} 1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$ avec $\forall i \in [\![1,\, r]\!]\, j_{i,i} = 1$ et $j_{i,k} = 0$ sinon.

Soit $u \in \mathscr{L}(E, E')$ $\dim E = p$, $\dim E' = n$, $\mathrm{rg}(u) = r$.

Il existe b une base de E et b' une base de E' tel que $\mathcal{M}_{b,b'}(u) = J_{n,p,r}$

Démonstration : $\exists S, S \oplus \mathrm{Ker}(u) = E$ et S isomorphique à $\mathrm{Im}(u)$, posons une base de S, puis la compéter, $t \mapsto u(t)$ bijective sur $S \to \mathrm{Im}(u)$

Matrice de changement de base : soit b et b' deux bases de E, on définit $\boldsymbol{P_b^{b'} = \mathcal{M}_b(b') = \mathcal{M}_{b',b}(\mathrm{id}_E)}$. Certaines matrices de $\mathcal{M}_n(\mathbb{K})$ ne seront jamais des matrices de changement de base.

17.2 Calcul matriciel

Structure de $\mathbb{K}$-espace vectoriel : soit $(A,\ B) \in \mathcal{M}_{n,p}(\mathbb{K})^2$. On définit les opérations $+$ et $\cdot$ par :

$$\boldsymbol{A+B=(a_{i,j}+b_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}} \qquad \boldsymbol{\lambda\cdot A=(\lambda\times a_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}}$$

$\boldsymbol{(\mathcal{M}_{n,p}(\mathbb{K}),\ +,\ \cdot)}$ est un $\mathbb{K}$-**espace vectoriel** par identification avec $\mathbb{K}^{[\![1,\,n]\!]\times[\![1,\,p]\!]}$.

Matrice élémentaire : soit $(a,b,n,p) \in (\mathbb{N}^*)^4$ avec $a \leqslant n$ et $b \leqslant p$, on définit la matrice élémentaire $\boldsymbol{E_{a,b}^{(n,p)}=(\delta_{i,a}\times\delta_{j,b})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}}$ la matrice nulle partout sauf en (a,b).

$c=\left(E_{i,j}^{(n,p)}\right)_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}$ est une **base** de $\mathcal{M}_{n,p}(\mathbb{K})$ car $\left(\begin{array}{ccc}\mathbb{K}^{[\![1,\,n]\!]\times[\![1,\,p]\!]} & \to & \mathcal{M}_{n,p}(\mathbb{K})\\ (\lambda_{i,j}) & \mapsto & \sum_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}}\lambda_{i,j}\cdot E_{i,j}^{(n,p)}\end{array}\right)$ est bijective. On connait alors la dimension de ce $\mathbb{K}$-ev : $\dim\mathcal{M}_{n,p}(\mathbb{K})=n\times p$. De plus, on a $u\mapsto\mathcal{M}_{b,b'}(u)\in\mathscr{L}\big(\mathscr{L}(E,E'),\ \mathcal{M}_{n,p}(\mathbb{K})\big)$ est isomorphique, donc $\dim\mathscr{L}(E,E')=n\times p$

Produit matriciel : soit $A\in\mathcal{M}_{\boldsymbol{n,p}}(\mathbb{K})$ et $B\in\mathcal{M}_{\boldsymbol{p,r}}(\mathbb{K})$. On définit le produit

$$\boldsymbol{A\times B}=\left(\sum_{\boldsymbol{k=1}}^{\boldsymbol{p}}\boldsymbol{a_{i,k}\times b_{k,j}}\right)_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant r}}\in\mathcal{M}_{\boldsymbol{n,r}}(\mathbb{K})$$

Cette loi vérifie l'associativité, la bilinéarité $(\alpha A+\beta B)\times(\gamma C+\delta D)=\alpha\gamma AC+\alpha\delta AD+\beta\gamma BC+\beta\delta BD$, mais est non-commutative. On a $\boldsymbol{E_{a,b}^{(n,p)}\times E_{c,d}^{(p,q)}=\delta_{b,c}\cdot E_{a,d}^{(n,q)}}$

Anneau des matrices : $(\mathcal{M}_n(\mathbb{K}),\ +,\ \times)$ est un anneau. On note $\mathrm{Gl}_n(\mathbb{K})$ l'ensemble des inversibles de $\mathcal{M}_n(\mathbb{K})$. $(\mathrm{Gl}_n(\mathbb{K}),\ \times)$ est un groupe.

Matrices remarquables : on pose les matrices carrées de taille n suivantes :

- $\boldsymbol{I_n}=(\delta_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}}$ l'identité, vérifiant $M_{p,n}\times I_n=M_{p,n}$ et $I_n\times M_{n,p}=M_{n,p}$
- les matrices d'homothétie ou scalaires, vérifiant $\exists\lambda\in\mathbb{K}, M=\lambda\cdot I_n=(\lambda\delta_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}}$. Leur ensemble est $\mathrm{Vect}(I_n)$
- les matrices diagonales $A=\begin{pmatrix}\lambda_1 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & \lambda_n\end{pmatrix}$. On note $\mathcal{D}_n(\mathbb{K})=\mathrm{Vect}\big((E_{i,i}^{(n,n)})_{1\leqslant i\leqslant n}\big)$
- les triangulaires supérieures vérifiant : $\forall(i,j)\in[\![1,\,n]\!]^2, i>j\Rightarrow a_{i,j}=0$. On a $\mathcal{T}_n^{(s)}(\mathbb{K})=\mathrm{Vect}\big((E_{i,j}^{(n,n)})_{1\leqslant i\leqslant j\leqslant n}\big)$
- les triangulaires inférieures vérifiant : $\forall(i,j)\in[\![1,\,n]\!]^2, i<j\Rightarrow a_{i,j}=0$. On a $\mathcal{T}_n^{(i)}(\mathbb{K})=\mathrm{Vect}\big((E_{i,j}^{(n,n)})_{1\leqslant j\leqslant i\leqslant n}\big)$
- les triangulaires stricts, triangulaire de diagonale nulle

$\mathcal{D}_n(\mathbb{K})$, $\mathcal{T}_n^{(s)}(\mathbb{K})$ et $\mathcal{T}_n^{(i)}(\mathbb{K})$ sont des sous-anneaux et des sous-espaces vectoriels de $\mathcal{M}_n(\mathbb{K})$.

Trace d'une matrice : on définit la forme linéaire $\mathbf{Tr}$: $\left\{\begin{array}{ccc} \mathcal{M}_n(\mathbb{K}) & \to & \mathbb{K} \\ \boldsymbol{A} & \mapsto & \sum_{i=1}^{n} \boldsymbol{a_{i,i}} \end{array}\right.$.
On a, pour $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et $B \in \mathcal{M}_{p,n}(\mathbb{K})$, $\mathbf{Tr(AB) = Tr(BA)}$, donc, pour $P \in \mathrm{Gl}_n(\mathbb{K})$, $\mathrm{Tr}(P^{-1}AP) = \mathrm{Tr}(A)$. On dit qu'elle est invariante par conjugaison.

Transposition : soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$ on définit la matrice transposée de A par ${}^tB = \left(a_(j,i)\right)_{\substack{1\leqslant j\leqslant p \\ 1\leqslant i\leqslant n}}$. Pour $(\alpha,\beta) \in [\![1,\,p]\!] \times [\![1,\,n]\!]$, ${}^t\boldsymbol{A_{\alpha,\beta}} = \boldsymbol{A_{\beta,\alpha}}$.

- ${}^t({}^t\boldsymbol{A}) = \boldsymbol{A}$ et $t\left\{\begin{array}{ccc} \mathcal{M}_{n,p}(\mathbb{K}) & \to & \mathcal{M}_{p,n}(\mathbb{K}) \\ A & \mapsto & {}^tA \end{array}\right.$ est isomorphique
- $\forall (C,D) \in \mathcal{M}_{n,p}(\mathbb{K}) \times \mathcal{M}_{p,q}(\mathbb{K}),\ {}^t\boldsymbol{(C \times D)} = {}^t\boldsymbol{D} \times {}^t\boldsymbol{C}$
- $\forall P \in \mathrm{Gl}_n(\mathbb{K}),\ {}^tP \in \mathrm{Gl}_n(\mathbb{K})$ et $({}^tP)^{-1} = {}^t(P^{-1})$

Symétrie et antisymétrique : on pose $\mathcal{S}_n(\mathbb{K}) = \{M \in \mathcal{M}_n(\mathbb{K}) \ / \ {}^tM = M\}$ l'ensemble des matrices symétriques et $\mathcal{A}_n(\mathbb{K}) = \{M \in \mathcal{M}_n(\mathbb{K}) \ / \ {}^tM = -M\}$ celui des matrices antisymétriques.
$\forall M \in \mathcal{M}_n(\mathbb{K}),\ \frac{1}{2}(M + {}^tM) \in \mathcal{S}_n(\mathbb{K})$ et $\frac{1}{2}(M - {}^tM) \in \mathcal{A}_n(\mathbb{K})$

17.3 Matrice et application linéaire en dimension finie

Produit et composé : soit $E_b \xrightarrow{u} F_{b'} \xrightarrow{v} G_{b''}$ avec b, b', b'' des bases et u, v linéaires. On a :

$$\boldsymbol{\mathcal{M}_{b,b''}(u \circ v) = \mathcal{M}_{b',b''}(v) \times \mathcal{M}_{b,b'}(u)}$$

Matrice et isomorphie : soit E et F deux $\mathbb{K}$-ev de dimension n, et b, b' leurs bases. on pose $u \in \mathscr{L}(E,F)$, on a alors :

$$\boldsymbol{u \text{ isomorphique} \quad \Leftrightarrow \quad \mathcal{M}_b(u) \text{ inversible}}$$

On a dans ce cas $\mathcal{M}_b\left(u^{-1}\right) = \left(\mathcal{M}_b(u)\right)^{-1}$

Démo par équivalences, u bijective $\Leftrightarrow \exists u^{-1}, u \circ u^{-1} = \mathrm{id}_E$ puis passage aux matrices.

Matrice et évaluation : soit $u \in \mathscr{L}(E,F)$ et $x \in E$, on a :

$$\mathcal{M}_{b'}(u(x)) = \mathcal{M}_{b,b'}(u) \times \mathcal{M}_b(x)$$

Application linéaire canoniquement associée à une matrice : on identifie $\mathcal{M}_n(\mathbb{K})$ à $\mathbb{K}^n$ et $\mathcal{M}_p(\mathbb{K})$ à $\mathbb{K}^p$, soit $A \in \mathcal{M}_{p,n}(\mathbb{K})$, on définit l'ALCA de A par :

$$\boldsymbol{\varphi_A} = \left\{\begin{array}{ccc} \mathbb{K}^{\boldsymbol{p}} & \to & \mathbb{K}^{\boldsymbol{n}} \\ X & \mapsto & AX \end{array}\right.$$

On a $\varphi_A \in \mathscr{L}(\mathbb{K}^p, \mathbb{K}^n)$, soit $b^{(p)}$ et $b^{(n)}$ les bases canoniques de $\mathbb{K}^p$ et $\mathbb{K}^n$. On a :

$$\mathcal{M}_{b^{(p)},\,b^{(n)}}(\varphi_A) = A \qquad \text{et} \qquad A \in \mathrm{Gl}_n(\mathbb{K}) \Leftrightarrow \varphi_A \in \mathrm{Gl}(\mathbb{K}^n)$$

Noyau, image et rang : pour A une matrice, on définit à partir de φ_A
— l'image $\mathrm{Im}(A) = \mathrm{Im}(\varphi_A) = \{AX,\ X \in \mathbb{K}^p\} = \mathrm{Vect}(C_1(A), \dots, C_2(A)$
— le noyau $\mathrm{Ker}(A) = \mathrm{Ker}(\varphi_A) = \{X \in \mathbb{K}^p \,/\, AX = 0_{\mathbb{K}^n}\}$
— le rang $\mathrm{rg}(A) = \mathrm{rg}(\varphi_A)$, on a $\mathrm{rg}(A) = p - \dim \mathrm{Ker}(A)$

Caractérisation d'inversibilité : on a des propriétés similaires aux automorphismes en dimension finie (page 50)

(i) $A \in \mathrm{Gl}_n(\mathbb{K})$ (iii) $\mathrm{rg}(A) = n$ (iv) $\exists B \in \mathcal{M}_n(\mathbb{K}), AB = I_n$
(ii) $\mathrm{Ker}(A) = \{0_n\}$ (v) $\exists B \in \mathcal{M}_b(\mathbb{K}), BA = I_n$

On peut donc déterminer l'inversibilité d'une matrice en montrant l'unicité d'une solution X de $AX = Y$, donc l'injectivité de φ_A

Inversibilité de matrices diagonales : soit $A \in \mathcal{T}_n^{(s)}(\mathbb{K})$, alors

$$\boldsymbol{A \in \mathrm{Gl}_n(\mathbb{K}) \quad \Leftrightarrow \quad \forall i \in [\![1,\ n]\!],\ a_{i,i} \neq 0_{\mathbb{K}}}$$

Dans ce cas, $A^{-1} \in \mathcal{T}_n^{(s)}(\mathbb{K})$ et $\forall i \in [\![1,\ n]\!], a_{i,i}^{-1} = \frac{1}{a_{i,i}}$
$\Rightarrow$ par contraposée, $\exists j, a_{j,j} = 0_{\mathbb{K}}$ alors $(C_1(\mathbb{K}), \dots, C_j(\mathbb{K}) \in \mathrm{Vect}(E_{1,1}^{(1,n)}, \dots, E_{j-1,1}^{(1,n)})$, donc lié. $\Leftarrow$ en résolvant le système $AX = Y$
Cet énoncé reste vrai avec $\mathcal{T}_n^{(i)}(\mathbb{K})$ et dans le cas de $\mathcal{D}_n(\mathbb{K})$ $(\forall i \in [\![1,\ n]\!], D_{i,i}^{-1} = \frac{1}{D_{i,i}})$

17.4 Changement de bases

Matrice de changement de base : soit (b, b') deux bases de E, on note $\boldsymbol{P_{b'}^{b} = \mathcal{M}_{b,\,b'}(\mathrm{id}_E)}$ la matrice des coordonnées de b dans b'. On a $\boldsymbol{P_b^{b'} \in \mathrm{Gl}_n(\mathbb{K})}$ et $\boldsymbol{(P_b^{b'})^{-1} = P_{b'}^{b}}$. Soit $u \in \mathscr{L}(E)$ et $x \in E$, on a :

- $\boldsymbol{\mathcal{M}_b(x) = P_{b'}^{b} \times \mathcal{M}_{b'}(x)}$
- $\boldsymbol{\mathcal{M}_b(u) = P_b^{b'} \times \mathcal{M}_{b'}(x) \times P_{b'}^{b}}$

Pour le retrouver : $E_{b'} \xrightarrow{\mathrm{id}_E} E_b \xrightarrow{u} E_b \xrightarrow{\mathrm{id}_E} E_{b'}$ donc en composant $\mathrm{id}_E \circ u \circ \mathrm{id}_E = u$, d'où $\mathcal{M}_{b,\,b'}(\mathrm{id}_E) \times \mathcal{M}_b(u) \times \mathcal{M}_{b',\,b}(\mathrm{id}_E) = \mathcal{M}_{b'}(u)$

Matrices équivalentes : deux matrices $(A, B) \in \mathcal{M}_{p,n}(\mathbb{K})$ sont équivalentes si $\boldsymbol{\exists (P, Q) \in \mathrm{Gl}_n(\mathbb{K}), A = PBQ}$. C'est une relation d'équivalence, et en notant $r = \mathrm{rg}(A)$, on a A équivalente à $J_{p,n,r}$. Il y a donc $\min(p, n) + 1$ classes d'équivalences. On a

$$A \text{ est équivalente à } B \Leftrightarrow \mathrm{rg}(A) = \mathrm{rg}(B)$$

$A \sim J_r$ d'après la réduction, $\Rightarrow$ en passant par les ALCA...

Rang et équivalence : soit $u \in \mathscr{L}(E, F)$ et b, b' des bases de E et F. Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$ on a :

$$\boldsymbol{\mathrm{rg}(u) = \mathrm{rg}\big[\mathcal{M}_{b,\,b'}(u)\big] \qquad \mathrm{rg}(A) = \mathrm{rg}({}^{\mathrm{t}}A)}$$

Matrice extraite : soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$, $n' \leqslant n$ et $p' \leqslant p$. On forme une matrice extraite de A en sélectionnant n' lignes et p' colonnes (on conserve l'ordre).

Rang d'une matrice : soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et A' extraite de A. on a $\boldsymbol{\mathrm{rg}(A') \leqslant \mathrm{rg}(A)}$

$$\boldsymbol{\forall \alpha \in \mathbb{N},\ \mathrm{rg}(A) \geqslant \alpha \ \Leftrightarrow\ \exists A' \text{ extraite de } A,\ A' \in \mathrm{Gl}_n(\mathbb{K})}$$

La liberté des colonnes extraites implique la liberté des colonnes. $\Rightarrow$ colonnes libres, puis ligne libre...

Matrices semblables : soit $(A, B) \in \mathcal{M}_n(\mathbb{K})^2$ on dit que A et B sont semblables lorsque $\boldsymbol{\exists P \in \mathrm{Gl}_n(\mathbb{K}),\ B = P^{-1}AP}$. C'est une relation d'équivalence. Si A et B semblables, alors $\mathrm{rg}(A) = \mathrm{rg}(B)$ et $\mathrm{Tr}(A) = \mathrm{Tr}(B)$. De plus $\forall k \in \mathbb{Z}, \boldsymbol{B^k = P^{-1}A^kP}$

$\mathcal{M}_b(u)$ et $\mathcal{M}_{b'}(u)$ sont semblables. Pour déterminer une matrice semblable à A, considérer φ_A puis chercher une base b tel que $\mathcal{M}_b(\varphi_A)$ soit simple.

Trace d'une fonction : soit $u \in \mathscr{L}(E)$, comme $\mathrm{Tr}(\mathcal{M}_b(u))$ ne dépend pas de b, on pose $\boldsymbol{\mathrm{Tr}(u) = \mathrm{Tr}(\mathcal{M}_b(u))}$. C'est une forme linéaire de $\mathscr{L}(E)$

Soit p un projecteur, on a $\mathrm{Tr}(p) = \mathrm{rg}(p)$. De même si $A \in \mathcal{M}_n(\mathbb{K})$ vérifie $A^2 = A$, alors $\mathrm{Tr}(A) = \mathrm{rg}(A)$
En effet : $\mathrm{Ker}(p) \oplus \mathrm{Im}(p) = E$, donc en exprimant $\mathcal{M}(p)$ dans les bases adaptées.

Matrices blocs : soit $A_{n,p}$, $B_{n,r}$, $C_{q,p}$, $D_{q,r}$ des matrices. On peut définir la matrice $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \mathcal{M}_{n+q,p+r}(\mathbb{K})$. Lorsque les matrices ont les bonnes tailles on peut additionner et multiplier par bloc.

