Applications linéaires

Dans tout le chapitre, $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$, en pratique $\mathbb{R}$ ou $\mathbb{C}$.

I Définition et opérations sur les applications linéaires

I.1 Définitions - Exemples

Proposition-Définition 1 : Application linéaire.

Soient E et F deux $\mathbb{K}$-ev. Pour une application $f : E \to F$ on a équivalence entre :

1. f préserve les sommes et les multiplications par un scalaire, i. e. :
   - $\forall u \in E,\ \forall \lambda \in \mathbb{K},\ f(\lambda u) = \lambda f(u)$.
   - $\forall u, v \in E,\ f(u+v) = f(u) + f(v)$.
2. f préserve les combinaisons linéaires, i. e. :
   $\forall (u,v) \in E^2,\ \forall (\lambda,\mu) \in \mathbb{K}^2,\ f(\lambda u + \mu v) = \lambda f(u) + \mu f(v)$.

On dit alors que f est une application linéaire. On note $\mathcal{L}(E,F)$ l'ensemble des applications linéaires de E dans F.

I.2 (Co)restriction

Proposition 1 .

Soient E, F des $\mathbb{K}$-ev, G un sev de E et H un sev de F.
Si $f : E \to F$ est linéaire et $f(G) \subset H$, alors $f_{|G}^{|H} : G \to H$ est linéaire.

I.3 Stabilité par combinaison linéaire

Théorème 1 .

Si f et g sont linéaires alors $\lambda f + \mu g$ est linéaire.

Théorème 2 : Reformulation.

$\mathcal{L}(E,F)$ est un sev de F^E. En particulier, $(\mathcal{L}(E,F), +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.

Définition 2 .

On appelle homothétie vectorielle de rapport λ, ou plus simplement homothétie de rapport λ l'application $\lambda \mathrm{id}_E : E \to E$. C'est une application linéaire.
On dit que $f \in \mathcal{L}(E)$ est une homothétie lorsque $\exists \lambda \in \mathbb{K}, \forall u \in E, f(u) = \lambda u$, i.e. $f = \lambda \mathrm{id}$.

I.4 Composition

Théorème 3 .

Soient $f \in \mathcal{L}(E,F)$ et $g \in \mathcal{L}(F,G)$. Alors $g \circ f \in \mathcal{L}(E,G)$.

Proposition 2 .

Soit $h \in F^E$ (une application quelconque !).
La composition par h à droite est distributive sur l'addition et compatible avec la multiplication externe :

1. $\forall f, g \in G^F,\ (f+g) \circ h = f \circ h + g \circ h$;
2. $\forall f \in G^F,\ \forall \lambda \in \mathbb{K},\ (\lambda f) \circ h = \lambda (f \circ h)$.

Remarquons que ces deux propriétés peuvent être synthétisées en une :

$\forall f, g \in G^F,\ \forall \lambda, \mu \in \mathbb{K},\ (\lambda f + \mu g) \circ h = \lambda (f \circ h) + \mu (g \circ h)$.

Théorème 4 .

Soient E, F, G des $\mathbb{K}$-ev et $h \in F^E$. L'application de précomposition par h $\left\{ \begin{array}{ccc} G^F & \to & G^E \\ f & \mapsto & f \circ h \end{array} \right.$ est linéaire.

Proposition 3 .

Soit E, F, G des $\mathbb{K}$-ev et $h \in G^F$. Supposons h linéaire.
Alors la composition par h à gauche est distributive sur l'addition et compatible avec la multiplication externe :

1. $\forall f, g \in F^E,\ h \circ (f+g) = h \circ f + h \circ g$.
2. $\forall f \in F^E,\ \forall \lambda \in \mathbb{K},\ h \circ (\lambda f) = \lambda (h \circ f)$.

Ou encore : $\forall f, g \in F^E,\ \forall \lambda, \mu \in \mathbb{K},\ h \circ (\lambda f + \mu g) = \lambda (h \circ f) + \mu (h \circ g)$.

Théorème 5 .

Soit E, F, G des $\mathbb{K}$-ev **et $h \in \mathcal{L}(F, G)$**. L'application de postcomposition par h $\left\{ \begin{array}{ccc} F^E & \to & G^E \\ f & \mapsto & h \circ f \end{array} \right.$ est linéaire.

Corollaire 1 .

Bilan : $\big(\mathcal{L}(E), +, \circ, \cdot\big)$ forme une $\mathbb{K}$-algèbre. En particulier $\big(\mathcal{L}(E), +, \circ\big)$ forme un anneau.

Définition 3 .

On dit qu'une application linéaire est un un endomorphisme de E lorsque c'est une application d'un $\mathbb{K}$-espace vectoriel E dans lui-même. On notera $\mathcal{L}(E)$ plutôt que $\mathcal{L}(E, E)$ l'ensemble des endomorphismes de E.

Corollaire 2 .

On peut appliquer un polynôme à un endomorphisme. On obtient un endomorphisme.

I.5 Réciproque

Théorème 6 .

Soient E et F deux espaces vectoriels, et $f \in \mathcal{L}(E, F)$. Si f est bijective alors $f^{-1} \in \mathcal{L}(F, E)$.

Définition 4 .

Une application linéaire bijective est appelée un isomorphisme.

Notation 1

S'il existe un isomorphisme d'un espace vectoriel E dans un espace vectoriel F, on dit que E et F sont isomorphes.

Remarque 1

Si E et F sont deux $\mathbb{K}$-espaces vectoriels de dimension finie et isomorphes, alors ils ont la même dimension.

I.6 Groupe linéaire

Définition 5 .

On dit qu'une application linéaire est un automorphisme de E lorsque c'est un isomorphisme de E dans E.
En bref : « auto = endo + iso ». On notera $GL(E)$ l'ensemble des automorphismes de E.

Théorème-définition 7 .

En particulier $\big(GL(E), \circ\big)$ forme un groupe. On l'appelle le groupe linéaire de E.

I.7 Formes linéaires

Définition 6 .

Une application linéaire d'un espace vectoriel E dans le corps de base $\mathbb{K}$ est appelée une forme linéaire sur E.
On notera E^* plutôt que $\mathcal{L}(E, \mathbb{K})$ l'ensemble des formes linéaires sur E.

II Propriété fondamentale

II.1 Exemple des droites.

Lemme 1 .

Soit D une droite (i. e. un $\mathbb{K}$-ev de dimension 1).
Une application $f : D \to D$ est linéaire si et seulement si c'est une homothétie.

II.2 Exemple de $\mathbb{K}^n$

Proposition 4 .

Soit $f : \mathbb{K}^q \to \mathbb{K}^p$; f est linéaire si et seulement s'il existe une matrice $A \in \mathcal{M}_{p,q}(\mathbb{K})$ telle que $f = \left\{ \begin{array}{ccc} \mathbb{K}^q & \to & \mathbb{K}^p \\ x & \mapsto & A \times x. \end{array} \right.$
Autrement dit, f est linéaire si et seulement s'il existe des scalaires $(a_{i,j})_{\substack{1 \leqslant i \leqslant p \\ 1 \leqslant j \leqslant q}}$ pour lesquels on peut écrire

$$f = \left\{ \begin{array}{ccc} \mathbb{K}^q & \to & \mathbb{K}^p \\ \begin{pmatrix} x_1 \\ \vdots \\ x_q \end{pmatrix} & \mapsto & \begin{pmatrix} a_{1,1}x_1 + a_{1,2}x_2 + \ldots + a_{1,q}x_q \\ \vdots \\ a_{p,1}x_1 + a_{p,2}x_2 + \ldots + a_{p,q}x_q \end{pmatrix} \end{array} \right. .$$

Remarque 2

Du coup, « dans $\mathbb{R}^n$ », toute application linéaire se représente canoniquement par une matrice [1], mais on a vu qu'un espace de dimension finie quelconque pouvait être ramené à $\mathbb{R}^n$ en le munissant d'une base : il sera donc possible en dimension finie, et pas seulement dans $\mathbb{R}^n$, de représenter les applications linéaires par des matrices. On verra plus tard, hein. Quant au cas de la dimension quelconque, on ne peut plus parler de matrice, mais on peut faire pareil quand même, c'est l'objet du paragraphe suivant.

II.3 Cas général

Théorème 8 : Propriété fondamentale des applications linéaires.

Soient E et F deux $\mathbb{K}$-espaces vectoriels. Toute application linéaire $f \in \mathcal{L}(E, F)$ est <u>entièrement</u> et <u>uniquement</u> déterminée par ses valeurs sur une base de E.

Autrement dit : soit $\mathcal{B} = (\varepsilon_i)_{i \in I}$ une base de E. Alors, pour toute famille $(y_i)_{i \in I}$ de vecteurs de F, il existe une unique application linéaire $f \in \mathcal{L}(E, F)$ telle que $\forall i \in I,\ f(\varepsilon_i) = y_i$.

II.4 Définition par restrictions

Théorème 9 : Propriété fondamentale généralisée.

Soient E et F deux $\mathbb{K}$-evs et $E_1, E_2, \ldots, E_p$ des sevs de E tels que $E_1 \oplus E_2 \oplus \cdots \oplus E_p = E$.
Soient $\varphi_1 \in \mathcal{L}(E_1, F)$, $\varphi_2 \in \mathcal{L}(E_2, F)$, …, $\varphi_p \in \mathcal{L}(E_p, F)$.
Alors il existe une unique application linéaire $\varphi \in \mathcal{L}(E, F)$ telle que $\forall i \in \{1, 2, \ldots, p\}$, $\varphi_{|E_i} = \varphi_i$.

III Noyau, image et rang

III.1 Image et noyau

Définition 7 : Rappel.

Soit $f \in \mathcal{L}(E, F)$.

- On appelle noyau de f l'ensemble $\mathrm{Ker}(f) = f^{-1}\big(\{0_F\}\big) = \{x \in E,\ f(x) = 0_F\} \subset E$.
- On appelle image de f l'ensemble $\mathrm{Im}(f) = f(E) = \{y \in F,\ \exists x \in E,\ y = f(x)\} \subset F$.

Théorème 10 : Rappel.

Soit $f \in \mathcal{L}(E, F)$.

- f injective $\Leftrightarrow \mathrm{Ker}(f) \subset \{0_E\} \Leftrightarrow \mathrm{Ker}(f) = \{0_E\}$.
- f surjective $\Leftrightarrow F \subset \mathrm{Im}(f) \Leftrightarrow \mathrm{Im}(f) = F$.

Remarque 3 On peut parler d'image ou noyau d'une matrice ; cela signifie image ou noyau de l'application linéaire canoniquement associée. (Voir juste au-dessus)

Théorème 11 .

Soit $f \in \mathcal{L}(E, F)$. Alors $\mathrm{Ker}(f)$ est un sous-espace vectoriel E et $\mathrm{Im}(f)$ est un sous-espace vectoriel F.

1. Et du coup on connaissait déjà. Boring.

III.2 Rang

Notation 2 Si $\mathcal{F}$ est une famille de vecteurs E et $f \in \mathcal{L}(E,F)$, on note $f(\mathcal{F})$ la famille obtenue en appliquant f aux vecteurs de $\mathcal{F}$. Ainsi, pour $\mathcal{F} = (u_i)_{i\in I}$, on a $f(\mathcal{F}) = \big(f(u_i)\big)_{i\in I}$.

Définition 8 .

Soit $f \in \mathcal{L}(E,F)$. On appelle rang de f et on note $\mathrm{rg}(f)$ la quantité $\mathrm{rg}(f) = \dim\big(\mathrm{Im}(f)\big)$.

Théorème 12 .

Le rang de f est un rang ! Plus précisément, pour $f \in \mathcal{L}(E,F)$ et pour toute base $\mathcal{B}$ de E, on a $\mathrm{rg}(f) = \mathrm{rg}\big(f(\mathcal{B})\big)$.

Théorème 13 : Propriétés "immédiates" du rang.

Soient E, F, G trois $\mathbb{K}$-espaces vectoriels.

1. Pour $f \in \mathcal{L}(E,F)$, on a $\mathrm{rg}(f) \leqslant \min(\dim(E), \dim(F))$.
2. Pour $f \in \mathcal{L}(E,F)$ et $g \in \mathcal{L}(F,G)$, on a $\mathrm{rg}(g\circ f) \leqslant \min(\mathrm{rg}(f), \mathrm{rg}(g))$, et, de plus :
3. si f est un isomorphisme alors $\mathrm{rg}(g\circ f) = \mathrm{rg}(g)$ et si g est un isomorphisme alors $\mathrm{rg}(g\circ f) = \mathrm{rg}(f)$. i. e. composer par un isomorphisme ne modifie pas le rang

III.3 Équations d'un hyperplan

Théorème 14 .

Les hyperplans sont exactement les noyaux des formes linéaires non nulles.

Définition 9 .

Soit H un hyperplan de E. On appelle équation de H une expression de la forme $\phi(x) = 0$ où ϕ est une forme linéaire telle que $\mathrm{Ker}(\phi) = H$. D'après le théorème **??**, tout hyperplan a une équation.

III.4 Théorème d'isomorphisme

Théorème 15 : Théorème d'isomorphisme.

Soient E et F deux $\mathbb{K}$-espaces vectoriels et $f \in \mathcal{L}(E,F)$.
Soit S un supplémentaire de $\mathrm{Ker}(f)$ dans E. Alors $f_{|S}^{|\mathrm{Im}(f)}$ est bien définie et c'est un isomorphisme.
On dit que f induit un isomorphisme de S sur $\mathrm{Im}(f)$.

IV Applications linéaires en dimension finie

IV.1 Théorème du rang

Théorème 16 : formule du rang.

Soit E et F deux $\mathbb{K}$-espaces vectoriels et $f \in \mathcal{L}(E,F)$. **On suppose que E est de dimension finie.** Alors $\dim\big(\mathrm{Ker}(f)\big) + \dim\big(\mathrm{Im}(f)\big) = \dim(E)$ i. e. $\mathrm{rg}(f) = \dim(E) - \dim(\mathrm{Ker}(f))$.

IV.2 Applications immédiates du théorème du rang

IV.3 Théorème du rang et *jectivité

Théorème 17 : Caractérisation par le rang.

Soient E et F deux K-espaces vectoriels de dimensions finies. Soit $f \in \mathcal{L}(E,F)$. Alors on a :

i/ f est surjective si et seulement si $\mathrm{rg}(f) = \dim(F)$;

ii/ f est injective si et seulement si $\mathrm{rg}(f) = \dim(E)$;

iii/ f est bijective si et seulement si $\mathrm{rg}(f) = \dim(E) = \dim(F)$.

Théorème 18 : Caractérisation des isomorphismes.

Soient E et F deux K-espaces vectoriels de même dimension finie n. Soit $f \in \mathcal{L}(E, F)$. Sont équivalentes :

i/ f est injective ;

ii/ f est surjective ;

iii/ f est un isomorphisme.

Remarque 4

On a un analogue ensembliste : Soit A, B deux ensembles tels que $\#A = \#B := n \in \mathbb{N}$.
Alors

$$\begin{aligned} f : A \to B \in & \\ \Leftrightarrow f \in & \\ \Leftrightarrow f \in & \end{aligned}$$

Théorème 19 : Caractérisation des automorphismes.

Soient E un K-espace vectoriel de dimension finie. Soit $f \in \mathcal{L}(E)$. Sont équivalentes :

i/ f est inversible à gauche ;

ii/ f est inversible à droite ;

iii/ f est un automorphisme.

IV.4 Deux applications de la théorie au calcul matriciel

V Endomorphismes remarquables

V.1 Endomorphismes nilpotents

Définition 10 .

Un endomorphisme $f \in \mathcal{L}(E)$ est dit nilpotent lorsque c'est un élément nilpotent de l'anneau $(\mathcal{L}(E), +, \circ)$.
L'unique entier p tel que $f^{p-1} \neq 0_{\mathcal{L}(E)}$ et $f^p = 0_{\mathcal{L}(E)}$ s'appelle l'indice de nilpotence de f.

Proposition 5 .

Si $\dim(E) < +\infty$ et $f \in \mathcal{L}(E)$ est nilpotent, alors l'indice de nilpotence de f est plus petit que $\dim(E)$.

V.2 Projections

Remarque 5

Soient F et G deux sous-espaces supplémentaires de E. Alors on a :

i/ $p_G^F = \mathrm{id}_E - p_F^G$;

ii/ $p_G^F \circ p_F^G = p_F^G \circ p_G^F = 0_{\mathcal{L}(E)}$.

Proposition 6 : Propriétés immédiates des projections.

Soient F et G deux sous-espaces supplémentaires de E. Alors on a :

i/ $\mathrm{Ker}(p_F^G) = G$;

ii/ $\mathrm{Im}(p_F^G) = F$;

iii/ $p_F^G \circ p_F^G = p_F^G$.

Théorème 20 : :mind_blown :.

Si p est un endomorphisme idempotent, alors p est une projection.

C'est la projection sur $\mathrm{Im}(p)$ parallèlement à $\mathrm{Ker}(p)$.

V.3 Symétries

Proposition 7 : Propriétés immédiates des projections.

Soient F et G deux sous-espaces supplémentaires de E. Alors on a :

i/ $\mathrm{Ker}(s_F^G - \mathrm{id}_E) = \mathrm{Im}(s_F^G + \mathrm{id}_E) = F$;

ii/ $\mathrm{Ker}(s_F^G + \mathrm{id}_E) = \mathrm{Im}(s_F^G - \mathrm{id}_E) = G$;

iii/ $s_G^F = -s_F^G$;

iv/ $s_F^G = p_F^G - p_G^F$;

v/ $s_F^G \circ s_F^G = \mathrm{id}_E$.

Théorème 21 .

Si s est un endomorphisme involutif, alors s est une symétrie.

C'est la symétrie par rapport à $\mathrm{Ker}(s - \mathrm{id}_E)$ parallèlement à $\mathrm{Ker}(s + \mathrm{id}_E)$.

Dérivabilité.

Contexte : dans tout le chapitre

- I désigne une réunion d'intervalles non triviaux ;
- f désigne une application de I dans $\mathbb{R}$, sauf mention du contraire.

I Rappels

I.1 Taux d'accroissement et dérivée

Définition 1 .

Soit $a \in I$. On appelle taux d'accroissement de f en a l'application $\tau_a : \left\{ \begin{array}{ccc} I \setminus \{a\} & \to & \mathbb{R} \\ x & \mapsto & \frac{f(x)-f(a)}{x-a} \end{array} \right.$.

Remarque 1

Pour a et x (distincts) dans I on a $\tau_x(a) = \tau_a(x)$.

Définition 2 .

1. Soit $a \in I$. On dit que f est dérivable en a lorsque $\lim_{x \to a} \tau_a(x)$ existe et est finie.
   Lorsque c'est le cas, cette limite est notée $f'(a)$ et s'appelle le nombre dérivé de f en a.
2. On dit que f est dérivable sur I lorsqu'elle est dérivable en tout point de I.
   Auquel cas l'application $f' : \left\{ \begin{array}{ccc} I & \to & I \\ a & \mapsto & f'(a) \end{array} \right.$ s'appelle la dérivée de f.
3. On dit que f est continûment dérivable sur I lorsqu'elle est dérivable sur I de dérivée continue.

Notation 1

1. On note $\mathcal{D}(I, \mathbb{R})$ ou $\mathcal{D}^1(I, \mathbb{R})$ l'ensemble des fonctions dérivables de I dans $\mathbb{R}$.
2. On note $\mathcal{C}^1(I, \mathbb{R})$ l'ensemble des fonctions continûment dérivables de I dans $\mathbb{R}$.

On a évidemment $\mathcal{C}^1(I, \mathbb{R}) \subset \mathcal{D}^1(I, \mathbb{R})$. **Remarque 2**

Il existe des fonctions $\mathcal{D}^1(I, \mathbb{R})$ mais pas $\mathcal{C}^1(I, \mathbb{R})$.

Définition 3 . Soit $a \in I$.

1. On dit que f est dérivable à droite en a lorsque τ_a a une limite à droite finie en a.
2. On dit que f est dérivable à gauche en a lorsque τ_a a une limite à gauche finie en a.

I.2 $DL_1(a)$ et applications

Théorème 1 .

Soit $a \in I$.

1. f est dérivable en a si et seulement si f a un $DL_1(a)$;
2. lorsque c'est le cas, ce $DL_1(a)$ est $f(a+h) = f(a) + f'(a)h + o(h)$.

Théorème 2 : (rappel).

Si f est dérivable, alors f est continue.

Théorème 3 : TDFC.

Soient $\left\{ \begin{array}{l} u \in \mathcal{D}^1(I, J) \\ v \in \mathcal{D}^1(J, \mathbb{R}). \end{array} \right.$ Alors on a $v \circ u \in \mathcal{D}^1(I, \mathbb{R})$ et $(v \circ u)' = u' \times v' \circ u$.

Théorème 4 .

Soient $f, g \in \mathcal{D}^1(I, \mathbb{R})$. Alors on a :

1. $\forall (\lambda, \mu) \in \mathbb{R}^2,\ \lambda f + \mu g \in \mathcal{D}^1(I, \mathbb{R})$ et $(\lambda f + \mu g)' = \lambda f' + \mu g'$;
2. $fg \in \mathcal{D}^1(I, \mathbb{R})$ et $(fg)' = f'g + fg'$;
3. si g ne s'annule pas, $\frac{f}{g} \in \mathcal{D}^1(I, \mathbb{R})$ et $\left(\frac{f}{g}\right)' = \frac{f'g - fg'}{g^2}$.

Corollaire 1 .

1. $\mathcal{D}^1(I,\mathbb{R})$ forme une sous-algèbre de $\mathbb{R}^I$;
2. $\mathcal{C}^1(I,\mathbb{R})$ forme une sous-algèbre de $\mathcal{D}^1(I,\mathbb{R})$;
3. $\partial : \left\{ \begin{array}{ccc} \mathcal{C}^1(I,\mathbb{R}) & \to & \mathcal{C}^0(I,\mathbb{R}) \\ f & \mapsto & f' \end{array} \right.$ est linéaire.

Théorème 5 : TDFR.

Soit $f : I \to J$ (I un intervalle). Si $\begin{cases} f \in (\mathrm{Bij} \cap \mathcal{D})(I,J) \\ f' \text{ ne s'annule pas} \end{cases}$ alors f^{-1} est dérivable sur J et $\left(f^{-1}\right)' = \dfrac{1}{f' \circ f^{-1}}$.

II Théorèmes de moyenne et applications

II.1 Point critique

Définition 4 .

On suppose $f \in \mathcal{D}^1(I,\mathbb{R})$. On appelle point critique de f un réel $a \in I$ pour lequel on a $f'(a) = 0$.

Théorème 6 : Lemme de Fermat sur les points critiques.

On suppose $f \in \mathcal{D}^1(I,\mathbb{R})$.

Si f atteint un extremum local en a, alors a est soit un point critique de f soit une extrémité de I.

II.2 Théorème de Rolle

Théorème 7 : Rolle.

Soient $a < b \in \mathbb{R}$ et $f \in \mathcal{C}([a,b],\mathbb{R}) \cap \mathcal{D}(]a,b[,\mathbb{R})$ telle que $f(a) = f(b)$.

Alors il existe $c \in]a,b[$ pour lequel on a $f'(c) = 0$.

II.3 Accroissements finis

Théorème 8 : Égalité des accroissements finis.

Soient $a < b \in \mathbb{R}$ et $f \in \mathcal{C}([a,b],\mathbb{R}) \cap \mathcal{D}(]a,b[,\mathbb{R})$. Alors il existe $c \in]a,b[$ pour lequel on a $f'(c) = \dfrac{f(b)-f(a)}{b-a}$.

Corollaire 2 : Inégalité des accroissements finis.

Soient $a < b \in \mathbb{R}$ et $f \in \mathcal{C}([a,b],\mathbb{R}) \cap \mathcal{D}(]a,b[,\mathbb{R})$. Alors :

1. $\inf\limits_{]a,b[} f' \leqslant \dfrac{f(b)-f(a)}{b-a} \leqslant \sup\limits_{]a,b[} f'$;
2. $\left| \dfrac{f(b)-f(a)}{b-a} \right| \leqslant \sup\limits_{]a,b[} |f'|$.

Théorème 9 : Reformulation de l'IAF.

On suppose que I est un intervalle et qu'on a $f \in \mathcal{D}^1(I,\mathbb{R})$. Alors :

1. pour $k \geqslant 0$, on a $f \in k{-}\mathcal{L} \Leftrightarrow |f'| \leqslant k$;
2. pour $f \in \mathcal{L} \Leftrightarrow |f'|$ bornée.

II.4 Application aux études globales

Théorème 10 : sur le signe de la dérivée.

On suppose que I est un intervalle et qu'on a $f \in \mathcal{D}(I,\mathbb{R})$.

1. $\left\{ \begin{array}{l} \text{Si } f' \geqslant 0 \text{ sur } I \text{ alors } f \text{ est croissante sur } I\,; \\ \text{si } f' \leqslant 0 \text{ sur } I \text{ alors } f \text{ est décroissante sur } I. \end{array} \right.$
2. $\left\{ \begin{array}{l} \text{Si } f' > 0 \text{ sur } I \text{ alors } f \text{ est strictement croissante sur } I\,; \\ \text{si } f' < 0 \text{ sur } I \text{ alors } f \text{ est strictement décroissante sur } I. \end{array} \right.$
3. Si $f' = 0$ sur I alors f est constante sur I.

II.5 $\mathcal{D}^1$ vs $\mathcal{C}^1$

Remarque 3

Ce théorème implique que les seules fonctions $\mathcal{C}_{pm}$ qui ont des primitives sont les fonctions continues, pourquoi ?

Théorème 11 : sur la limite de la dérivée.

Soit $f \in \mathcal{C}(I, \mathbb{R})$ et $a \in I$. On suppose de plus que f est dérivable sur $I \setminus \{a\}$.

1. Si $\lim\limits_{\substack{x \to a \\ x \neq a}} f'(x) = \ell \in \overline{\mathbb{R}}$ alors $\lim\limits_{x \to a} \frac{f(x)-f(a)}{x-a} = \ell$.
2. En particulier, si $\lim\limits_{\substack{x \to a \\ x \neq a}} f'(x) = \ell \in \mathbb{R}$ alors f est dérivable en a et $f'(a) = \ell$.

Théorème 12 : théorème de prolongement $\mathcal{C}^1$.

Soit $a \in I$ et $f \in \mathcal{C}^1(I \setminus \{a\}, \mathbb{R})$. On suppose qu'il existe deux réels ℓ_0 et ℓ_1 tels que $\left\{ \begin{array}{l} f(x) \xrightarrow[x \to a]{} \ell_0 \\ f'(x) \xrightarrow[x \to a]{} \ell_1. \end{array} \right.$

Alors f est prolongeable par continuité sur I et son prolongement est $\mathcal{C}^1(I, \mathbb{R})$.

En notant $f_\sim$ ce prolongement, on a $\left\{ \begin{array}{l} f_\sim(a) = \ell_0 \\ f'_\sim(a) = \ell_1. \end{array} \right.$

II.6 Convexité des fonctions dérivables

Définition 5 .

La fonction f est dite <u>convexe</u> lorsqu'on a $\forall x, y \in I,\ \forall t \in [0,1],\ g\big((1-t)x + ty\big) \leqslant (1-t)g(x) + tgf(y)$.

Remarque 4

On définit de même une fonction <u>concave</u> $g : I \to \mathbb{R}$ par $\forall x, y \in I,\ \forall t \in [0,1],\ g\big((1-t)x + ty\big) \geqslant (1-t)g(x) + tgf(y)$. Autrement dit, une fonction concave est l'opposée d'une fonction convexe, son graphe est **au dessus** de ses sécantes, son **hypographe** (l'ensemble des points du plan "sous" la courbe) est convexe, ses taux d'accroissements sont décroissants. L'étude des fonctions concaves est la même que celle des fonctions convexes, il suffit de renverser les inégalités. **Remarque 5**

Une fonction convexe n'a aucune raison d'être dérivable, par exemple $x \mapsto |x|$ est convexe.

Proposition 1 .

Supposons f dérivable sur I. Alors f est convexe si et seulement si f' est croissante.

En particulier, si f est deux fois dérivable, alors elle est convexe si et seulement si f'' est positive.

Définition 6 .

Soit $a \in I$. On dit que <u>f présente un point d'inflexion en a</u> lorsque f change de concavité en a.

Dérivabilité.

Contexte : dans tout le chapitre

- I désigne une réunion d'intervalles non triviaux ;
- f désigne une application de I dans $\mathbb{R}$, sauf mention du contraire.

I Rappels

I.1 Taux d'accroissement et dérivée

Définition 1 .

Soit $a \in I$. On appelle taux d'accroissement de f en a l'application $\tau_a : \left\{ \begin{array}{ccc} I \setminus \{a\} & \to & \mathbb{R} \\ x & \mapsto & \frac{f(x)-f(a)}{x-a} \end{array} \right.$.

Remarque 1

Pour a et x (distincts) dans I on a $\tau_x(a) = \tau_a(x)$.

Définition 2 .

1. Soit $a \in I$. On dit que f est dérivable en a lorsque $\lim\limits_{x \to a} \tau_a(x)$ existe et est finie.
   Lorsque c'est le cas, cette limite est notée $f'(a)$ et s'appelle le nombre dérivé de f en a.
2. On dit que f est dérivable sur I lorsqu'elle est dérivable en tout point de I.
   Auquel cas l'application $f' : \left\{ \begin{array}{ccc} I & \to & I \\ a & \mapsto & f'(a) \end{array} \right.$ s'appelle la dérivée de f.
3. On dit que f est continûment dérivable sur I lorsqu'elle est dérivable sur I de dérivée continue.

Notation 1

1. On note $\mathcal{D}(I, \mathbb{R})$ ou $\mathcal{D}^1(I, \mathbb{R})$ l'ensemble des fonctions dérivables de I dans $\mathbb{R}$.
2. On note $\mathcal{C}^1(I, \mathbb{R})$ l'ensemble des fonctions continûment dérivables de I dans $\mathbb{R}$.