Matrices diagonales blocs : soit $A \in \mathcal{M}_n(\mathbb{K})$ et $B \in \mathcal{M}_p(\mathbb{K})$, alors

$$M = \begin{bmatrix} A & 0_{n,p} \\ 0_{p,n} & B \end{bmatrix} \in \mathrm{Gl}_{n+p}(\mathbb{K}) \ \Leftrightarrow\ A \in \mathrm{Gl}_n(\mathbb{K}) \text{ et } B \in \mathrm{Gl}_p(\mathbb{K})$$

Matrice de fonction bloc : soit E de dimension $n+p$, soit $F \oplus G$, de dimension (n, p) et de bases (b_F, b_G), soit p le projecteur sur F parallèlement à G et q le projecteur associé, soit $u \in \mathscr{L}(E)$. On a $\mathcal{M}_b(u) = \begin{bmatrix} \mathcal{M}_{b_F}\left(pu|_F^F\right) & \mathcal{M}_{b_G}\left(qu|_G^F\right) \\ \mathcal{M}_{b_F}\left(pu|_F^G\right) & \mathcal{M}_{b_G}\left(qu|_G^G\right) \end{bmatrix} = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$

$$\boldsymbol{u(F) \subset F \Leftrightarrow C = 0_{p,n}} \qquad \boldsymbol{u(G) \subset G \Leftrightarrow B = 0_{n,p}}$$

Preuve en décomposant selon F et G.

18 Dérivation

18.1 Définition

Dérivée : soit $f : I \to \mathbb{K}$, et $a \in I$. On note $\tau_{f,a} = t \mapsto \frac{f(t)-f(a)}{t-a}$. On dit que f est dérivable en a lorsque :

$$\exists \boldsymbol{\ell} \in \mathbb{K}, \frac{\boldsymbol{f(t)-f(a)}}{\boldsymbol{t-a}} \xrightarrow[\boldsymbol{t \to a^{\neq}}]{} \boldsymbol{\ell}$$

ℓ est le nombre dérivé de f en a, noté $f'(a)$. Propositions équivalentes : $\exists \ell \in \mathbb{K}$

- $\frac{f(a+h)-f(a)}{h} \xrightarrow[h \to 0^{\neq}]{} \ell$
- $f(t) = f(a) + \ell(t-a) + \underset{t \to a^{\neq}}{o}(t-a)$
- $f(a+h) = f(a) + \ell(h) + \underset{h \to 0^{\neq}}{o}(h)$

La droite $\boldsymbol{y = f(a) + f'(a)(x-a)}$ est la tangente au graphe de f en $(a, f(a))$

Opération	$\lambda f + \mu g$	$f \times g$	$\frac{1}{g}$	$\frac{f}{g}$	$f \circ g$
Dérivée	$\lambda f'(a) + \mu g(a)$	$f'(a)g(a) + f(a)g'(a)$	$-\frac{g(a)}{g^2(a)}$	$\frac{f'(a)g(a) - f(a)g'(a)}{g^2(a)}$	$g'(a)f'(g(a))$

Table 6 – Opérations sur les dérivées

Dérivabilité : la dérivabilité implique la continuité, mais la réciproque est fausse.

Dérivabilité latérale : on définit similairement à la continuité la dérivabilité à droite et à gauche (table 5), on a alors :

$$f \text{ dérivable en } a \Leftrightarrow \begin{cases} f \text{ dérivable en } a^+ \text{ et } a^- \\ \lim\limits_{t \to a^+} \tau_{f,a}(t) = \lim\limits_{t \to a^-} \tau_{f,a}(t) \end{cases}$$

Bijection réciproque : soit f continue et bijective de I dans J, $a \in J$ tel que f soit dérivable en $f^{-1}(a)$, on a alors $\boldsymbol{f^{-1}}$ **dérivable en** $\boldsymbol{a} \Leftrightarrow \boldsymbol{f'\big(f^{-1}(a)\big) \neq 0}$ et on a alors $\big(f^{-1}\big)'(a) = \frac{1}{f'(f^{-1}(a))}$
$\Rightarrow f(f^{-1}(a)) = a$ donc $(f^{-1})'(a) \times f'\big(f^{-1}(a)\big) = 1 \Leftarrow \tau_{f^{-1},a} = \frac{1}{\tau_{f,a}}$

18.2 Grands théorèmes

Extremum local : soit $f : I \to \mathbb{R}$ et $a \in I$, on a :

$$\begin{cases} \exists \delta > 0, [a-\delta,\, a+\delta] \subset I \ (a \text{ n'est pas une borne}) \\ \quad \forall t \in [a-\delta,\, a+\delta], f(t) \leqslant f(a) \\ \quad \forall t \in [a-\delta,\, a+\delta], f(t) \geqslant f(a) \\ f \text{ dérivable en } a \end{cases} \Rightarrow \boldsymbol{f'(a) = 0}$$

Démo par double inégalité en étudiant la dérivée à droite et à gauche...

Théorème de Rolle : soit $f \in \mathscr{C}([a,b], \mathbb{R})$ dérivable sur $]a,b[$ vérifiant $f(a) = f(b)$, alors $\boldsymbol{\exists c \in]a,b[,\ f'(c) = 0}$
Démo : théorème des bornes atteintes donne l'existence d'extremum...

Égalité des accroissements finis : soit $(a,b) \in \mathbb{R}^2$, $a < b$ et $f : [a,b] \to \mathbb{R}$,

$$\begin{cases} f \text{ continue sur } [a,\ b] \\ f \text{ dérivable sur }]a,\ b[\end{cases} \Rightarrow \boldsymbol{\exists c \in]a,b[,\ f'(c) = \frac{f(b) - f(a)}{b-a}}$$

Poser $\varphi : t \mapsto f(t) - \frac{f(b)-f(a)}{b-a}(t-a)$ et se ramener à Rolle

Monotonie et nombre dérivée : soit $f : \mathscr{C}(I, \mathbb{R})$ dérivable sur $I \setminus \{\text{bornes}\}$

$$\begin{aligned} \forall t \in I \setminus \{\text{bornes}\},\ f'(t) \geqslant 0 &\Rightarrow f \text{ croissante} \\ \forall t \in I \setminus \{\text{bornes}\},\ f'(t) \leqslant 0 &\Rightarrow f \text{ décroissante} \end{aligned}$$

Démo : soit $a < b$, il existe c, $f'(c) \times (b-a) = f(b) - f(a)$ d'où le signe... la réciproque est vraie. La fonction est strictement monotone si :

$$\begin{cases} \forall t \in I \setminus \{\text{bornes}\},\ f'(t) \geqslant 0 \\ \{x \in I \,/\, f'(x) = 0\} \end{cases} \begin{array}{l} \text{ne contient aucun} \\ \text{intervalle non trivial} \end{array} \Leftrightarrow f \text{ strictement croissante}$$

$$\begin{cases} \forall t \in I \setminus \{\text{bornes}\},\ f'(t) \leqslant 0 \\ \{x \in I \,/\, f'(x) = 0\} \end{cases} \begin{array}{l} \text{ne contient aucun} \\ \text{intervalle non trivial} \end{array} \Leftrightarrow f \text{ strictement décroissante}$$

par l'absurde, non-stricte $\leftrightarrow$ intervalle non triviaux dans l'ens des annulations.

Inégalité des accroissements finis : soit $f : I \to \mathbb{K}$, et M un majorant de $|f'(I)|$

$$\begin{cases} f \text{ continue sur } I \\ f \text{ dérivable sur } I \setminus \{\text{bornes}\} \end{cases} \Rightarrow \boldsymbol{\forall (a,b) \in I^2,\ |f(b) - f(a)| \leqslant M \times |b-a|}$$

$f(b)-f(a) = |f(b) - f(a)|\, e^{i\theta}$ donc $f(b)e^{-i\theta}+f(a)e-i\theta$ réel, poser $\varphi : t \mapsto \mathrm{Re}(f(t)e^{-i\theta})$ il existe c, $\varphi'(c) = |f(b) - f(a)|$, or $\varphi'(c) \leqslant |f'(c)| \leqslant M$

Fonction constante : soit $f : I \to \mathbb{K}$, on démontre en utilisant l'inégalité ci-dessus que $\boldsymbol{f \text{ constante} \Leftrightarrow f' = 0}$

Fonction lipschitzienne : soit $f : I \to \mathbb{K}$ et $\lambda \geqslant 0$, on dit que f est λ-lipschitzienne lorsque $\forall (a,b) \in I^2,\ |f(b) - f(a)| \leqslant \lambda\, |b-a|$

Théorème des limites de la dérivée : soit $a \in I$ et $f : I \to \mathbb{K}$ on a :

$$\begin{cases} f \text{ dérivable sur } I \setminus \{a\} \\ f \text{ continue en } a \\ f'(t) \xrightarrow[t \to a]{} \ell \end{cases} \Rightarrow \left| \begin{array}{l} \text{si } \ell \in \mathbb{K}, \begin{cases} f \text{ dérivable en } a \text{ et } f' \text{ continue en } a \\ f'(a) = \ell \end{cases} \\ \text{si } \ell \in \{-\infty, +\infty\}, \ f \text{ non dérivable en } a \end{array} \right.$$

Démo par ε, $\exists \eta$, $|f'(x) - \ell| \leqslant \varepsilon$ poser $g : t \mapsto f(t) - \ell(t-a)$, $g' \leqslant \varepsilon$ sur $]a, x[$, donc $|g(x) - g(a)| \leqslant \varepsilon |x - a|$... Pour ∞, utiliser l'égalité des accroissements finis.

18.3 Fonctions de classe $\mathscr{C}^n$, $\mathscr{C}^\infty$

Définition : soit $f : I \to \mathbb{K}$, $f \in \mathscr{C}^n(I, \mathbb{K})$ s'il existe $(f_0, \ldots, f_n)$ vérifiant $f_0 = f$, $\forall i, f'_{i-1} = f_i$ et f_n continue. Une telle liste est unique, et on note $\boldsymbol{f^{(n)}}$ la dérivée n-ième de f. On a $\mathscr{C}^\infty(I, \mathbb{K}) = \bigcap_{n \in \mathbb{N}} \mathscr{C}^n(i, \mathbb{K})$
$\forall k \in [\![0, n]\!], \mathscr{C}^n(I, \mathbb{K}) \subset \mathscr{C}^k(I, \mathbb{K})$ et $\forall f \in \mathscr{C}^n$, $f^{(k)} \in \mathscr{C}^{n-k}$ et $(f^{(k)})^{(n-k)} = f^{(n)}$

Classe et récurrence : $\left| \begin{array}{l} f \in \mathscr{C}^1 \text{ et } f' \in \mathscr{C}^{n-1} \Rightarrow f \in \mathscr{C}^n \\ f \in \mathscr{C}^{n-1} \text{ et } f^{(n-1)} \in \mathscr{C}^1 \Rightarrow f \in \mathscr{C}^n \end{array} \right.$

Opérations : $\mathscr{C}^n(I, \mathbb{K})$ est un **sous-espace vectoriel** de $\mathbb{K}^I$ **stable par** $\times$. De plus $f \mapsto f^{(n)} \in \mathscr{L}(\mathscr{C}^n(i, \mathbb{K}), \mathbb{K}^I)$.

$$\forall (f, g) \in \mathscr{C}^n(I, \mathbb{K}) \ \boldsymbol{(f \times g)^{(n)} = \sum_{k=1}^{n} \binom{k}{n} f^{(k)} \times g^{(n-k)}}$$

Si $f \in \mathscr{C}^n(I, \mathbb{K} \setminus \{0\})$ ne s'annule jamais, alors $\frac{1}{f} \in \mathscr{C}^n(I, \mathbb{K})$. Démo par récurrence

Bijection réciproque : soit $f \in \mathscr{C}^n(I, J)$ bijective, on a $f^{-1} \in \mathscr{C}^n(J, I) \Leftrightarrow \forall t \in I, f'(t) \neq 0$

Construction de fonction de classe $\mathscr{C}^n$: soit I un intervalle, $a \in I$ et $fI \setminus \{a\} \to \mathbb{K}$, on a :

$$\begin{cases} f \in \mathscr{C}^n(I \setminus \{a\}, \mathbb{K}) \\ \exists (\ell_k)_{k \in [\![1, n]\!]} \in \mathbb{K}^n, f^{(k)}(t) \xrightarrow[t \to a^{\neq}]{} \ell_k \end{cases} \Rightarrow \widetilde{f} = \left(\begin{array}{ccc} I & \to & \mathbb{K} \\ t & \mapsto & \left| \begin{array}{l} f(t) \text{ si } t \neq a \\ \ell_0 \text{ si } t = a \end{array} \right. \end{array} \right) \in \mathscr{C}^n(I, \mathbb{K})$$

Et on a alors $\widetilde{f^{(k)}} t \mapsto f^{(k)}$ si $t = a, \ell_k$ si $t \neq a$

Preuve par récurrence finie montante.

Formulaire de dérivées n-ièmes : soit $n \in \mathbb{N}$, on a :

- $\dfrac{\mathrm{d}^n}{\mathrm{d}x^n}(x^p) = n! \binom{n}{p} x^{p-n} = \left| \begin{array}{ll} p(p-1)\ldots(p-n+1)x^{p-n} & \text{si } p > n \\ p! & \text{si } p = n \\ 0 & \text{si } p < n \end{array} \right.$
- $\dfrac{\mathrm{d}^n}{\mathrm{d}x^n}(e^{\lambda x}) = \lambda^n e^{\lambda x}$
- $\dfrac{\mathrm{d}^n}{\mathrm{d}x^n}\left(\dfrac{1}{x}\right) = \dfrac{(-1)^n n!}{x^{n+1}} = \dfrac{\mathrm{d}^{n+1}}{\mathrm{d}x^{n+1}}(\ln x)$
- $\dfrac{\mathrm{d}^n}{\mathrm{d}x^n}(\cos(\omega x)) = \omega^n \cos\left(\omega x + n\dfrac{\pi}{2}\right)$
- $\dfrac{\mathrm{d}^n}{\mathrm{d}x^n}(x^\alpha) = \alpha(\alpha-1)\ldots\alpha - n + 1 x^{\alpha - n}$

19 Polynômes

19.1 Polynômes et opérations

Polynôme : on définit ainsi le $\mathbb{K}$-espace vectoriel des polynômes à coefficient dans $\mathbb{K}$ d'indéterminée X : $\boldsymbol{\mathbb{K}[X] = \mathbb{K}^{(\mathbb{N})}}$.
On notera $X = (0, 1, 0, \ldots)$, et $X^k = (0, \ldots, 0, 1, 0, \ldots)$.
$\boldsymbol{(\mathbb{K}[X], +, \cdot)}$ est un $\mathbb{K}$-espace vectoriel de base canonique $(X^k)_{k\in\mathbb{N}}$
Pour $P \in \mathbb{K}[X]$, on peut donc écrire $P = \sum_{i\in\mathbb{N}} p_i X^i$

Remarque : il existe $N \in \mathbb{N}$, tel que $P = \sum_{i=0}^{N} p_i X^i$, de plus on a pour $(P, Q) \in \mathbb{K}[X]^2$

$$\boldsymbol{P = Q \Leftrightarrow \forall k \in \mathbb{N}, p_k = q_k}$$

Degré : soit $P \in \mathbb{K}[X]$, on pose $\boldsymbol{\deg(P) = \begin{cases} \max\{k \in \mathbb{N} \,/\, p_k \neq 0\} & \text{si } P \neq 0 \\ -\infty & \text{si } P = 0 \end{cases}}$

$\deg(P) \leqslant N \Leftrightarrow P = \sum_{i=0}^{N} p_i X^i \Leftrightarrow \forall k > N, p_k = 0$

$P \neq 0 \Leftrightarrow \deg(P) \in \mathbb{N}$

$\deg(P) = N \Leftrightarrow \deg(P) \leqslant N$ et $p_N \neq 0$

On appelle *coefficient dominant* le plus grand coefficient non nul $p_{\deg(P)}$. P est dit *unitaire* lorsque $p_{\deg(P)} = 1$.

Les sev $\mathbb{K}_n[X]$: on définit $\boldsymbol{\mathbb{K}_n[X] = \{P \in \mathbb{K}[X] \,/\, \deg(P) \leqslant n\}}$. Ce sont des sous-espaces vectoriels de $K[X]$ car $\mathbb{K}_n[X] = \mathrm{Vect}\big((X_k)_{k\leqslant n}\big) = \bigcap_{k\geqslant n} \mathrm{Ker}(P \mapsto p_k)$

Produit de Cauchy : soit (x_n) et $(y_n) \in \mathbb{K}^{\mathbb{N}}$, on définit le produit $\star$ par :

$$\boldsymbol{(x_n) \star (y_n) = \left(\sum_{k=1}^{n} x_k y_{n-k}\right)_{n\in\mathbb{N}}}$$

On a alors $\boldsymbol{(\mathbb{K}^n, +, \star)}$ est un anneau commutatif dont $\mathbb{K}[X]$ est un sous-anneau

Conséquences : on a alors $X^k = X \star \ldots \star X$ k fois et pour $A \in \mathbb{K}[X]$, la fonction $\mu_A = \begin{pmatrix} \mathbb{K}[X] & \to & \mathbb{K}[X] \\ P & \mapsto & A \star P \end{pmatrix} \in \mathscr{L}(\mathbb{K}[X])$. le produit est de plus bilinéaire.
On confondra le scalaire λ et le polynôme constant $\lambda \cdot X^0$, car ils ont les mêmes propriétés.

Opération et degré : soit $(P, Q) \in \mathbb{K}[X]^2$, on a $\boldsymbol{\deg(P \star Q) = \deg(P) + \deg(Q)}$ et $\boldsymbol{\deg(\lambda P + \mu Q) \leqslant \max\{\deg(P), \deg(Q)\}}$.
Démonstration en développant le produit et séparant les cas de nullité. Il en découle que $\boldsymbol{P \star Q = 0 \Leftrightarrow P = 0}$ ou $\boldsymbol{Q = 0}$ donc $P \neq 0$ et $P \star A = P \star B \Rightarrow A = B$

Composition : on définit le polynôme composé par $\boldsymbol{P \circ Q = P(Q) = \sum_{k=0}^{\infty} p_k Q^k}$.
$(A \star B)(C) = A(C) \star B(C)$, $(A + B)(C) = A(C) + B(C)$, $(A \circ B)(C) = A(B \circ C)$

19.2 Dérivation

Dérivation soit $P = \sum_{k=0}^{\infty} p_k X^k \in \mathbb{K}[X]$, on définit le polynôme dérivé P' par :

$$\boldsymbol{P' = \sum_{k=1}^{\infty} k p_k X^{k-1} = \sum_{j=0}^{\infty} (j+1) p_{j+1} X^j}$$

$D : P \mapsto P' \in \mathscr{L}(\mathbb{K}[X])$ et $\mathrm{Ker}(D) = \mathbb{K}_0[X]$, $\mathrm{Im}(D) = \mathbb{K}[X]$.
De plus, $\boldsymbol{\deg(P^{(n)}) \leqslant \deg(P) - n}$ (égalité si $P^{(n-1)}$ non constant)

Nilpotence : on a $D_{|\,\mathbb{K}_n[X]} \in \mathscr{L}(\mathbb{K}_n[X], \mathbb{K}_n[X])$ est nilpotente.