On a évidemment $\mathcal{C}^1(I, \mathbb{R}) \subset \mathcal{D}^1(I, \mathbb{R})$. **Remarque 2**

Il existe des fonctions $\mathcal{D}^1(I, \mathbb{R})$ mais pas $\mathcal{C}^1(I, \mathbb{R})$.

Définition 3 . Soit $a \in I$.

1. On dit que f est dérivable à droite en a lorsque τ_a a une limite à droite finie en a.
2. On dit que f est dérivable à gauche en a lorsque τ_a a une limite à gauche finie en a.

I.2 $DL_1(a)$ et applications

Théorème 1 .

Soit $a \in I$.

1. f est dérivable en a si et seulement si f a un $DL_1(a)$;
2. lorsque c'est le cas, ce $DL_1(a)$ est $f(a+h) = f(a) + f'(a)h + o(h)$.

Théorème 2 : (rappel).

Si f est dérivable, alors f est continue.

Théorème 3 : TDFC.

Soient $\left\{ \begin{array}{l} u \in \mathcal{D}^1(I, J) \\ v \in \mathcal{D}^1(J, \mathbb{R}). \end{array} \right.$ Alors on a $v \circ u \in \mathcal{D}^1(I, \mathbb{R})$ et $(v \circ u)' = u' \times v' \circ u$.

Théorème 4 .

Soient $f, g \in \mathcal{D}^1(I, \mathbb{R})$. Alors on a :

1. $\forall (\lambda, \mu) \in \mathbb{R}^2,\ \lambda f + \mu g \in \mathcal{D}^1(I, \mathbb{R})$ et $(\lambda f + \mu g)' = \lambda f' + \mu g'$;
2. $fg \in \mathcal{D}^1(I, \mathbb{R})$ et $(fg)' = f'g + fg'$;
3. si g ne s'annule pas, $\frac{f}{g} \in \mathcal{D}^1(I, \mathbb{R})$ et $\left(\frac{f}{g}\right)' = \frac{f'g - fg'}{g^2}$.

Corollaire 1 .

1. $\mathcal{D}^1(I,\mathbb{R})$ forme une sous-algèbre de $\mathbb{R}^I$;
2. $\mathcal{C}^1(I,\mathbb{R})$ forme une sous-algèbre de $\mathcal{D}^1(I,\mathbb{R})$;
3. $\partial : \left\{ \begin{array}{ccc} \mathcal{C}^1(I,\mathbb{R}) & \to & \mathcal{C}^0(I,\mathbb{R}) \\ f & \mapsto & f' \end{array} \right.$ est linéaire.

Théorème 5 : TDFR.
Soit $f : I \to J$ (I un intervalle). Si $\begin{cases} f \in (\mathrm{Bij} \cap \mathcal{D})(I,J) \\ f' \text{ ne s'annule pas} \end{cases}$ alors f^{-1} est dérivable sur J et $\left(f^{-1}\right)' = \dfrac{1}{f' \circ f^{-1}}$.

II Théorèmes de moyenne et applications

II.1 Point critique

Définition 4 .

On suppose $f \in \mathcal{D}^1(I,\mathbb{R})$. On appelle <u>point critique de f</u> un réel $a \in I$ pour lequel on a $f'(a) = 0$.

Théorème 6 : Lemme de Fermat sur les points critiques.

On suppose $f \in \mathcal{D}^1(I,\mathbb{R})$.

Si f atteint un extremum local en a, alors a est soit un point critique de f soit une extrémité de I.

II.2 Théorème de Rolle

Théorème 7 : Rolle.

Soient $a < b \in \mathbb{R}$ et $f \in \mathcal{C}([a,b],\mathbb{R}) \cap \mathcal{D}(]a,b[,\mathbb{R})$ telle que $f(a) = f(b)$.

Alors il existe $c \in]a,b[$ pour lequel on a $f'(c) = 0$.

II.3 Accroissements finis

Théorème 8 : Égalité des accroissements finis.

Soient $a < b \in \mathbb{R}$ et $f \in \mathcal{C}([a,b],\mathbb{R}) \cap \mathcal{D}(]a,b[,\mathbb{R})$. Alors il existe $c \in]a,b[$ pour lequel on a $f'(c) = \dfrac{f(b)-f(a)}{b-a}$.

Corollaire 2 : Inégalité des accroissements finis.

Soient $a < b \in \mathbb{R}$ et $f \in \mathcal{C}([a,b],\mathbb{R}) \cap \mathcal{D}(]a,b[,\mathbb{R})$. Alors :

1. $\inf\limits_{]a,b[} f' \leqslant \dfrac{f(b)-f(a)}{b-a} \leqslant \sup\limits_{]a,b[} f'$;
2. $\left|\dfrac{f(b)-f(a)}{b-a}\right| \leqslant \sup\limits_{]a,b[} |f'|$.

Théorème 9 : Reformulation de l'IAF.

On suppose que I est un intervalle et qu'on a $f \in \mathcal{D}^1(I,\mathbb{R})$. Alors :

1. pour $k \geqslant 0$, on a $f \in k{-}\mathcal{L} \Leftrightarrow |f'| \leqslant k$;
2. pour $f \in \mathcal{L} \Leftrightarrow |f'|$ bornée.

II.4 Application aux études globales

Théorème 10 : sur le signe de la dérivée.

On suppose que I est un intervalle et qu'on a $f \in \mathcal{D}(I,\mathbb{R})$.

1. $\left\{ \begin{array}{l} \text{Si } f' \geqslant 0 \text{ sur } I \text{ alors } f \text{ est croissante sur } I\,; \\ \text{si } f' \leqslant 0 \text{ sur } I \text{ alors } f \text{ est décroissante sur } I. \end{array} \right.$
2. $\left\{ \begin{array}{l} \text{Si } f' > 0 \text{ sur } I \text{ alors } f \text{ est strictement croissante sur } I\,; \\ \text{si } f' < 0 \text{ sur } I \text{ alors } f \text{ est strictement décroissante sur } I. \end{array} \right.$
3. Si $f' = 0$ sur I alors f est constante sur I.

II.5 $\mathcal{D}^1$ vs $\mathcal{C}^1$

Remarque 3

Ce théorème implique que les seules fonctions $\mathcal{C}_{pm}$ qui ont des primitives sont les fonctions continues, pourquoi ?

Théorème 11 : sur la limite de la dérivée.

Soit $f \in \mathcal{C}(I, \mathbb{R})$ et $a \in I$. On suppose de plus que f est dérivable sur $I \setminus \{a\}$.

1. Si $\lim\limits_{\substack{x \to a \\ x \neq a}} f'(x) = \ell \in \overline{\mathbb{R}}$ alors $\lim\limits_{x \to a} \frac{f(x)-f(a)}{x-a} = \ell$.
2. En particulier, si $\lim\limits_{\substack{x \to a \\ x \neq a}} f'(x) = \ell \in \mathbb{R}$ alors f est dérivable en a et $f'(a) = \ell$.

Théorème 12 : théorème de prolongement $\mathcal{C}^1$.

Soit $a \in I$ et $f \in \mathcal{C}^1(I \setminus \{a\}, \mathbb{R})$. On suppose qu'il existe deux réels ℓ_0 et ℓ_1 tels que $\left\{ \begin{array}{l} f(x) \underset{x \to a}{\longrightarrow} \ell_0 \\ f'(x) \underset{x \to a}{\longrightarrow} \ell_1. \end{array} \right.$

Alors f est prolongeable par continuité sur I et son prolongement est $\mathcal{C}^1(I, \mathbb{R})$.

En notant $f_\sim$ ce prolongement, on a $\left\{ \begin{array}{l} f_\sim(a) = \ell_0 \\ f'_\sim(a) = \ell_1. \end{array} \right.$

II.6 Convexité des fonctions dérivables

Définition 5 .

La fonction f est dite convexe lorsqu'on a $\forall x, y \in I,\ \forall t \in [0,1],\ g\big((1-t)x + ty\big) \leqslant (1-t)g(x) + tgf(y)$.

Remarque 4

On définit de même une fonction concave $g : I \to \mathbb{R}$ par $\forall x, y \in I,\ \forall t \in [0,1],\ g\big((1-t)x + ty\big) \geqslant (1-t)g(x) + tgf(y)$. Autrement dit, une fonction concave est l'opposée d'une fonction convexe, son graphe est **au dessus** de ses sécantes, son **hypographe** (l'ensemble des points du plan "sous" la courbe) est convexe, ses taux d'accroissements sont décroissants. L'étude des fonctions concaves est la même que celle des fonctions convexes, il suffit de renverser les inégalités. **Remarque 5**

Une fonction convexe n'a aucune raison d'être dérivable, par exemple $x \mapsto |x|$ est convexe.

Proposition 1 .

Supposons f dérivable sur I. Alors f est convexe si et seulement si f' est croissante.

En particulier, si f est deux fois dérivable, alors elle est convexe si et seulement si f'' est positive.

Définition 6 .

Soit $a \in I$. On dit que f présente un point d'inflexion en a lorsque f change de concavité en a.

Espaces préhilbertiens.

Contexte : dans tout le chapitre E désigne un $\mathbb{R}$-espace vectoriel. **À retenir** : la formule de projection !

I Produit scalaire

I.1 L'exemple du produit scalaire usuel sur $\mathbb{R}^n$

Théorème 1 . L'application $\langle \cdot, \cdot\cdot \rangle$ est :

0. à valeurs dans $\mathbb{R}$;
1. symétrique : $\forall x, y \in \mathbb{R}^n,\ \langle y, x\rangle = \langle x, y\rangle$;
2. bilinéaire : $\begin{cases} \forall x, y, z \in \mathbb{R}^n,\ \forall \lambda, \mu \in \mathbb{R},\ \langle \lambda x + \mu y, z\rangle = \lambda\langle x, z\rangle + \mu\langle y, z\rangle \text{ (linéarité à gauche)} \\ \forall x, y, z \in \mathbb{R}^n,\ \forall \lambda, \mu \in \mathbb{R},\ \langle x, \lambda y + \mu z\rangle = \lambda\langle x, y\rangle + \mu\langle x, z\rangle \text{ (linéarité à droite) ;} \end{cases}$
3. définie-positive : $\begin{cases} \forall x \in \mathbb{R}^n,\ \langle x, x\rangle \geqslant 0 \text{ (positivité)} \\ \forall x \in \mathbb{R}^n,\ \langle x, x\rangle = 0 \Rightarrow x = 0_E \text{ (caractère défini).} \end{cases}$

I.2 Définitions

Définition 1 : Produit scalaire sur E.

On appelle produit scalaire sur E une **forme bilinéaire symétrique définie positive sur E** c'est-à-dire une application $\Phi : E \times E \to \mathbb{R}$ telle que :

1. Φ est symétrique, i. e. $\forall x, y \in \mathbb{R}^n,\ \Phi(y, x) = \Phi(x, y)$;
2. Φ est bilinéaire, i. e. $\begin{cases} \forall x, y, z \in \mathbb{R}^n,\ \forall \lambda, \mu \in \mathbb{R},\ \Phi(\lambda x + \mu y, z) = \lambda\Phi(x, z) + \mu\Phi(y, z) \text{ (linéarité à gauche)} \\ \forall x, y, z \in \mathbb{R}^n,\ \forall \lambda, \mu \in \mathbb{R},\ \Phi(x, \lambda y + \mu z) = \lambda\Phi(x, y) + \mu\Phi(x, z) \text{ (linéarité à droite) ;} \end{cases}$
3. Φ est définie-positive, i. e. $\begin{cases} \forall x \in \mathbb{R}^n,\ \Phi(x, x) \geqslant 0 \text{ (positivité)} \\ \forall x \in \mathbb{R}^n,\ \Phi(x, x) = 0 \Rightarrow x = 0_E \text{ (caractère défini).} \end{cases}$

Remarque 1

1. Le fait que le corps soit $\mathbb{R}$ est donc essentiel pour pouvoir énoncer la positivité.
2. Pour montrer la bilinéarité, il est pratique de montrer d'abord la symétrie pour n'avoir que la linéarité d'un seul côté à montrer, comme on l'a fait plus haut pour le produit scalaire usuel sur $\mathbb{R}^n$.

Notation 1 On utilise souvent l'une des trois notations suivantes pour dénoter un produit scalaire Φ sur E. Étant donnés deux vecteurs x et y de E leur produit scalaire $\Phi(x, y)$ pourra se noter $(x|y)$ ou $\langle x, y\rangle$ ou $x \cdot y$.

Définition 2 .

1. On appelle espace préhilbertien un $\mathbb{R}$-espace vectoriel muni d'un produit scalaire (E, Φ).
2. On appelle espace euclidien un espace préhilbertien de dimension finie.

Proposition-Définition 3 : Produit scalaire canoniquement associé à une base.

Soit $\mathcal{B} = (\varepsilon_i)_{i\in I}$ une base de E.

On appelle produit scalaire canoniquement associé à $\mathcal{B}$ l'application $\begin{cases} E \times E & \to & \mathbb{R} \\ \left(\sum_{i\in I} x_i\varepsilon_i, \sum_{i\in I} y_i\varepsilon_i\right) & \mapsto & \sum_{i\in I} x_i yi. \end{cases}$

Le produit scalaire canoniquement associé à $\mathcal{B}$ est bien un produit scalaire !

Remarque 2

Dans la définition précédentes, toutes les sommes sont en fait finies (il n'y a qu'un nombre fini de termes non nuls) même pour I infini, et correspondent aux décompositions dans la base $\mathcal{B}$, il s'agit juste d'une notation pratique pour éviter les doubles indices.

I.3 Autres exemples

Théorème 2 .

Sur $E = \mathcal{C}([a,b],\mathbb{R})$ le produit scalaire intégral $\Phi = (f,g) \mapsto \int_a^b f(t)g(t)\ \mathrm{d}t$ est bien un produit scalaire.

Proposition 1 : La restriction d'un produit scalaire est un produit scalaire.

Autrement dit si $\Phi : E \times E \to \mathbb{R}$ est un produit scalaire sur E, et F est un sous-espace vectoriel de E, alors $\Phi_{|F\times F} : F \times F \to \mathbb{R}$ est un produit scalaire sur F.

I.4 Normes et distances

Définition 4 : Norme euclidienne.

Soit $\big(E, \langle \cdot, \cdot\cdot \rangle\big)$ un espace préhilbertien. On appelle norme euclidienne l'application $N : \left\{ \begin{array}{ccc} E & \to & \mathbb{R}_+ \\ u & \mapsto & \sqrt{\langle u, u\rangle}. \end{array} \right.$

Remarque 3 L'application N est bien définie par positivité du produit scalaire. **Notation 2** On utilise souvent l'une des deux notations suivantes pour dénoter la norme euclidienne de $(E, \langle \cdot, \cdot\cdot \rangle)$.
Étant donné un vecteur x de E sa norme euclidienne $N(x)$ pourra se noter $\|x\|$ ou $\|x\|_2$.

Théorème 3 : Inégalité de Cauchy-Schwarz.

Soit $\big(E, \langle \cdot, \cdot\cdot \rangle\big)$ un espace préhilbertien et $\|\cdot\|$ la norme associée. Pour tous $u, v \in E$ on a $|\langle u, v\rangle| \leqslant \|u\|\,\|v\|$.

Remarque 4

C'est évident dans $\mathbb{R}^2$ (ou $\mathbb{R}^3$) muni du produit scalaire usuel. Une formule et un dessin :

Théorème 4 : Cas d'égalité dans Cauchy-Schwarz.

Soit $\big(E, \langle \cdot, \cdot\cdot \rangle\big)$ un espace préhilbertien et $\|\cdot\|$ la norme associée.

Pour tous $u, v \in E$ on a $|\langle u, v\rangle| = \|u\|\,\|v\|$ ssi u et v sont colinéaires.

Théorème 5 : Propriétés d'une norme.

Soit $\big(E, \langle \cdot, \cdot\cdot \rangle\big)$ un espace préhilbertien. La norme euclidienne $N = u \mapsto \sqrt{\langle u, u\rangle}$

est une application $N : E \to \mathbb{R}_+$ qui vérifie :

1. l'homogénéité : $\forall u \in E,\ \forall \lambda \in \mathbb{R},\ N(\lambda u) = |\lambda| N(u)$;
2. la séparation : $\forall u \in E,\ N(u) = 0 \quad N(u) = 0 \Leftrightarrow u = 0_E$;
3. l'inégalité triangulaire : $\forall u, v \in E,\ N(u+v) \leq N(u) + N(v)$.

Théorème 6 : Identités de polarisation.

Soit $\big(E, \langle \cdot, \cdot\cdot \rangle\big)$ un espace préhilbertien de norme euclidienne $\|\cdot\|$. Soient u, v dans E. Alors :

1. $\langle u, v\rangle = \dfrac{\|u+v\|^2 - \|u\|^2 - \|v\|^2}{2}$;
2. $\langle u, v\rangle = \dfrac{\|u+v\|^2 - \|u-v\|^2}{4}$.

Définition 5 : Distance euclidienne.

Soit $\big(E, \langle\cdot, \cdot\cdot\rangle\big)$ un espace préhilbertien de norme euclidienne $\|\cdot\|$.

On appelle distance euclidienne entre A et B le réel positif $d(A, B) = \|B - A\|$.

Théorème 7 : Propriétés d'une distance.

Soit $\big(E, \langle\cdot, \cdot\cdot\rangle\big)$ un espace préhilbertien de norme euclidienne $\|\cdot\|$. La distance euclidienne $d = (A, B) \mapsto d(A, B)$ est une application $d : E \times E \to \mathbb{R}_+$ qui vérifie :

1. la symétrie : $\forall A, B \in E,\ d(A, B) = d(B, A)$;
2. la séparation : $\forall A, B \in E,\ d(A, B) = 0 \Leftrightarrow A = B$;
3. l'inégalité triangulaire : $\forall A, B, C \in E,\ d(A, C) \leqslant d(A, B) + d(B, C)$.

II Orthogonalité

II.1 Vecteurs orthogonaux

Définition 6 : Vecteur orthogonaux.

Soient $u,\ v \in E$. On dit que u et v sont orthogonaux lorsqu'on a $\langle u, v\rangle = 0$.

(C'est une relation symétrique par symétrie du produit scalaire.)

Notation 3 On le note $u \perp v$.

Théorème 8 : Pythagore.

Soient $u,\ v \in E$. Alors on a $u \perp v \Leftrightarrow \|u + v\|^2 = \|u\|^2 + \|v\|^2$.

II.2 Familles orthogonales

Définition 7 .

Une famille $(u_i)_{i \in I}$ de vecteurs de E est dire orthogonale lorsqu'on a $\forall i \neq j \in I,\ u_i \perp u_j$.

Théorème 9 : Pythagore généralisé.

Soient $n \in \mathbb{N}$ et $u_1, u_2, \dots u_n \in E$. Supposons la famille $(u_1, \dots, u_n)$ orthogonale.

Alors on a $\|u_1 + u_2 + \cdots + u_n\|^2 = \|u_1\|^2 + \|u_2\|^2 + \cdots + \|u_n\|^2$.

Théorème 10 .

Toute famille orthogonale formée de vecteurs non nuls est libre.

Proposition-Définition 8 . Soit $\mathcal{B} = (\varepsilon_i)_{i \in I}$.

1. On dit que $\mathcal{B}$ est une base orthogonale lorsque c'est à la fois une famille orthogonale et une base. Cela équivaut à dire que c'est une famille génératrice et orthogonale formée de vecteurs non nuls.
2. On dit que $\mathcal{B}$ est une base orthonormée (b.o.n.) lorsque c'est base orthogonale formée de vecteurs de norme 1. Cela équivaut à dire que $\mathcal{B}$ est génératrice et telle que $\forall i, j \in I,\ \langle \varepsilon_i, \varepsilon_j\rangle = \delta_{i,j}$.

II.3 Sous-espaces vectoriels orthogonaux

Définition 9 .

Soient F et G deux sevs de E. On dit que F et G sont orthogonaux lorsqu'on a $\forall u \in F,\ \forall v \in G,\ u \perp v$.

Notation 4 On le note $F \perp G$ aussi. **Remarque 5**

Si F et G sont orthogonaux alors $F \cap G = \{0_E\}$.

II.4 Orthogonal d'une partie ou d'un sev

Définition 10 : Orthogonal d'une partie.

Soit $X \subset E$. On appelle orthogonal de X l'ensemble $\{v \in E,\ \forall u \in X,\ v \perp u\}$.

II.5 Supplémentaire orthogonal

II.6 Cas d'un espace euclidien

III Projection orthogonale et applications

III.1 Formule de projection

III.2 Algorithme d'orthonormalisation de Gram-Schmidt

III.3 Magie des b.o.n.

III.4 Distance à un sous-espace vectoriel

Sous-espaces vectoriels en dimension finie

Dans tout le chapitre, $\mathbb{K}$ est un sous-corps de $\mathbb{C}$, et E désigne un $\mathbb{K}$-espace vectoriel.

I Sevs en dimension finie

I.1 Propriété fondamentale

Théorème 1 : Propriété fondamentale des sevs en dimension finie.

Supposons que E soit de dimension finie n, et F un sous-espace vectoriel de E. Alors :

1. F est un $\mathbb{K}$-espace vectoriel de dimension finie et $\dim F \leqslant \dim E$;
2. $\dim F = n$ si et seulement si $F = E$.

Remarque 1

Ce théorème a un **analogue ensembliste** : si A est un ensemble fini et B un ensemble tel que $B \subset A$ alors B est fini et $|B| \leqslant |A|$, avec égalité si et seulement si $A = B$. **Remarque 2**

• L'application "dimension" dim : $\{\text{sous-espaces vectoriels de } E\} \to \mathbb{N} \cup \{+\infty\}$ est donc croissante (pour l'inclusion).
• L'application "rang" rg : $\{\text{familles de vecteurs de } E\} \to \mathbb{N} \cup \{+\infty\}$ est donc une application croissante (pour la relation « être un sous-famille de ») puisque c'est $\dim \circ \mathrm{Vect}$.

I.2 Application aux supplémentaires

Théorème 2 .

Supposons que E soit de dimension finie, et F un sous-espace vectoriel de E. Alors :

1. F a un supplémentaire ;
2. pour tout supplémentaire G de F on a $\dim G = \dim E - \dim F$.

Remarque 3

Ce théorème a aussi un **analogue ensembliste** : si $B \amalg C = A$ avec A fini, alors $|B| + |C| = |A|$.

II Applications de la formule de Grassmann

II.1 Formule de Grassmann

Théorème 3 : Formule de Grassmann.

Supposons E de dimension finie. Soient F et G deux sous-espaces vectoriels de E. Alors on a :

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

Remarque 4

On a là encore un **analogue ensembliste** : si $B, C \subset A$ avec A fini alors $|B \cup C| = |B| + |C| - |B \cap C|$. **Remarque 5**

On retrouve qu'on a $\dim(F \oplus G) = \dim(F) + \dim(G)$.

II.2 Applications

Théorème 4 .

Soient E_1 et E_2 deux $\mathbb{K}$-espaces vectoriels de dimensions finies. Alors $\dim(E_1 \times E_2) = \dim(E_1) + \dim(E_2)$.

Théorème 5 : Caractérisation des supplémentaires en dimension finie.

Supposons que E soit de dimension finie n. Soient F, G deux sevs de E.

Les propositions suivantes sont équivalentes :

i/ $F \oplus G = E$;

ii/ $F \cap G = \{0_E\}$ et $\dim(F) + \dim(G) = n$;

iii/ $F + G = E$ et $\dim(F) + \dim(G) = n$.

Théorème 6 : Dimension d'une somme de m sevs.

Soient $F_1, \dots, F_m$ des sous-espaces vectoriels de E, supposé de dimension finie.

Alors on a : $\dim\left(\sum_{i=1}^{m} F_i\right) \leqslant \sum_{i=1}^{m} \dim(F_i)$, avec égalité si et seulement si la somme est directe.

II.3 Hyperplans en dimension finie

Théorème 7 .

Supposons $\dim(E) = n < +\infty$. Alors un hyperplan de E est exactement un sev de E de dimension $n-1$.

Théorème 8 .

Supposons E de dimension finie n. Soient $H_1, H_2, \dots, H_m$ des hyperplans de E.

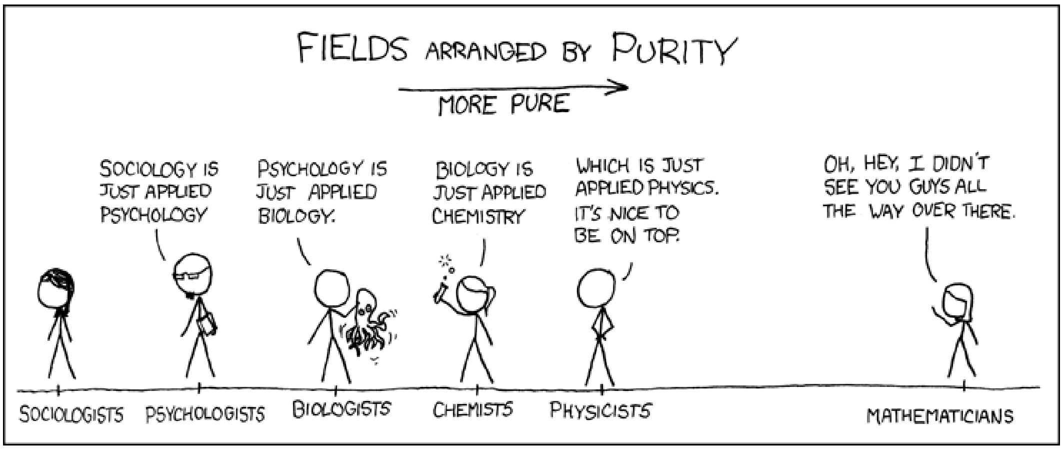
Alors on a $\dim(H_1 \cap H_2 \cap \dots \cap H_m) \geqslant n - m$.

Remarque 6

Soit $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{K}^n \setminus \{\overrightarrow{0}\}$. Alors $H = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},\ a_1x_1 + \dots + a_nx_n = 0 \right\}$ est un hyperplan de $\mathbb{K}^n$.

Théorème 9 .

L'ensemble des solutions d'un système linéaire homogène $\left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n,\ \left\| \begin{array}{c} a_{1,1}x_1 + \dots + a_{1,n}x_n = 0 \\ \vdots \\ a_{m,1}x_1 + \dots + a_{m,n}x_n = 0 \end{array} \right. \right\}$ forme un sev de $\mathbb{K}^n$ de dimension supérieure à $n - m$.



Espaces et sous-espaces vectoriels

On connaît moults $\mathbb{R}$-espaces vectoriels :

$(\mathcal{M}_{p,q}(\mathbb{R}),+,\cdot)$
$(\mathbb{R}^n,+,\cdot)$

$(\mathbb{R}[i],+,\cdot) \quad = \quad (\mathbb{C},+,\cdot)$
$(\mathbb{R}[\sqrt{2}],+,\cdot) \quad = \quad (\mathbb{R},+,\cdot)$
$(\mathbb{R}_n[X],+,\cdot)$

$(\mathcal{F}(I,\mathbb{R}),+,\cdot)$
$(\mathcal{C}(I,\mathbb{R}),+,\cdot)$
$(\mathbb{R}[X],+,\cdot)$

$(DL_n(0),+,\cdot)$
$(\mathbb{R}^{\mathbb{N}},+,\cdot)$

L'objectif : identifier une banque de théorèmes qui s'appliquent (entre autres) à **tous** les exemples précédents.

Dans toute la suite on fixe un sous-corps $\mathbb{K}$ de $\mathbb{C}$ (mais en vrai on ne regardera que $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$ – très éventuellement $\mathbb{Q}$).

Dans toute la suite, $(E,+,\cdot)$ désignera un <u>$\mathbb{K}$-espace vectoriel</u> (en abrégé $\mathbb{K}$-ev, c'est pas de moi). Rappel : cela signifie

i/ $(E,+)$ est un groupe <u>commutatif</u>

ii/ $\cdot$ est compatible avec $\times_{\mathbb{K}}$ et $1_{\mathbb{K}}$

iii/ $\cdot$ est distributive sur $+$

Dans ce contexte, les éléments de E sont appelés des **vecteurs** et les éléments de $\mathbb{K}$ des **scalaires**.

À comprendre tout de suite :

— Les trois opérations structurelles d'un $\mathbb{K}$-ev sont le vecteur nul, l'addition des vecteurs et la multiplication externe.

— On voit tout de suite qu'on peut combiner les deux dernières opérations avec la notion de **combinaison linéaire de deux vecteurs**. Une combinaison linéaire de deux vecteurs est une expression de la forme $\lambda u + \mu v$, où λ, μ sont des scalaires et u, v sont des vecteurs.

— Plus généralement, on voit qu'on peut combiner les trois opérations avec la notion de **combinaison linéaire**. Une combinaison linéaire est une expression de la forme $\sum_{i=1}^{r} \lambda_i u_i$ où r est un entier naturel, les λ_i des scalaires et les u_i des vecteurs.

On notera en abrégé « CL » pour « combinaison linéaire » (ce n'est pas de moi non plus).

I Sous-espaces vectoriels

I.1 Caractérisations équivalentes

Définition 1 .

On appelle sous-espace vectoriel de $(E,+,\cdot)$ (en abrégé « sev », toujours pas de moi) un ensemble F inclus dans E stable pour la structure d'espace vectoriel de E, c'est-à-dire tel que :

- $0_E \in F$,
- $\forall (x,y) \in F^2,\ x+y \in F$,
- $\forall x \in F,\ \forall \lambda \in \mathbb{K},\ \lambda x \in F$.

Théorème 1 : Utile à la démonstration.

Un sous-ensemble F de E est un sous-espace vectoriel de $(E,+,\cdot)$ si et seulement s'il est non vide et stable par combinaisons linéaires de deux vecteurs, c'est-à-dire $F \neq \emptyset$ et $\forall (\lambda,\mu) \in \mathbb{K}^2,\ \forall (x,y) \in F^2,\ \lambda x + \mu y \in F$.

Théorème 2 : Utile à l'exploitation .

Un sous-ensemble F de E est un sous-espace vectoriel de $(E,+,\cdot)$ si et seulement s'il est stable par combinaisons linéaires quelconques, c'est-à-dire si et seulement si on a :

$$\forall r \in \mathbb{N},\ \forall (\alpha_1,\ldots,\alpha_r) \in \mathbb{K}^r,\ \forall (u_1,\ldots,u_r) \in F^r,\ \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_r u_r \in F.$$

I.2 Exemples et contre-exemples

Remarque 1

Quand un pertie F de E est définie par un système d'équations linéaires homogènes, c'est toujours un sev. **Remarque 2**

Quand on a une partie F de E définie par paramétrage linéaire, c'est toujours un sev de E.

I.3 Structure d'espace vectoriel

Théorème 3 .

Si F est un sev de E, alors les lois de E induisent des lois sur F, et F, muni des lois induites, forme un $\mathbb{K}$-ev.

II Opérations sur les sevs

II.1 Intersection de sevs

Théorème 4 .

Soit $(F_i)_{i\in I}$ une famille de sevs de E. Alors $\bigcap_{i\in I} F_i$ est un sev de E.

Remarque 3

Ça marche pas pour $\cup$: Pour l'espace vectoriel $(\mathbb{R}^2,+,\cdot)$:

$$\left(\left\{\begin{pmatrix}0\\y\end{pmatrix}, y \in R\right\} \cup \left\{\begin{pmatrix}x\\0, x \in R\end{pmatrix}\right\}, +, \cdot\right)$$

N'est pas un sev : par exemple, il est pas stable par somme.

II.2 Sommes de sous-espaces vectoriels

Définition 2 .

Pour n un entier naturel et $F_1, F_2, \ldots, F_n$ des sous-espaces vectoriels de E, on appelle somme de $F_1, F_2, \ldots, F_n$ l'ensemble $F_1 + F_2 + \cdots + F_n = \{u_1 + u_2 + \cdots + u_n,\ u_1 \in F_1,\ u_2 \in F_2,\ \ldots, u_n \in F_n\}$.

Théorème 5 .

Pour n un entier naturel et $F_1, F_2, \ldots, F_n$ des sevs de E, $F_1 + F_2 + \cdots + F_n$ est un sev de E.

Remarque 4 La somme des sevs est :

- Idempotente : pour tout sev F de E, on a $F + F = F$;
- Commutative : pour tous sevs F et G de E, on a $F + G = G + F$;
- Associative : pour tous sevs F, G et H de E, on a $(F + G) + H = F + (G + H) = F + G + H$;
- Admet pour élément neutre le sous-espace nul : pour tout sev F de E, on a $F + \{0_E\} = \{0_E\} + F = F$.

Remarque 5

$(Ox) + (Oy) = F$

II.3 Sommes directes

Définition 3 .

Une somme $F = F_1 + F_2 + \cdots + F_n$ est dite directe lorsque tout vecteur u de F s'écrit **de façon unique** sous la forme $u = u_1 + u_2 + \cdots + u_n$ où l'on a $\forall i \in \{1, \ldots, n\},\ u_i \in F_i$. On note alors $F = F_1 \oplus F_2 \oplus \cdots \oplus F_n$.

Remarque 6

Une somme de **2** sevs (et pas plus) et directe ssi leur intersection est le sev nul.

Théorème 6 .

Une somme $F = F_1 + F_2 + \cdots + F_n$ est dite directe si et seulement si l'unique décomposition du vecteur nul dans la somme est $0_E = 0_{F_1} + \cdots + 0_{F_n}$.

II.4 Supplémentaires

Définition 4 .

Deux sous-espaces vectoriels F et G de E sont dit supplémentaires lorsqu'on a $F \oplus G = E$.

Proposition 1 : Caractérisation de supplémentarité.

Deux sevs F et G de E sont supplémentaires si et seulement si $\left\{ \begin{array}{l} F + G = E \\ F \cap G = \{0_E\} \end{array} \right.$.

III D'autres méthodes pour obtenir des $\mathbb{K}$-evs

III.1 Produits de $\mathbb{K}$-espaces vectoriels

Théorème 7 : Produit de $\mathbb{K}$-ev.

Soient $n \in \mathbb{N}$ et E_1, E_2, ..., E_n des $\mathbb{K}$-espaces vectoriels. L'ensemble $E_1 \times E_2 \times \cdots \times E_n$ est naturellement muni d'une structure d'espace vectoriel donnée par les opérations composante par composante :

- $0_{E_1 \times \cdots \times E_n} = (0_{E_1}, \ldots, 0_{E_n})$;
- $\forall (u_1, \ldots, u_n), (v_1, \ldots, v_n) \in E_1 \times E_2 \times \cdots \times E_n,\ (u_1, \ldots, u_n) + (v_1, \ldots, v_n) = (u_1 + v_1, \ldots, u_n + v_n)$;
- $\forall \lambda \in \mathbb{K},\ \forall (u_1, \ldots, u_n) \in E_1 \times E_2 \times \cdots \times E_n,\ \lambda \cdot (u_1, \ldots, u_n) = (\lambda u_1, \ldots, \lambda u_n)$.

III.2 Espaces vectoriels engendrés

Lemme 1 : CL de CL.

Soit $(E, +, \cdot)$ un $\mathbb{K}$-ev et $P \subset E$. Si un vecteur u de E peut s'obtenir comme CL de vecteurs pouvant eux-même s'obtenir comme CL de vecteurs de P, alors u est lui-même une CL de vecteurs de P.

Proposition 2 : Propriétés fondamentales de Vect.

1. Vect est extensive, c'est-à-dire : $\forall P \subset E,\ \text{Vect}\,(P) \supset P$
2. Vect est croissante pour l'inclusion, c'est-à-dire :$\forall P, Q \subset E,\ Q \subset E, P \subset Q \implies \text{Vect}\,(P) \subset \text{Vect}\,(Q)$
3. Vect est idempotente, c'est-à-dire : $\text{Vect} \circ \text{Vect} = \text{Vect}$

Remarque 7

Pour $P \subset E$, $P = \text{Vect}\,(P) \Leftrightarrow P$ est un sev

III.3 $\mathbb{K}$-evs et sevs remarquables

Définition 5 .

1. On appelle droite (vectorielle) un sev de E de la forme $\operatorname{Vect}(u)$ avec $u \neq 0_E$.
2. On appelle plan (vectoriel) un sev de E de la forme $\operatorname{Vect}(u, v)$ avec u et v non colinéaires, c'est-à-dire tel qu'aucun des deux n'est un multiple de l'autre.

Définition 6 .

On appelle hyperplan de E un sev de E dont un supplémentaire est une droite.

Familles en dimension finie

Dans tout le chapitre, $\mathbb{K}$ est un sous-corps de $\mathbb{C}$, et E désigne un $\mathbb{K}$-espace vectoriel.

N.B. : le fait que $\mathbb{K}$ soit un corps est essentiel. On verra dans la suite que c'est toujours la même propriété qui assure la plupart des résultats, à savoir : **on peut diviser par un scalaire non nul**.

I Espaces vectoriels de dimension finie

I.1 Extension et réduction

Lemme 1 : Principe de réduction d'une famille génératrice.

Soit $\mathcal{G} \sqcup (u)$ une famille génératrice de E. Si $u \in \mathrm{Vect}\,(\mathcal{G})$, alors la sous-famille $\mathcal{G}$ est génératrice de E.

Lemme 2 : Principe d'extension d'une famille libre.

Soit $\mathcal{L}$ une famille libre de E et $u \in E$. Si $u \notin \mathrm{Vect}\,(\mathcal{L})$ alors la famille $\mathcal{L} \sqcup (u)$ est libre.

Remarque 1

On retrouve un cas particulier du théorème sur les bases adaptées.

I.2 Définition – exemples

Définition 1 .

L'espace vectoriel E est dit <u>de dimension finie</u> lorsqu'il admet une famille génératrice finie. Sinon, il est dit de <u>dimension infinie</u>.

Remarque 2

Si E est un espace de dimension finie, il n'y a pas en général unicité d'une famille génératrice engendrant E. Par exemple, que les familles $\big(\mathrm{ch}, \mathrm{sh}\big)$ et $\big(\exp, t \mapsto \mathrm{e}^{-t}\big)$ engendrent le même espace vectoriel.

I.3 Existence de bases

Théorème 1 : de la base extraite.

On suppose que E est un espace vectoriel de dimension finie et $\mathcal{G}$ une famille génératrice finie de E. Alors :

1. E a une base finie :
2. toute sous-famille génératrice minimale de $\mathcal{G}$ et toute sous-famille libre maximale de $\mathcal{G}$ est une base de E.

Théorème 2 : de la base incomplète.

Soient $\mathcal{L}$ une famille libre et $\mathcal{G} = (v_1, \dots, v_m)$ une famille génératrice de E. Alors on peut choisir certains vecteurs $v_{i_1}, \dots, v_{i_r}$ de $\mathcal{G}$ de sorte que la famille $\mathcal{L} \sqcup (v_{i_1}, \dots, v_{i_r})$ soit une base de E.

Remarque 3

Ce théorème indique qu'en dimension finie les familles libres sont des « bases incomplètes », *i. e.* qu'on peut obtenir des bases en leur rajoutant convenablement des vecteurs (et de plus ces vecteurs peuvent être choisis dans n'importe quelle famille génératrice de E).

I.4 Dimension

Lemme 3 : Lemme d'échange (version simplifiée)..

Supposons que E soit de dimension finie. Soit $\mathcal{B}_1 = (u_i)_{i\in I}$ une base de E et $\mathcal{B}_2 = (\varepsilon_j)_{j\in\{1,\dots,s\}}$ une base finie de E. Alors :

$$\forall i_0 \in I,\ \exists j_0 \in \{1, \dots, s\},\ (u_i)_{i\in I\setminus\{i_0\}} \sqcup (\varepsilon_{j_0}) \text{ est une base de } E.$$

Autrement dit : **tout vecteur de $\boldsymbol{\mathcal{B}_1}$ peut être échangé contre un vecteur de $\boldsymbol{\mathcal{B}_2}$**, si celui-ci est bien choisi, la famille obtenue restera une base.

Théorème 3 .

Supposons E de dimension finie. Alors toutes les bases de E sont finies et de même cardinal.

Définition 2 .

Si E est de dimension finie, on appelle <u>dimension de E</u> et on note $\dim(E)$ le cardinal d'une base de E.

Si E n'est pas de dimension finie, on dit qu'il est de dimension infinie et non note $\dim(E) = +\infty$.

Remarque 4 On peut noter $\dim_{\mathbb{K}}(E)$ pour bien insister sur le fait que le corps de base est $\mathbb{K}$.

I.5 Morphisme de décomposition dans une base

Définition 3 .

Supposons que E est de dimension finie n et considérons $\mathcal{B} = (\varepsilon_1, \dots, \varepsilon_n)$ une base de E. Pour tout vecteur $u \in E$, on appelle <u>décomposition de u dans la base $\mathcal{B}$</u> et on note $\left|\, u \right._{\mathcal{B}}$ l'unique n-uplet $\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in \mathbb{K}^n$ tel qu'on ait $u = \lambda_1\varepsilon_1 + \cdots + \lambda_n\varepsilon_n$.

Proposition 1 : Morphisme de décomposition.

Soient E un $\mathbb{K}$-espace vectoriel de dimension finie n et $\mathcal{B} = (\varepsilon_1, \dots, \varepsilon_n)$ une base de E. Alors :

1. L'application $\left\{\begin{array}{ccc} E & \to & \mathbb{K}^n \\ u & \mapsto & \left|\, u \right._{\mathcal{B}} \end{array}\right.$ de décomposition dans $\mathcal{B}$ est bijective.
2. L'application $\left\{\begin{array}{ccc} E & \to & \mathbb{K}^n \\ u & \mapsto & \left|\, u \right._{\mathcal{B}} \end{array}\right.$ est linéaire, c'est-à-dire :

$$\forall (u,v) \in E^2,\ \forall (\lambda, \mu) \in \mathbb{K}^2,\quad \left|\, (\lambda u + \mu v) \right._{\mathcal{B}} = \lambda \cdot \left|\, u \right._{\mathcal{B}} + \mu \cdot \left|\, v \right._{\mathcal{B}}.$$

II Applications du TBE et du TBI

II.1 Cardinal d'une famille en dimension n

Lemme 4 .

Supposons que E est un $\mathbb{K}$-espace vectoriel de dimension finie n.

1. Toute famille génératrice de E possède au moins n éléments.
2. Toute famille libre de E possède au plus n éléments.

Corollaire 1 .

S'il existe une famille libre infinie de vecteurs de E, alors $\dim(E) = +\infty$.

Théorème 4 .

On contrapose le lemme **??**-2 : si $\dim(E) = n$, toute famille de $n+1$ vecteurs (ou plus) est liée.

Théorème 5 .

Supposons que E est un $\mathbb{K}$-espace vectoriel de dimension finie n. Soit $\mathcal{F}$ une famille à n éléments de E. Alors les trois propositions suivantes sont équivalentes :

i. $\mathcal{F}$ est libre.
ii. $\mathcal{F}$ est génératrice.
iii. $\mathcal{F}$ est une base.

II.2 Rang d'une famille de vecteurs

Définition 4 .

Soit $\mathcal{F}$ une famille finie de vecteurs de E. On appelle rang de $\mathcal{F}$ et on note $\mathrm{rg}(\mathcal{F})$ la dimension de $\mathrm{Vect}(\mathcal{F})$.

$$\mathrm{rg} := \dim \circ \mathrm{Vect}$$

Remarque 5

Le TBE se reformule comme suit : le rang de $\mathcal{F}$ est le cardinal maximal d'une sous-famille libre de $\mathcal{F}$.

Définition 5 : Opérations élémentaires sur une famille de vecteurs.

Soit $\mathcal{F} = (u_1, \dots, u_m)$ une famille finie de vecteurs de E.
On appelle opérations élémentaires sur les vecteurs de la famille $\mathcal{F}$ les opérations suivantes :

1. Échanger deux vecteurs de la famille.
2. Ajouter à un vecteur u_i de $\mathcal{F}$ un multiple d'un autre vecteur u_j de $\mathcal{F}$.
3. Multiplier un vecteur u_i de $\mathcal{F}$ par une constante non nulle.

Proposition 2 .

Soit $\mathcal{F} = (u_1, \dots, u_m)$ une famille finie de vecteurs de E. Toute famille $\mathcal{G}$ obtenue à partir de $\mathcal{F}$ par opérations élémentaires, et en enlevant le vecteur nul lorsqu'il se présente, a le même rang que $\mathcal{F}$.

II.3 Lien avec le rang d'une matrice

Remarque 6 : **Cas $E = \mathbb{K}^p$.**

Si $E = \mathbb{K}^p$ alors le rang de la famille $(u_1, \dots, u_q)$ est le rang (par colonnes) de la matrice $\begin{pmatrix} | & & | \\ u_1 & \cdots & u_q \\ | & & | \end{pmatrix} \in \mathcal{M}_{p,q}(\mathbb{K})$.

C'est un corollaire immédiat de la proposition précédente.

Remarque 7 : **Cas général.**

Si $\dim(E) = p$ et que $\mathcal{B}$ est une base **quelconque** de E alors le rang de la famille $(u_1, \dots, u_q)$ est le rang (par colonnes) de la matrice $\begin{pmatrix} | & & | \\ u_1 & \cdots & u_q \\ |_{\mathcal{B}} & & |_{\mathcal{B}} \end{pmatrix}$.

Définition 6 .

Supposons que E soit de dimension finie p. Soit $\mathcal{B}$ une base de E. Soit $\mathcal{F} = (u_1, \dots, u_q)$ une famille finie de vecteurs de E. On appelle matrice de $\mathcal{F}$ dans $\mathcal{B}$ la matrice $\begin{pmatrix} | & & | \\ u_1 & \cdots & u_q \\ |_{\mathcal{B}} & & |_{\mathcal{B}} \end{pmatrix}$.

III Applications

III.1 Suites récurrentes linéaires doubles

Notation 1 Dans la suite, pour $(a,b) \in \mathbb{K}^2$, on note $\mathcal{S}_{a,b} = \left\{ (u_n)_{n \in \mathbb{N}} \in \mathbb{K}^{\mathbb{N}},\ \forall n \in \mathbb{N},\ u_{n+2} = a u_{n+1} + b u_n \right\}$.
(Notation maison et conjoncturelle, c'est juste pour ne pas le réécrire à chaque fois.)

Proposition 3 .

Soit $(a,b) \in \mathbb{K}^2$. Alors $\mathcal{S}_{a,b}$ est un plan vectoriel.

Définition 7 .

On appelle polynôme caractéristique d'une suite de $\mathcal{S}_{a,b}$ le polynôme $P_{a,b} = X^2 - aX - b$.

Théorème 6 : Cas de deux racines..

Si on a $\Delta \neq 0$ alors, en notant r_1 et r_2 les deux racines distinctes dans $\mathbb{K}$ de $P_{a,b}$, on a

$$\mathcal{S}_{a,b} = \left\{ \left(\lambda\, r_1^n + \mu\, r_2^n \right)_{n \in \mathbb{N}},\ \binom{\lambda}{\mu} \in \mathbb{K}^2 \right\}.$$

Théorème 7 : Cas d'une racine double..

Si on a $\Delta = 0$ alors, en notant r_0 l'unique racine double de $P_{a,b}$, on a :

$$\mathcal{S}_{a,b} = \left\{ \left(\lambda\, r_0^n \; + \; \mu\, n\, r_0^{n-1} \right)_{n\in\mathbb{N}},\ \binom{\lambda}{\mu} \in \mathbb{K}^2 \right\}$$

(en convenant que le premier terme de la suite $\left(n\, r^{n-1} \right)_{n\in\mathbb{N}}$ est nul, y compris pour $r = 0$).

Théorème 8 : Cas sans racine..

On suppose ici $\mathbb{K} = \mathbb{R}$.

Si on a $\Delta < 0$ alors, en notant $r\mathrm{e}^{\mathrm{i}\theta}$ et $r\mathrm{e}^{-\mathrm{i}\theta}$ les deux racines complexes conjuguées de $P_{a,b}$, on a :

$$\mathcal{S}_{a,b} = \left\{ \left(r^n \left(\lambda \cos(n\theta) + \mu \sin(n\theta) \right) \right)_{n\in\mathbb{N}},\ \binom{\lambda}{\mu} \in \mathbb{K}^2 \right\}$$

III.2 Polynômes de Lagrange

Théorème-définition 9 .

La famille $\mathcal{L} = (L_0, \ldots, L_n)$ est une base de $\mathbb{K}_n[X]$. On l'appelle base de Lagrange associée à $a_0, \ldots, a_n$.

Les polynômes L_0, …, L_n s'appellent les polynômes de Lagrange associés à $a_0, \ldots, a_n$.

Remarque 8

Décomposer dans la base de Lagrange est trop simple ! En effet, pour tout polynôme $P \in \mathbb{K}_n[X]$ on a $\left. P \right|_{\mathcal{L}} = \begin{pmatrix} P(a_0) \\ P(a_1) \\ \vdots \\ P(a_n) \end{pmatrix}$.

Remarque 9

- L'approximation lagrangienne est donc concurrente de l'approximation taylorienne. Elle est localement moins précise mais permet de contrôler l'erreur globale.
- L'approximation lagrangienne donne naturellement lieu a des méthodes d'intégration numérique (le cas $n = 0$ correspond à la méthode des rectangles et le cas $n = 1$ à la méthode des trapèzes).

III.3 Base de Taylor

Théorème 10 .

Soit $a \in \mathbb{K}$.

$$(1, X - a, (X - a)^2, \ldots, (X - a)^n) =: \mathcal{T}$$

est une base de $\mathbb{K}_n[X]$.

Remarque 10

C'est un corollaire du TRI[1].

En effet c'est libre et pour tout polynôme $P \in \mathbb{R}_n[X]$, en notant $f = x \mapsto P(x)$

On a

$$\forall x \in \mathbb{R}, f(x) - T_n(x) = \int_a^x \frac{(x-t)^n}{n!} f^{(n+1)}(t)\ \mathrm{d}t$$
$$= 0$$

car $f \in \mathcal{C}^{n+1}([a, x], \mathbb{R})$

Donc $\forall x \in \mathbb{R}, f(x) = f(a) + f'(a)(x - a) + \cdots + f^{(n)} \frac{(x-a)^n}{n!}$

1. Taylor avec reste intégral

Donc

$$P = f(a) + f'(a)(X-a) + \cdots + \frac{f^{(n)(a)}}{n!}(X-a)^n$$

Donc la famille est génératrice.
Or elle a le bon nombre de vecteurs, donc c'est une base et

$$\left| P \right._{\mathcal{T}} = \begin{pmatrix} f(a) \\ f'(a) \\ \frac{1}{2}f''(a) \\ \vdots \\ \frac{1}{n!}f^{(n)}(a) \end{pmatrix}$$

Familles remarquables d'un espace vectoriel

Remarque 1

Pas un sev par exemple : $\mathbb{R}_{=n}[X] \cup \{0\}$ car $X^n - 1 - X^n \notin \mathbb{R}_{=n}[X] \cup \{0\}$

Remarque 2

Pas un sev par exemple : $\mathbb{R}_{=n}[X] \cup \{0\}$ car $X^n - 1 - X^n \notin \mathbb{R}_{=n}[X] \cup \{0\}$

I Familles et combinaisons linéaires

I.1 Familles

Définition 1 : Rappel.

Une famille $\mathcal{F} = (v_i)_{i \in I}$ est la donnée, pour tout élément i de l'ensemble d'indices I, d'un vecteur $v_i \in E$, i. e. une application $\mathcal{F} : I \to E$.

I.2 Sous-familles

Définition 2 : Sous-famille.

Soit $\mathcal{F}$ une famille. On appelle sous-famille de $\mathcal{F} = (v_i)_{i \in I}$ une famille obtenue en « retirant certains vecteurs à $\mathcal{F}$ », c'est-à-dire une famille de la forme $(v_i)_{i \in J}$ avec $J \subset I$.

I.3 Combinaisons linéaires

Définition 3 : Rappel.

On appelle combinaison linéaire des vecteurs d'une famille $\mathcal{F} = (v_i)_{i \in I}$ toute expression de la forme suivante : $\alpha_1 v_{i_1} + \alpha_2 v_{i_2} + \cdots + \alpha_r v_{i_r}$ où les α_k sont des scalaires et les i_k des éléments de I.

Remarque 3

Conséquence des deux identifications précédentes : une CL de $(v_1, \ldots, v_n)$ est toujours de la forme $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n$.

Remarque 4

À toute partie $P \subset E$, on peut canoniquement associer une famille : la famille $(v)_{v \in P}$. On peut donc sans difficulté parler de CL des vecteurs d'une partie de E. On retrouve alors la notion vue dans le chapitre précédent. En particulier, on peut parler du sous-espace vectoriel engendré par une famille.

II Familles remarquables

II.1 Liberté

Définition 4 .

Étant donnée une famille $\mathcal{F}$ de vecteurs de E, on appelle CL triviale des vecteurs de $\mathcal{F}$ la CL obtenue en prenant tous les α_k nuls. La CL triviale est nulle, au sens où elle s'évalue en 0_E, le vecteur nul de E. C'est une CL $(\alpha_1 x_1 + \cdots + \alpha_k x_k)$ où $\begin{cases} (\alpha_i) \in \mathbb{K} \\ (x_i) \in E \end{cases}$

Définition 5 : Liberté.

Une famille est dite libre lorsque sa seule CL nulle est la CL triviale. Dans le cas contraire, elle est dite liée.

Remarque 5

Pour tout $\begin{cases}(\alpha_1, \dots, \alpha_k) \in \mathbb{K}^k \\ (x_1, \dots, x_k) \in E^k\end{cases}$ tels que $\alpha_1 x_1 + \dots + \alpha_k x_k = 0$ alors $\alpha_1 = \alpha_2 = \dots = \alpha_k = 0$

Pour montrer qu'une famille est liée $\exists(\alpha_1, \dots, \alpha_k)$ non tous nuls, $\exists(x_1, \dots, x_k)$ tel que

$$\alpha_1 x_1 + \dots + \alpha_k x_k = 0.$$

Remarque 6

Par définition, une sous-famille d'une famille libre est libre. En contraposant, on obtient que si $\mathcal{F}$ a une sous-famille liée, alors $\mathcal{F}$ est liée. Par contre, une sous-famille d'une famille liée peut très bien être libre.
Soient $(j_1, \dots, j_k) \in J$. Soient $(\alpha_1, \dots, \alpha_k) \in \mathbb{K}^k$ et $(x_{j_1}, \dots, x_{j_k}) \in E^k$ tels que $\alpha_1, x_{j_1} + \dots + \alpha_k x_{j_k} = 0$.
On a $J \subset I$, donc $(j_1, \dots, j_k) \subset I$. Comme $(x_k)_{k \in I}$ est libre.
Donc $\alpha_1 = \dots = \alpha_k = 0$ Donc $(x_k)_{k \in J}$ est libre.
/!\ Une surfamille d'une famille liée est liée **mais** une sous-famille d'une famille liée peut être libre !
Par exemple, (e_1, e_2, e_3) est libre mais (e_1, e_2, e_2, e_1) est liée **Remarque 7**

La liberté est une notion intrinsèque, elle ne dépend pas de E.
Par exemple, la famille $\left(f_\lambda\right)_{\lambda \in \mathbb{R}}$ est aussi libre vue comme famille de vecteurs de $\mathbb{R}^{\mathbb{R}}$.

Définition 6 .
On dit que deux vecteurs u et v de E sont colinéaires, et on note $u \mathbin{/\!/} v$, lorsqu'on a :
$\exists k \in \mathbb{K}, u = kv$ ou $\exists k \in \mathbb{K}, v = ku$.

Remarque 8

0. La famille $\emptyset$ est libre. $\mathbb{T}\ \mathbb{R}\ \mathbb{I}\ \mathbb{V}\ \mathbb{I}\ \mathbb{A}\ \mathbb{L}$
1. Pour $u \in E$, la famille (u) est libre si et seulement si on a $u \neq 0_E$.
2. Pour $(u, v) \in E^2$, la famille (u, v) est libre si et seulement si u et v sont non colinéaires.

II.2 Caractère générateur

Définition 7 .
Une famille $\mathcal{F}$ de vecteurs de E est dite génératrice de E lorsque tout vecteur de E peut s'écrire comme CL des vecteurs de $\mathcal{F}$.

Remarque 9

La notion de famille génératrice n'est pas une notion intrinsèque, elle dépend de E.
Plus précisément, « $\mathcal{F}$ est génératrice de E » peut se reformuler « $E = \operatorname{Vect}(\mathcal{F})$ ». En particulier, toute famille $\mathcal{F}$ est toujours génératrice d'un $\mathbb{K}$-ev : le $\mathbb{K}$-ev $\operatorname{Vect}(\mathcal{F})$! **Remarque 10**

Toute famille $\mathcal{F}$ est génératrice de $\operatorname{Vect}(\mathcal{F})$

II.3 Bases

Définition 8 .
On dit d'une famille $\mathcal{B}$ de vecteurs de E que c'est une base de E lorsque tout vecteur de E peut s'écrire de façon unique comme CL des vecteurs de $\mathcal{B}$.

Proposition 1 : Reformulation de la définition.
Une famille $\mathcal{B}$ de vecteurs de E est une base si et seulement si elle est libre et génératrice de E.

Définition 9 : (informelle).
Lorsqu'un espace vectoriel E est livré en kit avec une base, c'est-à-dire lorsque les vecteurs de cet espace sont, par définition, des CL uniques des vecteurs d'une famille $\mathcal{C}$, cette famille est une base de E et on l'appelle la base canonique de E.

Remarque 11

$((1,0,\dots,0,\dots),(0,1,0,\dots),\dots)$ est une base de l'espace vectoriel des suites de la forme $(u_0,u_1,u_2,\dots,u_n,0,0,0,\dots)$ ie $\{$suites qui stationnent sur $0\}$ **Remarque 12**

À l'aide de la remarque **??**, on peut reformuler la définition 5 du chapitre précédent :

1. Une droite (vectorielle) est un sev de E ayant une base formée d'un seul vecteur.
2. Un plan (vectoriel) est un sev de E ayant une base formée de deux vecteurs.

II.4 Bases adaptées

Définition 10 .

Étant données deux familles $\mathcal{F}=(u_i)_{i\in I}$ et $\mathcal{G}=(v_j)_{j\in J}$, on notera (notation maison) $\mathcal{F}\sqcup\mathcal{G}$ la famille obtenue en concaténant $\mathcal{F}$ et $\mathcal{G}$, qu'on peut, par exemple, formellement définir par $\mathcal{F}\sqcup\mathcal{G}=(w_k)_{k\in K}$ où $K=I\times\{0\}\cup J\times\{1\}$ et $w_k=\begin{cases} u_i \text{ si } k \text{ est de la forme } (i,0)\\ v_j \text{ si } k \text{ est de la forme } (j,1).\end{cases}$

Def. 1: trou

$$A_1(X)B_2(X) = A_2(X)B_1(X)$$

Prop-Def. 2: Dem.