Propriétés algébriques : on retrouve les propriétés usuelles de la dérivation :

- $(P \circ Q)' = Q' \star (P' \circ Q)$ • $(P \star Q)' = P' \star Q + Q' \star P$ • $(P + Q)' = P' + Q' \ldots$

Formule de Taylor : soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$, alors

$$\boldsymbol{P = \sum_{k=0}^{\infty} \frac{P^{(k)}(0)}{k!} X^k} \qquad \boldsymbol{P = \sum_{k=0}^{\infty} \frac{P^{(k)}(a)}{k!} (X - a)^k}$$

Démo de la première coeff par coeff, pour la deuxième, poser $Q(X) = P(X + a)$

19.3 Racines et factorisation

Relation divise : soit $(P, Q) \in \mathbb{K}[X]$, on dit que Q *divise* P lorsque $\boldsymbol{\exists C \in \mathbb{K}[X], P = QC}$. Si $P \neq 0$, alors tous les polynômes constants λ et les polynômes associés $\{\lambda P, \lambda \in \mathbb{K}\}$ divisent P.
La relation être associé est une relation d'équivalence de classes $\{\mathrm{Cl}(Q), Q \text{ unitaire}\}$

Racines : soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$, on a les équivalences :

$$\begin{aligned} \boldsymbol{a} \text{ est une racine de } \boldsymbol{P} &\Leftrightarrow \boldsymbol{P(a) = 0} && \text{définition} \\ &\Leftrightarrow \boldsymbol{(X - a) \mid P} && \text{conséquence} \\ \boldsymbol{(a_i)} \text{ racines distinctes de } \boldsymbol{P} &\Leftrightarrow \boldsymbol{\exists Q, P(X) = (X - a_1) \ldots (X - a_n) Q(X)} \end{aligned}$$

$\Leftarrow$ Taylor et factoriser, pour la (2), $(a_2 - a_1)Q(a_2) = P(a_2) = 0$ donc $Q(a_2) = 0$

Racines et degré : soit $P \neq 0$ et $(a_1, \ldots, a_n)$ des racines deux à deux distinctes de P, on a $\boldsymbol{n \leqslant \deg(P)}$. Si l'on a un polynôme Q ayant une infinité de racines ou si $Q \in \mathbb{K}_n[X]$ possède $n + 1$ racines, alors $Q = 0$

Polynôme de Lagrange : soit $(a_1, \ldots, a_n) \in \mathbb{K}^n$ posons $\varphi : \begin{cases} \mathbb{K}_{n-1}[X] & \to & \mathbb{K}^n \\ P & \mapsto & (P(a_1), \ldots, P(a_n \end{cases}$
φ est un isomorphisme de groupe, car φ injective. Donc, il existe un unique polynôme P qui à $(a_1, \ldots, a_n)$ associe $(y_1, \ldots, y_n)$. On le construit avec les polynômes :

$$\boldsymbol{L_k = \prod_{\substack{i=1 \\ i \neq k}}^{n} \frac{X - a_i}{a_k - a_i}} \qquad \text{donc } \forall P \in \mathbb{K}_{n-1}(X), P(X) = \sum_{k=1}^{n} P(a_k) L_k(X)$$

(L_k) est une base de $\mathbb{K}_{n-1}(X)$ vérifiant $L_k(a_i) = \delta_{i,k}$, démo de l'égalité par différence, possession de n racines et majoration du degré. On en déduit que (L_k) est génératrice

La matrice de φ dans les bases canonique est $\begin{bmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{bmatrix}$ on peut déterminer son inverse en exprimant $\varphi^{-1} : (y_1, \ldots, y_n) \mapsto y_1 L_1(X) + \ldots + y_n L_n(X)$

Racines multiples : soit $\lambda \in \mathbb{K}$ et $P \in \mathbb{K}[X]$, on a l'équivalence :

$$\boldsymbol{\forall k \in [\![1, n]\!], P^{(k)}(\lambda) = 0 \Leftrightarrow (X - \lambda)^n \text{ divise } P}$$

On dit alors que λ est de multiplicité au moins n. $\Rightarrow$ Taylor, $\Leftarrow$ en dérivant le produit.

Factorisation globale soit $r \in \mathbb{N}, (n_i) \in \mathbb{N}^r, (\lambda_i) \in \mathbb{K}^r$ distincts et $P \in \mathbb{K}[X]$:

$$\begin{cases} P(\lambda_1) = \ldots = P^{(n_1)}(\lambda_1) = 0 \\ \quad \vdots \\ P(\lambda_r) = \ldots = P^{(n_r)}(\lambda_r) = 0 \end{cases} \Leftrightarrow \exists Q \in \mathbb{K}[X],\ P = Q \prod_{i=1}^{r} (X - \lambda_i)^{n_i}$$

$\Rightarrow$ immédiate, $\Leftarrow$ diviseurs $X - \lambda_i$ premiers entre eux, car les λ_i sont distincts.

Multiplicité : soit $P \in \mathbb{K}[X] \setminus \{0\}$ et $\lambda \in \mathbb{K}$, les entiers suivants existent alors :

$$\boldsymbol{\min \left\{ k \in \mathbb{N},\ / P^{(k)}(\lambda) \neq 0 \right\} = \max \left\{ k \in \mathbb{N},\ / (X - \lambda)^k \mid P \right\}}$$

On définit ainsi la multiplicité de λ. On a alors, en notant m_λ la multiplicité de λ, $\boldsymbol{\sum_{\lambda \in \mathbb{K}} m_\lambda \leqslant \deg(P)}$. Si $\sum m_\lambda > \deg(P)$, alors $P = 0$

Fonction polynomiale : on pose la définition suivante pour $t \in \mathbb{K}, P \in \mathbb{K}[X], I \subset \mathbb{K}$ et $f \in \mathbb{K}^I$

- morphisme d'évaluation en t, $\varphi_t : P \mapsto P(t)$
- fonction polynomiale associé à $P : t \mapsto P(t)$
- f est polynomiale s'il existe $A \in \mathbb{K}[X], \forall t \in I, f(t) = A(t)$. Si I est infini, on a unicité des coefficients de A car si A et B conviennent, $A - B$ a une infinité de racines.

Si I est un intervalle non trivial de $\mathbb{R}$, alors $f \in \mathscr{C}^\infty(I, \mathbb{R})$ et pour tout $k \in \mathbb{N}, \forall t \in I, f^{(k)}(t) = A^{(k)}(t)$. Si $\deg(A) > 1$, alors f' admet un nombre fini de racines et les variations de f sont donc contrôlées.

Polynômes scindés : un polynôme P est scindé dans $\mathbb{K}[X]$ s'il $\boldsymbol{\deg(P) \geqslant 1}$ et si l'une des propriétés équivalentes suivantes est vérifiée :

- $\displaystyle\sum_{\lambda\in\mathbb{K}} m_\lambda = \deg P$
- $\displaystyle P(X) = p_{\deg(P)} \prod_{\lambda\in\{\text{racines de } P\}} (X-\lambda)^{m_\lambda}$
- $\exists \mu \in \mathbb{K}^*, \exists(\lambda_1, \ldots, \lambda_{\deg(P)}) \in K^{\deg(P)}, \boldsymbol{P = \mu \prod_{i=1}^{\deg(P)} (X - \lambda_i)}$

Théorème de d'Alembert-Gauss : $\forall P \in \mathbb{C}[X]$ non-constant , $\boldsymbol{\exists \lambda \in \mathbb{C}, P(\lambda) = 0}$
On peut déduire de ce théorème que pour $P \in \mathbb{K}[X]$ non-constant de racines $(\lambda_1, \ldots, \lambda_n)$
— si $P \in \mathbb{C}[X]$ alors P est scindé : $\boldsymbol{P = \mu \prod (X - \lambda_i)}$
— si $P \in \mathbb{R}[X]$ alors $\exists(a_1, \ldots, a_p, b_1, \ldots, b_p)$ vérifiant $a_j^2 - 4b_j < 0$ tel que

$$\boldsymbol{P = \mu \prod (X - \lambda_i) \prod (X^2 + a_j X + b_j)}$$

$\exists \lambda, P = (X-\lambda)P_1$ or $P_1 \in \mathbb{C}[X]$..., pour le cas réel, on $\mu \prod_i (X - \lambda_i) Q$, $Q \in \mathbb{R}[X]$ n'a aucune racine réelle, or si $Q(z) = 0, Q(\overline{z}) = 0$, donc...

Polynômes et racines n-ièmes : soit $A(X)$ et $B(X) \in \mathbb{K}[X]$, on montre en factorisant par les racines, et remplaçant $B(X)$ par $B(z)$ pour tout z non racine que

$$\boldsymbol{X^n - 1 = \prod_{k=0}^{n-1} \left(X - e^{\frac{2ik\pi}{n}}\right)} \qquad \boldsymbol{A(X)^n - B(X)^n = \prod_{k=0}^{n-1} \left(A(X) - e^{\frac{2ik\pi}{n}} B(X)\right)}$$

Relation coefficient-racines : soit $P = p_n \prod_{k=1}^n (X - \lambda_k)$, on a les relations :

- $\displaystyle\sigma_1 = \sum_{k=1}^n \lambda_k = -1\frac{p_{n-1}}{p_n}$
- $\displaystyle\sigma_2 = \sum_{1\leqslant i<j\leqslant n} \lambda_i\lambda_j = (-1)^2\frac{p_{n-2}}{p_n}$
- $\displaystyle\sigma_{n-1} = \sum_{k=1}^n = (-1)^{n-1}\frac{p_1}{p_n}$
- $\displaystyle\sigma_n = \prod_{i=1}^n \lambda_i = (-1)^n\frac{p_0}{p_n}$

$$\text{Cas général : } \sigma_k = \sum_{I\in\mathscr{P}_{n-k}(\llbracket 1,n\rrbracket)} \left(\prod_{i\in I} \lambda_i\right) = (-1)^{n-k}\frac{p_{n-k}}{p_n}$$

19.4 Arithmétique dans $\mathbb{K}[X]$

Division euclidienne : soit $(A,B) \in \mathbb{K}[X] \times \mathbb{K}[X] \setminus \{0\}$,

il existe un unique couple $(Q,R) \in \mathbb{K}[X]^2$ vérifiant $\begin{cases} A = QB + R \\ \deg(R) \leqslant \deg(B) - 1 \end{cases}$

Unicité facile, pour l'existence, on pose $n \geqslant \deg(A), \deg(B)$ et $\varphi : \mathbb{K}_{n-\deg(B)}[X] \times \mathbb{K}_{\deg(B)-1}[X] \to \mathbb{K}_n[X]$ linéaire et injective, donc surjective.

Algorithme d'Euclide : pour $(A,B) \in \mathbb{K}[X]^2, B \neq 0$ on définit la suite d'Euclide

$$(p_n) = \begin{cases} p_0 = A \text{ et } p_1 = B \\ \forall n \geqslant 2, p_n = \left| \begin{array}{ll} p_{n-2} \bmod p_{n-1} & \text{si } p_{n-1} \neq 0 \\ 0 & \text{si } p_{n-1} = 0 \end{array} \right. \end{cases}$$

Il existe $N \in \mathbb{N}^*$, $\forall k \in [\![1,\ N]\!], p_k \neq 0$ et $\forall k > N, p_k = 0$. (suite de degré strictement décroissante). On a alors $\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(p_N)$ ($\mathcal{D}(p_i) \cap \mathcal{D}(p_{i+1}) = \mathcal{D}(p_{i-1}) \cap \mathcal{D}(p_i)$)

PGCD : soit $(A_1, A_2) \in \mathbb{K}[X]^2$ (A_2 non-nul), alors $E = \{\deg(P), P \in \mathcal{D}(A_1) \cap \mathcal{D}(A_2)\}$ admet un max. Un polynôme P est *pgcd* de (A_1, A_2) lorsque $\begin{cases} \boldsymbol{P \in \mathcal{D}(A_1) \cap \mathcal{D}(A_2)} \\ \boldsymbol{\deg(P) = \max E} \end{cases}$.
Tous les *pgcd* de (A_1, A_2) sont associés. On note $A \wedge B$ le *pgcd* unitaire. On pose $0 \wedge 0 = 0$
Association : p_N est un pgcd de (A_1, A_2) et $P \mid p_N$ or $\deg(P) = \deg(p_N)$. Le *pgcd* vérifie alors les propriétés :

- $(A \wedge B) \wedge C = A \wedge (B \wedge C)$
- $(CA) \wedge (CB) = C(A \wedge B)$
- $\boldsymbol{\exists (U,V) \in \mathbb{K}[X]^2, AU + BV = A \wedge B}$ (démo par la suite d'euclide)

PGCD multiple : l'associativité permet de définir $A_1 \wedge \ldots \wedge A_n$, on a alors :

- $\mathcal{D}(A_1) \cap \ldots \cap \mathcal{D}(A_n) = \mathcal{D}(A_1 \wedge \ldots \wedge A_n)$
- $A_1 \wedge \ldots \wedge A_n = 0 \Leftrightarrow (A_1, \ldots, A_n) = (0, \ldots, 0)$
- $\exists (U_1, \ldots, U_n) \in \mathbb{K}[X]^n, A_1U_1 + \ldots + A_nU_n = A_1 \wedge \ldots \wedge A_n$
- $\deg(A_1 \wedge \ldots \wedge A_n) = \max\{\deg(P), P \text{ diviseur des } A_i\}$ si $\forall i \in [\![1,\ n]\!], A_i \neq 0$

PPCM : P est *ppcm* de $(A,B) \in (\mathbb{K}[X]\setminus\{0\})^2$ si $\begin{cases} A \mid P \text{ et } B \mid P \\ \deg(P) = \min\{\deg(Q), A, B \mid Q\} \end{cases}$
alors, $P(A \wedge B)$ et AB sont associés, donc tous les *ppcm* sont associés. On note $A \vee B$ le *ppcm* unitaire et $A \vee B = 0$ si $A = 0$ ou $B = 0$. Finalement $\boldsymbol{P\mathbb{K}[X] = A\mathbb{K}[X] \cap B\mathbb{K}[X]}$. Le *ppcm* est associatif

$\supset$ faire la division de Q par P et exploiter la minimalité. Association par divisibilité, Bezout et écrire $A = Q_1(A \wedge B)$, alors $Q_1Q_2(A \wedge B)$ multiple de P...

Polynômes premiers entre eux : on reprend les mêmes définition que pour l'arithmétique dans $\mathbb{Z}$ (9.3 page 27) $(A_1, \dots, A_k)$ sont premier entre eux :
- dans leur ensemble si $A_1 \wedge \dots \wedge A_k = 1$
- deux à deux si $\forall (i, j) \in [\![1, k]\!]^2, i \neq j \Rightarrow A_i \wedge A_k = 1$.

On a alors les théorèmes suivants :
- $A_1 \wedge \dots \wedge A_k = 1 \Leftrightarrow \exists (U_1, \dots, U_k),\ A_1U_1 + \dots + A_kU_k = 1$
- $\left\{ \begin{array}{c} A_1 \wedge C = 1 \\ \vdots \\ A_k \wedge C = 1 \end{array} \right. \Rightarrow A_1 \times \dots \times A_k \wedge C = 1$ (multiplier les relations de Bezout)
  - $A \wedge B = 1 \Rightarrow \forall (n, p) \in \mathbb{N}^2,\ A^n \wedge B^p = 1$
- $A \wedge B = 1$ et $A \mid BC \Rightarrow A \mid C$ (Gauss)
- $\forall i, A_i \mid C$ et $A_1, \dots, A_k$ premier deux-à-deux $\Rightarrow A_1 \times \dots \times A_k \mid C$

Polynômes irréductibles : un polynôme P est irréductible s'il est non constant et si $\boldsymbol{\mathcal{D}(P) = \mathbb{K}^* \cup \{\lambda P, \lambda \in \mathbb{K}^*\}}$.
- les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1
- les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et ceux de degré 2 sans racine réelle.

Deux polynômes irréductibles non associé sont premiers entre eux. Démo en revenant aux factorisations

Ordre de multiplicité : on note $m_{\lambda,P}$ la multiplicité de λ en tant que racine de P. Soit $(A, B) \in \mathbb{K}[X]^2$, on a :
- $\boldsymbol{A \mid B \Leftrightarrow \forall \lambda \in \mathbb{C} m_{\lambda,A} \leqslant m_{\lambda,B}}$
- $\forall \lambda \in \mathbb{C}, \left\{ \begin{array}{l} m_{\lambda,A\wedge B} = \min m_{\lambda,A}, m_{\lambda,B} \\ m_{\lambda,A\vee B} = \max m_{\lambda,A}, m_{\lambda,B} \end{array} \right.$

Division euclidienne : on procède à la méthode par soustraction successive :

$$\begin{array}{rl|l} X^4 + 2X^3 - X^2 + X + 1 & & X^2 - X - 1 \\ \cline{3-3} -X^4 + X^3 + X^2 & & X^2 + 3X + 3 \\ \cline{1-1} 3X^3 + X + 1 & & \\ -3X^3 + 3X^2 + 3X & & \\ \cline{1-1} 3X^2 + 4X + 1 & & \\ -3X^2 + 3X + 3 & & \\ \cline{1-1} 7X + 4 & & \end{array}$$

```
Q, R = P_nul, A
p = deg(B)
while deg(R) ⩾ p:
    K = R[deg(R)]/B[q] X^(deg(AL)-p)
    Q = Q + K
    R = R - B*K
return Q, R
```

20 Fractions rationnelles

20.1 Ensemble $\mathbb{K}(X)$: structure

Construction : soit $(A, B, C, D) \in (\mathbb{K}[X] \times \mathbb{K}[X] \setminus \{0\})^2$. On définit la relation $\boldsymbol{(A, C) \sim (B, D) \Leftrightarrow AD = BC}$. C'est une relation d'équivalence. On note $\frac{A}{B}$ la classe de (A, B). $\boldsymbol{K(X) = \left\{ \frac{A}{B}, (A, B) \in \mathbb{K}[X] \times \mathbb{K}[X] \setminus \{0\} \right\}}$

Structure de corps : on définit les opérations $\frac{A}{B}+\frac{C}{D}=\frac{AD+CB}{BD}$ $\frac{A}{B}\times\frac{C}{D}=\frac{AC}{BD}$. Ces opérations respectent bien les classes d'équivalence. $\boldsymbol{(\mathbb{K}(X),+,\times)}$ est un corps, $0_{\mathbb{K}(X)}=\frac{0}{1}$, $1_{\mathbb{K}(X)}=\frac{1}{1}$. On identifiera par la suite $\mathbb{K}[X]$ à $\frac{A}{1}$ (mêmes opérations).

Structure de $\mathbb{K}$-espace vectoriel : on définit $\lambda\cdot\frac{A}{B}=\frac{\lambda\cdot A}{B}$. Alors $\boldsymbol{(\mathbb{K}(X),+,\cdot)}$ est un $\mathbb{K}$-espace vectoriel. $\mathbb{K}[X]$ en est un sous-espace donc sa dimension est infinie ($(X^k)_{k\in\mathbb{N}}$ libre et infinie). Une base de $\mathbb{C}(X)$ est $(X^k)_{k\in\mathbb{N}}\vee\left(\frac{1}{(X-\lambda)^k}\right)_{\substack{\lambda\in\mathbb{C}\\k\in\mathbb{N}}}$

Degré : soit $f=\frac{A}{B}\in\mathbb{K}(X)$, on pose $\boldsymbol{\deg(f)=\deg(A)-\deg(B)}$. On retrouve les propriétés :

- $\deg(fg)=\deg(f)+\deg(g)$
- $\deg(f/g)=\deg(f)-\deg(g)$
- $\deg(\lambda f+\mu g)\leqslant\max\{\deg(f),\deg(g)\}$

Le sev $\mathbb{K}_{-1}(X)$: on définit $\mathbb{K}_n(X)=\{f\in\mathbb{K}(X)\,/\,\deg(f)\leqslant n\}$. C'est un sev de $\mathbb{K}(X)$. On a notamment $\begin{cases}\boldsymbol{\mathbb{K}_{-1}(X)\text{ est un sev de }\mathbb{K}(X)}\\ \boldsymbol{\mathbb{K}_{-1}(X)\oplus\mathbb{K}[X]=\mathbb{K}(X)}\end{cases}$. On montre la supplémentarité en faisant la division euclidienne.

Forme irréductible : soit $f\in\mathbb{K}(X)$, il existe un unique couple $(A,B)\in\mathbb{K}[X]\times\mathbb{K}[X]\setminus\{0\}$ vérifiant $\boldsymbol{f=\frac{A}{B}}$ et $\boldsymbol{A\wedge B=1}$ et $\boldsymbol{B}$ **unitaire**.
Pour l'existence, poser $A_0=\frac{A}{A\wedge B}$..., l'unicité en exploitant le produit en croix

Racines et pôles : soit $f\in\mathbb{K}(X)$ de forme irréductible $\frac{A}{B}$.
— les racines ou les zéros de f sont les racines du numérateur $A(X)$
— les pôles de f sont les racines du dénominateur
On a $\{\text{pôles}\}\cap\{\text{racines}\}=\emptyset$. La multiplicité des pôles et des racines est définie.

Dérivée : soit $f\in\mathbb{K}(X)$, $f=\frac{A}{B}$, on définit la dérivé de f par $\boldsymbol{f'=\frac{A'B-B'A}{B^2}}$. Les relations usuelles de dérivation s'applique, en particulier, pour $g\in\mathbb{K}(X),B(g)\neq0$, on a $(f\circ g)'=f'(g(X))g'(X)$

20.2 Décomposition en éléments simples dans $\mathbb{C}(X)$ et $\mathbb{R}(X)$

Base de $\mathbb{C}(X)$: la famille

$$\boldsymbol{(X^k)_{k\in\mathbb{N}}\vee\left(\frac{1}{(X-\lambda)^k}\right)_{\substack{\lambda\in\mathbb{C}\\k\in\mathbb{N}}}\text{ est une base de }\mathbb{C}[X]\oplus\mathbb{C}_{-1}(X)=\mathbb{C}(X)}$$

Liberté : $\deg \frac{1}{(X-\lambda)^k} \leqslant -1$. On considère $\left(\frac{1}{(X-\lambda_1)^1}, \dots, \frac{1}{(X-\lambda_1)^N}, \dots, \frac{1}{(X-\lambda_p)^1}, \dots, \frac{1}{(X-\lambda_p)^N}\right)$.
On pose $\frac{\mu_i^{(j)}}{(1-\lambda_i)^j}$ tel que $\sum \frac{\mu}{X-\lambda} = 0$. Produit par $\prod_{i=1}^p (X-\lambda_i)^N$, puis pour $\alpha \in [\![1, p]\!]$, $Q_a = (X-\lambda_a)^N \sum_{j=1}^N \frac{\mu_i^{(j)}}{(X-\lambda_i)^j}$. $\deg(Q_a) \leqslant N-1$ or $(X-\lambda_a)^N \mid Q_a$ donc $Q_a = 0$...
Génératrice : $f = \frac{A}{B}$, $B = \mu \prod_{i=1}^n (X-\lambda_i)^{\alpha_i}$. $\varphi = \left(\begin{array}{ccc} \mathbb{K}_{\alpha_1-1}[X] \dots \mathbb{K}_{\alpha_n-1}[X] & \to & \mathbb{K}_{\deg(B)-1}[X] \\ (U_i) & \mapsto & \sum_{k=1}^p U_k \prod_{i\neq k}\end{array}\right.$
linéaire et injective (produit par dénominateur et divisibilité), donc surjective.

Décomposition en éléments simples : soit $f = \frac{A}{B} \in \mathbb{K}(X)$, si $\deg(f) \geqslant 1$, on fait la division euclidienne de A par B pour trouver la partie fractionnaire $Q \in \mathbb{K}[X]$
On factorise entièrement $B = \mu \prod_{i=1}^p (X-\lambda_i)^{\alpha_i} \prod_{j=1}^n (X^2 + a_i X + b_i)^{\beta_i}$ (si $f \in \mathbb{R}(X)$)

$$\text{Alors } \boldsymbol{f = Q + \sum_{i=1}^{p} \sum_{k=1}^{\alpha_i} \frac{\mu_i^{(k)}}{(X-\lambda_i)^k} + \sum_{j=1}^{n} \sum_{k=1}^{\beta_j} \frac{\gamma_j^{(k)} X + \delta_j^{(k)}}{(X^2 + a_j X + b_j)^k}}$$

Identification : on peut identifier les coefficients avec ces techniques :
- Q est le quotient de la division euclidienne
- symétrie et unicité (remplacer $f(X)$ par $f(-X)$ ou $\overline{f}(X)$
- pour un pôle simple ou maximal λ en évaluant $f(X-\lambda) = \frac{A}{(X-\lambda)Q}(X-\lambda) = \frac{A}{Q}$ donc $\mu_\lambda = \frac{A(\lambda)}{Q(\lambda)} = \frac{A(\lambda)}{B'(\lambda)}$
- produit par X^k et passage à la limite pour le coefficient dominant
- évaluation en plusieurs points et résolution de système

DES de $\frac{P'(X)}{P(X)}$: on écrit $P = \mu \prod_{i=1}^p (X-\lambda_i)^{\alpha_i} = \mu \prod_{j=1}^n (X-t_j)$, alors

$$\frac{P'(X)}{P(X)} = \sum_{i=1}^{p} \frac{\alpha_i}{(X-\lambda_i)} = \sum_{j=1}^{n} \frac{1}{X-t_j}$$

21 Développements limités

21.1 Formule de Taylor-Young

Une intégration de o : soit $a \in I$ intervalle non trivial de $\mathbb{R}$, $\varphi \in \mathscr{C}^1(I, \mathbb{K})$ et $n \in \mathbb{N}$:

$$\boldsymbol{\varphi'(t) = \underset{t\to a}{o}\left((t-a)^n\right) \quad \Rightarrow \quad \varphi(t) - \varphi(a) = \underset{t\to a}{o}\left((t-a)^{n+1}\right)}$$

Démo par ε, on trouve η en contrôlant $|\varphi'|$ puis l'inégalité des accroissements finis.

Formule de Taylor-Young : soit $n \in \mathbb{N}$, $f \in \mathscr{C}^n(I, \mathbb{K})$, et $a \in I$ on a :

$$\boldsymbol{f(t) = f(a) + (t-a)f'(a) + \frac{(t-a)^2}{2}f''(a) + \ldots \frac{(t-a)^n}{n!}f^{(n)}(a) + \underset{t\to a}{\mathrm{o}}\left((t-a)^n\right)}$$
$$\boldsymbol{= \sum_{i=0}^{n} \frac{(t-a)^i}{i!}f^{(i)}(a) + \underset{t\to a}{\mathrm{o}}\left((t-a)^n\right)}$$

on pose alors $P = \sum_{i=0}^{n} \frac{f^{(i)}(a)}{i!}X^i$ le polynôme de Taylor de f en a à l'ordre n

La démonstration se fait en intégrant successivement $f^{(n)}(t) = f^{(n)}(a) + \mathrm{o}(1)$

Formulaire de développements limités : on a les DL suivants en $t \to 0$:

- $\frac{1}{1-t} = 1 + t + t^2 + t^3 + \ldots + t^n + \underset{t\to 0}{\mathrm{o}}(t^n)$ $\qquad \frac{1}{1-t} - \sum_{i=0}^{n} t^i = \ldots$
- $\frac{1}{1+t} = 1 - t + t^2 - t^3 + \ldots (-1)^n t^n + \underset{t\to 0}{\mathrm{o}}(t^n)$ $\qquad \frac{1}{1+t} = \frac{1}{1-(-t)}$
- $\ln(1+t) = t - \frac{t^2}{2} + \frac{t^3}{3} - \ldots (-1)^{n+1}\frac{t^n}{n} + \underset{t\to 0}{\mathrm{o}}(t^n)$ $\qquad \frac{\mathrm{d}}{\mathrm{d}t}\big(ln(1+t)\big) = \ldots$
- $\arctan t = t - \frac{t^3}{3} + \frac{t^5}{5} - \ldots (-1)^n \frac{t^{2n+1}}{2n+1} + \underset{t\to 0}{\mathrm{o}}(t^{2n+1})$ $\qquad \arctan' = \ldots$
- $e^t = 1 + t + \frac{t^2}{2} + \frac{t^3}{6} + \ldots + \frac{t_n}{n!} + \underset{t\to 0}{\mathrm{o}}(t^n)$ $\qquad$ Taylor-Young
- $\cos t = 1 - \frac{t^2}{2} + \frac{t^4}{24} - \ldots + (-1)^p \frac{t^{2p}}{2p!} + \underset{t\to 0}{\mathrm{o}}(t^{2p})$
- $\sin t = t - \frac{t^3}{6} + \frac{t^5}{120} - \ldots + (-1)^{p+1}\frac{t^{2p+1}}{(2p+1)!} + \underset{t\to 0}{\mathrm{o}}(t^{2p+1})$
- $(1+t)^\alpha = 1 + \alpha t + \frac{\alpha(\alpha-1)}{2}t^2 + \ldots + \frac{\alpha\ldots(\alpha-n+1)}{n!}t^n + \underset{t\to 0}{\mathrm{o}}(t^n)$

21.2 Développement limités

Définition : on dit que $f \in \mathscr{C}(I, \mathbb{K})$ admet un développement limité à l'ordre n en a, noté $\boldsymbol{\mathrm{DL}_n(a)}$ lorsque

$$\exists (a_0, \ldots, a_n) \in \mathbb{K}^n, f(t) \underset{t\to a}{=} a_0 + a_1(t-a) + \ldots + a_n(t-a)^n + \underset{t\to a}{\mathrm{o}}\left((t-a)^n\right)$$

On appelle partie régulière de f en a à l'ordre n le polynôme $P = \sum_{i=0}^{n} a_i(X-t)^i$.
Lorsqu'il existe, le développement limité est unique.
Si f est paire, on sait, par unicité, que le DL n'admet que des termes en $(t-a)^{2p}$.
Inversement, si f est impaire, son DL ne contient que des termes en $(t-a)^{2p+1}$.
Déterminer un $\mathrm{DL}_n(a)$ de $f(t)$ revient à déterminer un $\mathrm{DL}_n(0)$ de $f(a+h)$

CS/CN de développement limités : f on a les propriétés :
- f admet un $\mathrm{DL}_0(a) \Leftrightarrow f$ continue en a. $f(t) = f(a) + \underset{t\to a}{o}(1)$
- f admet un $\mathrm{DL}_1(a) \Leftrightarrow f$ dérivable en a. $f(t) = f(a) + f'(a)(t-a) + \underset{t\to a}{o}(t-a)$
- f admet un $\mathrm{DL}_p(a)$ avec $p \geqslant n \Rightarrow f$ admet un $\mathrm{DL}_n(a)$
- $f \in \mathscr{C}^n(I, \mathbb{K}) \Rightarrow f$ admet un $\mathrm{DL}_n(a)$
- f dérivable et f' admet un $\mathrm{DL}_n(a) \Rightarrow f$ admet un $\mathrm{DL}_{n+1}(a)$
- f dérivable et $\begin{cases} f \text{ admet un } \mathrm{DL}_{n+1}(a) \\ f' \text{ admet un } \mathrm{DL}_n(a) \end{cases} \Rightarrow$ la partie régulière de $\mathrm{DL}_n(a)$ de f' est la dérivé de celle du $\mathrm{DL}_{n+1}(a)$ de f.

DL et étude locale : soit $f : I \to \mathbb{K}$ et $a \in I \setminus \{\text{bornes}\}$. On suppose que f admet un $\mathrm{DL}_2(a) : f(t) = f(a) + f'(a)(t-a) + a_2(t-a)^2$
- $f'(a) = 0$ et $a_2 > 0 \Rightarrow f$ admet un minimum local en a
- $f'(a) = 0$ et $a_2 < 0 \Rightarrow f$ admet un maximum local en a
- f admet un minimum local en $a \Rightarrow f'(a) = 0$ et $a_2 \geqslant 0$
- f admet un maximum local en $a \Rightarrow f'(a) = 0$ et $a_2 \leqslant 0$

Démo en étudiant la limite de $\frac{f(t)-f(a)}{(t-a)^2}$. Si $f \in \mathscr{C}^2(I, \mathbb{K}), a_2 = \frac{f''(a)}{2}$.
La droite $\boldsymbol{y = f(a) + f'(a)(x-a)}$ est la tangente au graphe de f en $(a, f(a))$. le premier terme $a_p \neq 0$ apparaissant dans le DL détermine par son signe et la parité de p comment f tend vers la tangente. (un tangente en $\pm\infty$ est un asymptote)

Opérations sur les DL : on définit la forme normalisée d'un DL_n en posant $j = \min\{k \in [\![0,\ n]\!] / a_k \neq 0\}$, $f(t) = (t-a)^j\big[a_j + \ldots + a_n(t-a)^{n-j} + o\big((t-a)^{n-j}\big)\big]$. Alors pour le DL_n de f et le DL_p g en a de premier termes non-nuls i et j, $f \times g$ admet un DL à l'ordre $i + j + \min\{n-i, p+j\}$ (et de même pour le quotient)

22 Intégration

On note a, b deux réels, $a < b$, $\mathscr{B}([a,b], \mathbb{K})$ le sev des fonction bornés de $\mathbb{K}^{[a,b]}$ contenant les fonction continues, et $\mathscr{E}([a,b], \mathbb{K})$ l'ensemble des fonction escaliers.

22.1 Intégration d'un fonction escalier sur $[a, b]$

Le sev $\mathscr{E}([a,b], \mathbb{K})$: soit $f : [a,b] \to \mathbb{K}$ on dit que f est une fonction escalier si

$$\boldsymbol{\exists n \in \mathbb{N}^*, \exists (t_0, \ldots, t_n) \in [a,b]^{n+1}, \begin{cases} a = t_0 < \ldots < t_n = b \\ \forall i \in [\![0,\ n-1]\!]\,, f_{|]t_i, t_{i+1}[} \text{ est constante} \end{cases}}$$

Cette liste est une subdivision de $[a, b]$ adaptée à f. On peut lui insérer un nombre fini d'éléments et rester adapté. $\forall (f, g) \in \mathscr{E}([a,b], \mathbb{K})^2, \exists$ une subdivision adaptée à f et g. D'où $\mathscr{E}([a,b], \mathbb{K})$ est stable par somme et produit. De plus, $\mathscr{E}([a,b], \mathbb{K}) \subset \mathscr{B}([a,b], \mathbb{K})$. et contient les fonctions constantes sauf en un nb fini de points.

Intégration : pour $f \in \mathscr{E}([a,b],\mathbb{K})$ et $\sigma = (t_0, \dots, t_n)$ une subdivision de $[a,b]$ adaptée à f on pose :

$$\boldsymbol{I(f,\sigma) = \sum_{i=0}^{n-1} (t_{i+1} - t_i) f\left(\frac{t_{i+1}+t_i}{2}\right)}$$

$I(f,\sigma)$ ne dépend pas σ, on l'appelle intégrale de f entre a et b, noté $\boldsymbol{\int_{[a,b]} f}$

Propriétés de l'intégrale : pour la fonction intègre $S : \varphi \to \int_{[a,b]} \varphi$ on a

- S est une forme linéaire sur $\mathscr{E}([a,b],\mathbb{K})$ (stable par $+$ et $\cdot$)
- si f est constante égale à λ, $\boldsymbol{\int_{[a,b]} f = \lambda(b-a)}$
- si $\varphi_1 = \varphi_2$ sauf en un nombre fini de points, $\int_{[a,b]} \varphi_1 = \int_{[a,b]} \varphi_2$
- si $M \geqslant |\varphi_1|$, $\left|\int_{[a,b]} \varphi_1\right| \leqslant M(b-a)$ et $\left|\int_{[a,b]} \varphi_1\varphi_2\right| \leqslant M \int_{[a,b]} |\varphi_2|$
- si $\varphi \in \mathscr{E}([a,b],\mathbb{R})$, alors $\begin{cases} \varphi \geqslant 0 \Rightarrow \int_{[a,b]} \varphi \geqslant 0 \\ \boldsymbol{\varphi_1 \geqslant \varphi_2 \Rightarrow \int_{[a,b]} \varphi_1 \geqslant \int_{[a,b]} \varphi_2} \end{cases}$
- $\mathrm{Re}\left(\int_{[a,b]} \varphi\right) = \int_{[a,b]} \mathrm{Re}(\varphi)$, $\mathrm{Im}\left(\int_{[a,b]} \varphi\right) = \int_{[a,b]} \mathrm{Im}(\varphi)$ et $\overline{\int_{[a,b]} \varphi} = \int_{[a,b]} \overline{\varphi}$

22.2 Intégration de fonctions continues par morceaux

Le sev $\mathscr{C}^0_{\mathbf{pm}}([a,b],\mathbb{K})$: soit $f \in \mathbb{K}^{[a,b]}$, f est continue par morceaux s'il existe $(t_0, \dots, t_n)$ une subdivision tel que :

$$\boldsymbol{\forall i \in [\![0,\, n-1]\!],\, f_{|]t_i,t_{i+1}[} \text{ continue et admet des limites finies en } t_i^+ \text{ et } t_{i+1}^-}$$

Alors, $f \in \mathscr{C}^0_{\mathrm{pm}}([a,b],\mathbb{K}) \subset \mathscr{B}([a,b],\mathbb{K})$, stable par combinaison linéaire et produit. On a $\mathscr{C}^0_{\mathrm{pm}}([a,b],\mathbb{K}) = \mathscr{E}([a,b],\mathbb{K}) + \mathscr{C}^0([a,b],\mathbb{K})$

Démo : bornes atteintes sur $f_{|]t_i,t_{i+1}[}$ prolongée, et construction d'un fonction continue à partir de f en lui sommant une fonction escalier...

Théorème de Heine : soit f continue sur un segment $[a,b]$, alors

$$\boldsymbol{\forall \varepsilon > 0,\, \exists \eta > 0,\, \forall (x,y) \in [a,b]^2,\, |x-y| \leqslant \eta \Rightarrow |f(x) - f(y)| \leqslant \varepsilon}$$

On dit que f est uniformément continue. On en déduit que

$$\boldsymbol{\forall \varepsilon > 0,\, \exists \varphi \in \mathscr{E}([a,b],\mathbb{K}),\, \forall t \in [a,b],\, |f(t) - \varphi(t)| \leqslant \varepsilon}$$

Heine par l'absurde, on construit (x_n) et (y_n), elles admettent des sous-suites convergentes. On construit φ par la méthode des rectangle.

Approximation uniforme : pour tout $f \in \mathscr{C}^0_{\mathrm{pm}}([a,b],\mathbb{K})$, pour tout $n \in \mathbb{N}$, il existe $\varphi_n \in \mathscr{E}([a,b],\mathbb{K})$ tel que

$$\boldsymbol{\sup_{[a,b]} |f - \varphi_n| \xrightarrow[n \to +\infty]{} 0}$$

Existence et unicité de limites : on a $I_n = \int_{[a,b]} \varphi_n$ converge vers un valeur indépendante de φ_n.
(I_n) admet un valeur d'adhérence d'après BW, l'unicité vient de $\left|\int_{[a,b]} \varphi_{u(p)} - \int_{[a,b]} \varphi_{v(p)}\right| \leqslant \int_{[a,b]} \left|\varphi_{u(p)} - \varphi_{v(p)}\right|$ or $\left|\varphi_{u(p)} - \varphi_{v(p)}\right| \to 0$. L'indépendance de φ_n se montre de la même manière.