Existance Soit $\frac{A}{B} \in \mathbb{K}[X]$
Notons $D := A \wedge B$
Puis $\begin{cases} \tilde{A} &= \frac{A}{D} \\ \tilde{D} &= \frac{B}{D} \end{cases}$
Par homogénéité de PGCD :

$$\tilde{A} \wedge \tilde{B} = 1$$

On note μ le coefficient dominant de B puis

$$P = \frac{\tilde{A}}{\mu}$$
$$Q = \frac{\tilde{B}}{\mu}$$

On a bien $\begin{cases} P \wedge Q = 1 \\ \frac{P}{Q} = \frac{\tilde{A}}{\tilde{B}} = \frac{A}{B} \\ Q \text{ unitaire} \end{cases}$

Unicité Supposons avoir deux formes irréductibles

$$\frac{A}{B} = \frac{P_1}{Q_1} = \frac{P_2}{Q_2}$$

donc $P_1Q_2 = P_2Q_1$
On a

$$\begin{cases} Q_1 & |P_1Q_2 \\ P_1 \wedge Q_1 & = 1 \end{cases}$$

$$\begin{aligned} \text{donc } Q_1|Q_2 &\qquad \text{d'après le lemme de Gauss} \\ Q_2|Q_1 &\qquad \text{de même} \end{aligned}$$

Or Q_1, Q_2 sont unitaires donc $Q_1 = Q_2$
En réinjectant et par intégrité $P_1 = P_2$

Exercice 1

$$P' \wedge P = 1 \iff P \text{ unitaire et toutes ses racines sont simples}$$

Prop-Def. 3 dem. L'indépendance au représentant choisi

Prop-Def. 5 dem. Soit $F = \frac{A}{B} = \frac{C}{D}$
$i.e. A \times D = C \times B$
On veut montrer

$$\begin{aligned}
\frac{A'B - AB'}{B^2} &= \frac{C'D - D'C}{D^2} \\
\iff D^2(A'B - B'A) &= B^2(C'D - D'C) \\
\iff A'BD^2 - ADB'D &= C'B^2DB - CD'B^2 \\
\iff A'BD^2 - BCB'D &= C'BDB - ADD'B \\
\iff BD(A'D - CB') &= BD(C'B - AD') \\
\iff A'D - CB' &= C'B - AD' \\
\iff A'D + AD' &= C'B + CB' \\
\iff (AD)' &= (BC)'
\end{aligned}$$

C'est vrai, ouf!!!

Exemple 1

$$\frac{aX + b}{cX + d}$$

Exemple 2: Trou juste avant

$$F' \leq \deg F - 1$$

Exemple 2

$$\begin{aligned}
\deg \left(\frac{aX + b}{cX + d} \right)' &= \frac{a(cX + d) - c(aX + b)}{(cX + d)^2} \\
&= \frac{ad - bc}{(cX + d)^2} \\
&= -2
\end{aligned}$$

Def. 7: Reformulation, trous

1. λ n'est ni un zéro ni un pôle.
2. λ est un zéro de multiplicité $a - b$
3. λ est pôle de multiplicité $b - a$

Remq. 5: Trou les zéros de $\frac{A}{B}$

Prop-Def. 9: Dem. D'après le théorème de division euclidienne

$$\exists!(Q,R),\ \begin{cases} A & = BQ + R \\ Q & \in \mathbb{K}[X] \\ R & \in \mathbb{K}_{\deg B - 1}[X] \end{cases}$$

$$\iff \exists!(Q,R),\ \begin{cases} F & = Q + \frac{R}{B} \\ Q & \in \mathbb{K}[X] \\ \deg R & < \deg B \end{cases}$$

$$\iff \exists!(Q,R),\ \begin{cases} F & = Q + G \\ Q & \in \mathbb{K}[X] \\ \underbrace{\deg(BG) - \deg B}_{\deg G} & < 0 \end{cases}$$

Exemple: partie polynomiale de $\frac{X^3+2X+1}{X^2-1}$

$$\begin{array}{c|c} X^3 + 2X + 1 & X^2 - 1 \\ X^3 - X & \text{X} \\ 3X + 1 & \end{array}$$

$$\frac{X^3 + 2X + 1}{X^2 - 1} = \underbrace{X}_{\text{partie polynomiale}} + \frac{3X+1}{X^2+1}$$

Thm. 2 Si $B = \mu(X - \lambda_1)\cdots(X - \lambda_n)$ alors il existe Q unique et $(\alpha_1, \ldots, \alpha_n)$ uniques tels que

$$\frac{A}{B} = Q + \frac{\alpha_1}{X - \lambda_1} + \cdots + \frac{\alpha_n}{X - \lambda_n}$$

et Q est la partie polynomiale de $\frac{A}{B}$

Thm. 2: Dem. D'après le théorème de division euclidienne, il suffit de montrer que

$$\forall R \in \mathbb{R}_{\deg B - 1}[X],\ \exists! \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in \mathbb{K}^n,\ \frac{R}{B} = \frac{\alpha_1}{X - \lambda_1} + \cdots + \frac{\alpha_n}{X - \lambda_n}$$

Notons $\begin{cases} E & = \mathbb{K}^n \\ F & = \frac{1}{B} \underbrace{\mathbb{K}_{\deg B - 1}[X]}_{\text{polynômes de degré} < \deg B} \end{cases}$

$$\phi : \begin{cases} E & \to F \\ \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} & \mapsto \frac{\alpha_1}{X - \lambda_1} + \cdots + \frac{\alpha_n}{X - \lambda_n} \end{cases}$$

On a

$$
\begin{aligned}
&\dim\left(\mathbb{K}_{\deg B-1}[X]\right) = n \\
\implies &\dim\left(\frac{1}{B}\mathbb{K}_{\deg B-1}[X]\right) = n \\
&\text{et } \dim \mathbb{K}^n = n
\end{aligned}
$$

ϕ est linéaire par distributivité de $\cdot$ sur $+$
Par caractérisation des isomorphismes en dimension finie:

$$\phi \text{ bijective} \iff \phi \text{ injective}$$

$$\operatorname{Ker}\phi = \left\{ \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in \mathbb{K}^n,\ \frac{\alpha_1}{X-\lambda_1} + \cdots + \frac{\alpha_n}{X-\lambda_n} = 0 \right\}$$

Or $\left(\frac{1}{X-\lambda_1},\ \frac{1}{X-\lambda_2},\ \ldots,\ \frac{1}{X-\lambda_n}\right)$ est *libre*
Donc $\operatorname{Ker}\phi = \{0\}$ donc ϕ est bijective
$i.e. \forall \frac{R}{B} \in F,\ \exists! \begin{pmatrix} \alpha_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{K}^n,\ \phi \begin{pmatrix} \alpha_1 \\ \vdots \\ a_n \end{pmatrix} = \frac{R}{B}$
$i.e. \forall R \in \mathbb{R}_{\deg B-1}[X],\ \exists! \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in \mathbb{K}^n,\ \frac{R}{B} = \frac{\alpha_1}{X-\lambda_1} + \cdots + \frac{\alpha_n}{X-\lambda_n}$

Exemple DES de $\frac{1}{(X^2+1)(X^2+4)}$

$$\frac{1}{(X^2+1)(X^2+4)} = \frac{\alpha X+\beta}{X^2+1} + \frac{\gamma X+\delta}{X^2+4}$$

Passons par $\mathbb{C}(X)$

$$
\begin{aligned}
\frac{1}{(X^2+1)(X^2+4)} &= \frac{a}{X-i} + \frac{b}{X+i} + \frac{c}{X-2i} + \frac{d}{X+2i} \\
\frac{1}{(X+i)(X-i)} a + (X-i)(\ldots) \quad \times (X-i)a & \qquad = -\frac{i}{6} \impliedby X = i \\
b = \overline{a} = \frac{i}{6} & \qquad \text{par unicité de la DES} \\
\frac{1}{(X^2+1)(X+2i)} c + (X-i)(\ldots) \quad \times (X-2i)a & \qquad = \frac{i}{12} \impliedby X = 2i \\
b = \overline{c} = -\frac{i}{12} & \qquad \text{par unicité de la DES}
\end{aligned}
$$

En regroupant chaque pôle avec son conjugué:

$$
\begin{aligned}
\frac{1}{(X^2+1)(X^2+4)} &= \frac{1}{6}\left(\frac{i}{X+i} - \frac{i}{X-i}\right) + \frac{1}{12}\left(\frac{i}{X-2i} - \frac{i}{X+2i}\right) \\
&= \frac{1}{6}\frac{2}{X^2+1} + \frac{1}{12}\frac{-4}{X^2+4} \\
&= \frac{1/3}{X^2+1} - \frac{1/3}{X^2+4}
\end{aligned}
$$

Thm. 3: Dem.

$$
\begin{aligned}
P &= \mu \prod_{i=1}^{r} (X-\lambda_i)^{m_i} \\
\deg P &= \sum_{k=1}^{r} m_k \\
P' &=
\end{aligned}
$$

En général:

$$
\left(\prod_{i=1}^{n} u_i\right)' = \sum_{k=1}^{n} u_1 \cdots u_{i-1} \cdot u_i' \cdot u_{i+1} \cdots u_n
$$

$$
\begin{aligned}
P' &= \mu \sum_{k=1}^{r} (X-\lambda_1)^{m_1} \times \ldots \times (X-\lambda_{i-1})^{m_{i-1}} \times ((X-\lambda_i)^{m_i})' \times (X-\lambda_{i+1})^{m_{i+1}} \times \ldots \times (X-\lambda_r)^{m_r} \\
\frac{P'}{P} &= \sum_{k=1}^{r} \frac{(X-\lambda_1)^{m_1} \times \ldots \times (X-\lambda_{i-1})^{m_{i-1}} \times m_i \times (X-\lambda_{i+1})^{m_{i+1}} \times \ldots \times (X-\lambda_r)^{m_r}}{(X-\lambda_1)^{m_1} \times \ldots \times (X-\lambda_{i-1})^{m_{i-1}} \times (X-\lambda_i)^{m_i} \times (X-\lambda_{i+1})^{m_{i+1}} \times \ldots \times (X-\lambda_r)^{m_r}} \\
&= \sum_{k=1}^{r} \frac{m_i}{X-\lambda_i}
\end{aligned}
$$

App. 7 Cherchons les solutions non nulles
Notons $n := \deg P$

$$
\begin{aligned}
P'|P &\iff \exists Q \in \mathbb{R}[X],\ P = P' \times Q \\
&\iff \exists Q \in \mathbb{R}_1[X],\ P = P' \times Q && \text{pour des raisons de degré} \\
&\iff \exists \lambda \in \mathbb{R},\ P = P' \times \frac{1}{n}(X-\lambda) && \text{pour des raisons de coefficient dominant} \iff \exists \lambda \in \mathbb{R}, \frac{P'}{P} = \frac{n}{X-\lambda} \\
&\iff \exists \lambda \in \mathbb{R}, P = \mu(X-\lambda)^n
\end{aligned}
$$

Limites d'une fonction.

Contexte : dans tout le chapitre

- I désigne une réunion d'intervalles non triviaux, par exemple $[1,2[$ ou $\mathbb{R}^*$ ou $D_{\tan}$;
- $f : I \to \mathbb{R}$ désigne une application de I dans $\mathbb{R}$;
- a désigne un point adhérent à I.

La notion de point adhérent est présentée dans la partie I.1., mais pour une réunion d'intervalles non triviaux on peut simplement dire qu'un point adhérent à I est ou bien un élément de I ou bien une extrémité de I.
Par exemple l'ensemble des points adhérents à $]-1,2]\cup]3,+\infty[$ est $[-1,2]\cup[3,+\infty]$.

I Voisinages

I.1 Définition

Définition 1 : Voisinage.

Soit $\alpha \in \overline{\mathbb{R}}$.

1. Si $\alpha \in \mathbb{R}$, on appelle <u>voisinage de α</u> tout ensemble V_α vérifiant $\exists \varepsilon > 0,\ ]\alpha-\varepsilon, \alpha+\varepsilon[\subset V_\alpha$.
2. Si $\alpha = +\infty$, on appelle <u>voisinage de α</u> tout ensemble $V_{+\infty}$ vérifiant $\exists A \in \mathbb{R},\ ]A, +\infty[\subset V_{+\infty}$.
3. Si $\alpha = -\infty$, on appelle <u>voisinage de α</u> tout ensemble $V_{-\infty}$ vérifiant $\exists B \in \mathbb{R},\ ]-\infty, B[\subset V_{-\infty}$.

Notation 1 Pour écrire des énoncés formels portant sur les voisinages, notons $\boldsymbol{\mathcal{V}_a}$ l'ensemble des voisinages de a.

Définition 2 : Point adhérent.

On dit que $a \in \overline{\mathbb{R}}$ est un <u>point adhérent à I</u> lorsque tout voisinage de a rencontre I.
Autrement dit : pour tout voisinage V_a de a, on a $V_a \cap I \neq \emptyset$.
On note $\overline{I}$ l'ensemble des points adhérents à I.

I.2 Propriétés des voisinages

Remarque 1

Une partie $P \subset \mathbb{R}$ est voisinage de chacun de ses éléments si et seulement si ....

Proposition 1 : Intersection.

Pour tout $\alpha \in \overline{\mathbb{R}}$, l'intersection de deux voisinages de α est un voisinage de α.

Proposition 2 : Séparation.

Soient $\alpha \neq \beta$ deux éléments distincts de $\overline{\mathbb{R}}$.
Alors il existe un voisinage V_α de α et un voisinage V_β de β tels que $V_\alpha \cap V_\beta = \emptyset$.

I.3 Propriétés locales

Définition 3 .

On dit qu'une propriété $P(f)$ portant sur f est <u>vraie au voisinage de a</u> lorsqu'il existe un voisinage de a sur lequel la propriété est vraie, i. e. pour lequel $P(f_{|V_\alpha})$ est vraie.

Définition 4 .

On dit que f atteint un extremum local (maximum local ou minimum local) en $x_0 \in I$ lorsqu'il existe un voisinage de x_0 sur lequel $f(x_0)$ est un extremum (maximum ou minimum) de f.

II Limites

II.1 Définition

Définition 5 .

On dit que <u>f a pour limite ℓ en a</u> et on note $f \underset{a}{\longrightarrow} \ell$ ou $f(x) \underset{x \to a}{\longrightarrow} \ell$ lorsque la propriété suivante est vérifiée :

pour tout voisinage V_ℓ de ℓ, il existe un voisinage V_a de a tel que $\forall x \in I \cap V_a,\ f(x) \in V_\ell$.

Remarque 2

Cette définition est la définition **francophone** de la limite. En particulier, si f est définie en a (*i. e.* $a \in I$ et pas seulement $a \in \overline{I}$) et que $f \underset{a}{\longrightarrow} \ell$, alors nécessairement $\ell = f(a)$ (la réciproque étant fausse).

Par exemple l'application $\chi_{\{0\}} = x \mapsto \begin{cases} 1 \text{ si } x = 0 \\ 0 \text{ sinon} \end{cases}$ n'a pas de limite en 0. On verra plus bas la version anglophone.

Dessin :

Théorème 1 : Unicité de la limite.

Si f a une limite en a alors cette limite est unique, on la note alors $\lim\limits_a f$ ou $\lim\limits_{x \to a} f(a)$.

Notation 2 Sous réserve d'existence, on notera donc $\lim\limits_a f$ ou $\lim\limits_{x \to a} f(x)$ l'unique limite de f en a.

Définition 6 : Limites à gauche, à droite.

1. On dit que <u>f a pour limite à gauche ℓ en a</u> et on note $f \underset{a^-}{\longrightarrow} \ell$ ou $f(x) \underset{x \to a^-}{\longrightarrow} \ell$ lorsqu'on a $f_{|I \cap]-\infty, a[} \underset{a}{\longrightarrow} \ell$.
2. On dit que <u>f a pour limite à droite ℓ en a</u> et on note $f \underset{a^+}{\longrightarrow} \ell$ ou $f(x) \underset{x \to a^+}{\longrightarrow} \ell$ lorsqu'on a $f_{|I \cap]a, +\infty[} \underset{a}{\longrightarrow} \ell$.

Notation 3 L'unicité de la limite implique l'unicité des limites à gauche et à droite. Sous réserve d'existence, on notera donc $\ell = \lim\limits_{a^-} f$ ou $\ell = \lim\limits_{x \to a^-} f(x)$ pour $f \underset{a^-}{\longrightarrow} \ell$; et $\ell = \lim\limits_{a^+} f$ ou $\ell = \lim\limits_{x \to a^+} f(x)$ pour $f \underset{a^+}{\longrightarrow} \ell$.

Proposition 3 : Lien avec les limites.

On a deux cas :

1. Si $a \notin I$, alors : $f \underset{a}{\longrightarrow} \ell \iff f \underset{a^-}{\longrightarrow} \ell$ et $f \underset{a^+}{\longrightarrow} \ell$.
2. Si $a \in I$, alors : $f \underset{a}{\longrightarrow} \ell \iff f \underset{a^-}{\longrightarrow} \ell$ et $f \underset{a^+}{\longrightarrow} \ell$ et $f(a) = \ell$.

Remarque 3

Si le second point vous perturbe (sait-on jamais) et que vous auriez voulu que $\chi_{\{0\}} = x \mapsto \begin{cases} 1 \text{ si } x = 0 \\ 0 \text{ sinon} \end{cases}$ ait une limite en 0, c'est que vous avez en tête la **version anglo-saxonne** de la définition de la limite. Avec le vocabulaire francophone, on parle de **limite épointée** : <u>f a pour limite épointée ℓ en a</u> lorsque $f_{|I \setminus \{a\}} \underset{a}{\longrightarrow} \ell$.
Évidemment, dans le cas où $a \notin I$, limite et limite épointée coïncident.

II.2 Critères d'existence de limite

Théorème 2 .

Si f a une limite finie en a, alors f est bornée **au voisinage de $\boldsymbol{a}$**.

Théorème 3 : TLM, version fonctions.

Soient $f \in \mathbb{R}^I$ **croissante** et $a \in \overline{I}$. Alors :

i. Si f est définie à gauche en a, $\lim\limits_{a^-} f$ existe.

ii. Si f est définie à droite en a, $\lim\limits_{a^+} f$ existe.

iii. Toutes les inégalités suivantes sont vraies lorsqu'elles ont un sens : $\lim\limits_{a^-} f \leqslant f(a) \leqslant \lim\limits_{a^+} f$.

Énoncé analogue pour f décroissante.

Remarque 4
Pour le troisième point, si par exemple la fonction est définie au voisinage de a sauf en a, on a seulement $\lim\limits_{a^-} f \leqslant \lim\limits_{a^+} f$. Si la fonction est définie à droite de a et en a, mais pas à gauche de a, on a seulement $f(a) \leqslant \lim\limits_{a^+} f$. Etc.

Théorème 4 : TDG, version fonctions.

Soient f, g, h trois fonctions comme la fonction f du préambule.

a. Convergence par encadrement : supposons $\begin{cases} f \leqslant g \leqslant h \text{ au voisinage de } a \\ \exists \ell \in \mathbb{R},\ f \underset{a}{\longrightarrow} \ell \text{ et } h \underset{a}{\longrightarrow} \ell. \end{cases}$ Alors $g \underset{a}{\longrightarrow} \ell$.

b. Divergence par minoration : supposons $\begin{cases} f \leqslant g \text{ au voisinage de } a \\ f \underset{a}{\longrightarrow} +\infty. \end{cases}$ Alors $g \underset{a}{\longrightarrow} +\infty$.

Divergence par majoration : supposons $\begin{cases} g \leqslant h \text{ au voisinage de } a \\ h \underset{a}{\longrightarrow} -\infty. \end{cases}$ Alors $g \underset{a}{\longrightarrow} -\infty$.

II.3 Opérations sur les limites

Théorème 5 : Opérations algébriques sur les limites.

Soient f, g comme dans le préambule ; $\ell_1, \ell_2 \in \overline{\mathbb{R}}$; et $\square \in \{+, -, \times, \div\}$.

Supposons qu'on ait $f \underset{a}{\longrightarrow} \ell_1$, qu'on ait $g \underset{a}{\longrightarrow} \ell_2$, et que $\ell_1 \square \ell_2$ ait un sens.

Alors $f \square g \underset{a}{\longrightarrow} \ell_1 \square \ell_2$.

Théorème 6 : Compositions de limites.

Soient I et J deux réunions d'intervalles non triviaux, $a \in \overline{I}$, $b \in \overline{J}$ et $\begin{cases} f : I \to J \\ g : J \to \mathbb{R} \end{cases}$, telles que $\begin{cases} \lim\limits_{a} f = b \\ \lim\limits_{b} g = c. \end{cases}$

Alors $\lim\limits_{a} g \circ f = c$.

Remarque 5

On voit là la grande force de la version francophone de la limite. Pour obtenir une version de ce théorème qui reste vraie avec la version anglophone, il faut se contorsionner.

II.4 Caractérisation séquentielle de la limite et applications

Théorème 7 : Caractérisation séquentielle de la limite.

Les propositions suivantes sont équivalentes :

i. $f \underset{a}{\longrightarrow} \ell$;

ii. $\forall (u_n)_{\in \mathbb{N}} \in I^{\mathbb{N}},\ u_n \to a \Rightarrow f(u_n) \to \ell$.

Remarque 6

En utilisant la caractérisation séquentielle de la limite, on peut redémontrer les théorèmes précédents (opérations algébriques, composition, TdG, et même TLM) plus facilement qu'à l'aide de la définition !

Théorème 8 : Stabilité des inégalités larges par passage à la limite.

Si $f \leqslant g$ au voisinage de a et qu'on a $f \underset{a}{\longrightarrow} \ell_1$ et $g \underset{a}{\longrightarrow} \ell_2$ alors $\ell_1 \leqslant \ell_2$.

Fonctions "mieux que dérivables".

Contexte : dans tout le chapitre
- I désigne une réunion d'intervalles non triviaux ;
- f désigne une application de I dans $\mathbb{R}$, sauf mention du contraire.

I Dérivées d'ordre supérieur

I.1 Définitions

Définition 1 .

1. f est dite n fois dérivable lorsque f', f'', ..., $f^{(n)}$ existent ;
2. f est dite n fois continûment dérivable lorsque f', f'', ..., $f^{(n)}$ existent et $f^{(n)}$ est continue ;
3. f est dite indéfiniment dérivable lorsque pour tout entier $k \in \mathbb{N}$, $f^{(k)}$ existe.

Notation 1

1. Pour $n \geqslant 1$, on note $\mathcal{D}^n(I,\mathbb{R})$ l'ensemble des fonctions n fois dérivables de I dans $\mathbb{R}$;
2. pour $n \in \mathbb{N}$, on note $\mathcal{C}^n(I,\mathbb{R})$ l'ensemble des fonctions n fois continûment dérivables de I dans $\mathbb{R}$;
3. on note $\mathcal{C}^\infty(I,\mathbb{R})$ l'ensemble des fonctions indéfiniment dérivables de I dans $\mathbb{R}$.

Remarque 1

- Pour $n \in \mathbb{N}$ on a $\mathcal{C}^n(I,\mathbb{R}) = \{f',\ f \in \mathcal{C}^{n+1}(I,\mathbb{R})\}$ et, si $n \geqslant 1$, $\mathcal{D}^n(I,\mathbb{R}) = \{f',\ f \in \mathcal{D}^{n+1}(I,\mathbb{R})\}$.
- La tradition veut qu'on note $\mathcal{D}^0(I,\mathbb{R})$ l'ensemble $\{f',\ f \in \mathcal{D}^1(I,\mathbb{R})\}$ des fonctions de I dans $\mathbb{R}$ qui sont des dérivées.

I.2 Structure

I.3 Prolongement $\mathcal{C}^n$

Théorème 1 : propriétés de la n-dérivation.

Soient $n \in \mathbb{N}$ et $f, g \in \mathcal{D}^n(I,\mathbb{R})$. Alors on a :

1. Linéarité : $\forall(\lambda,\mu) \in \mathbb{R}^2,\ \lambda f + \mu g \in \mathcal{D}^n(I,\mathbb{R})$ et $(\lambda f + \mu g)^{(n)} = \lambda f^{(n)} + \mu g^{(n)}$;
2. Leibniz : $fg \in \mathcal{D}^n(I,\mathbb{R})$ et $(fg)^{(n)} = \sum\limits_{k=0}^{n} \binom{n}{k} f^{(k)} g^{(n-k)}$;
3. Faà di Bruno ~~light~~ per i bambini : $\forall(\alpha,\beta) \in \mathbb{R}^2,\ x \mapsto f(\alpha x+\beta) \in \mathcal{D}^n(I,\mathbb{R})$ et $\big(x \mapsto f(\alpha x+\beta)\big)^{(k)} = x \mapsto \alpha^n f^{(n)}(\alpha x+\beta)$.

Plus généralement :

4. $\forall f \in \mathcal{D}^n(I,J),\ \forall g \in \mathcal{D}^n(J,\mathbb{R}),\ g \circ f \in \mathcal{D}^n(I,\mathbb{R})$;
5. Soit $f \in \mathcal{D}^n(I,J)$ bijective telle que f' ne s'annule pas, alors $f^{-1} \in \mathcal{D}^n(J,I)$ (pour I un intervalle).

Remarque : si on suppose plutôt $f, g \in \mathcal{C}^n(I,\mathbb{R})$, alors il en va de même pour $\lambda f + \mu g$, fg, $x \mapsto f(\alpha x+\beta)$, $f \circ g$ ou f^{-1}.

Démonstration. Le point 2. a déjà été démontré, les autres s'obtiennent par récurrence : exercice. □

Application 1 $\mathcal{D}^n(I,\mathbb{R})$, $\mathcal{C}^n(I,\mathbb{R})$ et $\mathcal{C}^\infty(I,\mathbb{R})$ sont des sous-algèbres de $(\mathbb{R}^I, +, \times, \cdot)$.

On a déjà vu beaucoup d'applications de la formule de Leibniz donc on n'y revient pas ici.

Théorème 2 : théorème de prolongement $\mathcal{C}^n$.

Soit $a \in I$ et $f \in \mathcal{C}^n(I \setminus \{a\},\mathbb{R})$. On suppose qu'il existe $n+1$ réels ℓ_0, ..., ℓ_n tels que
$$\begin{cases} f(x) \underset{x\to a}{\longrightarrow} \ell_0 \\ f'(x) \underset{x\to a}{\longrightarrow} \ell_1 \\ \vdots \\ f^{(n)}(x) \underset{x\to a}{\longrightarrow} \ell_n. \end{cases}$$
Alors f est prolongeable par continuité sur I et son prolongement est $\mathcal{C}^n(I,\mathbb{R})$.
En notant encore f ce prolongement, on a $f(a) = \ell_0,\ f'(a) = \ell_1,\ \ldots,\ f^{(n)}(a) = \ell_n$.

II Formules de Taylor

II.1 Contexte

Définition 2 .

Soient $a \in I$ et $f \in \mathcal{D}^n(I,\mathbb{R})$.

1. On appelle polynôme de Taylor de f en a à l'ordre n le polynôme
$$T_n(X) = f(a) + f'(a)(X-a) + \frac{f''(a)}{2}(X-a)^2 + \ldots + \frac{f^{(n)}(a)}{n!}(X-a)^n.$$
2. On appelle reste de Taylor de f en a à l'ordre n l'application
$$R_n = x \mapsto f(x) - T_n(x) = x \mapsto f(x) - f(a) - f'(a)(x-a) - \frac{f''(a)}{2}(x-a)^2 - \ldots - \frac{f^{(n)}(a)}{n!}(x-a)^n.$$

II.2 Taylor avec reste intégral

Théorème 3 : Formule de Taylor avec reste intégral.

Soient $n \in \mathbb{N}$, $a \in \mathbb{R}$, $x \in \mathbb{R}$ et $f \in \mathcal{C}^{n+1}([a,x],\mathbb{R})$ (ou $\mathcal{C}^{n+1}([x,a],\mathbb{R})$). Alors on a

$$\begin{aligned} R_n(x) &= \int_a^x \frac{(x-t)^n}{n!} f^{(n+1)}(t)\,\mathrm{d}t \qquad \text{i. e.} \\ f(x) &= f(a) + f'(a)(x-a) + \frac{f''(a)}{2}(x-a)^2 + \ldots + \frac{f^{(n)}(a)}{n!}(x-a)^n + \int_a^x \frac{(x-t)^n}{n!} f^{(n+1)}(t)\,\mathrm{d}t \end{aligned}$$

Remarque 2

L'égalité de Taylor avec reste intégral généralise donc le théorème fondamental de l'analyse.

II.3 Taylor Lagrange

Théorème 4 : Inégalité de Taylor-Lagrange.

Soient $n \in \mathbb{N}$, $a \in \mathbb{R}$, $x \in \mathbb{R}$ et $f \in \mathcal{C}^{n+1}([a,x],\mathbb{R})$ (ou $\mathcal{C}^{n+1}([x,a],\mathbb{R})$).

Alors on a : $\left|R_n(x)\right| = \left|f(x) - T_n(x)\right| \leqslant \dfrac{|x-a|^{n+1}}{(n+1)!} \sup\limits_{[a,x]} \left|f^{(n+1)}\right|$

II.4 Taylor-Young

Lemme 1 : « $\displaystyle\int o(x^n) = o\left(x^{n+1}\right)$ ».

Soient $n \in \mathbb{N}$ et $x \in \mathbb{R}$. On a alors : $\displaystyle\int_0^x o_0(t^n)\,\mathrm{d}t = o_0\left(x^{n+1}\right)$

Théorème 5 : Taylor-Young.

Soient $n \in \mathbb{N}$, $a \in \mathbb{R}$, $x \in \mathbb{R}$ et $f \in \mathcal{C}^n([a,x],\mathbb{R})$ (ou $\mathcal{C}^n([x,a],\mathbb{R})$). Alors on a

$$\begin{aligned} f(x) &= T_n(x) + o_a\left((x-a)^n\right) \\ &= f(a) + f'(a)(x-a) + \frac{f''(a)}{2}(x-a)^2 + \ldots + \frac{f^{(n)}(a)}{n!}(x-a)^n + o_a\left((x-a)^n\right) \end{aligned}$$

II.5 Développements limités

Définition 3 : (rappel).

On appelle développement limité (DL) de f un développement asymptotique de f formé de monômes.

Plus précisément, pour $a \in \overline{I}$, on peut définir un $DL_n(a)$ de f comme suit :

- si $a = 0$, un $DL_n(0)$ de f est une réécriture de la forme $f(x) = a_0 + a_1 x + \cdots + a_n x^n + o(x^n)$;
- si $a \in \mathbb{R}$, un $DL_n(a)$ de f est une réécriture de la forme $f(x) = a_0 + a_1(x-a) + \cdots + a_n(x-a)^n + o\big((x-a)^n\big)$;
- si $a = \pm\infty$, un $DL_n(\pm\infty)$ de f est une réécriture de la forme $f(x) = a_0 + \frac{a_1}{x} + \cdots + \frac{a_n}{x^n} + o\Big(\frac{1}{x^n}\Big)$.