Intégration : soit $f \in \mathscr{C}^0_{\text{pm}}([a,b],\mathbb{K})$; il existe $\varphi_n \in \mathscr{E}([a,b],\mathbb{K})^{\mathbb{N}}$ tel que $\sup_{[a,b]} |f - \varphi_n| \xrightarrow[n \to +\infty]{} 0$, on définit alors

$$\int_{[a,b]} \boldsymbol{f} = \lim_{n \to +\infty} \int_{[a,b]} \boldsymbol{\varphi_n} \qquad \text{(définition indépendante de } (\varphi_n))$$

Propriétés de l'intégrale : elle prolonge l'intégrale sur $\mathscr{E}([a,b],\mathbb{K})$ et vérifie pour $(f,g) \in \mathscr{C}^0_{\text{pm}}([a,b],\mathbb{K})^2$, $|g| \leqslant m$

- $\left|\int_{[a,b]} f\right| \leqslant \int_{[a,b]} |f|$
- $\left|\int_{[a,b]} g\right| \leqslant m(b-a)$
- $\left|\int_{[a,b]} fg\right| \leqslant M \int_{[a,b]} |f|$
- $\left|\int_{[a,b]} fg\right| \leqslant \sqrt{\int_{[a,b]} |f|^2} \times \sqrt{\int_{[a,b]} |g|^2}$
- $f \geqslant 0 \Rightarrow \int_{[a,b]} f \geqslant 0$
- $f \geqslant g \Rightarrow \int_{[a,b]} f \geqslant \int_{[a,b]} g$
- $\text{Re/Im}\left(\int_{[a,b]} f\right) = \int_{[a,b]} \text{Re/Im}(f)$
- $\overline{\int_{[a,b]} f} = \int_{[a,b]} \overline{f}$

Revenir à la définition, et montrer que si φ_n convient pour f, $|\varphi_n|$ convient pour $|f|$

Strict positivité : soit $f \in \mathscr{C}^0([a,b],\mathbb{R})$ non nulle à valeur positive, on a $\boldsymbol{\int_{[a,b]} f > 0}$
Preuve par ε, en construisant une fonction de $\mathscr{E}$ entre f et 0

Intégrale nulle : soit f continue et positive sur $[a,b]$, on sait que $\boldsymbol{\int_{[a,b]} f = 0 \Rightarrow \forall t \in [a,b], f(t) = 0}$

22.3 Intégrale orientée

Définition : soit I un intervalle de $\mathbb{R}$, et $f \in \mathbb{K}^I$. On dit que f est continue par morceaux sur I, lorsque $\forall (a,b) \in I^2, a < b \Rightarrow f_{|[a,b]} \in \mathscr{C}^0_{\text{pm}}([a,b],\mathbb{K})$. Dans ce cas, on définit pour $(a,b) \in I^2$:

$$\int_a^b \boldsymbol{f(t)\,dt} = \begin{cases} +\int_{[a,b]} \boldsymbol{f} & \text{si } a < b \\ -\int_{[b,a]} \boldsymbol{f} & \text{si } a > b \\ \boldsymbol{0} & \text{si } a = b \end{cases}$$

Elle vérifie les inégalités usuelles sous réserve de signe $\left|\int_a^b f(t)\,dt\right| \leqslant \int_{\min\{a,b\}}^{\max\{a,b\}} |f(t)|\,dt$, ainsi que les inégalités strictes ci-dessus.

Relation de Chasles : soit $(\alpha,\beta,\gamma)\in I^3$, et $f\in\mathscr{C}^0_{\text{pm}}(I^3,\mathbb{K})$, on a :

$$\int_{\boldsymbol{\alpha}}^{\gamma} f(t)\,\mathrm{d}t=\int_{\boldsymbol{\alpha}}^{\boldsymbol{\beta}} f(t)\,\mathrm{d}t+\int_{\boldsymbol{\beta}}^{\gamma} f(t)\,\mathrm{d}t$$

Cas $\alpha<\beta<\gamma$, on revient au définition (φ_n)..., les autres cas s'en déduisent facilement.

Théorème fondamental de l'analyse : soit $f\in\mathscr{C}^0(I,\mathbb{K})$ et $\alpha\in I$. On pose $g=\begin{pmatrix} I & \to & \mathbb{K}\\ \boldsymbol{x} & \mapsto & \boldsymbol{\int_\alpha^x f(t)\,\mathrm{d}t}\end{pmatrix}$. On a $g\in\mathscr{C}^1(I,\mathbb{K})$ et $g'=f$.
Réciproquement, pour $F\in\mathscr{C}^1(I,\mathbb{K})$ tel que $F'=f$, on a $\boldsymbol{\int_\alpha^\beta f(t)\,\mathrm{d}t=F(\beta)-F(\alpha)}$

Par ε, taux d'accroissement $\frac{1}{x-x_0}\int_{x_0}^x f(t)-f(x_0)\,\mathrm{d}t$ et la continuité de f.

Primitives : l'ensemble $\left\{\left(x\mapsto\int_\alpha^x f(t)\,\mathrm{d}t+\lambda\right),\lambda\in\mathbb{K}\right\}\subset\mathbb{K}^I$ est l'ensemble solution de $y'=f$. La fonction $x\mapsto\int_\alpha^x f(t)\,\mathrm{d}t$ est l'unique solution vérifiant $y(\alpha)=0$

Changement de variable : soit $J\xrightarrow{\varphi}I\xrightarrow{f}\mathbb{K}$, avec $\varphi\in\mathscr{C}^1$, $f\in\mathscr{C}^0$ soit $(\alpha,\beta)\in J^2$, on montrer via les primitives F et $F\circ\varphi$ que :

$$\int_\alpha^\beta f\big(\varphi t\big)\times\varphi'(u)\,\mathrm{d}t=\int_{\varphi(\alpha)}^{\varphi(\beta)} f(u)\,\mathrm{d}u$$

Intégration par partie : soit $(u,v)\in\mathscr{C}^1(I,\mathbb{K})$, et $(a,b)\in I$, on sait que :

$$\int_a^b u'(t)v(t)\,\mathrm{d}t=[u(t)v(t)]_a^b-\int_a^b u(t)v'(t)\,\mathrm{d}t$$

Fonctions paires et impaire : soit $a\in\mathbb{R}$ et $(f,g)\in\mathscr{C}^0([-a,a],\mathbb{R})$ paires et impaires, alors $\int_{-a}^a f=2\int_0^a f$ et $\int_{-a}^a g=0$, preuve par changement de variable.

Formule de Taylor avec reste intégral : pour $n\in\mathbb{N}$, $f\in\mathscr{C}^{n+1}(I,\mathbb{K})$, et $(a,b)\in I^2$, on a l'égalité :

$$\boldsymbol{f(b)=\sum_{k=0}^{n}\frac{(b-a)^k}{k!}f^{(k)}(a)+\int_a^b\frac{(b-t)^n}{n!}f^{n+1}(t)\,\mathrm{d}t}$$

On la montre par récurrence, en partant de $f(b)=f(a)+\int_a^b\frac{(b-t)^0}{0!}f'(t)\,\mathrm{d}t$, puis en intégrant par parties.

Inégalité de Taylor-Lagrange : soit $n\in\mathbb{N}$, $f\in\mathscr{C}^{n+1}(I,\mathbb{K})$ et $M>0$ un majorant de $\left|f^{(n+1)}\right|$, on a l'inégalité :

$$f(b)-\sum_{k=0}^{n}\frac{(b-a)^k}{k!}f^{(k)}(a)\leqslant M\frac{|b-a|^{n+1}}{(n+1)!}$$

Dans l'égalité précédente, remplacer $t=a+u(b-a)$ pour intégrer entre 0 et 1

Sommes de Riemann : soit $f \in \mathscr{C}^0(I, \mathbb{K})$ et $(a, b) \in I$, $R_n = \frac{b-a}{n} \sum_{k=0}^{n-1} f\left(a + k\frac{b-a}{n}\right)$., On a alors $(R_n) \xrightarrow[n \to +\infty]{} \int_a^b f$, on peut majorer l'erreur si f est de classe $\mathscr{C}^1$ par $O\left(\frac{1}{n}\right)$. Il s'agit de la méthode des rectangles à gauche. On peut également appliquer cette méthode à droite $S_n = R_n - f(a) + f(b)$, au point médian en $\frac{1}{2}(a_k + a_{k+1}$.
On peut avoir une suite convergeant plus rapidement pour des fonctions de classe $\mathscr{C}^2$ et plus (ex : trapèzes $T_n = \frac{1}{2}(R_n + S_n)$ en $O\left(\frac{1}{n^2}\right)$

Calcul intégral : on peut intégrer toute fonction rationnelle sur un intervalle ou le dénominateur ne s'annule pas : (pour le trinômes, mettre sous forme canonique)

$$\int_a^b \frac{1}{(x-\lambda)^k} \mathrm{d}x = \begin{cases} \left[\frac{-1}{(k-1)(x-\lambda)^{k-1}}\right]_a^b & \text{si } k \geqslant 2 \\ \left[\ln(x-\lambda)\right]_a^b & \text{si } k = 1 \end{cases}$$

$$\int_a^b \frac{2x+\alpha}{(x^2+\alpha x+\beta)^k} \mathrm{d}x = \begin{cases} \left[\frac{-1}{(k-1)(x^2+\alpha x+\beta)^{k-1}}\right]_a^b & \text{si } k \geqslant 2 \\ \left[\ln(x^2+\alpha x+\beta)\right]_a^b & \text{si } k = 1 \end{cases}$$

Pour le cas $\frac{1}{x^2+\alpha x+\beta}$, trouver une relation de récurrence par IPP, ou changer de variable pour se ramener à arctan′.

23 Opérations élémentaires sur les matrices

23.1 Opérations élémentaires

Définition : pour $(n, p) \in (\mathbb{N}^*)^2$ et $A \in \mathcal{M}_{n,p}(\mathbb{K})$, $(a, b) \in [\![1,\, n]\!]^2$, $(\alpha, \beta) \in [\![1,\, p]\!]^2$ et $\lambda \in \mathbb{K}$ $q = n$ ou p on définit les opérations élémentaires suivante :

Nom	Opération	Matrice	Inverse
Échange	$\boldsymbol{L_a \leftrightarrow L_b}$ $\boldsymbol{C_\alpha \leftrightarrow C_\beta}$	$I_q - E_{a,a}^{(q,q)} - E_{b,b}^{(q,q)} + E_{a,b}^{(q,q)} + E_{b,a}^{(q,q)}$	$L_a \leftrightarrow L_b$
Dilatation	$\lambda \neq 0$, $\boldsymbol{L_a \leftarrow \lambda \cdot L_a}$ $\boldsymbol{C_\alpha \leftarrow \lambda \cdot C_\alpha}$	$I_q + (\lambda - 1)E_{a,a}^{(q,q)}$	$L_a \leftarrow \frac{1}{\lambda} \cdot L_a$
Transvection	$a \neq b$ $\boldsymbol{L_a \leftarrow L_a + \lambda \cdot L_b}$ $\alpha \neq \beta$ $\boldsymbol{C_\alpha \leftarrow C_\alpha + \lambda \cdot C_\beta}$	$I_n + \lambda E_{a,b}^{(n,n)}$ $I_p + \lambda E_{\beta,\alpha}^{(p,p)}$	$L_a \leftarrow L_a - \lambda \cdot L_b$

TABLE 7 – Opérations élémentaires sur les matrices

Les matrices d'opérations sont définies en effectuant la même opération élémentaire sur l'identité. On a alors pour E un matrice opération ligne et $\widetilde{E}$ une matrice opération colonne : $\boldsymbol{A' = EA}$ et $\boldsymbol{A'' = A\widetilde{E}}$.

Algorithme de calcul du rang : les matrices résultantes d'opérations sont équivalentes, leur rang est donc le même. Pour $\begin{bmatrix} a_{1,1} & L_{1,p-1} \\ 0_{n-1,p} & \widetilde{A}_{n-1,p-1} \end{bmatrix}$ on a $\boldsymbol{\mathrm{rg}(A) = 1 + \mathrm{rg}(\widetilde{A})}$, car

$\widetilde{A}$ équivalente à J_r...
Algorithme : $r = 0$, tant que la matrice est non-nulle

1. Choisir un coefficient non nul et le placer en haut à gauche
2. Annuler par transvection la première colonne sauf en haut
3. recommencer avec la matrice extraite de $(2, 2)$ à (n, p), $r = r + 1$

Conservation par les opération : soit $A \in \mathcal{M}_n(\mathbb{K})$, B une matrice construite à partir d'opérations élémentaires sur les lignes de A et C construite à partir d'opérations sur les colonnes. Alors il existe (Q, P) inversibles, $B = QA$, $C = AP$

$$\boldsymbol{\mathrm{rg}(A) = \mathrm{rg}(B) = \mathrm{rg}(C) \qquad \mathrm{Ker}(B) = \mathrm{Ker}(A) \qquad \mathrm{Im}(C) = \mathrm{Im}(A)}$$

Décomposition dans $\mathrm{Gl}_n(\mathbb{K})$ **:** pour $A \in \mathrm{Gl}_n(\mathbb{K})$, il existe $p \in \mathbb{N}$ et $(E_1, \ldots, E_p)$ des matrices d'opérations élémentaires sur le lignes telles que $\boldsymbol{E_1 \ldots E_n A = I_n}$, on en déduit alors un inverse de A $(E_1 \ldots E_n)$, en faisant les mêmes opérations élémentaires sur A et l'identité.
Preuve par récurrence, on passe de $\begin{bmatrix} I_k & M \\ 0 & B \end{bmatrix}$ à la matrice du rang $k+1$ en trouvant un coeff non nul dans la première colonne de B (car $\mathrm{rg}(B) = n - k$), l'amenant en haut de B (échange), le normalisant puis annulant tous les autres par transvection.

23.2 Systèmes linéaires

Système : pour S un système linéaire à n équations et p inconnues, on pose $A \in \mathcal{M}_{n,p}(\mathbb{K})$ la matrice des coefficients, et $b \in \mathcal{M}_{n,1}(\mathbb{K})$ la matrice des seconds membres. On, pour $x \in \mathbb{K}^p$, x est solution de $S \Leftrightarrow Ax = b$
$Ax = 0$ est le système homogène lié à S et a pour ensemble solution $\mathrm{Ker}(A)$. De façon générale, on a pour $x \in \mathbb{K}^p$

$$\boldsymbol{\mathscr{S}(S) = \emptyset} \text{ ou } \boldsymbol{\mathscr{S}(S) = \{x_0\} + \mathrm{Ker}(A) = \{x_0 + t, t \in \mathrm{Ker}(A)\}}$$

Opération sur les systèmes : on peut résoudre un système en partant de la matrice $\left[\, A \,\vdots\, b \,\right]$. Les opérations élémentaires sur les lignes ne modifient pas l'ensemble solution, et on peut intervertir deux colonnes de A : $i, j < p$ si on interverti également solution. On peut donc trianguliariser le système avec un méthode du pivot de Gauss (6.1 page 17) on obtient $r = \mathrm{rg}(A)$ pivots non nuls, $n - r$ équations de compatibilité et $p - r$ inconnues secondaires.

Systèmes (n, n) **:** si A est inversible, on parle de système de Crameur, il a alors une unique solution $A^{-1}b$

24 Déterminant

24.1 Étude succincte du groupe $(\mathscr{S}_n, \circ)$

Définition : $\mathscr{S}_n = \{\text{bijections de } [\![1,\, n]\!] \text{ dans } [\![1,\, n]\!]\}$, c'est-à-dire l'ensemble des permutations, on a $\#\mathscr{S}_n = n!$. Il possède les éléments remarquables suivant :

- Transposition $\tau_{i,j}$ pour $i \neq j \in [\![1,\, n]\!]$ défini par $\tau_{i,i}(k) = \left| \begin{smallmatrix} k \text{ si } k \notin \{i,j\} \\ i \text{ si } k = j \\ j \text{ si } k = i \end{smallmatrix} \right.$. Il y a $\binom{2}{n}$ transpositions. $\tau_{i,j}^2 = \mathrm{id}_{[\![1,\, n]\!]}$
- p-cycle $(a_1,\, \ldots,\, a_p)$ distincts 2-à-2. défini par $f(k) = \left| \begin{smallmatrix} k \text{ si } k \notin \{a_1,\, \ldots,\, a_p\} \\ a_{i+1} \text{ si } k = a_i \text{ et } i < p \\ a_1 \text{ si } k = a_p \end{smallmatrix} \right.$. Elle est d'ordre p. Il y a $\binom{n}{p}(p-1)!$ p-cycles. Un p cycle est le produit de $p-1$ transpositions

Cycles à support disjoint : la liste $(a_1,\, \ldots,\, a_p)$ est appelée support du cycle $(a_1,\, \ldots,\, a_p)$. Deux cycles à support disjoint commutent.

$$\forall \boldsymbol{f} \in \mathscr{S}_{\boldsymbol{n}}, \begin{cases} \exists ! \boldsymbol{p} \in \mathbb{N} \\ \exists ! (\boldsymbol{c_1}, \ldots, \boldsymbol{c_p}) \textbf{ des cycles à support disjoint} \end{cases}, \boldsymbol{f = c_1 \circ \ldots \circ c_p}$$

Morphisme signature il existe un unique morphisme $\boldsymbol{\varepsilon : \mathscr{S}_n \longrightarrow \{-1, 1\}}$ non constant

Unicité : on montre que pour τ un transposition, $\varepsilon(\tau) = -1$, or toute fonction peut se décomposer en transposition. Existence, la construire à partir de $\varepsilon(\tau) = -1$.

Permutation paires : on pose $\boldsymbol{\mathscr{A}_n = \mathbf{Ker}(\varepsilon)}$, l'ensemble des permutations paires. $\mathscr{A}_n$ est un sous-groupe de $\mathscr{S}_n$ de cardinal $\frac{1}{2}n!$. En effet, pour τ une transposition, $\begin{pmatrix} \mathscr{S}_n \setminus \mathscr{A}_n & \to & \mathscr{A}_n \\ \sigma & \mapsto & \tau \circ \sigma \end{pmatrix}$ et $\begin{pmatrix} \mathscr{S}_n \setminus \mathscr{A}_n & \to & \mathscr{A}_n \\ \sigma & \mapsto & \sigma \circ \tau \end{pmatrix}$ sont bijectives.

24.2 Déterminant

Fonction p-linéaires alternées : soit E un $\mathbb{K}$-ev, $p \in \mathbb{N}$ et $\varphi : E^p \to \mathbb{K}$.
φ est **p-linéaire** lorsqu'elle est linéaire par rapport à chacune de se variables :

$$\forall (v_1, \ldots, v_p) \in E^p, \forall i \in [\![1,\, p]\!], \begin{pmatrix} E & \to & \mathbb{K} \\ x & \mapsto & (v_1, \ldots, v_{i-1}, x, v_{i+1}, \ldots, v_p) \end{pmatrix} \in \mathscr{L}(E,\, \mathbb{K})$$

φ est **alterné** lorsque l'image d'une p-liste ayant deux fois le même vecteur est nulle.

$$\forall (v_1,\, \ldots,\, v_p) \in E^p, \left[\exists (i,j) \in [\![1,\, p]\!]^2, v_i = v_j \text{ et } i \neq j\right] \Rightarrow \varphi(v_1,\, \ldots,\, v_p) = 0$$

Si φ est p-linéaire alternée, alors on a les propriétés :

- pour $\sigma \in \mathscr{S}_n$, et $(v_1, \ldots, v_p) \in E^p$ $\varphi(v_{\sigma(1)},\, \ldots,\, v_{\sigma(p)}) = \varepsilon(\sigma) \times \varphi(v_1,\, \ldots,\, v_p)$

— si $(v_1, \dots, v_p) \in E^p$ est liée, alors $\varphi(v_1, \dots, v_p) = 0$
— en posant $y_i = x_i + \sum_{j \neq i} \lambda_j v_j$, on a $\varphi(y_1, \dots, y_p) = \varphi(v_1, \dots, v_p)$

DÉTERMINANT : pour E un $\mathbb{K}$ espace vectoriel de dimension finie n, et $b = (e_1, \dots, e_n)$ une base de E, on pose $(e_1^*, \dots, e_n^*)$ les formes coordonnés associés.

$$\boldsymbol{\det_b} = \left(\begin{array}{ccc} \boldsymbol{E^n} & \to & \mathbb{K} \\ (x_1, \dots, x_n) & \mapsto & \displaystyle\sum_{\boldsymbol{\sigma \in \mathscr{S}_n}} \boldsymbol{\varepsilon(\sigma)} \prod_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{e^*_{\sigma(i)}(x_i)} \end{array} \right)$$

C'est une forme n-linéaire alternée non nulle, $\det_b(b) = 1$

Alternée : poser τ qui inverse les deux éléments identiques, puis décomposer sur les fonctions paires et impaires.

Propriétés : soit $\varphi : E^n \to \mathbb{K}$ une forme n-linéaire alternée, alors
$\forall (x_1, \dots, x_n) \in E^n, \boldsymbol{\varphi(x_1, \dots, x_n) = \varphi(e_1, \dots, e_n) \times \det_b(x_1, \dots, x_n)}$

On en déduit que pour $a \in E^n$, $\left| \begin{array}{rcl} \boldsymbol{a \text{ est liée}} & \boldsymbol{\Leftrightarrow} & \boldsymbol{\det_b(a) = 0} \\ \boldsymbol{a \text{ est libre}} & \boldsymbol{\Leftrightarrow} & \boldsymbol{\det_b(a) \neq 0} \end{array} \right.$
Décomposer $x_1, \dots, x_n$ dans la base b. Si a libre, alors a est une base.

Déterminant d'un matrice carré : soit b la base canonique de $\mathbb{K}^n$, soit $A \in \mathcal{M}_n(\mathbb{K})$, on définit le déterminant de A par $\boldsymbol{\det(A) = \sum_{\sigma \in \mathscr{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} A_{\sigma(i),i}}$ on a alors $\det A = \det_b\big(C_1(A), \dots C_n(A)\big)$

$$\boldsymbol{\det(A \times B) = \det(A) \times \det(B)}$$

Poser $\varphi(x_1, \dots, x_n) = (Ax_1, \dots, Ax_n)$ n-linéaire alterné et $\varphi(C_1(B), \dots) = \det(AB)$

- $\det({}^tA) = \det A$
- $\det(BA) = \det(AB)$
- $\det(P^{-1}AP) = \det(A)$
- $\det(P^{-1}) = (\det(P))^{-1}$
- $\det(A^n) = (\det(A))^n$
- $\det(\lambda A) = \lambda^n \det A$
- $\det(T \in T_n(\mathbb{K})) = \displaystyle\sum_{i=1}^{n} T_{i,i}$
- $\det(A_1 \times \ldots \times A_k) = \displaystyle\prod_{i=1}^{k} \det A_k$
- $A \in \mathrm{Gl}_n(\mathbb{K}) \Leftrightarrow \det(A) \neq 0$

Opérations élémentaires : un transvection ne change pas le déterminant, un échange inverse son signe et une dilatation de facteur λ le multiplie par λ.

Déterminant de matrices blocs : on a $\det \begin{bmatrix} A_1 & \cdot & B \\ \vdots & \ddots & \vdots \\ 0 & \cdots & A_n \end{bmatrix} = \displaystyle\prod_{i=1}^{n} \det(A_i)$

On montre les cas $\begin{bmatrix} A & B \\ 0 & I_p \end{bmatrix}$ et $\begin{bmatrix} I_q & B \\ 0 & A \end{bmatrix}$ en posant $\varphi : (x_1, \dots, x_p) \mapsto \det \begin{bmatrix} x_1 | \dots | x_p & B \\ 0 & I_p \end{bmatrix}$, p-linéaire alternée, puis un produit pour se ramener au cas général

Développement par ligne et colonne : pour $A \in \mathcal{M}_n(\mathbb{K})$, et $(i,j) \in [\![1,\ n]\!]$, on note $\widetilde{A_{i,j}}$ la matrice extraite en suppriment la i-ème ligne et la j-ième colonne de A.

$$\boldsymbol{\det(A) = \sum_{k=1}^{n} A_{i,k}(-1)^{i+k} \det(\widetilde{A_{i,k}})} \qquad \boldsymbol{\det(A) = \sum_{k=1}^{n} A_{k,j}(-1)^{k+j} \det(\widetilde{A_{k,j}})}$$

Développer la j-ième colonne sur la base canonique puis utiliser la n-linéarité et permuter les colonnes puis les lignes pour amener le vecteur e_i en haut à droite

Comatrice : pour $A \in \mathcal{M}_n(\mathbb{K})$, on définit la comatrice de A par $\boldsymbol{\mathrm{Com}(A) = \left((-1)^{i+j0} \det(\widetilde{A_{k,j}})\right)_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}}}$, Elle vérifier ${}^t\mathrm{Com}(A)A = A{}^t\mathrm{Com}(A) = \det(A)I_n$, donc si A inversible, $A^{-1} = \frac{1}{\det(A)}{}^t\mathrm{Com}(A)$
Pour $i \neq j$, partir $\det[C_1(A), \ldots, C_i(A), \ldots, C_i(A), \ldots, C_n(A)] = 0$

Systèmes de Crameur : pour $A \in \mathrm{Gl}_n(\mathbb{K})$, $(x,y) \in (\mathbb{K}^n)^2$, il existe unique solution du système $Ax = y : A^{-1}y$. Si on pose pour $j \in [\![1,\ n]\!]$, $A_j = [C_1(A), \ldots, C_{j-1}(A), y, C_{j+1}(A), \ldots$
on a alors $A^{-1}(y) = \dfrac{1}{\det A}\begin{pmatrix} \det(A_1) \\ \vdots \\ \det(A_n) \end{pmatrix}$

Déterminant de Vandermonde : pour $(z_1, \ldots, z_n) \in \mathbb{K}^n$, on a :

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ z_1 & z_2 & \cdots & z_n \\ z_1^2 & z_2^2 & \cdots & z_n^2 \\ \vdots & \vdots & & \vdots \\ z_1^{n-1} & z_2^{n-1} & \cdots & z_n^{n-1} \end{vmatrix} = \prod_{1 \leqslant i < j \leqslant n} (z_j - z_i)$$

Par récurrence, poser $P = \begin{vmatrix} 1 & \cdots & 1 & X^0 \\ \vdots & & \vdots & \vdots \\ z_1^{n-1} & \cdots & z_{n-1}^{n-1} & X^{n-1} \end{vmatrix}$ de degré $n-1$ ayant $n-1$ racines...

24.3 Déterminant d'un endomorphisme en dimension finie

Définition : pour E un $\mathbb{K}$-ev de dimension n, et (b, b') deux bases de E, on a pour $u \in \mathscr{L}(E)$, $\det(\mathcal{M}_b(u)) = \det(\mathcal{M}_{b'}(u))$, on pose donc $\det(u) = \det(\mathcal{M}_b(u))$

- $\det(u \circ v) = \det(u) \times \det(v)$
- $\det(u^k) = \det(u)^k$
- $\det(\lambda u) = \lambda^{\dim E} \det(u)$
- $u \in \mathrm{Gl}(E) \Leftrightarrow \det(u) \neq 0$

Puis pour $(x_1, \ldots, x_n) \in E^n$, $\det(u(x_1),\ \ldots,\ u(x_n)) = \det(u) \times \det(x_1,\ \ldots,\ x_n)$

24.4 Orientation d'une base d'un $\mathbb{R}$ espace vectoriel

Orientation : soit E un $\mathbb{R}$-ev et b et b' deux bases de E on dit que b et b' ont même orientation lorsque $\det{}_b(b') > 0$, C'est une relation d'équivalence dont l'ensemble quotient admet deux éléments. Pour une base de référence b_0, on appelle base directe une base ayant la même orientation que b_0, et indirecte les autres.

25 Équations différentielles

25.1 Équations différentielles à coefficients constants

Équation du premier ordre : soit $a \in \mathbb{K}$ et I un intervalle non trivial de $\mathbb{R}$. L'ensemble solution de l'équation différentielle $\boldsymbol{y' + ay = 0}$ est l'ensemble :

$$\mathscr{S}_E = \left\{ \begin{array}{ccc} I & \to & \mathbb{K} \\ t & \mapsto & \boldsymbol{\lambda e^{-at}} \end{array} , \lambda \in \mathbb{K} \right\} = \{f \in \mathscr{D}(I, \mathbb{K}) \,/\, \forall t \in I, f'(t) + af(t) = 0\}$$

Démo, poser $g = e^{at} f$, $g' = 0$ sur l'intervalle I donc g constante

Équation du premier ordre : soit $a \in \mathbb{K}^*$ et $(b, c) \in \mathbb{K}^2$, on note $P(X) = aX^2 + bX + c$ le polynôme caractéristique de l'équation $\boldsymbol{ay'' + by' + cy = 0}$, et (z_1, z_2) ses solutions. Les solution de l'équation différentielle sont alors :

Cas 1 $\begin{array}{l} z_1 \neq z_2 \\ (z_1, z_2) \in \mathbb{K}^2 \end{array}$ $\quad \mathscr{S}_E = \left\{ \begin{array}{ccc} I & \to & \mathbb{K} \\ t & \mapsto & \boldsymbol{\lambda e^{z_1 t} + \mu e^{z_2 t}} \end{array} , (\lambda, \mu) \in \mathbb{K}^2 \right\}$

Cas 2 $z_1 = z_2$ $\quad \mathscr{S}_E = \left\{ \begin{array}{ccc} I & \to & \mathbb{K} \\ t & \mapsto & \boldsymbol{(\lambda + \mu t) e^{z_1 t}} \end{array} , (\lambda, \mu) \in \mathbb{K}^2 \right\}$

Cas 3 $\begin{array}{l} \mathbb{K} = \mathbb{R} \\ (z_1, z_2) \in (\mathbb{C} \setminus \mathbb{R})^2 \end{array}$ $\quad \mathscr{S}_E = \left\{ \begin{array}{ccc} I & \to & \mathbb{K} \\ t & \mapsto & \boldsymbol{e^{rt}\big(\lambda \cos(\omega t) + \mu \sin(\omega t)\big)} \end{array} , (\lambda, \mu) \in \mathbb{R}^2 \right\}$

Poser $g = e^{z_1 t} f$, on a $ag''(t) + P'(z_1)g'(t) + P(z_1)g(t) = 0$, donc...

Dimension des ensembles : pour une équation du premier ordre, $\mathscr{S}_E$ est un sev de $\mathbb{K}^I$ de dimension 1, et de dimension 2 pour un équation de second ordre (liberté des familles génératrices)

25.2 Premier ordre : coefficients non-constants

Résolution : soit $(a, b) \in \mathscr{C}(I, \mathbb{K})^2$, on veut résoudre $\boldsymbol{y' + a(t)y = b(t)}$, il existe $A \in \mathscr{C}^2(I, \mathbb{K})$ une primitive de a. Soit $f \in \mathscr{D}(I, \mathbb{K})$, $g : t \mapsto f(t)e^{A(t)}$ dérivable et $g' = t \mapsto e^{A(t)}(f'(t) + a(t)f(t))$, on en déduit que

$$\mathscr{S}_E = \left\{ \begin{array}{ccc} I & \to & \mathbb{K} \\ t & \mapsto & \boldsymbol{e^{-A(t)} \int_{t_0}^{t} e^{A(s)} b(s) \,\mathrm{d}s + \lambda e^{-A(t)}} \end{array} , \lambda \in \mathbb{K} \right\}$$

Solution homogène et particulière : $y' + a(t)y = 0$ est l'équation homogène associé. Son ensemble solution est un sev de dimension 1, pour f_0 une solution non nulle de (E_H) et f_1 un solution particulière de (E), on a $\mathscr{S}_H = \{\lambda f_0, \lambda \in \mathbb{K}\}$ et $\mathscr{S}_E = \{\lambda f_0 + f_1, \lambda \in \mathbb{K}\}$

Pour b_1, b_2 continue et f_1, f_2 solution de $E_h = b_1(t)$ et $E_h = b_2(t)$, on a $\lambda f_1 + \mu f_2$ est solution de $y' + a(t)y = \lambda b_1(t) + \mu b_2(t)$

Problème de Cauchy : pour $t_0 \in I$ et $y_0 \in \mathbb{K}$, le système $\begin{cases} y' + a(t)y = b(t) \\ y(t_0) = y_0 \end{cases}$ admet un unique solution. On en déduit que les graphes de solutions sont disjoints sur I, (et donc supérieurs ou inférieurs partout si $\mathbb{K} = \mathbb{R}$)

Méthode de variation de la constante : résoudre l'équation homogène en la transformant en $\frac{y'}{y} = a(t)$ donc $\ln(y) = A(t)$, puis à partir de la solution, transformer la constante en fonction pour trouver une solution particulière.

Raccord : pour une équation du style $a(t)y' + y = b(t)$ ou a s'annule sur $\mathbb{R}$, on résoud l'équation sur $\mathbb{R} \setminus \{\text{zéros de } a\}$, et on raisonne pas CN/CS en exploitant la dérivabilité et contiuité au point de raccord.

25.3 Second ordre : coefficient constant et second membre

Résolution : pour $ay'' + by' + cy = d(t), a \neq 0, d \in \mathscr{C}(I, \mathbb{K})$ si on a (f_0, f_1) une base de l'ensemble solution de l'équation homogène et f_2 une solution particulière, alors $\boldsymbol{\mathscr{S}_E = \{f_2 + \lambda f_0 + \mu f_1, (\lambda, \mu) \in \mathbb{K}^2\}}$

Solution particulière de $ay'' + by' + cy = Ae^{\lambda t}$: On pose $P = aX^2 + bX + c$.

— Cas $P(\lambda) \neq 0$, alors $t \mapsto \frac{A}{P(\lambda)} e^{\lambda t} \in \mathscr{S}_E$

— Cas $P(\lambda) = 0, P'(\lambda) \neq 0$, alors $t \mapsto \frac{A}{P'(\lambda)} te^{\lambda t} \in \mathscr{S}_E$

— Cas $P(\lambda) = 0, P'(\lambda) = 0, P''(\lambda) \neq 0$, alors $t \mapsto \frac{A}{P''(\lambda)} t^2 e^{\lambda t} \in \mathscr{S}_E$

Solution particulière de $ay'' + by' + cy = A\sin(\omega t)$: pour $(a, b, c) \in \mathbb{R}$, on pour φ une solution de $ay'' + by + c = Ae^{i\omega t}$, on a $\Re(\varphi)$ solution de $ay'' + by + c = A\cos(\omega t)$ et $\Im(\varphi)$ solution de $ay'' + by + c = A\sin(\omega t)$

Problème de Cauchy d'ordre 2 : soit $a \in \mathbb{R}^*$, $(b, c) \in \mathbb{R}^2$, $d \in \mathscr{C}(I, \mathbb{K})$, $t_0 \in I$ et $(y_0, v_0) \in \mathbb{K}^2$ le système $\begin{cases} ay'' + by + c = d(t) \\ y(t_0) = y_0 \\ y'(t_0) = v_0 \end{cases}$ admet une unique solution.

26 Espaces euclidiens

26.1 Produit scalaire

Définition : soit E un $\mathbb{R}$-ev, $\varphi : E^2 \to \mathbb{R}$, est un produit scalaire sur E si elle est :
- bilinéaire (linéaire par rapport au deux variable)
- symétrique ($\forall (x,y) \in E^2, \varphi(x,y) = \varphi(y,x)$)
- positive ($\forall x \in E, \varphi(x,x) \geqslant 0$)
- définie ($\forall x \in E, \varphi(x,x) = 0_{\mathbb{R}} \Leftrightarrow x = 0_E$)

On dit que (E,φ) est un espace préhilbertien réel, ou euclidien si E est de dimension finie.
On définit la norme euclidienne de $x \in E$ par $\|x\| = \sqrt{\varphi(x,x)}$

Exemple : $\begin{pmatrix} (\mathbb{R}^n)^2 & \to & \mathbb{R} \\ ((x_i),(y_i)) & \mapsto & \sum_{i=1}^n x_i y_i \end{pmatrix}$ et $\begin{pmatrix} \mathscr{C}([a,b],\mathbb{R}) & \to & \mathbb{R} \\ (f,g) & \mapsto & \int_a^b f(t)g(t)\mathrm{d}t \end{pmatrix}$

Propriétés : si φ est un produit scalaire alors pour tout $(x,y) \in E^2$

- $\forall \lambda \in \mathbb{R}, \|\lambda x\| = |\lambda| \, \|\overrightarrow{x}\|$
- $\forall x \in E \setminus \{0_E\}, \|x\| > 0$
- Inégalité de Cauchy Schwarz : $\begin{cases} \boldsymbol{\varphi(x,y) \leqslant \|x\| \times \|y\|} \\ \varphi(x,y) = \|x\| \times \|y\| \Leftrightarrow (x,y) \text{ est liée} \end{cases}$
- Inégalité triangulaire : $\begin{cases} \boldsymbol{\|x+y\| \leqslant \|x\| + \|y\|} \text{ et } \boldsymbol{|\|x\| - \|y\|| \leqslant \|x \pm y\|} \\ \|x+y\| \leqslant \|x\| + \|y\| \Leftrightarrow \exists \lambda \in \mathbb{R}^+, x = \lambda y \text{ ou } y = \lambda x \end{cases}$

Pour CS : $y \neq 0_E$, partir de $\varphi(x+ty, x+ty) \geqslant 0$ et développer. On a également :

- $\|x+y\|^2 = \|x\|^2 + \|y\|^2 + 2\varphi(x,y)$
- $\|x-y\|^2 = \|x\|^2 + \|y\|^2 - 2\varphi(x,y)$
- $\|x+y\|^2 + \|x-y\|^2 = \|x\|^2 + \|y\|^2$
- $\varphi(x,y) = \frac{1}{2}(\|x+y\|^2 - \|x\|^2 - \|y\|^2)$
- $\varphi(x,y) = \frac{1}{2}(\|x\|^2 + \|y\|^2 - \|x+y\|)$
- $\varphi(x,y) = \frac{1}{2}(\|x+y\|^2 - \|x-y\|^2)$
- $\|e_1 + \ldots + e_n\|^2 = \sum_{i=1}^n \|e_i\|^2 + 2\sum_{1 \leqslant i < j \leqslant n} \varphi(e_i, e_j)$

26.2 Orthogonalité

Définition : soit $(E, \langle \cdot, \cdot \rangle)$ un espace préhilbertien réel, $(x,y) \in E^2$, F et G des sev et $(A,B) \in \mathscr{P}(E)^2$,
- x et y sont *orthogonaux* lorsque $\langle x, y \rangle = 0_{\mathbb{R}}$
- x est *unitaire* lorsque $\|x\| = 1_{\mathbb{R}}$
- F et G sont *orthogonaux* lorsque $\forall (f,g) \in F \times G, \langle f, g \rangle = 0_{\mathbb{R}}$
- on définit l'*orthogonal* de A : $A^\perp = \{u \in E \,/\, \forall a \in A, \langle u, a \rangle = 0_{\mathbb{R}}\}$
- (e_i) est une *famille orthogonale* lorsque $\forall (i,j) \in I^2, i \neq j \Rightarrow \langle e_i, e_j \rangle = 0_{\mathbb{R}}$
- (e_i) est une famille orthonormée lorsque $\forall (i,j) \in I^2, \langle e_i, e_j \rangle = \delta_{i,j}$
- si $F \oplus F^\perp$, on définit le *projecteur orthogonal* à F : $p_{F,F^\perp}$
- $p \in \mathscr{L}(E)$ est un projecteur orthogonal si $p^2 = p$ et $\mathrm{Im}(p) = \mathrm{Ker}(p)^\perp$

Propriétés : on a alors :
- le seul vecteur orthogonal à tout autre ou/et à lui même est nul
- pour $F_1, \dots, F_p$ 2-à-2 orthogonaux, $F_1 \oplus \dots \oplus F_p$ existe
- pour $A \subset B \subset E$, $A^\perp$ est un sev de E et $B^\perp \subset A^\perp$
- pour (e_i) orthogonale et $(\lambda_i) \in \mathbb{R}^{(I)}$, $\left\|\sum_{i\in I} \lambda_i e_i\right\|^2 = \sum_{i\in I} \|e_i\|^2$
- une famille (e_i) orthogonale de vecteurs non-nuls est libre.
- pour F un sev de E, $F \oplus F^\perp$ existe
- pour G un sev de E, $\boldsymbol{G \perp F}$ et $\boldsymbol{G \oplus F = E \Rightarrow G = F^\perp}$

Base orthonormée : soit E un espace préhilbertien, on suppose qu'il existe $b = (e_i)_{i\in I}$ une base orthonormée de E. On a alors pour $(x, y) \in E^2$,

$$x = \sum_{i\in I} \langle x,\, e_i\rangle\, e_i \quad \text{et} \quad \langle x,\, y\rangle = \sum_{i\in I} \langle x,\, e_i\rangle \langle y,\, e_i\rangle$$

$x = \sum_{i\in I} \lambda_i e_i$, donc $\langle x,\, e_i\rangle = \lambda_i$ par orthogonalité de b
Pour F un sev de E vérifiant $F \oplus F^\perp = E$, et admettant une base orthonormée $(e_i)_{i\in I}$, p_F la projection orthonormale à F existe alors.

$$\forall x \in E,\ p_F(x) = \sum_{i\in I} \langle x,\, e_i\rangle\, e_i \text{ et } p_{F^\perp}(x) = x - \sum_{i\in I} \langle x,\, e_i\rangle\, e_i$$

Si la base n'est pas normée, on a $\frac{\langle x, e_i\rangle}{\|e_i\|^2} e_i$

Existence d'une base orthonormée : tout espace euclidien réel (muni du produit scalaire et de dimension fini) admet au moins une base orthonormale

() pour $E = \{0_E\}$, $\frac{e}{\|e\|} \in E \setminus \{0\}$ si $\dim E = 1$, puis par récurrence sur $\dim E$, prendre $e \in E^*$, $H = \{e\}^\perp = \mathrm{Ker}(\langle e, \cdot\rangle)$ est un hyperplan orthogonal à $\mathrm{Vect}(e)$ donc...