Remarque 3

Un DL n'existe pas toujours. Par exemple, pour $a \in I$, et pour résumer ce qu'on a vu précédemment :

1. f continue en $a \Leftrightarrow f$ a un $DL_0(a)$;
2. f dérivable en $a \Leftrightarrow f$ a un $DL_1(a)$;
3. f $\mathcal{C}^n$ au voisinage de $a \Rightarrow f$ a un $DL_n(a)$.

Ainsi $x \mapsto \lfloor x \rfloor$ n'a de $DL_n(0)$ pour aucune valeurs de n ; $x \mapsto |x|$ n'a de $DL_n(0)$ que pour $n = 0$, etc. **Remarque 4**

Attention, Taylor-Young donne seulement une **condition suffisante** d'existence de DL. Exemple :

$$f(x) := \begin{cases} x^2 \sin \frac{1}{x} & \text{si } x \neq 0 \\ 0 & \text{sinon} \end{cases}$$

n'est pas $\mathcal{C}^1$ mais elle a un $DL_1(0)$ car elle est dérivable :

$$f(x) = 0 + 0x + o(x)$$

Plus généralement, on montre de même que :

$$f_n(x) := \begin{cases} x^{n+1} \sin \frac{1}{x^n} & \text{si } x \neq 0 \\ 0 & \text{sinon} \end{cases}$$

n'est pas $\mathcal{C}^1$ (donc pas $\mathcal{C}^n$) mais elle a un $DL_n(0)$:
Pour $x \neq 0$, f_n est dérivable en x et

$$\begin{aligned} f_n'(x) &= (n+1)x^n \sin \frac{1}{x^n} + \cancel{x^{n+1}} \frac{-n}{\cancel{x^{n+1}}} \cos \frac{1}{x^n} \\ &= \underbrace{(n+1)x^n \sin \frac{1}{x^n}}_{\substack{\longrightarrow 0 \\ x\to 0}} + \underbrace{-n \cos \frac{1}{x^n}}_{\substack{\longrightarrow \text{PDL} \\ x\to 0}} \end{aligned}$$

D'où f_n' n'a pas de limite.
De plus,

$$\begin{aligned} f_n'(0) &= \lim_{x\to 0} \tau_{x,f}(0) \\ &= x^n \sin \frac{1}{x^n} \\ &\underset{\infty}{\longrightarrow} 0 \end{aligned}$$

Enfin,

$$f_n(x) = 0 + 0x + 0x^2 + \cdots + 0x^n + o(x^n) = o(x^n)$$

Théorème 6 .

Pour tout $a \in \overline{I}$ et tout $n \in \mathbb{N}$, un $DL_n(a)$ de f est toujours unique.

Corollaire 1 .

Supposons que f a un $DL_n(0)$.

1. Si f est paire, alors le $DL_n(0)$ de f est pair.
2. Si f est impaire, alors le $DL_n(0)$ de f est impair.

Théorème 7 .

On peut intégrer un $DL_n(a)$.

III Bilan des inclusions rencontrées

IV Extension aux fonctions à valeurs dans $\mathbb{C}$ ou $\mathbb{R}^n$

$\mathbb{K}[X]$

Contexte : dans ce chapitre, $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$ (mais en pratique on prendra $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$).

Objectifs du chapitre :

— Définir rigoureusement les objets rencontrés en TACMAS.

— Démontrer les théorèmes admis en TACMAS.

— Décrire l'arithmétique de $\mathbb{K}[X]$.

I Construction. Structure.

I.1 Algèbre $\mathbb{K}[X]$

Définition 1 .

- On appelle indéterminée la lettre X.
- On appelle polynôme en X à coefficients dans $\mathbb{K}$ toute combinaison linéaire formelle de puissances de l'indéterminée X.
- On appelle monôme tout polynôme de la forme a_nX^n.

Définition 2 .

On appelle degré de P l'élément de $\mathbb{N} \cup \{-\infty\}$ suivant : $\deg(P) = \sup\limits_{\overline{\mathbb{R}}} \{i,\ a_i \neq 0\}$.

Ainsi un polynôme est nul si et seulement si son degré est $-\infty$ et, si $a_n \neq 0$, alors $\deg(a_0+a_1X+\cdots+a_nX^n) = n$.

Notation 1

- On note $\mathbb{K}[X]$ l'ensemble de tous les polynômes à coefficients dans $\mathbb{K}$.
- On note $\mathbb{K}_n[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$ de degré $\leqslant n$.

Remarque 1

On peut donc agréablement noter un polynôme $\sum\limits_{k=0}^{+\infty} a_kX^k$, où la suite $(a_k)_{k\in\mathbb{N}}$ est nulle à partir d'un certain rang (on dit aussi qu'elle est presque nulle). Le polynôme nul correspond alors à la suite $(a_k)_{k\in\mathbb{N}}$ telle que $a_k = 0$ pour tout $k \in \mathbb{N}$.

Théorème 1 : Identification.

Deux polynômes sont égaux si et seulement si les suites presque nulles $(a_k)_{k\in\mathbb{N}}$ et $(b_k)_{k\in\mathbb{N}}$ sont identiques.
Dit autrement : $P = Q \Leftrightarrow \forall k \in \mathbb{N},\ a_k = b_k$.

I.2 Structure d'algèbre

Définition 3 .

On définit une loi de composition interne $+$ sur $\mathbb{K}[X]$ de la manière suivante :
si $P = \sum\limits_{k=0}^{+\infty} a_kX^k$ et $Q = \sum\limits_{k=0}^{+\infty} b_kX^k$ sont deux éléments de $\mathbb{K}[X]$, on note $P+Q$ le polynôme :

$P + Q = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_n + b_n)X^n$.

Proposition 1 .

$(\mathbb{K}[X], +)$ forme un groupe de neutre le polynôme nul.

Remarque 2

$\Psi : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K}^{\mathbb{N}} \\ P = a_0 + a_1X + \cdots + a_nX^n & \mapsto & (a_0, a_1, \cdots, a_n, 0, 0, \dots, 0, \dots) \end{array} \right.$ est un morphisme de groupe.

$Im(\Psi) = \mathbb{K}^{(\mathbb{N})}$ (les suites presque nulles). La corestriction $\Psi : \mathbb{K}[X] \to \mathbb{K}^{(\mathbb{N})}$ est un isomorphisme de groupe.

Définition 4 .

On définit une loi de composition externe $\cdot : \left\{ \begin{array}{ccc} \mathbb{K} \times \mathbb{K}[X] & \to & \mathbb{K}[X] \\ (\lambda, P) & \mapsto & \lambda \cdot P \end{array} \right.$ par : si $P = \displaystyle\sum_{k=0}^{+\infty} a_kX^k$ alors $\lambda \cdot P = (\lambda a_0) + (\lambda a_1)X + \cdots + (\lambda a_n)X^n$

Proposition 2 .

$(\mathbb{K}[X], +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.

Remarque 3

$\Psi : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K}^{(\mathbb{N})} \\ P = a_0 + \cdots + a_nX^n & \mapsto & (a_0, \cdots, a_n, 0, \dots, 0, \dots) \end{array} \right.$ est un isomorphisme de $\mathbb{K}$-ev.

Remarque 4

- Par définition, $\mathbb{K}[X]$ a une base canonique : $(1, X, X^2, \dots, X^n, \dots)$.
- $\mathbb{K}_n[X]$ est clairement un sev de $\mathbb{K}[X]$ qui a aussi une base canonique : $(1, X, X^2, \dots, X^n)$.

Définition 5 .

Soit $P = \displaystyle\sum_{k=0}^{n} a_kX^k$ et $Q = \displaystyle\sum_{j=0}^{m} b_jX^j$.

On définit le polynôme noté $P \times Q$ par : $P \times Q = \displaystyle\sum_{k=0}^{n+m} c_kX^k$ avec $c_k = \displaystyle\sum_{i+j=k} a_ib_j = \sum_{r=0}^{k} a_rb_{k-r}$.

Notation 2 Pour un polynôme P quelconque, on note évidemment $P^2 = P \times P$, $P^3 = P^2 \times P$, etc.

Théorème 2 .

$(\mathbb{K}[X], +, \times)$ est un anneau commutatif, d'élément unité le polynôme constant 1.

Corollaire 1 : Structure de $\mathbb{K}$-algèbre.

$(\mathbb{K}[X], +, \times, \cdot)$ forme une $\mathbb{K}$-algèbre.

Remarque 5

$\mathbb{K}_n[X]$ **n'est pas** un sous-anneau de $\mathbb{K}[X]$ pour $n \geqslant 1$!

Proposition 3 .

L'anneau $\mathbb{K}[X]$ est intègre, c'est-à-dire qu'un produit de deux polynômes est nul si et seulement si un des deux facteurs est nul.

I.3 Applications polynomiales

Définition 6 .

Soit $(\mathcal{A}, +, \times, \cdot)$ une $\mathbb{K}$-algèbre. Pour tout polynôme $P = \displaystyle\sum_{k=0}^{d} a_kX^k$ de $\mathbb{K}[X]$ on peut considérer l'application polynomiale associée à P dans $\mathcal{A}$, simplement définie par : $\widetilde{P}^{\mathcal{A}} \left\{ \begin{array}{ccc} \mathcal{A} & \to & \mathcal{A} \\ A & \mapsto & \displaystyle\sum_{k=0}^{d} a_kA^k \end{array} \right.$, la somme et les multiplications considérées dans cette expression étant celles de l'algèbre $\mathcal{A}$.

Théorème 3 : Lien polynôme/application polynomiale.

Si $\mathcal{A} \neq \{0\}$ alors $P \mapsto \tilde{P}$ est un morphisme d'algèbres injectif, c'est-à-dire :

1. $\forall (P,Q) \in \mathbb{K}[X]^2,\ \forall (\lambda,\mu) \in \mathbb{K}^2\ \widetilde{\lambda P + \mu Q}^{\mathcal{A}} = \lambda \widetilde{P}^{\mathcal{A}} + \mu \widetilde{Q}^{\mathcal{A}}$ (linéarité) ;
2. $\forall (P,Q) \in \mathbb{K}[X]^2,\ \widetilde{PQ}^{\mathcal{A}} = \widetilde{P}^{\mathcal{A}}\, \widetilde{Q}^{\mathcal{A}}$ (préservation des produits) ;
3. $\forall (P,Q) \in \mathbb{K}[X]^2,\ \widetilde{P}^{\mathcal{A}} = \widetilde{Q}^{\mathcal{A}} \Rightarrow P = Q$ (injectivité).

Remarque 6

On a vu dans le corollaire 1 que $(\mathbb{K}[X], +, \times, \cdot)$ est justement une $\mathbb{K}$-algèbre.

À tout polynôme P, on peut donc associer une application $\widetilde{P}^{\mathbb{K}[X]} : \mathbb{K}[X] \to \mathbb{K}[X]$! **Remarque 7**

On a donc toujours : $P(X) = P$!

Définition 7 .

Soient $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q \in \mathbb{K}[X]$.

On définit le polynôme composé $P \circ Q$, noté parfois simplement $P(Q)$, par : $P \circ Q = \widetilde{P}^{\mathbb{K}[X]}(Q) = \sum_{k=0}^{+\infty} a_k Q^k$.

I.4 Dérivation des polynômes

Définition 8 .

Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{K}[X]$.

On appelle <u>polynôme dérivé</u> de P le polynôme $P' = \sum_{k=1}^{d} a_k k X^{k-1}$ i. e. $P' = \sum_{k=0}^{d-1} (k+1) a_{k+1} X^k$.

Théorème 4 : Propriétés de la dérivation.

- $P \mapsto P'$ est linéaire, donc $P \mapsto P^{(n)}$ est linéaire ;
- $\forall (P,Q) \in \mathbb{K}[X],\ (PQ)' = P'Q + PQ'$, donc $\forall (P,Q) \in \mathbb{K}[X],\ (PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$;
- $\forall (P,Q) \in \mathbb{K}[X],\ (P \circ Q)' = Q' \times P' \circ Q$, donc $\forall P \in \mathbb{K}[X],\ \forall (\alpha,\beta) \in \mathbb{K}^2,\ P^{(n)}(\alpha X + \beta) = \alpha^n P^{(n)}(\alpha X + \beta)$.

Théorème 5 : Taylor pour les polynômes.

- En 0 : $P(X) = \sum_{k=0}^{\deg(P)} \dfrac{P^{(k)}(0)}{k!} X^k$.
- En λ : $P(X+\lambda) = \sum_{k=0}^{\deg(P)} \dfrac{P^{(k)}(\lambda)}{k!} X^k$.
- En λ (v2) : $P(X) = \sum_{k=0}^{\deg(P)} \dfrac{P^{(k)}(\lambda)}{k!} (X-\lambda)^k$.

I.5 Propriétés du degré

Proposition 4 : Degré d'une dérivée.

Soit P un polynôme. Alors on a :

- $\deg(P') = \begin{cases} \deg(P) - 1 \text{ si } \deg(P) \geqslant 1 \\ -\infty \text{ sinon.} \end{cases}$
- $\deg(P^{(n)}) = \begin{cases} \deg(P) - n \text{ si } \deg(P) \geqslant n \\ -\infty \text{ sinon.} \end{cases}$

Théorème 6 : Degré d'une CL.

Soient P et Q deux polynômes, λ un scalaire. Alors on a :

1. $\deg(P+Q) \leqslant \max(\deg P, \deg Q)$;
2. si $\deg(P) \neq \deg(Q)$, alors $\deg(P+Q) = \max(\deg P, \deg Q)$;
3. si $\lambda \neq 0$, alors $\deg(\lambda P) = \deg(P)$.

Théorème 7 : Degré d'un produit.

Soient P et Q deux polynômes. Alors on a : $\deg(P \times Q) = \deg(P) + \deg(Q)$.

Remarque 8

La proposition précédente montre à nouveau que $\mathbb{K}_n[X]$ n'est pas un sous-anneau de $\mathbb{K}[X]$ pour $n \geqslant 1$.

On peut aussi l'utiliser pour retrouver l'intégrité de $\mathbb{K}[X]$ en une demi-ligne !

Corollaire 2 : Degré d'une puissance.

Soit P un polynôme et $n \in \mathbb{N}$. Alors on a : $\deg(P^n) = n \deg(P)$.

Théorème 8 : Degré d'une composée.

Soient P un polynôme **et Q un polynôme non constant**. Alors on a : $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

Remarque 9

Si Q est constant il peut se produire qu'il soit une racine de P et dans ce cas on a $P \circ Q = 0$...

II Racines

II.1 Division euclidienne

Théorème 9 : Division euclidienne.

Soit $(A, B) \in \mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$.
Alors il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que : $A = BQ + R$ et $\deg(R) < \deg(B)$.

Proposition 5 : Invariance par extension de corps.

Soit $(A, B) \in \mathbb{R}[X] \times (\mathbb{R}[X] \setminus \{0\})$ $\Big($ en particulier on a $(A, B) \in \mathbb{C}[X] \times (\mathbb{C}[X] \setminus \{0\})$ $\Big)$.

Le quotient et le reste de la division euclidienne de A par B sont les mêmes pour la division euclidienne dans $\mathbb{C}[X]$ que pour la division euclidienne dans $\mathbb{R}[X]$.

II.2 Racines

Proposition-Définition 9 .

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Sont équivalentes :

1. $P(\alpha) = 0$.
2. Le polynôme $(X - \alpha)$ divise P.

On dit alors que α est une racine de P dans $\mathbb{K}$.

Théorème 10 : **très important.**

1. Un polynôme de degré $n \geqslant 0$ a au plus n racines.
2. Si $P \in \mathbb{K}[X]$ a une infinité de racines alors $P = 0$.
3. Si $P \in \mathbb{K}_n[X]$ a $n+1$ racines alors $P = 0$.

Définition 10 .

Un polynôme P de degré n est dit :

- scindé lorsqu'il peut s'écrire $P(X) = a_n(X - \lambda_1) \cdots (X - \lambda_n)$.
- scindé à racines simples lorsqu'il peut s'écrire $P(X) = a_n(X - \lambda_1) \cdots (X - \lambda_n)$ avec les λ_i distincts.

Théorème 11 : de d'Alembert-Gauss (rappel).

Tout polynôme de $\mathbb{C}[X]$ est scindé dans $\mathbb{C}$.

II.3 Relations coefficients-racines

Proposition 6 : Cas $n = 3$.

Supposons $a_3X^3 + a_2X^2 + a_1X + a_0$ scindé de racines $\lambda_1, \lambda_2, \lambda_3$. Alors :

$$\begin{cases} \frac{a_2}{a_3} = -(\lambda_1 + \lambda_2 + \lambda_3) \\ \frac{a_1}{a_3} = +(\lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3) \\ \frac{a_0}{a_3} = -\lambda_1\lambda_2\lambda_3 \end{cases}$$

Théorème 12 : Cas général.

Supposons $a_nX^n + \cdots + a_1X + a_0$ scindé de racines $\lambda_1, \lambda_2, \ldots, \lambda_n$.

On appelle k^e expression symétrique élémentaire le scalaire $\sigma_k = \sum\limits_{1\leqslant i_1 < i_2 < \cdots < i_k \leqslant n} \lambda_{i_1}\lambda_{i_2}\cdots\lambda_{i_k}$.

Supposons $a_nX^n + \cdots + a_1X + a_0$ scindé de racines $\lambda_1, \lambda_2, \ldots \lambda_n$. Alors :

Pour tout $0 \leqslant i \leqslant n$ on a $\dfrac{a_i}{a_n} = (-1)^{n-i}\sigma_{n-i}$

II.4 Multiplicité

Proposition-Définition 11 : Racines multiples.

Soit $P \in \mathbb{K}[X] \setminus \{0\}$, $\alpha \in \mathbb{K}$ et $r \in \mathbb{N}$. Les trois propositions suivantes sont équivalentes :

i. $r = \max\{k \in \mathbb{N} \setminus \{0\},\ (X-\alpha)^k \text{ divise } P\}$.

ii. On peut écrire $P = (X-\alpha)^r Q$ avec $Q(\alpha) \neq 0$.

iii. $P(\alpha) = 0,\ P'(\alpha) = 0, \ldots,\ P^{(r-1)}(\alpha) = 0$ et $P^{(r)}(\alpha) \neq 0$.

Lorsqu'elles sont vérifiées, on dit que α est une racine de multiplicité r de P.

Pour $r = 1$ on parle de racine simple, pour $r = 2$ de racine double, pour $r = 3$ de racine triple, etc.

On parle de racine multiple dès qu'on a $r \geqslant 2$.

Remarque 10

L'exercice CCINP $n°85$ consiste essentiellement en cette question de cours ! **Remarque 11**

Avec la définition précédente, on peut donc dire que α est racine de multiplicité 0 de P si et seulement si ce n'est pas une racine de P (c'est dans le programme). On peut aussi dire que tout scalaire est racine de multiplicité infinie du polynôme nul. **Remarque 12**

Si P est un polynôme admettant des racines distinctes α_i, pour $i \in \{1, \ldots, s\}$, de multiplicités respectives r_i, alors P est divisible par $(X-\alpha_1)^{r_1}(X-\alpha_2)^{r_2}\ldots(X-\alpha_s)^{r_s} = \prod\limits_{i=1}^{s}(X-\alpha_i)^{r_i}$.

Corollaire 3 .

Soit $n \in \mathbb{N}$ et $P \in \mathbb{K}_n[X]$.

1. P a au plus n racines **comptées avec leur multiplicité**.
2. P est scindé si et seulement si il a n racines **comptées avec leur multiplicité**.
3. Si P a au moins $n+1$ racines **comptées avec multiplicité**, c'est le polynôme nul.

II.5 Racines complexes d'un polynôme de $\mathbb{R}[X]$

Définition 12 .

Pour $P \in \mathbb{C}[X]$, on appelle **polynôme conjugué** de $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ le polynôme $\overline{P}$ défini par $\overline{P}(X) = \overline{a_0} + \overline{a_1}X + \overline{a_2}X^2 + \cdots + \overline{a_n}X^n$.

Remarque 13

La conjugaison étant un automorphisme de corps involutif sur $\mathbb{C}$ elle induit un automorphisme d'anneau involutif sur $\mathbb{C}[X]$. Elle est de plus compatible avec la dérivation et avec $P \mapsto \tilde{P}$.

III Arithmétique dans $\mathbb{K}[X]$

III.1 Divisibilité des polynômes

III.2 Propriétés algébriques de la divisibilité

III.3 PGCD

III.4 Polynômes premiers entre eux

Remarque 14 $\overline{P} = P \Leftrightarrow P \in \mathbb{R}[X]$. **C'est à ça que sert à la conjugaison des polynômes.**

Corollaire 4 .

Soit $P \in \mathbb{R}[X]$ et $\alpha \in \mathbb{C}$.

1. α racine de $P \Leftrightarrow \overline{\alpha}$ racine de P.
2. α racine de P de multiplicité $k \Leftrightarrow \overline{\alpha}$ racine de P de multiplicité k.

Démonstration. 1. Il suffit de montrer l'implication directe par involutivité de la conjugaison.

Supposons $P(\alpha) = 0$. On a $P \in \mathbb{R}[X]$ donc $\overline{P} = P$.

On conjugue : $\overline{P(\alpha)} = \overline{0}$ *i. e.* $\overline{P}(\overline{\alpha}) = 0$ *i. e.* $P(\overline{\alpha}) = 0$. Youpie.

2. Il suffit de montrer l'implication directe par involutivité de la conjugaison.

α est racine de P de multiplicité k signifie que α est racine de P, P', …, $P^{(k-1)}$ mais pas de $P^{(k)}$.

On utilise le point 1. sur P, P', …, $P^{(k-1)}$ et sa contraposée sur $P^{(k)}$.

□

Corollaire 5 .

Soit $P \in \mathbb{R}_{2n+1}[X]$. Alors P a une racine **réelle**.

Démonstration. D'après d'Alembert-Gauss, P a $2n+1$ racines complexes comptées avec multiplicité.

Or P est à coefficients réels donc ses racines vont par paires avec leur conjugué qui a la même multiplicité.

Montrons que l'une est réelle par l'absurde : si ce n'était pas le cas on aurait un nombre pair de racines comptées avec leur multiplicité. C'est une contradiction. □

On aurait aussi pu utiliser le TVI !

Lorsqu'on a un anneau, on a une arithmétique (qui consiste, essentiellement, en l'étude de sa relation de divisibilité). L'arithmétique d'un anneau dans lequelle on a un théorème de division euclidienne est essentiellement la même que celle de $\mathbb{Z}$: nous allons l'illustrer ici, en prenant notre sur cours sur $\mathbb{Z}$ et en le recopiant. Recopier, c'est le bien. Avec l'ordinateur en plus ça va vite.

Définition 13 .

On dit d'un polynôme B de $\mathbb{K}[X]$ qu'il divise un polynôme A de $\mathbb{K}[X]$, et on écrit $B \mid A$, lorsqu'il existe un polynôme C de $\mathbb{K}[X]$ vérifiant $A = BC$. On dit alors de B qu'il est un diviseur de A, et de A qu'il est un multiple de B.

Notation 3

- L'ensemble des multiples de P dans $\mathbb{K}[X]$ se note $P\mathbb{K}[X]$.
- On pourra, comme dans $\mathbb{Z}$, noter $D(P)$ l'ensemble des diviseurs de P.

Proposition 7 : Inversibles de $\mathbb{K}[X]$. L'ensemble des inversibles de $\mathbb{K}[X]$ est $\mathbb{K}[X]^\times = \mathbb{K}^*$

Démonstration. $\boxed{\supset}$ Si $c \in \mathbb{K}^*$ alors c est inversible puisque son inverse est c^{-1}.

$\boxed{\subset}$ Soit P un polynôme inversible et notons Q son inverse. On a $PQ = 1$ donc $\deg(PQ) = 0$.
D'après la formule des degrés $\deg(P) + \deg(Q) = 0$. Donc $\deg(P) = \deg(Q) = 0$ et en particulier $P \in \mathbb{K}^*$. □

Proposition 8 .

La relation de divisibilité sur $\mathbb{K}[X]$ est réflexive et transitive mais n'est pas antisymétrique.

Si on la restreint à l'ensemble $\mathcal{U}$ des polynômes unitaires de $\mathbb{K}[X]$, elle devient alors antisymétrique et est par conséquent une relation d'ordre sur $\mathcal{U}$. Idem sur $\mathcal{U} \cup \{0\}$ si on ne veut pas se priver du polynôme nul.

Démonstration.
- Réflexivité : soit $P \in \mathbb{K}[X]$. On a $1 \in \mathbb{K}[X]$ et $P = 1 \times P$ donc $P \mid P$.
- Transitivité : soient $P, Q, R \in \mathbb{K}[X]$ et supposons $P \mid Q$ et $Q \mid R$. Il existe donc $S, T \in \mathbb{K}[X]$ tels que $Q = PS$ et $R = QT$, donc $R = P(ST)$ et donc $P \mid R$.
- La relation de divisibilité n'est pas antisymétrique sur $\mathbb{K}[X]$: $3X^2 \mid X^2$ et $X^2 \mid 3X^2$ mais $X^2 \neq 3X^2$.
- Plaçons-nous maintenant dans $\mathcal{U} \cup \{0\}$: soit $(P, Q) \in \big(\mathcal{U} \cup \{0\}\big)^2$ et supposons $P \mid Q$ et $Q \mid P$. Il existe $S \in \mathbb{K}[X]$ tel que $Q = SP$ et il existe $T \in \mathbb{K}[X]$ tel que $P = TQ$. On en déduit $P = STP$ et donc on a soit $P = 0$, soit $ST = 1$ par intégrité.
- Évidemment, restreindre une relation antisymétrique donne une relation antisymétrique, donc la divisibilité est aussi un ordre sur $\mathcal{U}$. □

On retiendra donc que $\mathcal{U}$ **joue dans** $\mathbb{K}[X]$ **le rôle joué dans** $\mathbb{Z}$ **par** $\mathbb{N} \setminus \{0\}$.

Proposition-Définition 14 .

On dit de deux polynômes P et Q qu'ils sont associés lorsqu'une des propositions suivantes est vérifiées :

- $P \mid Q$ et $Q \mid P$;
- il existe $\lambda \in \mathbb{K}^*$ tel que $P = \lambda Q$.

L'association est donc la relation d'équivalence canoniquement associée à la divisibilité. La multiplication par un scalaire non nul joue dans $\mathbb{K}[X]$ le rôle joué par la multiplication par ± 1 dans $\mathbb{Z}$. On retrouve bien que $\mathcal{U}$ joue dans $\mathbb{K}[X]$ le rôle joué dans $\mathbb{Z}$ par $\mathbb{N} \setminus \{0\}$. On voit en particulier que tout polynôme non nul est associé à un unique polynôme unitaire.

Démonstration. $\boxed{\Rightarrow}$ Soit $(P, Q) \in \mathbb{K}[X]^2$ tels que $P|Q$ et $Q|P$.
Ainsi il existe $C \in \mathbb{K}[X]$ tel que $P = QS$ et $T \in \mathbb{K}[X]$ tel que $Q = PT$.
On a en particulier les relations $\deg(P) = \deg(Q) + \deg(S)$ et $\deg(Q) = \deg(P) + \deg(T)$, dont on déduit en réinjectant : $\deg(S) + \deg(T) = 0$. Et donc $\deg(S) = \deg(T) = 0$. Ainsi S est un polynôme constant non nul ; en posant $\lambda = S$, on a bien $P = \lambda Q$ avec $\lambda \in \mathbb{K}^*$.

$\boxed{\Leftarrow}$ λ et $\frac{1}{\lambda}$ sont dans $\mathbb{K}[X]$ donc lol. □

Proposition 9 .

La divisibilité est stable par :

- CL : si $C \mid A$ et $C \mid B$ alors $C \mid AU + BV$.
- Produit : $\begin{cases} \text{si } A \mid B \text{ alors } AC \mid BC\,; \\ \text{si } A \mid B \text{ et } P \mid Q \text{ alors } AP \mid BQ. \end{cases}$
- Puissances : si $n \in \mathbb{N}$ et $A \mid B$ alors $A^n \mid B^n$.

Démonstration. Fastoche (recopier le cours sur $\mathbb{Z}$). □

Proposition 10 .

La divisibilité est invariante par extension de corps : si $P,\ Q \in \mathbb{R}[X]$ alors $P \mid Q$ dans $\mathbb{R}[X]$ si et seulement si $P \mid Q$ dans $\mathbb{C}[X]$.

Démonstration. Immédiat car il suffit d'utiliser le lien divisibilité/division euclidienne et l'invariance de la division euclidienne par extension de corps. □

Définition 15 .

Soient P et Q dans $\mathbb{K}[X]$.

1. On dit que D est **un** pgcd de P et Q lorsque c'est un plus grand diviseur de P et de Q (pour la divisibilité).
2. Il existe un unique pgcd unitaire (ou nul), on l'appelle **le** pgcd et on le note $\mathrm{PGCD}(P,Q)$ ou $P \wedge Q$.

Exercice 1. Reformuler cette définition.

- — $D|P$ et $D|Q$
  — $\forall R \in \mathbb{K}[X], (R|P \text{ et } R|Q) \implies R|D$
- $P \wedge Q = \inf_{(\mathcal{U}\cup\{0\},\ |)}\{P,Q\}$
- $\mathcal{D}(D) = \mathcal{D}(P) \cap \mathcal{D}(Q)$

Proposition 11 : Propriétés immédiates du PGCD.

- Homogénéité : si K est unitaire alors $KA \wedge KB = K(A \wedge B)$;
- Commutativité : $B \wedge A = A \wedge B$;
- Associativité : $(A \wedge B) \wedge C = A \wedge (B \wedge C)$.

Pour montrer l'existence, ne faisons pas comme dans $\mathbb{Z}$ (on pourrait), mais utilisons l'algorithme d'Euclide.

Lemme 1 : Lemme préparatoire à l'algorithme d'Euclide.