Sev de dimension fini : soit E un espace préhilbertien réel, et F un sev de E de dimension finie, on a $F \oplus F^\perp = E$
$\supset \exists (e_i)$ base orthonormé de $F, \forall x \in E, \forall e \in F, \left\langle x - \sum_{i\in I} \langle x,\, e_i\rangle\, e_i,\, e\right\rangle = \dots$

Base orthogonale incomplète : soit E un espace euclidien et $(e_1, \dots, e_p)$ une famille orthogonale de E. Il existe $(e_{p+1}, \dots, e_n) \in E^{n-p}$ tel que $(e_1, \dots, e_n)$ soit une base de E. (Base du supplémentaire orthogonal...)

Distance à un sous-espace vectoriel : soit E un espace préhilbertien réel et F un sev de E. Pour $x \in E$, on définit la distance de x à F par : $\boldsymbol{\mathrm{d}(x, F) = \inf\{\|x - e\|,\, e \in F\}}$
Si $F \oplus F^\perp = E$, alors $\boldsymbol{\mathrm{d}(x, F) = \|x - p_F(x)\|}$ car $\|x - p_F(x) + p_F(x) - e\| = \dots$
De plus pour $e \in F$, $\|x - e\| = \mathrm{d}(x, F) \Leftrightarrow e = p_F(x)$

Procédé de Gram-Schmitt : soit E un eph, et $(e_1, \dots, e_p)$ une famille libre de E

$$\text{on pose : } \begin{cases} F_1 = \text{Vect}(e_1) & u_1 = \frac{e_1}{\|e_1\|} \\ \forall k \in [\![2, p]\!] \quad F_k = \text{Vect}(e_1, \dots, e_k) & u_k = \frac{e_1 - p_{F_{k-1}}(e_1)}{\left\|e_1 - p_{F_{k-1}}(e_1)\right\|} \end{cases}$$

Alors $(u_1, \dots, u_k)$ est l'unique famille orthonormé qui vérifie $\forall k \in [\![1, p]\!]$, $F_k = \text{Vect}(u_1, \dots, u_k)$ et $\langle e_k, u_k \rangle > 0$. $(u_1, \dots, u_k)$ et $(e_1, \dots, e_k)$ ont même orientation. Démo par récurrence forte, $\exists$ en mq $u_k \in F_{k+1}^\perp$, unicité en utilisant la norme.

26.3 Endomorphismes remarquables d'un espace euclidien

Isométrie vectorielle : $\varphi \in \mathscr{L}(E)$ est un isométrie vectorielle lorsque :

$$\boldsymbol{\forall x \in E,\ \|\varphi(x)\| = \|x\|}$$

On note $\mathcal{O}(E)$ le groupe orthogonal de E, l'ensemble des isométries, c'est un sous-groupe de $(\text{Gl}(E), \circ)$

Caractérisation : soit $\varphi \in \mathscr{L}(E)$, on a les équivalences :

1. $\varphi \in \mathcal{O}(E)$
2. $\forall (x, y) \in E^2, \langle \varphi(x), \varphi(y) \rangle = \langle x, y \rangle$
3. $\forall b$ b.o.n. de $E, \varphi(b)$ est une b.o.n. de E
4. $\exists b$ b.o.n. de $E, \varphi(b)$ est une b.o.n. de E

Symétrie orthogonale : soit F un sev de E, tel que $F \oplus F^\perp = E$, on appelle symétrie orthogonale d'axe F la symétrie d'axe F parallèlement à $F^\perp$. Lorsque F est un hyperplan on parle de réflexion d'axe F.

Une symétrie $(s \in \mathscr{L}(E), s^2 = \text{id}_E)$ est orthogonale si $\text{Ker}(s - \text{id}_E)^\perp = \text{Ker}(s + \text{id}_E)$

Matrice orthogonales : une matrice A est orthogonale si elle vérifie $\boldsymbol{{}^tAA = I_n}$ ou $\boldsymbol{A\,{}^tA = I_n}$.

On note $\mathcal{O}_n(\mathbb{R})$ ou $\mathcal{O}(n)$ le groupe des matrice orthogonale, c'est un sous-groupe de $(\text{Gl}_n(\mathbb{R}), \times)$.

Caractérisation : soit $A \in \mathcal{M}_n(\mathbb{R})$ et φ son ALCA, on a les équivalences

1. $A \in \mathcal{O}_n(\mathbb{R})$
2. $\big(C_1(A), \dots, C_n(A)$ est une bon de $\mathbb{R}^n$
3. $\varphi_A \in \mathcal{O}(E)$
4. ${}^tA \in \mathcal{O}_n(\mathbb{R})$
5. $\big(L_1(A), \dots, L_n(A)$ est une bon de $\mathbb{R}^n$

Conservation de la norme car $\|Ax\| = \sqrt{\sum (Ax)_{k,1}(Ax)_{k,1}} = \sqrt{\sum ({}^tx\,{}^tA)_{1,k}(Ax)_{k,1}}$

Déterminant : soit $A \in \mathcal{O}_n(\mathbb{R})$, on a $\det A \in \{-1, 1\}$. On définit alors le groupe spécial orthogonale $\mathcal{SO}_n(\mathbb{R}) = \{A \in \mathcal{O}_n(\mathbb{R}) \,/\, \det A = 1\}$. C'est un sous-groupe de $(\mathcal{O}_n(\mathbb{R}), \times)$ non-commutatif si $n \geqslant 3$. Ses éléments sont appelés matrice de rotation.

Lien entre $\mathcal{O}(E)$ et $\mathcal{O}_n(\mathbb{R})$: soit E un espace euclidien de dimension n, $u \in \mathscr{L}(E)$, b une base orthonormée de E et b' un famille de n vecteurs de E. On

$$\boldsymbol{u \in \mathcal{O}(E) \Leftrightarrow \mathcal{M}_b(u) \in \mathcal{O}_n(\mathbb{K})}$$
$$b' \text{ est une bon de } E \Leftrightarrow \mathcal{M}_b(b') \in \mathcal{O}_n(\mathbb{R})$$

$\mathcal{M}_b(u)$ est la matrice $\langle u(e_i), e_j \rangle$ (faire apparaitre le $\langle \cdot, \cdot \rangle$ des colonnes dans $\mathbb{R}^n$
Si b et b' sont deux bon de E, $P_b^{b'} \in \mathcal{O}_n(\mathbb{R})$ et $P_{b'}^b = (P_b^{b'})^{-1} = {}^t(P_b^{b'})$

Isométrie positives/négatives : on a $\forall u \in \mathcal{O}(E), \det(u) \in \{-1, 1\}$
- si $\det(u) = 1$, on parle d'isométrie positive/directe ou de rotation, on note $\mathcal{SO}(E)$ le groupe des rotations (sous groupe de $(\mathcal{O}(E), \times)$)
- si $\det(u) = -1$, on parle d'isométrie négative/indirecte

Pour b une bon de E, $\begin{pmatrix} \mathcal{O}(E) & \to & \mathcal{O}_n(\mathbb{R}) \\ u & \mapsto & \mathcal{M}_b(u) \end{pmatrix}$ et $\begin{pmatrix} \mathcal{SO}(E) & \to & \mathcal{SO}_n(\mathbb{R}) \\ u & \mapsto & \mathcal{M}_b(u) \end{pmatrix}$ sont des isomorphismes de groupe.

Orientation : on oriente E par le choix d'une base de référence. Il existe b un base orthonormée directe de E, pour b' une famille de n vecteurs de E, on a

$$b' \text{ est une base orthonormée directe } \Leftrightarrow \mathcal{M}_b(b') \in \mathcal{SO}(E)$$

Produit mixte : soit $v_1, \ldots, v_n \in E^n$ on définit le produit mixte $\boldsymbol{[v_1, \ldots, v_n] = \det_b(v_1, \ldots, v_n)}$ avec b une base orthonormé directe de E. (Bonne définition car indépendant de la base grâce au caractère n-linéaire alterné de det)

Cas de la dimension 2 : soit E un plan euclidien, on connait les ensembles $\mathcal{SO}_2(\mathbb{R})$ et $\mathcal{O}_2^-(\mathbb{R})$

$$\mathcal{SO}_2(\mathbb{R}) = \left\{ \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \theta \in \mathbb{R} \right\} \qquad \mathcal{O}_2^-(\mathbb{R}) = \left\{ \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}, \theta \in \mathbb{R} \right\}$$

De plus $R(\theta)$: $\begin{pmatrix} (\mathbb{R}, +) & \to & (\mathcal{SO}_2(\mathbb{R}), \times) \\ \theta & \mapsto & \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \end{pmatrix}$ et $\begin{pmatrix} (\mathbb{U}, \times) & \to & (\mathcal{SO}_2(\mathbb{R}), \times) \\ z & \mapsto & \begin{pmatrix} \Re(z) & -\Im(z) \\ \Im(z) & \Re(z) \end{pmatrix} \end{pmatrix}$ sont des morphisme de groupe (respectivement surjectif de noyau $2\pi\mathbb{Z}$ et bijectif)
Utiliser l'orthonormalité des colonnes pour trouver θ

Lien avec $\mathcal{O}(E)$: on en déduit une caractérisation de $\mathcal{SO}(E)$ et $\mathcal{O}^-(E)$
- $\mathcal{O}(E) \setminus \mathcal{SO}(E) = \{\text{réflexions de } E\}$
- $\forall f \in \mathcal{SO}(E), \exists \theta \in \mathbb{R}, \forall b \text{ bon de } E, \mathcal{M}_b(f) = R(\theta)$

$f \in \mathcal{O}^-(E)$ vérifier $f^2 = \mathrm{id}_E$..., changement de base et le morphisme $R(\theta)$ pour $\mathcal{SO}(E)$

Angle orienté : soit E un plan euclidien, $(x, y) \in (E \setminus \{0_E\})^2$, il existe un unique fonction $f \in \mathcal{SO}(E)$ vérifiant : $f\left(\frac{x}{\|x\|}\right) = \frac{y}{\|y\|}$. (Compléter les bond $\frac{x}{\|x\|}$ et $\frac{y}{\|y\|}$ pour l'existence, l'unicité découle de la caractérisation ci-dessus). Il existe θ unique modulo 2π telle que $f = R(\theta)$. On définit $\boldsymbol{(\widehat{x, y}) = \theta}$ l'angle orienté entre x et y.
Dans un espace euclidien, on définit l'angle non-orienté par $\arccos\left(\frac{\langle x, y\rangle}{\|x\|\|y\|}\right)$
Dans un plan, $(\widehat{x, y}) = \pm \arccos\left(\frac{\langle x, y\rangle}{\|x\|\|y\|}\right)$
Finalement $\langle x,\, y\rangle = \|x\|\,\|y\| \cos(\widehat{x, y})$ et $[x, y] = \|x\|\,\|y\| \sin(\widehat{x, y})$

27 Probabilités

27.1 Probabilité sur un ensemble fini

Vocabulaire : soit Ω un ensemble fini appelé univers
- $\mathcal{P}(\Omega)$ est appelé tribu des évènements, ses éléments sont des évènements
- Ω est l'évènement certain, $\emptyset$ l'évènement impossible
- un singleton est un évènement élémentaire
- deux évènements d'intersection vide sont incompatibles
- $(A_i)_{i\in I} \in \mathcal{P}(\Omega)^I$ est un système complet d'évènements lorsque : $A_i \cap A_j = \emptyset$ et $\bigcup_{i\in I} A_i = \Omega$

Probabilité sur un ensemble fini : pour $\Omega \neq \emptyset$, on dit que P est une mesure de probabilité lorsque :
- P est une fonction de $\mathcal{P}(\Omega) \to [0,\, 1]$
- $P(\Omega) = 1$
- $\forall (A, B) \in \mathcal{P}(\Omega)^2,\ \boldsymbol{A \cap B = \emptyset \Rightarrow P(A \cup B) = P(A) + P(B)}$

Propriétés : pour P une probabilité définie sur Ω, $(A, B) \in \mathcal{P}(\Omega)^2$ et (B_i) un système complet d'évènements :

- $P(\emptyset) = 0$
- $P(\overline{A}) = 1 - P(A)$
- $P(A \cup B) = P(A) + P(B) - P(A \cap B)$
- $B \subset A \Rightarrow P(B) \leqslant P(A)$
- $\forall (A_i)_{i\in I} \in \mathcal{P}(\Omega)^I, P\left(\bigcup_{i\in I} A_i\right) \leqslant \sum_{i\in I} P(A_i)$ (la réunion disjointe implique l'égalité)
- $P(A) = \sum_i P(A \cap B_i)$
- $P(A) = \sum_{a\in A} P(\{a\})$

Démo en se ramenant à des réunions disjointes.
Si $P(A) = 0$ on dit que A est négligeable, si $P(A) = 1$, A est presque sûr.

Construction d'une probabilité : pour $\omega \in \Omega$, on associe $t_\omega \in [0, 1]$, $\sum_{\omega\in\Omega} t_\omega = 1$. Il existe alors une unique mesure de probabilité P vérifiant $\forall \omega \in \Omega, P(\{\omega\}) = t_\omega$
Unicité grâc à la réunion disjointe, existence déjà définie...

Probabilité conditionnelle : soit B un évènement non négligeable, on définit la probabilité sachant B par $P(A\,|B) = \boldsymbol{P_B(A) = \dfrac{P(A \cap B)}{P(B)}}$. C'est une autre mesure de probabilité. Elle vérifie

— formule des probabilités composées : pour $(A_i)_{i\in[\![1,\,p]\!]}$, $P(A_1 \cap \ldots \cap A_{p-1}) \neq 0$:

$$P(A_1 \cap \ldots A_p) = P(A_1) \times P_{A_1}(A_2) \times P_{A_1\cap A_2}(A_3) \times \ldots \times P_{A_1\cap \ldots A_{p-1}}(A_p)$$

— formule des probabilités totales, pour $(B_i)_{i\in I}$ un système complet d'évènements

$$P(A) = \sum_{i\in I} P(B_i) \times P_{B_i}(A_i)$$

— formules de Baizes : pour A et B non négligeables : $P_B(A) = \dfrac{P(A)}{P(B)} P_A(B)$

Indépendance : deux évènements A et B sont indépendant lorsque $\boldsymbol{P(A \cap B) = P(A) \times P(B)}$, c'est-à-dire lorsque $P(B) = 0$ ou $[P(B) \neq 0$ et $P(A) = P_B(A)]$
Une famille $(A_i)_{i\in I}$ est mutuellement indépendante lorsque

$$\forall J \in \mathcal{P}(I),\ P\left(\bigcap_{j\in J} A_j\right) = \prod_{j\in J} P(A_j)$$

L'indépendance mutuelle implique l'indépendance 2-à-2. Si $(A_1,\,\ldots,\,A_n)$ est mutuellement indépendante, alors toute liste $(B_1,\,\ldots,\,B_n) \in \left\{A_1, \overline{A_1}\right\} \times \ldots \times \left\{A_n, \overline{A_n}\right\}$ l'est également (preuve par récurrence).

27.2 Variables aléatoires

Définition : une variable aléatoire est une fonction X de Ω vers un ensemble E. X est une variable aléatoire réelle lorsque $X(\Omega) \subset \mathbb{R}$. Pour Y, Z deux variables aléatoires, $(Y, Z) : \omega \mapsto (Y(\omega), Z(\omega))$ est aussi une variable aléatoire.
Si f est une fonction définie sur $Y(\Omega)$, $f(Y) = \omega \mapsto f(Y(\omega))$ est aussi une variable aléatoire.

Évènements : pour $Y : \Omega \to E$ une variable aléatoire, $e \in E$, on définit l'évènement $\{Y = e\} = \{\omega \in \Omega\,/\,Y(\omega) = e\}$, de même on définit pour $A \subset E$ l'évènement $\{Y \in A\}$. Dans le cas réel, on définit aussi $\{Y \geqslant e\}$ ...
La famille $(\{Y = e\})_{e\in E}$ est la famille des évènements élémentaires de E. On définit la probabilité $P^Y : \left\{\begin{array}{ccc} \mathcal{P}(E) & \to & [0,\,1] \\ A & \mapsto & P(\{Y \in A\}) \end{array}\right.$. C'est une mesure de probabilité sur E appelé loi de Y. Deux variables X et Y ont la même loi, noté $X \sim Y$ lorsqu'il existe E fini tel que $\left\{\begin{array}{l} X(\Omega) \cup Y(\Omega) \subset E \\ \forall e \in E, P(\{X = e\}) = P(\{Y = e\}) \end{array}\right.$

Loi conjointe, loi marginale : soit X_1, X_2 deux variables aléatoires et $Z = (X_1, X_2)$, on appelle loi conjointe la loi de Z et loi marginales les loi de X_1 et X_2, on peut retrouver les lois marginales à partir de la loi conjointe $P(X_1 = e) = \sum_{y \in X_2(\Omega)} P(Z = (e, y))$. On ne peut pas en revanche déterminer la loi conjointe à partir des lois marginales.

Composition : soit X_1, X_2 deux variables aléatoire à valeurs dans E, et $f : E \to F$, si $X_1 \sim X_2$ alors $f(X_1) \sim f(X_2)$

Somme de variables : pour X_1, X_2 deux variables aléatoire réelles et $Z = X_1 + X_2$, la loi de (X_1, X_2) détermine la loi de Z : $P(Z = z) = \sum_{x \in \Omega(X_1)} P\big((X_1, X_2) = (x, z - x)\big)$

Nom	Paramètres	Symbole	$X(\Omega) \subset \bullet$	Probabilité
De Bernouilli	$p \in [0,\ 1]$	$\mathscr{B}(p)$	$\{0,\ 1\}$	$P(X = 1) = p$ $P(X = 0) = 1 - p$
Uniforme	Ensemble fini E	$\mathscr{U}(E)$	E	$P(X = e) = \dfrac{1}{\#E}$
Binomiale	$n \in \mathbb{N}, p \in [0, 1]$	$\mathscr{B}(n, p)$	$[\![0,\ n]\!]$	$P(X = k) = \begin{pmatrix} k \\ n \end{pmatrix} p^k (1-p)^{n-k}$

TABLE 8 – Lois de probabilités usuelles sur un ensemble fini

Indépendance : des variables aléatoires $X_1, \ldots, X_n$ sont mutuellement indépendantes lorsque l'une des propriétés équivalentes suivante est vérifié :
- $\forall (A_i) \in \prod \mathcal{P}(X_i(\Omega)),\ \{X_1 \in A_1\}, \ldots, \{X_n \in A_n\}$ mutuellement indépendants.
- $\forall (A_i) \in \prod \mathcal{P}(X_i(\Omega)),\ P(\bigcap_{i=1}^n \{X_i \in A_i\}) = \prod_{i=1}^n P(X_i = A_i)$
- $\forall (e_i) \in \prod X_i(\Omega)),\ P(\bigcap_{i=1}^n \{X_i = e_i\}) = \prod_{i=1}^n P(X_i = e_i)$

$3 \Rightarrow 1$ en décomposant A_i comme union d'évènements élémentaires. Si $X_1, \ldots, X_n$ sont mutuellement indépendants, $\forall J \subset [\![1,\ n]\!]$, $(X_j)_{j \in J}$ sont mutuellement indépendante. Et pour $f_1, \ldots, f_n$, $f_1(X_1), \ldots, f_n(X_n)$ mutuellement indépendante.

Loi binomiale : si $X_1, \ldots, X_n$ sont des variables aléatoires suivant la loi de Bernouilli de paramètre p, alors $X_1 + \ldots + X_n \sim \mathscr{B}(n, p)$

ESPÉRANCE, VARIANCE, COVARIANCE : soit X une variable aléatoire, on définit :

- l'espérance de X : $\mathbb{E}(X) = \sum_{x \in X(\Omega)} x P(X = x)$
- la variance de X : $\mathbb{V}(X) = \mathbb{E}\big((X - \mathbb{E}(X))^2\big)$
- la cavariance de X et Y : $\mathrm{Cov}(X, Y) = \mathbb{E}\big((X - \mathbb{E}(X))(Y - \mathbb{E}(Y)\big)$

Linéarité de l'espérance : on a pour X, Y des variables aléatoire réelles, $(\lambda, \mu) \in \mathbb{R}^2$, $\mathbb{E}(\lambda X + \mu Y) = \lambda \mathbb{E}(X) + \mu \mathbb{E}(Y)$
De plus, pour $f : X(\Omega) \to \mathbb{R}$, $\mathbb{E}(f(X)) = \sum_{x \in X(\Omega)} f(x) P(X = x)$

Variance : On en déduit que $V(X) = \mathbb{E}(X^2) - (\mathbb{E}(X))^2$, d'où les relations suivantes : (étudier $\mathbb{E}(X(X-1))$ pour $\mathscr{B}(n,p)$. on appelle moment d'ordre k de X le réal $\mathbb{E}(X^k)$

Loi	$\mathscr{B}(p)$	$\mathscr{U}(\llbracket 1,\ n \rrbracket)$	$\mathscr{B}(n,p)$
Espérance	p	$\frac{n+1}{2}$	np
Variance	$p(1-p)$	$\frac{n^2-1}{12}$	$np(1-p)$

TABLE 9 – Espérance et variance des lois usuelles

Propriétés de calcul : pour (X,Y) des variables aléatoires réelles :

- $\mathbb{V}(\alpha X + \beta) = \alpha^2 \mathbb{V}(X)$
- $\mathrm{Cov}(\cdot,\ \cdot)$ bilinéaire symétrique
- $\mathrm{Cov}(X,Y) = \mathbb{E}(X \times Y) - \mathbb{E}(X)\mathbb{E}(Y)$
- $\mathbb{V}\left(\sum_{i=1}^{n} X_i\right) = \sum_{i=1}^{n} \mathbb{V}(X_i) + 2\sum_{1 \leqslant i < j \leqslant n} \mathrm{Cov}(X_i, X_j)$

Si les variables sont indépendantes :

- $\begin{cases} \mathrm{Cov}(X,Y) = 0 \\ \mathbb{E}(X \times Y) = \mathbb{E}(X)\mathbb{E}(Y) \end{cases}$
- $\mathbb{V}\left(\sum_{i=1}^{n} X_i\right) = \sum_{i=1}^{n} \mathbb{V}(X_i)$

Inégalités remarquables : pour (X,Y) deux variables aléatoires réelles :

— $X \geqslant 0 \Rightarrow \mathbb{E}(X) \geqslant 0$ et $X \geqslant Y \Rightarrow \mathbb{E}(X) \geqslant \mathbb{E}(Y)$

— $\mathbb{V}(X) \geqslant 0$ ce qui permet de définir l'écart-type $\sigma(X) = \sqrt{\mathbb{V}(X)}$

— $\boldsymbol{X \geqslant 0 \Rightarrow \forall \varepsilon > 0,\ P(X \geqslant \varepsilon) \leqslant \dfrac{\mathbb{E}(X)}{\varepsilon}}$ (inégalité de Markov)

— $\boldsymbol{\forall \varepsilon > 0,\ P(|X - \mathbb{E}(X)| \geqslant \varepsilon) \leqslant \dfrac{\mathbb{V}(X)}{\varepsilon^2}}$ (inégalité de Bienaymé-Tchebytchev)

On montre Markov en posant $A = \{\omega \in \Omega \,/\, X(\omega) \geqslant \epsilon\}$ puis étudiant $\mathbb{1}_A$.

Remarque : $\begin{cases} \mathbb{E}(X) = 0 \text{ et } X \geqslant 0 \Leftrightarrow P(X=0) = 1 \text{ et } X \geqslant 0 \\ \mathbb{V}(X) = 0 \Leftrightarrow \exists \mu \in \mathbb{R}, P(X = \mu) = 1 \end{cases}$

Variables centrées et réduites : X est une variable aléatoire réelle.On dit que X est *centrée* lorsque $\mathbb{E}(X) = 0$ et *réduite* lorsque $\mathbb{V}(X) = 1$

$X - E(X)$ est une variable centré, et, si $\mathbb{V}(X) > 0$, $\frac{X - \mathbb{E}(X)}{\sqrt{\mathbb{V}(X)}}$ est centré réduite.

Loi conditionnelle : soit X et Y deux variables aléatoire, et $Y \in Y(\Omega)$ tel que $P(Y = y) \neq 0$, alors $(\Omega, \mathcal{P}(\Omega), P_{\{Y=y\}})$ est un espace probabilisé fini et la loi de X sur cette espace est appelé loi conditionnelle sachant $\{Y = y\}$

28 Séries numériques :

28.1 Généralités

Définition : $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$,soit $(u_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$. La sérié numérique de terme général u_n, noté $\sum u_n$ est le couple $\big((u_n)_{n\in\mathbb{N}}, (\sum_{i=0}^{n} u_i)_{n\in\mathbb{N}}\big)$. On appelle la suite $(\sum_{i=0}^{n} u_i)_{n\in\mathbb{N}}$ somme partielle de la série $\sum u_n$

Nature d'un série : on dit qu'une série est convergente si sa somme partielle est convergente. Elle est divergente sinon. On ne change pas la nature d'un série en modifiant, ajoutant ou supprimant un nombre fini de terme.
Exemple : $\sum z^n$ est convergente si et seulement si $|z| < 1$, $\sum \frac{1}{n}$ diverge.

Somme et reste d'une série convergente : soit $\sum u_n$ une série *convergente*. On définit la somme S de la série

$$\sum_{k=0}^{+\infty} u_k = \lim_{n\to+\infty} \sum_{k=0}^{n} u_k$$

Pour $N \in \mathbb{N}$, le reste R_N de la série est $\sum_{k=N+1}^{+\infty} u_k$, on a $S = S_N + R_N$ et $R_N \xrightarrow[n\to+\infty]{} 0$

Opérations sur les séries convergentes : soit $\sum u_n$ et $\sum v_n$ deux séries convergentes, et $(\alpha, \beta) \in \mathbb{K}^2$, alors $\sum(\alpha u_n + \beta v_n)$ est une série convergente de somme $\alpha \sum_{k=0}^{+infty} u_k + \beta \sum_{k=0}^{+\infty} v_k$
Si $\sum z_n$ est un série complexe, alors $\sum z_n$ converge si et seulement si $\sum \mathrm{Re}(z_n)$ et $\sum \mathrm{Im}(z_n)$ convergent.

Séries télescopiques : soit $(u_n) \in \mathbb{K}^{\mathbb{N}}$, alors $\sum(u_{n+1} - u_n)$ est une série convergente si et seulement si (u_n) converge.

Divergence grossière : soit $\sum u_n$ une série,

$$\sum u_n \text{ est convergente } \Rightarrow u_n \to 0 \qquad (u_n) \not\to 0 \Rightarrow \sum u_n \text{ est divergente}$$

Relation série-intégrale : pour $f : \mathbb{R} \to \mathbb{R}$ continue par morceaux et monotone, on peut encadrer $\sum_{k=a}^{b} f(k)$ par $\int_a^b f + f(a)$ et $\int_a^b f + f(b)$

Série de Riemann : soit $\alpha \in \mathbb{R}$, on a :

$$\sum \frac{1}{n^\alpha} \text{ converge } \Leftrightarrow \alpha > 1$$

divergence grossière si $\alpha < 0$, on encadre avec des intégrales pour les autres cas.

28.2 Critères de convergence

Séries à termes positifs : soit $\sum u_n$ une série à terme générale positif, alors $\sum u_n$ converge si et seulement si $\forall n \in \mathbb{N} \sum_{k=0}^{n} u_k$ majoré. Sinon $\sum u_k$ diverge (la suite des sommes partielles tend vers $+\infty$

Comparaison de séries : soit $\sum u_n$ et $\sum v_n$ des séries. telles que $\forall n \in \mathbb{N}, 0 \leqslant u_n \leqslant v_n$, alors

$$\sum v_n \text{ converge } \Rightarrow \sum u_n \text{ converge}$$

Absolue convergence : soit $\sum u_n$ une série, $\sum u_n$ est absolument convergente lorsque $\sum |u_n|$ est convergente.
L'absolue convergence implique la convergence (la réciproque est fausse). Démo, cas réel, $u_n^+ = \max(u_n, 0)$ et $u_n^- = \max(-u_n, 0)$, alors $0 \leqslant u_n^+, u_n^- \leqslant |u_n|$... complexe, de même avec Re et Im

Théorèmes de comparaison : pour $\sum u_n$ et $\sum v_n$ deux séries :
- si $u_n = O(v_n)$ et $\sum |v_n|$ converge, alors $\sum |u_n| \sum u_n$ convergent.
- si u_n et v_n sont positifs et $v_n \sim u_n$, alors $\sum u_n$ et $\sum v_n$ ont même nature.

Si $u_n \sim v_n$, $u_n < 0$ et $v_n < 0$, on a également même convergence.

Règle de l'ordre (du n^α) : soit $\sum u_n$ une série. Si il existe $\alpha > 1$ tel que $u_n n^\alpha \xrightarrow[n \to +\infty]{} 0$, alors $\sum |u_n|$ et $\sum u_n$ converge (en effet, $u_n = O(\frac{1}{n^\alpha})$

Règle de d'Alembert : soit $\sum u_n$ une suite telle que $\left|\frac{u_{n+1}}{u_n}\right| \xrightarrow[n \to +\infty]{} \lambda$, on a alors les implications :
- $\lambda \in [0, 1[\Rightarrow \sum u_n$ converge
- $\lambda > 1 \Rightarrow \sum u_n$ diverge grossièrement

Démo : il existe μ entre λ et 1, et n_0 tel que $\forall n > n_0, \left|\frac{u_{n+1}}{u_n}\right| \geqslant \mu$...

Démonstration de la formule de Stirling : $n! \sim \sqrt{2\pi n} n^n e^{-n}$. On a déjà montrer que si $\frac{n!}{\sqrt{n} n^n e^{-n}} \to K > 0$ alors $K = 2\pi$
$x_n = \ln \frac{n!}{\sqrt{n} n^n e^{-n}}$, $\sum x_n - x_{n-1}$ converge (on utilise la règle du n^α

28.3 Écriture décimale propre des réels

Bijection avec $\mathbb{R}$: on définit l'ensemble de suite

$$E = \left\{ u_n \in \mathbb{Z}^{\mathbb{N}} \;\middle|\; \begin{array}{l} \forall n \geqslant 1, u_n \in [\![0,\ 9]\!] \\ \forall n \geqslant 1, \exists p \geqslant n, u_p \neq 9 \end{array} \right\}$$

On construit alors $u : \begin{pmatrix} \mathbb{R} & \to & E \\ x & \mapsto & \left(\lfloor x \rfloor\right) \vee \left(\lfloor 10^n x \rfloor - 10 \lfloor 10^{n-1} x \rfloor\right)_{n \geqslant 1} \end{pmatrix}$. C'est une bijection de $\mathbb{R} \to E$ de bijection réciproque $u^{-1} : \begin{pmatrix} E & \to & \mathbb{R} \\ u_n & \mapsto & \sum_{k=0}^{+\infty} \frac{u_k}{10^k} \end{pmatrix}$
Bonne définition : encadrer les parties entières, et monter une absurdité si l'on a que des 9. Injectivité $\sum_{k=0}^{+\infty} \frac{u(y)_k}{10^k} = y$

29 Géométrie affine

29.1 Structure affine d'un $\mathbb{K}$-ev

Définition : soit E un $\mathbb{K}$-ev et $(a, b) \in E^2$, on pose $\overrightarrow{ab} = b - a$. b et a sont appelés points de E, et $\overrightarrow{ab}$ vecteur de E.
Pour $\overrightarrow{u} \in E$, on définit la translation $t_{\overrightarrow{u}} : \begin{cases} E & \to & E \\ x & \mapsto & x + \overrightarrow{u} \end{cases}$, on a $\forall (\overrightarrow{u}, \overrightarrow{v}) \in E^2, t_{\overrightarrow{u}} \circ t_{\overrightarrow{v}} = t_{\overrightarrow{v}} \circ t_{\overrightarrow{u}} = t_{\overrightarrow{u}+\overrightarrow{v}}$. De plus $t_{\overrightarrow{0_E}} = \mathrm{id}_E$ donc $\{t_{\overrightarrow{u}}, \overrightarrow{u} \in E\}$ est un sous-groupe de $(\mathscr{S}_E, \circ)$

Repère affine : pour a_0 un point et $b = (e_i)_{i \in I}$ une base de E, on définit le repère affine (a_0, b). Alors, pour tout $m \in E$, il existe une unique famille presque nulle $(\lambda_i)_{i \in I}$ telle que $m = a_0 + \sum_{i \in I} \lambda_i e_i$, on parle de coordonnées dans le repère (a_0, b) de m, il s'agit des coordonnées dans la base b de $\overrightarrow{a_0 m}$

Sous-espace affine : soit $A \subset E$, on dit que A est un sous-espace affine de E lorsqu'il existe $a \in E$ et F un sev de E tel que

$$A = a + F = \{a + f,\ f \in F\}$$

Un tel F est unique et appelé direction de A. On a alors $\forall a \in A, A = a + F$ et $F = \left\{\overrightarrow{ab}, (a, b) \in A^2\right\}$

Intersection de sous-espaces : soit $(A_i)_{i \in I}$ une famille de sous-espaces affines de directions respectives $(F_i)_{i \in I}$. Si $\bigcap_{i \in I} A_i \neq \emptyset$ alors $\bigcap_{i \in I} A_i$ est un sous-espace affine de E de direction $\bigcap_{i \in I} F_i$

Équation linéaire avec second membre : soit E et F deux espaces vectoriels $u \in \mathscr{L}(E, F)$ et $y \in F$. S'il existe une solution particulière x_0 de l'équation $u(x) = y$, alors l'ensemble solution est $x_0 + \mathrm{Ker}(u)$

29.2 Hyperplan affines d'un espace euclidien

Vecteur normal : soit H un hyperplan affine de direction F, $F^\perp$ est une droite vectorielle dont les vecteurs non-nuls sont appelés vecteurs normaux.
Il existe deux vecteurs normaux unitaires. On oriente l'hyperplan en en choisissant un $\overrightarrow{n}$. Une base $(e_0, \ldots, e_{p-1})$ de F est directe si et seulement si $(e_0, \ldots, e_{p-1}, \overrightarrow{n})$ est une base directe de E.

Caractérisation par le produit scalaire : soit $a \in E$, $\overrightarrow{n} \in E \setminus \{0_E\}$ et $H \subset E$

$$H \text{ est un hyperplan affine de } E \text{ de vecteur normal } \overrightarrow{n}$$
$$\Leftrightarrow$$
$$\exists \lambda \in \mathbb{R},\ H = \{m \in E \,/\, \langle \overrightarrow{am}, \overrightarrow{n} \rangle = \lambda\}$$

Démo : H hyperplan $\Leftrightarrow H = m_0 + \{\overrightarrow{n}\}^\perp$...

Équation cartésienne : soit E un espace euclidien de dimension p et de repère (a_0, b) avec $b = (e_i)$ orthonormale. Soit $(\alpha_1, \ldots, \alpha_p, \alpha) \in \mathbb{R}^{p+1}$ non tous nul et $m \in E$ de coordonnées $(x_1, \ldots, x_p)$. L'ensemble $\{\sum_{i=1}^p \alpha_i x_i + \alpha = 0, m \in E\}$ est un hyperplan affine de E de vecteur normal $\overrightarrow{n}$: $\sum_{i=1}^p \alpha_i e_i$

Proportionnalité des équations : soit H un hyperplan affine définit par $\sum_{i=1}^p \alpha_i x_i + \alpha = 0$ et $\sum_{i=1}^p \beta_i x_i + \beta = 0$, alors il existe $\lambda \in \mathbb{R}^*$ tel que $(\alpha_1, \ldots, \alpha_p, \alpha) = (\beta_1, \ldots, \beta_p, \beta)$ (les vecteurs normaux sont colinéaires)

Distance à un hyperplan : on définit la distance d'un point a à l'hyperplan affine H de vecteur normal $\overrightarrow{n}$ contenant m_0 d'équation $\sum_{i=1}^p \alpha_i x_i + \alpha = 0$ par :

$$\mathrm{d}(a, H) = \inf\left\{\left\|\overrightarrow{ah}\right\|, h \in H\right\}$$

alors $\mathrm{d}(a, H) = \dfrac{|\langle \overrightarrow{am_0}, \overrightarrow{n} \rangle|}{\|\overrightarrow{n}\|} = \dfrac{|\alpha_1 t_1 + \ldots + \alpha_p t_p + \alpha|}{\sqrt{\alpha_1^2 + \ldots + \alpha_p^2}}$ où $(t_1, \ldots, t_p)$ sont les coordonnés de a. Démonstration en construisant le projeté orthogonal $h = a + \frac{|\langle \overrightarrow{am_0}, \overrightarrow{n} \rangle|}{\|\overrightarrow{n}\|^2} \overrightarrow{n}$ et vérifiant les inégalités de la borne inf.