1. Si R est le reste dans la division euclidienne de A par B alors $A \wedge B = B \wedge R$.
2. Si D est unitaire, $D \wedge 0 = D$.

Démonstration.
1. Il suffit de montrer que les diviseurs communs à A et B sont les mêmes que les diviseurs communs à B et R. Cela provient de la stabilité par CL avec les deux CL $A = BQ + R$ et $R = A - BQ$.
2. Les diviseurs communs à D et 0 sont juste les diviseurs de D d'où le résultat.

□

L'existence du PGCD est assurée par l'algorithme d'Euclide :

- On pose $R_0 = A$ et $R_1 = B$.
- Tant que $R_{n+1} \neq 0$ on définit R_{n+2} comme le reste dans la DE de R_n par R_{n+1}.
- Le PGCD est le dernier reste non nul R_n (au coefficient dominant près).

Reste à montrer la terminaison et la correction de cet algorithme.

Démonstration. On copie le cours sur $\mathbb{Z}$.

- Terminaison : par division euclidienne, pour tout $n \geqslant 1$ tel que $R_n \neq 0$, on a $\deg(R_{n+1}) < \deg(R_n)$. On a donc $\deg(B) = \deg(R_1) > \deg(R_2) > \deg(R_3) > \cdots$. Comme il n'y a qu'un nombre fini d'éléments dans $\{-\infty\} \cup \{0, \ldots, \deg(B)\}$, il existe nécessairement un rang $N \geqslant 2$ tel que $\deg(R_N) = -\infty$, c'est-à-dire $R_N = 0$ et $\deg(R_{N-1}) \geqslant 0$. D'où la terminaison.
- Correction : on a alors, par le lemme préparatoire, $R_{n-1} \wedge R_n = R_n \wedge R_{n+1}$ pour tout $n \in \{1, \ldots, N-1\}$. Donc : $A \wedge B = R_0 \wedge R_1 = R_1 \wedge R_2 = \cdots = R_{N-2} \wedge R_{N-1} = R_{N-1} \wedge R_N = R_{N-1} \wedge 0$. Le PGCD est donc associé à R_{N-1}. □

Exercice 2. Calculons par exemple $\left(X^6+1\right) \wedge \left(X^4+1\right)$.

Théorème 13 : Théorème d'Eudoxe (théorème "sur la relation de Bézout").

Si $D = A \wedge B$ alors $\exists (U,V) \in \mathbb{K}[X]^2,\ AU + BV = D$.

Formulation moderne : pour D unitaire : $D = A \wedge B \Leftrightarrow A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$.

Démonstration. Il suffit de remonter l'algorithme d'Euclide. □

Exercice 3. Trouvons une relation de Bézout pour $A = X^6 + 1$ et $B = X^4 + 1$.

Proposition 12 .

Le PGCD est invariant par extension de corps : si $P, Q \in \mathbb{R}[X]$ alors le pgcd de P et Q dans $\mathbb{R}[X]$ est le même que dans $\mathbb{C}[X]$.

Démonstration. Immédiat d'après le lien divisibilité/division euclidienne et l'invariance de la division euclidienne par extension de corps. □

Exercice 4. Calculons $\left(X^6 - 1\right) \wedge \left(X^4 - 1\right)$.

Définition 16 .

On dit que deux polynômes P et Q sont premiers entre eux lorsque $P \wedge Q = 1$.

Proposition 13 .

Le caractère "premiers entre eux" est invariant par extension de corps : $P,\ Q \in \mathbb{R}[X]$ sont premiers entre eux dans $\mathbb{R}[X]$ si et seulement si ils le sont dans $\mathbb{C}[X]$.

Remarque 15

L'homogénéïté entraîne que si A et B sont non nuls et D est leur PGCD, alors $\dfrac{A}{D}$ et $\dfrac{B}{D}$ sont premiers entre eux.

Théorème 14 : Théorème de Bézout.

Soient A et B deux polynômes. On a $A \wedge B = 1 \Leftrightarrow \exists (U,V),\ AU + BV = 1$.

Théorème 15 : Lemme de Gauss.

Si $\begin{cases} A \wedge B = 1 \\ A | BC \end{cases}$ alors $A|C$.

III.5 PPCM

Définition 17 .

Soient P et Q dans $\mathbb{K}[X]$.

1. On dit que M est **un** ppcm de P et Q lorsque c'est un plus petit multiple de P et de Q.
2. Il existe un unique ppcm unitaire (ou nul), on l'appelle **le** ppcm et on le note $\mathrm{ppcm}(P,Q)$ ou $P \vee Q$.

Proposition 14 : Propriétés immédiates du PPCM.

- Homogénéité : si K est unitaire alors $KA \vee KB = K(A \vee B)$;
- Commutativité : $B \vee A \ = \ A \vee B$;
- Associativité : $(A \vee B) \vee C = A \vee (B \vee C)$.

Remarque 16

Si A et B sont unitaires, alors $(A \wedge B) \times (A \vee B) = A \times B$.

Proposition 15 .

Le PPCM est invariant par extension de corps : si $P, Q \in \mathbb{R}[X]$ alors le ppcm de P et Q dans $\mathbb{R}[X]$ est le même que dans $\mathbb{C}[X]$.

III.6 Polynômes irréductibles

Définition 18 .

Un polynôme $P \in \mathbb{K}[X] \setminus \mathbb{K}$ est dit irréductible lorsqu'on a :

$$\forall (U,V) \in \mathbb{K}[X]^2,\ P = UV \ \Rightarrow \left\{ \begin{array}{l} U \text{ inversible} \\ V \text{ associé à } P \end{array} \right. \quad \text{ou} \quad \left\{ \begin{array}{l} U \text{ associé à } P \\ V \text{ inversible} \end{array} \right.$$

Théorème 16 : Théorème de décomposition.

Tout polynôme peut s'écrire comme produit de polynômes irréductibles, de façon unique à l'ordre des facteurs près et à association près.

Théorème 17 : Irréductibles de $\mathbb{C}$.

Les irréductibles unitaires de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Théorème 18 : Irréductibles de $\mathbb{R}$.

Les irréductibles unitaires de $\mathbb{R}[X]$ sont

— les $X - \lambda,\ \lambda \in \mathbb{R}$;

— les $X^2 + bX + c$, $\Delta < 0$.

Probabilités

Les trois théorèmes importants de ce chapitre sont :

- la formule des probabilités composées ;
- la formule des probabilités totales ;
- la formule de Bayes.

I Expériences aléatoires

I.1 Définition

Définition (informelle) 1 : Expérience aléatoire.

Une expérience aléatoire est une expérience dont l'ensemble des issues possibles est connue mais dont l'issue n'est pas connue avant de réaliser l'expérience.

I.2 L'expérience aléatoire « `Choisir(MPSI)` »

I.3 Modélisation

Remarque 1

Cette année, on considèrera uniquement le cas où Ω est fini. C'est très restrictif mais philosophiquement plus honnête.

II Espaces probabilisés finis

II.1 Espaces probabilisables finis

Définition 2 .

On appelle espace probabilisable fini un couple $(\Omega, \mathcal{P}(\Omega))$ où Ω est un ensemble fini.

Remarque 2

Comme annoncé dans la remarque 1, on se limite donc au cas fini. C'est très embêtant car on s'interdit des expériences aléatoires très simples[1] dont on a envie de parler, comme par exemple :

- lancer un dé jusqu'à obtenir 6 ;
- choisir un réel uniformément au hasard entre 0 et 1 ;
- ...

On verra quand même en TD une astuce permettant d'intégrer malgré tout les expériences du type « lancer un dé jusqu'à obtenir 6 » au programme de MPSI.[2].

Définition 3 .

On appelle ≪ système complet d'événements ≫ (en abrégé sce) une famille $(A_1, \dots, A_n)$ telle que

$$\begin{cases} \forall i \neq j,\ A_i \text{ et } A_j \text{ sont incompatibles;} \\ \text{et } A_1 \cup \cdots \cup A_n = \Omega\ ; \end{cases}$$

autrement dit telle que $A_1 \amalg A_2 \amalg \cdots \amalg A_n = \Omega$.

1. Mais non accessibles à l'être humain.
2. C'est comme d'habitude, on prend un gros marteau et on tape fort.

II.2 Probabilité

Définition 4 .

Soit Ω un ensemble fini. On appelle probabilité sur Ω une application $P : \mathcal{P}(\Omega) \to [0,1]$ telle que :

1. $P(\Omega) = 1$;
2. pour tout couple (A, B) d'événements incompatibles, $P(A \amalg B) = P(A) + P(B)$.

Remarque 3

Lorsqu'on modélise une expérience aléatoire, on ne la modélise pas seulement par Ω, mais par l'espace probabilisé $\big(\Omega, \mathcal{P}(\Omega), P\big)$.

Théorème 1 : théorème de caractérisation.

Soit Ω un ensemble fini.

1. Si $P : \mathcal{P}(\Omega) \to [0,1]$ est une probabilité alors $\sum\limits_{\omega \in \Omega} P(\{\omega\}) = 1$.
2. Réciproquement, si $p : \Omega \to [0,1]$ vérifie $\sum\limits_{\omega \in \Omega} p(\omega) = 1$ alors l'application naturellement induite $P : \left\{ \begin{array}{ccc} \mathcal{P}(\Omega) & \to & [0,1] \\ A & \mapsto & \sum\limits_{\omega \in A} p(\omega) \end{array} \right.$ est bien définie et c'est une probabilité.

II.3 Propriétés immédiates

Proposition 1 .

Soit $\big(\Omega, \mathcal{P}(\Omega), P\big)$ un espace probabilisé. On a :

0. $P(\emptyset) = 0$;
1. pour tout $A \in \mathcal{P}(\Omega)$, $P({}^{c}A) = 1 - P(A)$;
2. P est croissante pour l'inclusion ;
3. pour tous $A,\ B \in \mathcal{P}(\Omega)$, $P(A \cup B) = P(A) + P(B) - P(A \cap B)$;

III Indépendance

Définition 5 .

Soit $\big(\Omega, \mathcal{P}(\Omega), P\big)$ un espace probabilisé.
Deux événements A et B sont dit <u>indépendants</u> lorsqu'on a $P(A \cap B) = P(A)P(B)$.

Remarque 4

Considérons l'expérience aléatoire « on lance un dé vert et un dé bleu ».
Faute d'information supplémentaire, on la modélise par $\big(\Omega, \mathcal{P}(\Omega), P\big)$ où $\begin{cases} \Omega & = [\![1,6]\!]^2 \\ P & = P_U \end{cases}$ Montrer que cette modélisation implique que les deux lancés sont indépendants (commencer par donner un sens à cette phrase).
On note "couleur $\to i$" := "le dé couleur donne i"
Soient $\begin{cases} V_i : & = \text{"le dé vert donne } i\text{"} \\ B_j : & = \text{"le dé bleu donne } j\text{"} \end{cases}$.

$$
\begin{aligned}
P(V_i) &= P(\{i\} \times \{1, \ldots, 6\}) \\
&= \frac{|\{i\} \times \{1, \ldots, 6\}|}{|\Omega|} \\
&= \frac{6}{36} = \frac{1}{6} \\
P(B_j) &= P(\{j\} \times \{1, \ldots, 6\}) \\
&= \frac{|\{j\} \times \{1, \ldots, 6\}|}{|\Omega|} \\
&= \frac{6}{36} = \frac{1}{6} \\
P(V_i \cap B_j) &= P(\{i, j\}) \\
&= \frac{1}{36} \\
&= \frac{1}{6} \cdot \frac{1}{6} \\
&= P(V_i)P(B_j)
\end{aligned}
$$

III.1 Indépendance mutuelle

Définition 6 .

Soit $\big(\Omega, \mathcal{P}(\Omega), P\big)$ un espace probabilisé et $(A_1, \ldots, A_n)$ une famille d'événements.
On dit que $A_1, \ldots, A_n$ sont mutuellement indépendants lorsqu'on a :
$\forall k \in \{1, \ldots, n\},\ \forall i_1 < i_2 < \cdots < i_k \in \{1, \ldots, n\},\ P(A_{i_1} \cap A_{i_2} \cap \cdots A_{i_k}) = P(A_{i_1})P(A_{i_2}) \cdots P(A_{i_k})$.

Remarque 5

1. Si $A_1, \ldots, A_n$ sont mutuellement indépendants, alors
   - ils sont indépendants 2 à 2 (*i. e.* $\forall i \neq j,\ P(A_i \cap A_j) = P(A_i)P(A_j)$) ;
   - et ils sont indépendants n à n (*i. e.* $P(A_1 \cap \cdots \cap A_n) = P(A_1) \times \cdots \times P(A_n)$).
2. L'indépendance 2 à 2 n'implique pas l'indépendance mutuelle.
3. L'indépendance n à n n'implique pas l'indépendance mutuelle.

IV Probabilités conditionnelles

IV.1 Définition

Définition 7 .

Soit $\big(\Omega, \mathcal{P}(\Omega), P\big)$ un espace probabilisé, A un événement et B un événement de probabilité non nulle. On appelle probabilité de A sachant B et on note $P_B(A)$ ou $P(A \,|\, B)$ le quotient $P_B(A) = \dfrac{P(A \cap B)}{P(B)}$.

Théorème 2 .

Soit B un événement de probabilité non nulle.
L'application $P_B : \left\{ \begin{array}{ccc} \mathcal{P}(\Omega) & \to & [0, 1] \\ A & \mapsto & P_B(A) \end{array} \right.$ est une probabilité.

Remarque 6

Si A et B sont deux événement de probabilités non nulles alors :

1. $P(A \cap B) = P(A) \times P(B|A)$;
2. $P(A \cap B) = P(B) \times P(A|B)$.

IV.2 Formule des probabilités composées

Théorème 3 : Formule des probabilités composées.

Soit $\big(\Omega, \mathcal{P}(\Omega), P\big)$ un espace probabilisé et $(A_1, \dots, A_n)$ une famille d'événements tels que $P(A_1 \cap \dots \cap A_{n-1}) \neq 0$. Alors :

1. $\forall k \leqslant n-1,\ P(A_1 \cap \dots \cap A_k) \neq 0$;
2. $P(A_1 \cap \dots \cap A_{n-1} \cap A_n) = P(A_1)P_{A_1}(A_2)P_{A_1 \cap A_2}(A_3) \cdots P_{A_1 \cap \dots \cap A_{n-1}}(A_n)$.

IV.3 Formule des probabilités totales

Théorème 4 : Formule des probabilités totales.

Soit $(A_1, A_2, \dots, A_n)$ un système complet d'événements de probabiltés non nulles et B un événement. On a : $P(B) = \displaystyle\sum_{k=1}^{n} P(A_k)P_{A_k}(B)$.

Remarque 7

La formule reste vraie si certains A_i sont de probabilité nulle avec la convention $0 \cdot P(B|A) = 0$

IV.4 Formule de Bayes

Théorème 5 : Petite formule de Bayes.

Soient A et B deux événements de probabiltés non nulles. On a : $P_B(A) = \dfrac{P(A)P_A(B)}{P(B)}$.

Théorème 6 : Grosse formule de Bayes.

Soit $(A_1, A_2, \dots, A_n)$ un système complet d'événements de probabiltés non nulles et B un événement de probabilité non nulle. On a, pour tout $k \in \{1, \dots, n\}$, $P_B(A_k) = \dfrac{P(A_k)P_{A_k}(B)}{\sum\limits_{i=1}^{n} P(A_i)P_{A_i}(B)}$.

Relations de comparaison.

Notations (rappels) :

1. « On a $P(n)$ APCR » signifie : $\exists n_0 \in \mathbb{N},\ \forall n \geqslant n_0,\ P(n)$;
2. Pour a fini, « on a $P(x)$ au voisinage de a » signifie : $\exists \epsilon > 0,\ \forall x \in]a-\varepsilon, a+\varepsilon[,\ P\big(x\big)$;
3. Pour $a = +\infty$, « on a $P(x)$ au voisinage de a » signifie : $\exists A > 0,\ \forall x \in]A, +\infty[,\ P\big(x\big)$;
4. Pour $a = -\infty$, « on a $P(x)$ au voisinage de a » signifie : $\exists B < 0,\ \forall x \in]-\infty, B[,\ P\big(x\big)$.

I Domination

I.1 Définitions

Définition 1 : Domination pour les suites.

Soient $(u_n)_{n\in\mathbb{N}}$, $(v_n)_{n\in\mathbb{N}}$ deux suites.

1. Si $(v_n)_n$ ne s'annule pas, on dit que $(u_n)_n$ est dominée par $(v_n)_{n\in\mathbb{N}}$ lorsque $\left(\dfrac{|u_n|}{|v_n|}\right)_{n\in\mathbb{N}}$ est majorée.
2. Plus généralement, on dit que $(u_n)_n$ est dominée par $(v_n)_{n\in\mathbb{N}}$ lorsqu'on a $\exists K \geqslant 0,\ |u_n| \leqslant K|v_n|$ APCR.

Lorsque c'est le cas, on note $u_n = \mathcal{O}(v_n)$.

Notation 1

1. On a vu qu'on note $u_n = \mathcal{O}(v_n)$ pour « $(u_n)_n$ est dominée par $(v_n)_n$ ».
2. On notera aussi $\mathcal{O}(v_n)$ l'ensemble de toutes les suites dominées par $(v_n)_n$.
3. On notera aussi $u_n = v_n + \mathcal{O}(w_n)$ pour $u_n - v_n = \mathcal{O}(w_n)$.

Définition 2 : Domination pour les fonctions.

Soient $f, g : I \to \mathbb{R}$ et a un point adhérent à I.

1. Si g ne s'annule pas au voisinage de a, on dit que f est dominée par g au voisinage de a lorsque $\left(\dfrac{|f|}{|g|}\right)$ est majorée au voisinage de a.
2. En général, on dit que f est dominée par g au voisinage de a lorsqu'on a $\exists K \geqslant 0,\ |f| \leqslant K|g|$ au voisinage de a.

Lorsque c'est le cas, on note $f = \mathcal{O}_a(g)$ $\Big($ou, si le contexte ne laisse pas d'ambiguïté sur a : $f = \mathcal{O}(g)\Big)$.

On peut également noter $f(x) = \mathcal{O}_a(g(x))$. On reprend aussi les deux autres notations vues pour les suites.

I.2 Propriétés

Proposition 1 .

La relation de domination (« est dominé par ») est un préordre.

Théorème 1 : Propriétés algébriques de la domination.

La relation de domination

1. absorbe les constantes : si $\lambda \neq 0$ alors $\mathcal{O}_a(\lambda f) = \mathcal{O}_a(f)$;
2. est stable par somme au sens suivant : si $f = \mathcal{O}_a(u)$ et $g = \mathcal{O}_a(v)$ alors $f + g = \mathcal{O}_a(|u| + |v|)$;
3. est stable par produit : si $f = \mathcal{O}_a(u)$ et $g = \mathcal{O}_a(v)$ alors $fg = \mathcal{O}_a(uv)$.

Remarque 1

Le point 2. est surtout intéressant pour son cas particulier suivant : $\boxed{\text{si } f = \mathcal{O}_a(u) \text{ et } g = \mathcal{O}_a(u) \text{ alors } f + g = \mathcal{O}_a(u)}$.

Proposition 2 : Grands O de 0 et de 1.

1. $f = \mathcal{O}_a(1) \Leftrightarrow f$ est bornée au voisinage de a
2. $f = \mathcal{O}_a(0) \Leftrightarrow f = x \mapsto 0$ au voisinage de a

Corollaire 1 : Zone rouge.

Si on est amené à écrire $u_n = \mathcal{O}(0)$ ou $f = \mathcal{O}(0)$, <u>c'est très probablement qu'on a fait une erreur</u> !

II Négligeabilité

II.1 Définitions

Définition 3 : Négligeabilité pour les suites.

Soient $(u_n)_{n\in\mathbb{N}}$, $(v_n)_{n\in\mathbb{N}}$ deux suites.

1. Si $(v_n)_n$ ne s'annule pas, on dit que $(u_n)_n$ est négligeable devant $(v_n)_{n\in\mathbb{N}}$ lorsqu'on a $\dfrac{u_n}{v_n} \to 0$.
2. En général, on dit que $(u_n)_n$ est négligeable devant $(v_n)_{n\in\mathbb{N}}$ lorsque $\exists(\varepsilon_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$, $\begin{cases} u_n = \varepsilon_n v_n \text{ APCR} \\ \varepsilon_n \to 0. \end{cases}$

Lorsque c'est le cas, on note $u_n = o(v_n)$.

Notation 2

1. On a vu qu'on note $u_n = o(v_n)$ pour « $(u_n)_n$ est négligeable devant $(v_n)_n$ ».
2. On notera aussi $o(v_n)$ l'ensemble de toutes les suites dominées par $(v_n)_n$.
3. On notera aussi $u_n = v_n + o(w_n)$ pour $u_n - v_n = o(w_n)$.

Définition 4 : Négligeabilité pour les fonctions.

Soient $f, g : I \to \mathbb{R}$ et a un point adhérent à I.

1. Si $g \neq 0$ au voisinage de a, on dit que f est négligeable devant g au voisinage de a lorsqu'on a $\dfrac{f(x)}{g(x)} \underset{x\to a}{\longrightarrow} 0$.
2. En général, on dit que f est négligeable devant g au voisinage de a lorsqu'il existe $\varepsilon : \begin{cases} I & \to & \mathbb{R} \\ x & \mapsto & \varepsilon(x) \end{cases}$ telle que $\begin{cases} f(x) = \varepsilon(x)g(x) \text{ au voisinage de } a \\ \varepsilon(x) \underset{x\to a}{\longrightarrow} 0. \end{cases}$

Lorsque c'est le cas, on note $f = o_a(g)$ (ou, si le contexte ne laisse pas d'ambiguïté sur a : $f = o(g)$).

On peut également noter $f(x) = o_a(g(x))$. On reprend aussi les deux autres notations vues pour les suites.

II.2 Négligeabilités classiques

Proposition 3 .

Soient $\alpha, \beta \in \mathbb{R}$ et $a, b > 0$.

1. $x^\alpha = o_{+x\to\infty}(x^\beta) \Leftrightarrow \frac{\mathrm{id}^\alpha}{\mathrm{id}^\beta} \underset{\infty}{\longrightarrow} 0 \Leftrightarrow \frac{1}{\mathrm{id}^{\beta-\alpha}} \underset{x\to\infty}{\longrightarrow} 0 \Leftrightarrow \beta > \alpha$
2. $x^\alpha = o_0(x^\beta) \Leftrightarrow \mathrm{id}^{\alpha-\beta} \underset{\infty}{\longrightarrow} 0 \Leftrightarrow \alpha > \beta$
3. $a^x = o_{+\infty}(b^x) \Leftrightarrow \frac{a^x}{b^x} \underset{x\to\infty}{\longrightarrow} 0 \Leftrightarrow \left(\frac{b}{a}\right)^x \underset{x\to\infty}{\longrightarrow} 0 \Leftrightarrow b > a$

Théorème 2 : Croissances comparées.

Pour $\alpha, \beta > 0$: 1. $x^\alpha = o_{+\infty}\left(\mathrm{e}^{\beta x}\right)$ 2. $\ln(x)^\alpha = o_{+\infty}\left(x^\beta\right)$ 3. $\mathrm{e}^{\beta x} = o_{-\infty}\left(\dfrac{1}{x^\alpha}\right)$ 4. $\ln(x)^\beta = o_{0^+}\left(\dfrac{1}{x^\alpha}\right)$

Théorème 3 : Cas des suites.

Soient $\alpha, \beta > 0$ et $q > 1$. On a : 1. $n^\alpha = o\left(q^n\right)$ 2. $\ln(n)^\alpha = o\left(n^\beta\right)$ 3. $q^n = o\left(n!\right)$ 4. $n! = o\left(n^n\right)$

II.3 Propriétés

Proposition 4 .

La relation de négligeabilité (« est négligeable devant ») est transitive.

Théorème 4 : Propriétés algébriques de la négligeabilité.

La relation de négligeabilité

1. absorbe les constantes : si $\lambda \neq 0$ alors $o_a(\lambda f) = o_a(f)$;
2. est stable par somme :
   i/ si $f = o_a(u)$ et $g = o_a(v)$ alors $f + g = o_a(|u| + |v|)$;
   ii/ si $f = o_a(u)$ et $g = o_a(u)$ alors $f + g = o_a(u)$;
3. est stable par produit :
   i/ si $f = o_a(u)$ et $g = o_a(v)$ alors $fg = o_a(uv)$;
   ii/ si $f = o_a(u)$ alors $fg = o_a(ug)$.

Proposition 5 : Petits o de 0 et de 1.

1. $f = o_a(1) \Leftrightarrow$ ....

2. $f = o_a(0) \Leftrightarrow$ ....

Corollaire 2 : Zone rouge.

Si on est amené à écrire $u_n = o(0)$ ou $f = o(0)$, c'est très probablement qu'on a fait une erreur !

III Équivalence

III.1 Définitions

Définition 5 : Équivalence pour les suites.

Soient $(u_n)_{n\in\mathbb{N}}$, $(v_n)_{n\in\mathbb{N}}$ deux suites.

1. Si $(v_n)_n$ ne s'annule pas, on dit que $(u_n)_n$ est équivalente à $(v_n)_{n\in\mathbb{N}}$ lorsqu'on a $\dfrac{u_n}{v_n} \to 1$.
2. En général, on dit que $(u_n)_n$ est équivalente à $(v_n)_{n\in\mathbb{N}}$ lorsque $\exists(\gamma_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$, $\begin{cases} u_n = \gamma_n v_n \text{ APCR} \\ \gamma_n \to 1. \end{cases}$

Lorsque c'est le cas, on note $u_n \sim v_n$.

Définition 6 : Équivalence pour les fonctions.

Soient $f, g : I \to \mathbb{R}$ et a un point adhérent à I.

1. Si g NSP au voisinage de a, on dit que f est équivalente à g au voisinage de a lorsqu'on a $\dfrac{f(x)}{g(x)} \underset{x\to a}{\longrightarrow} 1$.
2. En général, on dit que f est équivalente à g au voisinage de a lorsqu'il existe ε : $\begin{cases} I & \to & \mathbb{R} \\ x & \mapsto & \gamma(x) \end{cases}$ telle que $\begin{cases} f(x) = \gamma(x)g(x) \text{ au voisinage de } a \\ \gamma(x) \underset{x\to a}{\longrightarrow} 1. \end{cases}$

Lorsque c'est le cas, on note $f \sim_a g$ (ou $f \sim g$, ou $f(x) \sim_{x\to a} g(x)$).

Remarque 2

L'intérêt de la relation d'équivalence est de calculer des équivalents simples pour simplifier l'étude en cours. Un équivalent qui se présente comme une somme n'est certainement pas un équivalent simple, donc est sans intérêt en tant qu'équivalent.

III.2 Équivalents classiques

Proposition 6 : Équivalent d'une fraction rationnelle en 0 et $\pm\infty$.

Soient $P(x) = a_n x^n + \cdots + a_{n_0} x^{n_0}$ $(a_n, a_{n_0} \neq 0)$ et $Q(x) = b_m x^m + \cdots + b_{m_0} x^{m_0}$ $(b_m, b_{m_0} \neq 0)$ deux polynômes.

1. $\dfrac{P(x)}{Q(x)} \sim_{\pm\infty}$ .... ;
2. $\dfrac{P(x)}{Q(x)} \sim_0$ .... ;

Remarque 3

En particulier, pour un polynôme $P(x) = a_n x^n + \cdots + a_{n_0} x^{n_0}$ $(a_n, a_{n_0} \neq 0)$, on obtient :

Définition 7 : Série harmonique.

On note $H_n = \displaystyle\sum_{k=1}^{n} \frac{1}{k}$. La suite $(H_n)_n$ s'appelle la série harmonique.

Proposition 7 : Série harmonique.

On a $H_n \sim \ln(n)$.

Théorème 5 : Formule de Stirling.

$n! \sim \sqrt{2\pi n}\left(\dfrac{n}{\mathrm{e}}\right)^n$

III.3 Propriétés

Proposition 8 .

La relation d'équivalence (« est équivalente à ») est... une relation d'équivalence. Eh oui.

Théorème 6 .

Deux fonction équivalentes ont, sous réserve d'existence, même limite et même signe au voisinage de a.

Théorème 7 : Propriétés algébriques de l'équivalence.

La relation d'équivalence

1. est stable par produit : si $f \sim u$ et $g \sim v$ alors $fg \sim uv$;
2. est stable par quotient : si $f \sim u$, $g \sim v$ et v ne s'annule pas au voisinage de a, alors $\dfrac{f}{g} \sim \dfrac{u}{v}$;
3. est stable par puissance <u>constante</u> : si $f \sim g$ et $\alpha \in \mathbb{R}$ alors $f^\alpha \sim g^\alpha$.

Proposition 9 : Équivalents constants.

1. Si $\ell \in \mathbb{R}^*$, $f \sim_a \ell \Leftrightarrow$ ....
2. $f \sim_a 0 \Leftrightarrow$ ....

Corollaire 3 : Zone rouge.

Si on est amené à écrire $u_n \sim 0$ ou $f \sim 0$, <u>c'est très probablement qu'on a fait une erreur</u> !

III.4 Lien avec la négligeabilité.

Théorème 8 : lien avec la négligeabilité.

$$\begin{aligned} f \sim_a g \quad &\Leftrightarrow \quad f = g + o_a(g) \\ &\Leftrightarrow \quad f = g + o_a(f) \end{aligned}$$

Corollaire 4 .

Tout DL est équivalent à son premier terme non nul s'il en existe un.
Autrement dit si a_{n_0} est le premier a_i non nul dans l'expression précédente, alors $f(x) \sim_0 a_{n_0} x^{n_0}$.

IV Développements asymptotiques

Définition 8 : Développement asymptotique.

On notera DA pour « développement asymptotique ».

1. On appelle DA à un terme de f en a une expression de la forme $f = g + o_a(g)$ où g est un équivalent **simple** [a] de f.
2. On appelle DA à deux termes de f en a une expression de la forme $f = g + h + o_a(h)$ où :
$\begin{cases} g \text{ est un équivalent } \textbf{simple} \text{ de } f \ ; \\ h \text{ est un équivalent } \textbf{simple} \text{ de } f - g. \end{cases}$
3. On appelle DA à trois termes de f en a une expression de la forme $f = g + h + u + o_a(u)$ où :
$\begin{cases} g \text{ est un équivalent } \textbf{simple} \text{ de } f \ ; \\ h \text{ est un équivalent } \textbf{simple} \text{ de } f - g \ ; \\ u \text{ est un équivalent } \textbf{simple} \text{ de } f - g - h. \end{cases}$

Et cætera.

[a] Vu le lien équivalence/négligeabilité, c'est nécessairement un équivalent de f.

Sous espaces affines

Dans tout le chapitre, $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$ et E un $\mathbb{K}$-espace vectoriel.

I Généralités

I.1 Sous-espaces affines

Définition 1 : Translation.
Soit $a \in E$. On appelle translation de vecteur a l'application $\tau_a : \left\{\begin{array}{ccc} E & \to & E \\ x & \mapsto & x+a. \end{array}\right.$

Définition 2 .
Soit $\overrightarrow{W}$ un sev de E et $a \in E$. On appelle sous-espace affine de direction $\overrightarrow{W}$ et passant par a l'ensemble $W = \tau_a(\overrightarrow{W}) = a + \overrightarrow{W} = \left\{a + w,\ w \in \overrightarrow{W}\right\}$.

Remarque 1

1. Le sous-espace vectoriel $\overrightarrow{W}$ est unique. On dit que $\overrightarrow{W}$ est la direction de W.
2. Par contre, l'élément a ne l'est pas. Plus précisément, on a : $\forall b \in W,\ W = b + \overrightarrow{W}$. □

Proposition 1 : Structure d'espace affine.
Soit W un sous-espace affine de E. L'opération $\to$ définie de W^2 dans $\overrightarrow{W}$ vérifie les propriétés suivantes :

1. Relation dite "de Chasles" : $\forall (A, B, C) \in W^3,\ \overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$.
2. Bijection points/vecteurs à origine fixée : $\forall \Omega \in W,\ \forall w \in \overrightarrow{W},\ \exists! A \in W,\ \overrightarrow{\Omega A} = w$.

I.2 Propriétés

Définition 3 .
Soit W un sous-espace affine de E. On appelle dimension de W la dimension de $\overrightarrow{W}$, on note $\dim(\overrightarrow{W}) =: \dim(W)$.

Définition 4 .
Soit W un sous-espace affine de E. Soit truc $\in \left\{\text{droite, plan, hyperplan, } \ldots\right\}$.
On dit que W est un truc affine lorsque $\overrightarrow{W}$ est un truc (vectoriel).

Théorème 1 .
Une intersection de sous-espaces affines est soit vide, soit un sous-espace affine.

I.3 Repères

Définition 5 .
Soit $W = a + \overrightarrow{W}$ un sous-espace affine de E. On appelle repère de W tout couple $(\Omega, \mathcal{B})$ avec $\Omega \in W$ et $\mathcal{B}$ une base de $\overrightarrow{W}$ (en particulier, on *peut* prendre $\Omega = a$).
Si $\dim(W) < +\infty$, pour tout point $A \in W$, on appelle coordonnées de A dans $\mathcal{R}$ le n-uplet $\left|\ \overrightarrow{\Omega A}\ \right._{\mathcal{B}}$.

II L'exemple fondamental

II.1 L'exemple fondamental de sous-espace affine

Théorème 2 : Exemple fondamental de sous-espace affine.
Soient E et F deux $\mathbb{K}$-espaces vectoriels, $f \in \mathcal{L}(E, F)$ et $b \in F$.
Alors $W = \left\{x \in E,\ f(x) = b\right\}$ est vide ou est un sous-espace affine de direction $\mathrm{Ker}(f)$.

II.2 Illustrations

III Applications

III.1 Suites récurrentes affines doubles

Notation 1 (maison) : $E_{a,b,(c_n)_n} = \Big\{(u_n)_n \in \mathbb{K}^{\mathbb{N}},\ \forall n \in \mathbb{N},\ u_{n+2} = au_{n+1} + bu_n + c_n\Big\}$.

Proposition 2 .
$E_{a,b,(c_n)_n}$ est un sous-espace affine de $\mathbb{R}^{\mathbb{N}}$, de direction $\mathcal{S}_{a,b}$.

Proposition 3 : Recette de grand-mère..
Notons $\chi(X) = X^2 - aX - b$ le polynôme caractéristique.

Si $(c_n)_n$ est de la forme $\big(P(n)q^n\big)_n$ avec P un polynôme de degré p alors :

- Si q n'est pas racine de χ alors il existe une solution particulière de la forme $\big(q^nQ(n)\big)_n$ où $\deg(Q) = p$.
- Si q est racine simple de χ alors il existe une solution particulière de la forme $\big(nq^nQ(n)\big)_n$ où $\deg(Q) = p$.
- Si q est racine double de χ alors il existe une solution particulière de la forme $\big(n^2q^nQ(n)\big)_n$ où $\deg(Q) = p$.

III.2 Polynômes de Lagrange : le retour

Théorème 3 .

L'ensemble $\big\{P \in \mathbb{K}[X],\ \forall i \in \{0,\dots,n\},\ P(\alpha_i) = \beta_i\big\}$ est un sous-espace affine de $\mathbb{K}[X]$.

- Sa direction est : $\Big(\prod_{i=0}^{n}(X - \alpha_i)\Big)\mathbb{K}[X]$.

- Il passe par : $L(X) = \sum_{k=0}^{n} \beta_i L_i(X)$.

III.3 Systèmes linéaires

Théorème 4 : Théorème de structure affine.
L'ensemble des solutions d'un système linéaire est vide ou bien un sous-espace affine de $\mathbb{K}^n$ de direction l'ensemble des solutions du système linéaire homogène associé.

III.4 Distance à un hyperplan affine

Lemme 1 .
Soient $M, N, a \in E$ Alors

$$d(\tau_a(M), \tau_a(N)) = d(M, N)$$

Théorème 5 .
La distance d'un point M à l'hyperplan affine passant par un point A et ayant pour vecteur normal unitaire η est $\big|\langle \overrightarrow{AM}, \eta\rangle\big|$.

Bilan sur les structures algébriques.

I Structures

I.1 Groupes

Définition 1 : Groupe.

Un groupe est un couple $(G, \cdot)$, où G est un ensemble et $\cdot : G \times G \to G$ une **loi de composition interne**, vérifiant les axiomes suivants :

1. $\cdot$ est associative, c'est-à-dire : $\forall (a, b, c) \in G^3, a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
2. $\cdot$ a un élément neutre, c'est-à-dire : $\exists e \in G, \forall a \in G, a \cdot e = e \cdot a = a$,
3. tout élément de G a un symétrique pour $\cdot$, c'est-à-dire : $\forall x \in G, \exists y \in G, x \cdot y = y \cdot x = e$.

Remarque 1

C'est l'associativité de $\cdot$ qui nous autorise à écrire $a \cdot b \cdot c$ au lieu de $(a \cdot b) \cdot c$ ou $a \cdot (b \cdot c)$ (ces expressions étant égales).

Définition 2 : Commutativité.

Un groupe $(G, \cdot)$ est dit commutatif (ou abélien) lorsque la loi $\cdot$ est commutative, c'est-à-dire : $\forall (a, b) \in G^2, a \cdot b = b \cdot a$.

Définition 3 : Groupe symétrique.

On appelle groupe symétrique le groupe $(S_n, \circ)$ où $S_n = S_{\{1,2,\dots,n\}}$ est l'ensemble des bijections de $\{1, 2, \dots, n\}$ dans $\{1, 2, \dots, n\}$.

Proposition 1 : Unicité du neutre et des symétriques.

1. Dans un groupe, l'élément neutre est en réalité unique.
2. De plus, tous les éléments ont en réalité un unique symétrique.

Remarque 2

Ce théorème nous autorise à écrire x^{-1} pour dénoter **le** symétrique de x.

Théorème 1 : Symétrique d'un produit.

Dans un groupe, on a $(xy)^{-1} = y^{-1}x^{-1}$.

Définition 4 : Groupe produit.

Étant donnés deux groupes $(G_1, \cdot)$ et $(G_2, *)$, on appelle **groupe produit de** $(G_1, \cdot)$ **et** $(G_2, *)$ le couple $(G_1 \times G_2, \star)$ où $\star$ est définie par $(x_1, x_2) \star (y_1, y_2) = (x_1 \cdot y_1, x_2 * y_2)$

Proposition 2 : Groupe produit.

Les groupes produits sont des groupes.

I.2 Anneaux

Définition 5 : Anneaux.

Un anneau est un triplet $(A, +, \times)$, où A est un ensemble et $+, \times : A \times A \to A$ deux lois de composition internes, vérifiant les axiomes suivants :

1. $(A, +)$ forme un groupe commutatif,
2. $\times$ a un élément neutre,
3. $\times$ est associative,
4. $\times$ est distributive sur $+$, c'est-à-dire $\forall (a, b, c) \in A^3, a \times (b + c) = a \times b + a \times c$ (distributivité à gauche) et $\forall (a, b, c) \in A^3, (a + b) \times c = a \times c + b \times c$ (distributivité à droite).

Remarque 3

De la même façon que pour les groupes, le neutre de $+$ est unique, les symétriques pour $+$ sont uniques, le neutre pour $\times$ est unique, et les symétriques pour $\times$, lorsqu'ils existent, sont uniques.

On a donc coutume de toujours noter :

i/ 0_A ou 0 le neutre de $+$,

ii/ $-a$ le symétrique de a pour $+$, qu'on appelle opposé de a,

iii/ 1_A ou 1 le neutre de $\times$,

iv/ a^{-1} l'éventuel symétrique de a pour $\times$, s'il existe, qu'on appelle alors inverse de a.

Définition 6 : Commutativité.

Un anneau est dit commutatif si la loi $\times$ est commutative.

Proposition 3 : 0_A est absorbant.

Dans un anneau $(A,+,\times)$, l'élément 0_A est absorbant pour la loi $\times$, c'est-à-dire $\forall a \in A, a \times 0_A = 0_A$.

Proposition 4 : Opposé et multiplication.

Dans un anneau $(A,+,\times)$, on a, pour tout $a \in A$, $-a = (-1_A) \times a$.

Théorème 2 : Binôme de Newton.

Soient $(A,+,\times)$ un anneau, $n \in \mathbb{N}$, et $a, b \in A$ qui commutent. Alors on a : $(a+b)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

Théorème 3 : Identité géométrique généralisée.

Soient $(A,+,\times)$ un anneau, $n \in \mathbb{N}$, $a, b \in A$ qui commutent. Alors on a : $a^n - b^n = (a-b) \displaystyle\sum_{k=0}^{n-1} a^{n-1-k} b^k$.

Définition 7 : Intégrité.

Un anneau commutatif non nul $(A,+,\times)$ est dit **intègre** lorsqu'on a $\forall (a,b) \in A, a \times b = 0_A \Leftrightarrow a = 0_A$ ou $b = 0_A$.

Remarque 4

Dans la littérature, on trouve parfois d'autres définitions de l'intégrité, qui rajoutent une hypothèse de commutativité et/ou une hypothèse de non nullité. Comme le programme n'est pas explicite sur la définition à prendre, je vous donne celle que j'utilise.

Définition 8 : Divisibilité.

Dans tout anneau commutatif, pour tout couple (a,b) d'éléments de A, on dit que a divise b et on note $a|b$ lorsqu'on a $\exists k \in A, b = a \times k$.

Notation 1 Étant donné un anneau $(A,+_A,\times_A)$ on note $A^\times$ l'ensemble des inversibles de A (pour $\times_A$). **Remarque 5**

Soit $(A,+_A,\times_A)$ un anneau. On a $\forall (a,b) \in A^\times,\ a \times_A b \in A^\times$. Autrement dit $\times_A$ peut être vue comme une lci sur $A^\times$.

Théorème 4 : Groupe des inversibles d'un anneau.

$(A^\times, \times_A)$ forme un groupe, on l'appelle **groupe des inversibles de** $(A,+_A,\times_A)$.

I.3 Corps

Définition 9 : Corps.

Un corps est un triplet $(\mathbb{K}, +, \times)$, où $\mathbb{K}$ est un ensemble et $+, \times : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ deux lois de composition internes, vérifiant les axiomes suivants :

1. $(\mathbb{K}, +, \times)$ forme un anneau **commutatif et non nul**.
2. Tout élément de $\mathbb{K} \setminus \{0\}$ a un inverse.

Ce qui peut se reformuler :

1. $(\mathbb{K}, +)$ forme un groupe commutatif.
2. $(\mathbb{K} \setminus \{0\}, \times)$ forme un groupe commutatif.
3. $\times$ est distributive sur $+$

Proposition 5 .

Un corps est un anneau intègre.

I.4 Espaces vectoriels sur un corps

Définition 10 : K-ev.

Étant donné un corps $\mathbb{K}$, en contexte une bonne fois pour toute [a], un espace vectoriel sur $\mathbb{K}$ (ou $\mathbb{K}$-ev) est un triplet $(E, +, \cdot)$, où E est un ensemble, $+ : E \times E \to E$ une loi de composition interne et $\cdot : \mathbb{K} \times E \to E$ une loi de composition *externe* vérifiant les axiomes suivants :

1. $(E, +)$ forme un groupe **commutatif** (on note 0_E ou parfois $\overrightarrow{0}$ son élément neutre),
2. $\cdot$ est distributive à gauche et à droite sur $+$,
3. $\cdot$ est compatible avec $\times$ et 1_K.

a. C'est du pipo. En pratique on suppose $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$... très éventuellement $\mathbb{Q}$.

Proposition 6 : $\mathbf{0}_K$ et $\mathbf{0}_E$ sont absorbants.

1. Dans un $\mathbb{K}$-ev E, on a $\forall x \in E, 0_K \cdot x = 0_E$.
2. Dans un $\mathbb{K}$-ev E, on a $\forall \lambda \in \mathbb{K}, \lambda \cdot 0_E = 0_E$.

Corollaire 1 : Opposé et multiplication externe.

Dans un $\mathbb{K}$-ev E, on a, pour tout $x \in E$, $-x = (-1_{\mathbb{K}}) \cdot x$.

Proposition 7 : Produit nul dans un espace vectoriel.

Dans un $\mathbb{K}$-ev E, on a, pour tout $x \in E$ et tout $\lambda \in \mathbb{K}$, on a : $\lambda \cdot x = 0_E \Leftrightarrow \lambda = 0_{\mathbb{K}}$ ou $x = 0_E$.

I.5 Algèbre (unitaire, sur un corps)

Définition 11 : $\mathbb{K}$-algèbre.

Étant donné un corps $(\mathbb{K}, +_{\mathbb{K}}, \times_{\mathbb{K}})$ (comprendre : $\mathbb{R}$ ou $\mathbb{C}$), une algèbre unitaire sur $\mathbb{K}$ (abrégeons : une $\mathbb{K}$-alg) est un quadruplet $(\mathcal{A}, +, \times, \cdot)$, où $\mathcal{A}$ est un ensemble, $+, \times : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ deux lois de composition internes et $\cdot : \mathbb{K} \times \mathcal{A} \to \mathcal{A}$ une loi de composition externe vérifiant les axiomes suivants :

1. $(\mathcal{A}, +, \times)$ forme un anneau (on notera $0_{\mathcal{A}}$ et $1_{\mathcal{A}}$ ses éléments neutres),
2. $(\mathcal{A}, +, \cdot)$ est un $\mathbb{K}$-ev,
3. $\cdot$ et $\times$ sont compatibles : $(a \cdot x) \times (b \cdot y) = (a \times_{\mathbb{K}} b) \cdot (x \times y)$.

II Sous-structures

II.1 Sous-groupes

Définition 12 : Sous-groupe.

Soit $(G, \cdot)$ un groupe. On appelle sous-groupe de G un ensemble H inclus dans G stable pour la structure de groupe de G c'est-à-dire tel que :

1. $e \in H$ (en notant e le neutre de G),
2. $\forall (x, y) \in H^2, x \cdot y \in H$,
3. $\forall x \in H, x^{-1} \in H$ (en notant x^{-1} le symétrique de x pour $\cdot$).

Théorème 5 : Sous-groupe.

Si H est un sous-groupe de G, alors les lois de G induisent des lois sur H et H, muni des lois induites, forme un groupe.

Proposition 8 : Transitivité de "être un sous-groupe de".

Un sous-groupe d'un sous-groupe est un sous-groupe.

Remarque 6

Un sous-groupe d'un groupe commutatif est commutatif.

II.2 Sous-anneaux

Définition 13 : Sous-anneau.

Soit $(A, +, \times)$ un anneau. On appelle sous-anneau de A un ensemble B inclus dans A stable pour la structure d'anneau de A c'est-à-dire tel que :

1. $0_A,\ 1_A \in B$,
2. $\forall (x, y) \in B^2, x + y \in B$,
3. $\forall x \in B, -x \in B$,
4. $\forall (x, y) \in B^2, x \times y \in B$.

Proposition 9 : Sous-anneau.

Si B est un sous-anneau de A, alors les lois de A induisent des lois sur B, et B, muni des lois induites, forme un anneau.

Proposition 10 .

Un sous-anneau d'un sous-anneau est un sous-anneau.

Remarque 7

1. Un sous-anneau d'un anneau commutatif est commutatif.
2. Un sous-anneau d'un anneau intègre est intègre.

II.3 Sous-corps

Définition 14 : Sous-corps.

Soit $(\mathbb{K}, +, \times)$ un anneau. On appelle sous-corps de $\mathbb{K}$ un ensemble L inclus dans $\mathbb{K}$ stable pour la structure de corps de $\mathbb{K}$ c'est-à-dire tel que :

1. $(L, +, \times)$ forme un sous-anneau de $\mathbb{K}$ (reprendre les 4 axiomes).
2. L'inverse de tout élément de Ł $\setminus \{0\}$ **est dans** L.

Proposition 11 : Sous-corps.

Si L est un sous-corps de K, alors les lois de K induisent des lois sur L, et L muni des lois induites forme un corps.

Proposition 12 .

Un sous-corps d'un sous-corps est un sous-corps.

II.4 Sous-espace vectoriel

Définition 15 : Sous-espace vectoriel.

Soit $(E,+,\cdot)$ un $\mathbb{K}$-ev. On appelle sev de E un ensemble F inclus dans E stable pour la structure de $\mathbb{K}$-ev de E c'est-à-dire tel que :

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

Proposition 13 : Sev.

Si F est un sev de E, alors les lois de E induisent des lois sur F, et F, muni des lois induites, forme un $\mathbb{K}$-ev.

Proposition 14 .

Un sev d'un sev est un sev.

II.5 Sous-algèbres

III Morphismes

III.1 Morphismes de groupe

Définition 16 : Morphisme de groupe.

Étant donnés deux groupes $(G_1,\star)$ et $(G_2,\Box)$, on appelle **morphisme de groupe** (mdg) de $(G_1,\star)$ dans $(G_2,\Box)$ une application $f : G_1 \to G_2$ qui préserve la structure de groupe, c'est-à-dire telle que :

i/ $f(e_1) = e_2$

ii/ $\forall x \in G_1, f(x^{-1}) = f(x)^{-1}$

iii/ $\forall (x,y) \in G_1^2, f(x \star y) = f(x) \Box f(y)$

Théorème 6 : Morphisme de groupe.

Étant donnés deux groupes $(G_1,\star)$ et $(G_2,\Box)$, une application $f : G_1 \to G_2$ est un mdg si et seulement si elle préserve les produits, c'est-à-dire $\forall (x,y) \in G_1^2, f(x \star y) = f(x) \Box f(y)$.

Définition 17 : Isomorphisme de groupe.

On appelle **isomorphisme de groupe** un morphisme de groupe bijectif.

Théorème 7 : Isomorphisme de groupe.

L'application réciproque d'un isomorphisme de groupe est un isomorphisme de groupe.

Proposition 15 : Préservation des propriétés par isomorphisme.

Si $(G_1,\star)$ et $(G_2,\Box)$ sont isomorphes, alors $(G_1,\star)$ est commutatif si et seulement si $(G_2,\Box)$ l'est.

Théorème 8 : Structure catégorielle.

i/ L'identité d'un groupe est toujours un morphisme de groupe.

ii/ La composée de deux morphismes de groupes est un morphisme de groupe.

Définition 18 : Image, Noyau.

Étant donné un morphisme de groupe $f : (G_1,\star) \to (G_2,\Box)$, on appelle :

- Noyau de f la partie de G_1 suivante : $\mathrm{Ker}(f) = \{x \in G_1,\ f(x) = e_2\} = f^{\leftarrow}(\{e_2\})$.
- Image de f la partie de G_2 suivante : $\mathrm{Im}(f) = \{f(x),\ x \in G_1\} = f^{\rightarrow}(G_1)$.

Théorème 9 : Caractérisation de l'injectivité et la surjectivité.

Soit f un mdg de $(G_1, \star)$ dans $(G_2, \square)$

i/ f est surjective si et seulement si $\mathrm{Im}(f) = G_2$

ii/ f est injective si et seulement si $\mathrm{Ker}(f) = \{e_1\}$

iii/ f est un isomorphisme si et seulement si $\mathrm{Im}(f) = G_2$ et $\mathrm{Ker}(f) = \{e_1\}$.

Théorème 10 : Structure d'un noyau, d'une image.

Soit f un mdg de $(G_1, \star)$ dans $(G_2, \square)$

i/ $\mathrm{Ker}(f)$ est un sous-groupe de $(G_1, \star)$

ii/ $\mathrm{Im}(f)$ est un sous-groupe de $(G_2, \square)$

III.2 Morphismes d'anneau

Définition 19 : Morphisme d'anneau.

Étant donnés deux anneaux $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$, on appelle **morphisme d'anneau** (mda) de $(A, +_A, \times_A)$ dans $(B, +_B, \times_B)$ une application $f : A \to B$ qui préserve la structure d'anneau, c'est-à-dire tq :

i/ $f(0_A) = 0_B$

ii/ $\forall x \in A, f(-x) = -f(x)$

iii/ $\forall (x, y) \in A^2, f(x +_A y) = f(x) +_B f(y)$

iv/ $f(1_A) = 1_B$

v/ $\forall (x, y) \in A^2, f(x \times_A y) = f(x) \times_B f(y)$

Proposition 16 : Morphisme d'anneau.

Étant donnés deux anneaux $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$, une application $f : A \to B$ est un mda ssi

i/ $\forall (x, y) \in A^2, f(x +_A y) = f(x) +_B f(y)$

ii/ $f(1_A) = 1_B$

iii/ $\forall (x, y) \in A^2, f(x \times_A y) = f(x) \times_B f(y)$

Définition 20 : Isomorphisme d'anneau.

On appelle **isomorphisme d'anneau** un morphisme d'anneau bijectif.

Proposition 17 : Isomorphisme d'anneau.

L'application réciproque d'un isomorphisme d'anneau est un isomorphisme d'anneau.

Définition 21 : Morphisme de corps.

Étant donnés deux corps $(\mathbb{K}_A, +_A, \times_A)$ et $(\mathbb{K}_B, +_B, \times_B)$, on appelle **morphisme de corps** de $(\mathbb{K}_A, +_A, \times_A)$ dans $(\mathbb{K}_B, +_B, \times_B)$ une application $f : \mathbb{K}_A \to \mathbb{K}_B$ qui préserve la structure de corps, c'est-à-dire telle que :

i/ $f(0_A) = 0_B$

ii/ $\forall x \in A, f(-x) = -f(x)$

iii/ $\forall (x, y) \in \mathbb{K}_A^2, f(x +_A y) = f(x) +_B f(y)$

iv/ $f(1_A) = 1_B$

v/ $\forall (x, y) \in \mathbb{K}_A^2, f(x \times_A y) = f(x) \times_B f(y)$

vi/ $\forall x \in \mathbb{K}_A^\times, f(x^{-1}) = f(x)^{-1}$

Proposition 18 : Morphisme de corps.

Étant donnés deux corps $(\mathbb{K}_A, +_A, \times_A)$ et $(\mathbb{K}_B, +_B, \times_B)$ et une application $f : \mathbb{K}_A \to \mathbb{K}_B$, sont équivalentes :

a. f est un morphisme de corps

b. f est un morphisme d'anneau de $\mathbb{K}_A$ dans $\mathbb{K}_B$

c. i/ $f(1_A) = 1_B$

  ii/ $\forall (x, y) \in A^2, f(x +_A y) = f(x) +_B f(y)$

  iii/ $\forall (x, y) \in A^2, f(x \times_A y) = f(x) \times_B f(y)$

Proposition 19 : Préservation des propriétés par isomorphisme.

Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux isomorphes.

i/ A est commutatif si et seulement si B est commutatif

ii/ A est intègre si et seulement si B est intègre

iii/ A est un corps si et seulement si B est un corps

Proposition 20 : Structure catégorielle.

i/ L'identité d'un anneau est toujours un morphisme d'anneau.

ii/ La composée de deux morphismes d'anneaux est un morphisme d'anneau.

Définition 22 : Image, Noyau.

Pour f un mda de $(A, +_A, \times_A)$ dans $(B, +_B, \times_B)$

- Noyau de f : $\mathrm{Ker}(f) = \{x \in A,\ f(x) = 0_B\}$.
- Image de f : $\mathrm{Im}(f) = \{f(x),\ x \in A\}$.

Proposition 21 : Caractérisation de l'injectivité et la surjectivité.

Pour f un mda de $(A, +_A, \times_A)$ dans $(B, +_B, \times_B)$

i/ f est surjective si et seulement si $\mathrm{Im}(f) = B$

ii/ f est injective si et seulement si $\mathrm{Ker}(f) = \{0_A\}$

iii/ f est un isomorphisme si et seulement si $\mathrm{Im}(f) = B$ et $\mathrm{Ker}(f) = \{0_A\}$.

III.3 Applications linéaires

Définition 23 : Application linéaire.

Étant donnés un corps $\mathbb{K}$ et deux $\mathbb{K}$-espaces vectoriels $(E_1, +, \cdot)$ et $(E_2, +, \cdot)$, on appelle **application linéaire** ("morphisme d'espace vectoriel") de $(E_1, +, \cdot)$ dans $(E_2, +, \cdot)$ une application $f : E_1 \to E_2$ qui préserve la structure d'espace vectoriel, c'est-à-dire telle que :

i/ $f(0) = 0$

ii/ $\forall x \in E_1, \forall \lambda \in \mathbb{K} f(\lambda x) = \lambda f(x)$

iii/ $\forall (x, y) \in E_1^2, f(x + y) = f(x) + f(y)$

Théorème 11 : Application linéaire.

$f : E_1 \to E_2$ est une application linéaire ssi on a : $\forall (x, y) \in E_1^2, \forall (\lambda, \mu) \in \mathbb{K}^2, f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$.

Théorème 12 : Structure catégorielle.

i/ L'identité d'un espace vectoriel est toujours une application linéaire.

ii/ La composée de deux application linéaires est une application linéaire.

Définition 24 : Image, Noyau.

Pour $f : E_1 \to E_2$ une application linéaire, on appelle :

- Noyau de f la partie de E_1 suivante : $\mathrm{Ker}(f) = \{x \in E_1,\ f(x) = 0\}$.
- Image de f la partie de E_2 suivante : $\mathrm{Im}(f) = \{f(x),\ x \in E_1\}$.

Théorème 13 : Caractérisation de l'injectivité et la surjectivité.

Pour $f : E_1 \to E_2$ une application linéaire :

i/ f est surjective si et seulement si $\mathrm{Im}(f) = E_2$

ii/ f est injective si et seulement si $\mathrm{Ker}(f) = \{0\}$

iii/ f est un isomorphisme si et seulement si $\mathrm{Im}(f) = E_2$ et $\mathrm{Ker}(f) = \{0\}$.

Théorème 14 : Structure d'un noyau, d'une image.

$\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$ sont des sous-espaces vectoriels .

IV Conclusion

Variables aléatoires finies

L'idée : plutôt que de modéliser une expérience aléatoire par un espace probabilisé trop grossier, on *postule* qu'un espace probabilisé $(\Omega, \mathcal{P}(\Omega), P)$ le modélise finement et on considère une application $X : \Omega \to E$ où E correspond aux évéments observables ou qui nous intéressent.

Exemple 1 On lance un dé de 6 non pipé. Modéliser cette expérience aléatoire en posant $\Omega = \{1, 2, \ldots, 6\}$ oblige à identifier des situations très différentes, et est abusif car un résultat de l'expérience n'est pas un nombre. On peut aussi postuler l'existence d'un espace probabilisé $(\Omega, \mathcal{P}(\Omega), P)$ modélisant finement cette expérience et considérer l'application

$$X : \left\{ \begin{array}{lll} \Omega & \to & \{1, 2, \ldots, 6\} \\ \omega & \mapsto & \text{le nombre lu sur la face supérieure du dé lorsque } \omega \text{ est réalisée.} \end{array} \right.$$

Exemple 2 On lance deux dés de 6 non pipés. Quelle que soit la modélisation choisie pour cette expérience aléatoire, on peut souhaiter ne s'intéresser qu'à la somme des deux valeurs obtenues (par exemple parce qu'on joue à un jeu dont le gagnant est celui qui réalise la plus grande somme). On s'intéresse alors naturellement à l'application

$$X : \left\{ \begin{array}{lll} \Omega & \to & \{2, 3, \ldots, 12\} \\ \omega & \mapsto & \text{la somme des résultats des dés lorsque } \omega \text{ est réalisée.} \end{array} \right.$$

Les valeurs prises par X **correspondent aux évéments qui nous intéressent**.
En particulier les événements $\{\omega \in \Omega, X(\omega) = i\}$, où i parcourt les valeurs prises par X :

- auraient pu former l'ensemble Ω si on avait voulu modéliser très grossièrement (mais beurk !) ;
- forment un système complet d'événements (est-ce qu'on sait encore ce que c'est ?).

Dans tout le chapitre, $(\Omega, \mathcal{P}(\Omega), P)$ désigne un espace probabilisé, et E désigne un ensemble.

I Variables aléatoires

I.1 Définition et autres exemples

Définition 1 : Variable aléatoire.

1. On appelle <u>variable aléatoire</u> (si grosse paresse : <u>v.a.</u>) une application $X : \Omega \to E$.
2. Si $E \subset \mathbb{R}$, on dit que X est une <u>variable aléatoire réelle</u>, dans toute la suite <u>v.a.r.</u>
3. Si $E \subset \mathbb{R}^n$ pour un entier n, on dit que X est un <u>vecteur aléatoire</u>, dans la suite $\underline{\overrightarrow{\text{v.a.}}}$.

I.2 Terminologie et notations

Notation 1 Si $X : \Omega \to E$ est une variable aléatoire, on notera :

- $(X = x)$ l'événement $X^{-1}\big(\{x\}\big)$, pour $x \in E$;
- $(X \in A)$ l'événement $X^{-1}\big(A\big)$, pour $A \subset E$.

Si de plus X est une v.a.r. (*i. e.* si on a $E \subset \mathbb{R}$), on notera :

- $(X \leqslant x)$ l'événement $X^{-1}\big(]-\infty, x]\big)$;
- $(X < x)$ l'événement $X^{-1}\big(]-\infty, x[\big)$;
- $(X \geqslant x)$ l'événement $X^{-1}\big([x, \infty[\big)$;
- $(X > x)$ l'événement $X^{-1}\big(]x, +\infty[\big)$.

Remarque 1

La famille des $(X = x)_{x\in X(\Omega)}$ forme un système complet d'événements. **Notation 2** Si F est un ensemble et $f : E \to F$ est une application, on pourra noter $f(X)$ la variable aléatoire $f \circ X$. En effet, ces gens (les probabilistes) sont des barbares.

I.3 Loi d'une variable aléatoire réelle

Définition 2 : Loi.

Soit $X : \Omega \to E$ une variable aléatoire. On appelle loi de X l'application $P_X : \left\{ \begin{array}{ccc} \mathcal{P}\big(X(\Omega)\big) & \to & [0,1] \\ A & \mapsto & P(X \in A) \end{array} \right.$

Remarque 2

On identifiera fréquemment P_X avec son prolongement naturel à $\mathcal{P}(E)$, parfois plus pratique à décrire :

$$P_X : \left\{ \begin{array}{ccc} \mathcal{P}(E) & \to & [0,1] \\ A & \mapsto & P(X \in A) \end{array} \right. .$$

Théorème 1 .

Soit $X : \Omega \to E$ une variable aléatoire.

Alors $P_X : \mathcal{P}(X(\Omega)) \to [0,1]$ est une probabilité.

Bien sûr, de même, $P_X : \mathcal{P}(E) \to [0,1]$ est une probabilité.

II Lois usuelles

II.1 Loi uniforme finie

Définition 3 .

On dit que X suit la loi uniforme sur E et on note $X \sim \mathcal{U}(E)$ lorsqu'on a $P_X = P_u$ (sur E), i. e. lorsqu'on a $\forall x \in E,\ P(X = x) = \dfrac{1}{|E|}$. Si $E = \{a, a+1, \dots, b\}$ on note $X \sim \mathcal{U}(a; b)$.

II.2 Loi de Bernoulli

Définition 4 .

Soit $p \in [0,1]$. On dit que X suit la loi de Bernoulli de paramètre p et on note $X \sim \mathcal{B}(p)$ lorsqu'on a $X(\Omega) \subset \{0,1\}$ et $P(X = 1) = p$, donc $P(X = 0) = 1 - p = q$.

Théorème 2 .

Une v.a.r. suit une loi de Bernoulli si et seulement si c'est une fonction indicatrice.
Autrement dit : $\Big(\exists p \in [0,1],\ X \sim \mathcal{B}(p)\Big) \Leftrightarrow \Big(\exists A \in \mathcal{P}(\Omega),\ X = 1\!\!1_A\Big)$.

II.3 Loi binomiale

Définition 5 .

Soit $n \in \mathbb{N}$ et $p \in [0,1]$. On dit que X suit la loi binomiale de paramètres n et p et on note $X \sim \mathcal{B}(n,p)$ lorsqu'on a $X(\Omega) \subset \{0, 1, \dots, n\}$ et $\forall k \in \{0, \dots, n\},\ P(X = k) = \binom{n}{k} p^k q^{n-k}$ où bien sûr $q = 1 - p$.

II.4 Exercice classique : décrire la loi d'une v.a.r. donnée

III Espérance. Variance.

III.1 Espérance

Définition 6 : Espérance.

On appelle espérance de X le nombre $E(X) = \displaystyle\sum_{x\in X(\Omega)} P(X = x)\, x$.

Théorème 3 : Propriétés de l'espérance.

1. On a : $E(X) = \sum_{\omega \in \Omega} X(\omega) P(\{\omega\})$.
2. L'espérance est :
   — linéaire : $\forall X, Y : \Omega \to \mathbb{R},\ \forall \lambda, \mu \in \mathbb{R}^2,\ E(\lambda X + \mu Y) = \lambda E(X) + \mu E(Y)$;
   — positive : $\forall X : \Omega \to \mathbb{R},\ X \geqslant 0 \Rightarrow E(X) \geqslant 0$;
   — croissante : $\forall X, Y : \Omega \to \mathbb{R},\ X \leqslant Y \Rightarrow E(X) \leqslant E(Y)$.
3. Si X est constante, i. e. il existe m tel que $X(\Omega) = \{m\}$, alors $E(X) = m$.

III.2 Variance

Définition 7 : Variance.

On appelle <u>variance de X</u> le nombre $V(X) = E\big((X - E(X))^2\big)$.

Remarque 3

On met un carré car :

— ça permet d'augmenter les gros écarts et diminuer les petits écarts (erreurs de mesure, e.g.)

— ça devient presque un produit skyler

Remarque 4

Par positivité de l'espérance, on a toujours $V(X) \geqslant 0$. Ceci permet de définir <u>l'écart-type de X</u> $\sigma(X) = \sqrt{V(X)}$.

Terminologie : lorsqu'on a $V(X) = 1$ (*i. e.* $\sigma(X) = 1$), on dit que <u>X est réduite</u>.

Exemple 3 Déterminons la variance de la variable aléatoire de l'exemple **??**. On reprend $X : \begin{cases} \Omega & \to \{1, \dots, 6\} \\ \omega & \mapsto \text{la valeur du dé} \end{cases}$

Remarque 5

C'est un cas particulier de la loi uniforme

Théorème 4 : Propriétés de la variance.

1. Formule de Kœnig : $V(X) = E(X^2) - E(X)^2$.
2. Si $a, b \in \mathbb{R}$ alors $V(aX + b) = a^2 V(X)$.
3. Si X est constante, alors $V(X) = 0$.

III.3 Théorème de transfert

Théorème 5 : Formule de transfert.

Soit $Z : \Omega \to E$ une variable aléatoire (non nécessairement réelle) et $f : E \to \mathbb{R}$. Alors :

$$E(f(Z)) = \sum_{z \in Z(\Omega)} f(z) P(Z = z)$$

III.4 Deux inégalités fondamentales

Théorème 6 : Inégalité de Markov.

Supposons X **positive**. Soit $\alpha > 0$. Alors $P(X \geqslant \alpha) \leqslant \dfrac{E(X)}{\alpha}$.

Théorème 7 : Inégalité de Bienaymé-Tchebychev.

Soit $\varepsilon > 0$. Alors $P\big(|X - E(X)| \geqslant \varepsilon\big) \leqslant \dfrac{V(X)}{\varepsilon^2}$.

III.5 Espérance et variance des lois usuelles

Remarque 6

Si $X \sim \mathcal{U}(a;b)$, l'espérance et la variance de X ne sont pas explicitement au programme ; mais on les verra en TD.

$$X(\Omega) \subset \{0,1\} \qquad \begin{cases} P(X=0) & = 1-p = q \\ P(X=1) & = p \end{cases}$$

- $E(X) = \sum_{x\in X(\Omega)} P(X=x)x = 0q + 1p = p$
- $V(X) = E(X^2) - E(X)^2$ or $X^2 = X$ donc $V(X) = E(X) - E(X)^2 = p - p^2 = p(1-p) = pq$

Théorème 8 : Cas d'une loi de Bernoulli.

On suppose $X \sim \mathcal{B}(p)$ pour un certain $p \in [0,1]$ (on note $q = 1-p$). Alors :

$$X(\Omega) \subset \{0,\dots,n\}$$
$$P(X=k) = \binom{n}{k} p^k q^{n-k}$$

- $E(X) = np$
- $V(X) = npq$

Théorème 9 : Cas d'une loi Binomiale.

On suppose $X \sim \mathcal{B}(n,p)$ pour un certain $(n,p) \in \mathbb{N} \times [0,1]$ (on note $q = 1-p$). Alors :

- $E(X) = np$
- $V(X) = npq$

IV Indépendance

IV.1 Indépendance de deux variables aléatoires

Théorème 10 .

Soient $X : \Omega \to E$ et $Y : \Omega \to F$ deux variables aléatoires indépendantes, et $f : E \to E'$ et $g : F \to F'$ deux applications. Alors $f(X)$ et $g(Y)$ sont indépendantes.

IV.2 Indépendance, espérance et variance

Théorème 11 .

Soient X et Y deux v.a.r. Si X et Y sont indépendantes, alors $E(XY) = E(X)E(Y)$.

Corollaire 1 .

Soient X et Y deux v.a.r. Si X et Y sont indépendantes, alors $V(X+Y) = V(X) + V(Y)$.

Théorème 12 .

Soient $X_1, \dots, X_n$ des v.a.r. indépendantes deux à deux, alors $V(X_1 + \dots + X_n) = V(X_1) + \dots + V(X_n)$.

IV.3 Indépendance mutuelle

Théorème 13 .

Soient $p \in [0,1]$ et X_1, X_2, …, X_n des variables aléatoires **mutuellement indépendantes** telles que $\forall i,\ X_i \sim \mathcal{B}(p)$. Alors $X_1 + X_2 + \dots + X_n \sim \mathcal{B}(n,p)$.

V Vecteurs aléatoires

V.1 Exemples

Remarque 7

"Théorème de Nil Venet" : quitte à considérer que Ω modélise la réalisation de toutes les expériences aléatoires possibles et imaginables, on peut toujours considérer que deux variables aléatoires quelconques sont définies sur le même univers Ω.

V.2 Lois associées à un vecteur aléatoire

Définition 8 .

Soit $Z = \binom{X}{Y}$ un couple aléatoire.

- On appelle loi conjointe de X et Y la loi de Z.
- On appelle lois marginales de Z les lois de X et Y.

Remarque 8

1. Le tableau donne seulement les $P(Z = (x, y))$ mais d'après .... cela suffit.
2. Le tableau de la loi conjointe illustre qu'en général on a seulement $(X, Y)(\Omega)$ ..... $X(\Omega) \times Y(\Omega)$.
3. Une fois obtenu le tableau de la loi conjointe, on en déduit les lois marginales en ....
4. Cet exemple en particulier illustre que ....
5. **Cependant**, ...

Définition 9 .

Soit $Z = \binom{X}{Y}$ et $A \in X(\Omega)$. On appelle loi de Y conditionnellement à $X \in A$ (ou loi de Y sachant $X \in A$) l'application $\left\{ \begin{array}{ccc} \mathcal{P}(Y(\Omega)) & \rightarrow & [0,1] \\ B & \mapsto & P_{X\in A}(Y \in B) \end{array} \right.$.

V.3 Covariance

Définition 10 .

Soit $\binom{X}{Y}$ un couple aléatoire. On appelle covariance de X et Y le réel $\mathrm{Cov}(X, Y) = E((X - E(X))(Y - E(Y)))$.

Théorème 14 : Kœnig-Huygens.

Soit $\binom{X}{Y}$ un couple aléatoire. Alors $\mathrm{Cov}(X, Y) = E(XY) - E(X)E(Y)$.

Théorème 15 .

Soit $\binom{X}{Y}$ un couple aléatoire. Si X et Y sont indépendantes alors ....

Remarque 9

La réciproque est fausse **et on l'a déjà vu** !

En effet :

Théorème 16 .

La covariance est une forme bilinéaire, symétrique, et positive (seulement).

Corollaire 2 : Cauchy-Schwarz.

Soit $\binom{X}{Y}$ un couple aléatoire. Alors $|\mathrm{Cov}(X,Y)| \leqslant \sigma(X)\sigma(Y)$.

Théorème 17 .

Soient X_1, ..., X_n des var sur Ω. $V(X_1 + \cdots + X_n) =$ ....

V.4 Indépendance vs décorrélation

Définition 11 .

Soit $\binom{X}{Y}$ un couple aléatoire. On appelle coefficient de corrélation de X et Y le réel $\rho_{X,Y} = \dfrac{\mathrm{Cov}(X,Y)}{\sigma(X)\sigma(Y)}$.

Définition 12 .

Soit $\binom{X}{Y}$ un couple aléatoire. On dit que X et Y sont <u>décorrélées</u> lorsqu'on a $\rho_{X,Y} = 0$, i. e. $\mathrm{Cov}(X,Y) = 0$.

Lemme 1 .

Soit X une v.a.r. finie. On a $V(X) = 0 \Leftrightarrow X$ constante.

Corollaire 3 .

Soit $\binom{X}{Y}$ un couple aléatoire avec X non constante. On a $|\rho_{X,Y}| = 1 \Leftrightarrow \exists (a,b) \in \mathbb{R}^2,\ Y = aX + b$.

\end exemple \end document

Équations différentielles linéaires.

Contexte : dans tout le chapitre, I désigne un intervalle non trivial, et $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

Notation 1 Pour gagner un peu de place et de temps :

ED : Équation différentielle.

EDL : Équation différentielle linéaire.

Notation 2 Pour gagner un peu de place et de temps :

ED : Équation différentielle.

EDL : Équation différentielle linéaire.

I Généralités sur les EDL

I.1 Terminologie

Définition 1 : EDL sur I.

On appelle EDL sur I une équation dont l'inconnue est une fonction $y \in \mathcal{D}^n$ et de la forme

$$\forall t,\ a_n(t)y^{(n)}(t) + \cdots + a_1(t)y'(t) + a_0(t)y(t) = b(t) \qquad \text{où :}$$

- $n \in \mathbb{N}$ est appelé l'ordre de l'EDL ;
- $a_0, a_1, \dots, a_n \in \mathcal{C}(I, \mathbb{K})$ sont appelés les coefficients de l'EDL ;
- $b \in \mathcal{C}(I, \mathbb{K})$ est appelé le second membre de l'EDL.

Définition 2 : Solution d'une EDL.

On appelle solution locale de l'EDL un couple (J, y) avec J un intervalle inclus dans I et $y \in \mathcal{D}^n(J, \mathbb{K})$ qui vérifie l'équation (pour $t \in J$). Pour $J = I$ on parle de solution globale, celles qui nous intéressent en priorité.

I.2 Théorème de Cauchy-linéaire.

Définition 3 : Problème de Cauchy.

On appelle problème de Cauchy un système de la forme

$$\begin{cases} y^{(n)}(t) + a_{n-1}(t)y^{(n-1)}(t) + \cdots + a_0(t)y(t) = b(t) \\ y(t_0) = \alpha_0 \\ \vdots \\ y^{(n-1)}(t_0) = \alpha_{n-1} \end{cases}$$

où $t_0 \in I$ et $(\alpha_0, \dots, \alpha_{n-1}) \in \mathbb{K}^n$. (Et où les a_i et b sont $\mathcal{D}^n(I, \mathbb{K})$ comme d'habitude.)

Théorème 1 : Cauchy linéaire.

Un problème de Cauchy a toujours une unique solution.

I.3 Théorème de structure affine

Théorème 2 : de structure affine.

L'ensemble des solutions (globales) d'une EDL résolue est un sea de direction l'ensemble des solutions de l'EDLH associée. Sa dimension est l'ordre de l'EDL.

Théorème 3 : Principe de superposition.

Soient $a_0, \dots, a_n, b, b_1 \in \mathcal{D}^n(I, \mathbb{K})$.

Si y_1 est solution de $y^{(n)}(t) + a_{n-1}(t)y^{(n-1)}(t) + \cdots + a_0(t)y(t) = b_1(t)$;

et y_2 est solution de $y^{(n)}(t) + a_{n-1}(t)y^{(n-1)}(t) + \cdots + a_0(t)y(t) = b_2(t)$;

alors $\lambda y_1 + \mu y_2$ est solution de $y^{(n)}(t) + a_{n-1}(t)y^{(n-1)}(t) + \cdots + a_0(t)y(t) = \lambda b_1(t) + \mu b_2(t)$.

II EDL du premier ordre

II.1 Cas résolu homogène

Théorème 4 .

L'ensemble des solutions globales est .... où ....

II.2 Cas résolu non homogène

Théorème 5 : Variations de la constante.

En gardant les mêmes notations que précédemment, on peut toujours trouver une solution particulière de la forme $t \mapsto K(t)\mathrm{e}^{A(t)}$ à l'aide d'un simple calcul de primitive.

II.3 Cas non résolu

III EDL du second ordre à coefficients constants

III.1 Cas homogène

Définition 4 .

On appelle polynôme caractéristique de l'EDL le polynôme $\chi(X) = aX^2 + bX + c$.

Théorème 6 : Second ordre à coefficients constants, cas homogène.

Notons S_H l'ensemble des solutions globales.

1. Si χ a deux racines r_1, r_2 dans $\mathbb{K}$ alors l'ensemble des solutions est $S_H = \left\{t \mapsto A\mathrm{e}^{r_1 t} + B\mathrm{e}^{r_2 t},\ \binom{A}{B} \in \mathbb{K}^2\right\}$.
2. Si χ a une racine double r_0 dans $\mathbb{K}$ alors l'ensemble des solutions est $S_H = \left\{t \mapsto (A+Bt)\mathrm{e}^{r_0 t},\ \binom{A}{B} \in \mathbb{K}^2\right\}$.
3. Pour $\mathbb{K} = \mathbb{R}$, si χ a deux racines complexes conjuguées $\alpha + \mathbf{i}\omega$ et $\alpha - \mathbf{i}\omega$ alors on a $S_H = \left\{t \mapsto \mathrm{e}^{\alpha t}(A\cos(\omega t) + B\sin(\omega t)),\ \binom{A}{B} \in \mathbb{R}^2\right\}$.

III.2 Cas d'un second membre de la forme $P(t)\mathrm{e}^{\gamma t}$

Théorème 7 .

L'équation $ay''(t) + by'(t) + cy(t) = P(t)\mathrm{e}^{\gamma t}$ a toujours une solution particulière de la forme $t^\mu Q(t)\mathrm{e}^{\gamma t}$ où :

- μ est la multiplicité de γ comme racine de χ
- Q est un polynôme de même degré que P.

IV Autres équations différentielles

IV.1 Méthode d'Euler

Remarque 1

Même dans le cas $y'(t) + a(t)y(t) = b(t)$ la méthode d'Euler peut être utile car

IV.2 Changement de fonction inconnue

IV.3 Changement de variable

IV.4 Équations à variables séparées

Def. 1: trou

$$A_1(X)B_2(X) = A_2(X)B_1(X)$$

Prop-Def. 2: Dem.

Existance Soit $\frac{A}{B} \in \mathbb{K}[X]$
Notons $D := A \wedge B$
Puis $\begin{cases} \tilde{A} &= \frac{A}{D} \\ \tilde{D} &= \frac{B}{D} \end{cases}$
Par homogénéité de PGCD :

$$\tilde{A} \wedge \tilde{B} = 1$$

On note μ le coefficient dominant de B puis

$$P = \frac{\tilde{A}}{\mu}$$
$$Q = \frac{\tilde{B}}{\mu}$$

On a bien $\begin{cases} P \wedge Q = 1 \\ \frac{P}{Q} = \frac{\tilde{A}}{\tilde{B}} = \frac{A}{B} \\ Q \text{ unitaire} \end{cases}$

Unicité Supposons avoir deux formes irréductibles

$$\frac{A}{B} = \frac{P_1}{Q_1} = \frac{P_2}{Q_2}$$

donc $P_1Q_2 = P_2Q_1$
On a

$$\begin{cases} Q_1 & |P_1Q_2 \\ P_1 \wedge Q_1 & = 1 \end{cases}$$

$$\text{donc } Q_1|Q_2 \qquad \text{d'après le lemme de Gauss}$$
$$Q_2|Q_1 \qquad \text{de même}$$

Or Q_1, Q_2 sont unitaires donc $Q_1 = Q_2$
En réinjectant et par intégrité $P_1 = P_2$

Exercice 1

$$P' \wedge P = 1 \iff P \text{ unitaire et toutes ses racines sont simples}$$

Prop-Def. 3 dem. L'indépendance au représentant choisi

Prop-Def. 5 dem. Soit $F = \frac{A}{B} = \frac{C}{D}$
$i.e. A \times D = C \times B$
On veut montrer

$$\begin{aligned} \frac{A'B - AB'}{B^2} &= \frac{C'D - D'C}{D^2} \\ \iff D^2(A'B - B'A) &= B^2(C'D - D'C) \\ \iff A'BD^2 - ADB'D &= C'B^2DB - CD'B^2 \\ \iff A'BD^2 - BCB'D &= C'BDB - ADD'B \\ \iff BD(A'D - CB') &= BD(C'B - AD') \\ \iff A'D - CB' &= C'B - AD' \\ \iff A'D + AD' &= C'B + CB' \\ \iff (AD)' &= (BC)' \end{aligned}$$

C'est vrai, ouf!!!

Exemple 1

$$\frac{aX + b}{cX + d}$$

Exemple 2: Trou juste avant

$$F' \leq \deg F - 1$$

Exemple 2

$$\begin{aligned} \deg \left(\frac{aX + b}{cX + d} \right)' &= \frac{a(cX + d) - c(aX + b)}{(cX + d)^2} \\ &= \frac{ad - bc}{(cX + d)^2} \\ &= -2 \end{aligned}$$

Def. 7: Reformulation, trous

1. λ n'est ni un zéro ni un pôle.
2. λ est un zéro de multiplicité $a - b$
3. λ est pôle de multiplicité $b - a$

Remq. 5: Trou les zéros de $\frac{A}{B}$

Prop-Def. 9: Dem. D'après le théorème de division euclidienne

$$\exists!(Q,R),\ \begin{cases} A & = BQ+R \\ Q & \in \mathbb{K}[X] \\ R & \in \mathbb{K}_{\deg B-1}[X] \end{cases}$$

$$\iff \exists!(Q,R),\ \begin{cases} F & = Q+\frac{R}{B} \\ Q & \in \mathbb{K}[X] \\ \deg R & < \deg B \end{cases}$$

$$\iff \exists!(Q,R),\ \begin{cases} F & = Q+G \\ Q & \in \mathbb{K}[X] \\ \underbrace{\deg(BG)-\deg B}_{\deg G} & < 0 \end{cases}$$

Exemple: partie polynomiale de $\frac{X^3+2X+1}{X^2-1}$

$$\begin{array}{c|c} X^3+2X+1 & X^2-1 \\ X^3-X & \text{X} \\ 3X+1 & \end{array}$$

$$\frac{X^3+2X+1}{X^2-1} = \underbrace{X}_{\text{partie polynomiale}} + \frac{3X+1}{X^2+1}$$

Thm. 2 Si $B=\mu(X-\lambda_1)\cdots(X-\lambda_n)$ alors il existe Q unique et $(\alpha_1,\dots,\alpha_n)$ uniques tels que

$$\frac{A}{B} = Q + \frac{\alpha_1}{X-\lambda_1}+\cdots+\frac{\alpha_n}{X-\lambda_n}$$

et Q est la partie polynomiale de $\frac{A}{B}$

Thm. 2: Dem. D'après le théorème de division euclidienne, il suffit de montrer que

$$\forall R\in\mathbb{R}_{\deg B-1}[X],\ \exists! \begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_n\end{pmatrix}\in\mathbb{K}^n,\ \frac{R}{B} = \frac{\alpha_1}{X-\lambda_1}+\cdots+\frac{\alpha_n}{X-\lambda_n}$$

Notons $\begin{cases} E & = \mathbb{K}^n \\ F & = \frac{1}{B} \qquad \underbrace{\mathbb{K}_{\deg B-1}[X]}_{\text{polynômes de degré} < \deg B} \end{cases}$

$$\phi : \begin{cases} E & \to F \\ \begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_n\end{pmatrix} & \mapsto \frac{\alpha_1}{X-\lambda_1}+\cdots+\frac{\alpha_n}{X-\lambda_n} \end{cases}$$

On a

$$\begin{aligned} &\dim\left(\mathbb{K}_{\deg B-1}[X]\right) = n \\ \implies &\dim\left(\frac{1}{B}\mathbb{K}_{\deg B-1}[X]\right) = n \\ &\text{et } \dim \mathbb{K}^n = n \end{aligned}$$

ϕ est linéaire par distributivité de $\cdot$ sur $+$
Par caractérisation des isomorphismes en dimension finie:

$$\phi \text{ bijective} \iff \phi \text{ injective}$$

$$\operatorname{Ker}\phi = \left\{ \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in \mathbb{K}^n,\ \frac{\alpha_1}{X-\lambda_1} + \cdots + \frac{\alpha_n}{X-\lambda_n} = 0 \right\}$$

Or $\left(\frac{1}{X-\lambda_1},\ \frac{1}{X-\lambda_2},\ \ldots,\ \frac{1}{X-\lambda_n}\right)$ est *libre*
Donc $\operatorname{Ker}\phi = \{0\}$ donc ϕ est bijective
$i.e.\forall \frac{R}{B} \in F,\ \exists! \begin{pmatrix} \alpha_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{K}^n,\ \phi \begin{pmatrix} \alpha_1 \\ \vdots \\ a_n \end{pmatrix} = \frac{R}{B}$
$i.e.\forall R \in \mathbb{R}_{\deg B-1}[X],\ \exists! \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in \mathbb{K}^n,\ \frac{R}{B} = \frac{\alpha_1}{X-\lambda_1} + \cdots + \frac{\alpha_n}{X-\lambda_n}$

Exemple DES de $\frac{1}{(X^2+1)(X^2+4)}$

$$\frac{1}{(X^2+1)(X^2+4)} = \frac{\alpha X + \beta}{X^2+1} + \frac{\gamma X + \delta}{X^2+4}$$

Passons par $\mathbb{C}(X)$

$$\begin{aligned} \frac{1}{(X^2+1)(X^2+4)} &= \frac{a}{X-i} + \frac{b}{X+i} + \frac{c}{X-2i} + \frac{d}{X+2i} \\ \frac{1}{(X+i)(X-i)} a + (X-i)(\ldots) \quad \times (X-i)a & \qquad = -\frac{i}{6} \impliedby X = i \\ b = \overline{a} = \frac{i}{6} & \qquad \text{par unicité de la DES} \\ \frac{1}{(X^2+1)(X+2i)} c + (X-i)(\ldots) \quad \times (X-2i)a & \qquad = \frac{i}{12} \impliedby X = 2i \\ b = \overline{c} = -\frac{i}{12} & \qquad \text{par unicité de la DES} \end{aligned}$$

En regroupant chaque pôle avec son conjugué:

$$
\begin{aligned}
\frac{1}{(X^2+1)(X^2+4)} &= \frac{1}{6}\left(\frac{i}{X+i} - \frac{i}{X-i}\right) + \frac{1}{12}\left(\frac{i}{X-2i} - \frac{i}{X+2i}\right) \\
&= \frac{1}{6}\frac{2}{X^2+1} + \frac{1}{12}\frac{-4}{X^2+4} \\
&= \frac{1/3}{X^2+1} - \frac{1/3}{X^2+4}
\end{aligned}
$$

Thm. 3: Dem.

$$
\begin{aligned}
P &= \mu \prod_{i=1}^{r} (X-\lambda_i)^{m_i} \\
\deg P &= \sum_{k=1}^{r} m_k \\
P' &=
\end{aligned}
$$

En général:

$$
\left(\prod_{i=1}^{n} u_i\right)' = \sum_{k=1}^{n} u_1 \cdots u_{i-1} \cdot u_i' \cdot u_{i+1} \cdots u_n
$$

$$
\begin{aligned}
P' &= \mu \sum_{k=1}^{r} (X-\lambda_1)^{m_1} \times \ldots \times (X-\lambda_{i-1})^{m_{i-1}} \times ((X-\lambda_i)^{m_i})' \times (X-\lambda_{i+1})^{m_{i+1}} \times \ldots \times (X-\lambda_r)^{m_r} \\
\frac{P'}{P} &= \sum_{k=1}^{r} \frac{(X-\lambda_1)^{m_1} \times \ldots \times (X-\lambda_{i-1})^{m_{i-1}} \times m_i \times (X-\lambda_{i+1})^{m_{i+1}} \times \ldots \times (X-\lambda_r)^{m_r}}{(X-\lambda_1)^{m_1} \times \ldots \times (X-\lambda_{i-1})^{m_{i-1}} \times (X-\lambda_i)^{m_i} \times (X-\lambda_{i+1})^{m_{i+1}} \times \ldots \times (X-\lambda_r)^{m_r}} \\
&= \sum_{k=1}^{r} \frac{m_i}{X-\lambda_i}
\end{aligned}
$$

App. 7 Cherchons les solutions non nulles
Notons $n := \deg P$

$$
\begin{aligned}
P'|P &\iff \exists Q \in \mathbb{R}[X],\ P = P' \times Q \\
&\iff \exists Q \in \mathbb{R}_1[X],\ P = P' \times Q && \text{pour des raisons de degré} \\
&\iff \exists \lambda \in \mathbb{R},\ P = P' \times \frac{1}{n}(X-\lambda) && \text{pour des raisons de coefficient dominant} \iff \exists \lambda \in \mathbb{R}, \frac{P'}{P} = \frac{n}{X-\lambda} \\
&\iff \exists \lambda \in \mathbb{R}, P = \mu (X-\lambda)^n
\end{aligned}
$$