Mathématiques MPSI 2021–2022

Thomas MEGARBANE

Table des matières

Chapitre 1

Logique et raisonnements

I Assertions

Définition I.1. *On appelle* ***assertion*** *(ou* ***proposition****) une phrase qui est soit vraie soit fausse (et pas les deux).*
Une assertion peut dépendre d'une variable x, et on la note alors $A(x)$.
On dit que deux assertions A et B sont ***équivalentes****, ce que l'on note $A \equiv B$, si elles ont toujours la même valeur de vérité.*

Exemples I.2.
- *"2 est plus petit que 3" est une assertion vraie ;*
- *"5 est plus grand que 3" est une assertion fausse ;*
- *l'assertion $A(x)$ ="x est un nombre premier" dépend de x : elle est vraie si $x = 2$ et fausse si $x = 10$ par exemple.*

Définition I.3. *Si A et B sont deux assertions, on définit les assertions suivantes :*

1. *(non A) : qui est vraie si A est fausse, et fausse sinon, qu'on appelle la* ***négation****, notée $\neg A$;*
2. *(A ou B) : qui est vraie si l'une des deux assertions est vraie, et fausse sinon, qu'on appelle la* ***disjonction****, notée $A \vee B$;*
3. *(A et B) : qui est vraie si les deux assertions sont vraies, et fausse sinon, qu'on appelle la* ***conjonction****, notée $A \wedge B$.*

Exemples I.4. *Si A ="n est un multiple de 2" et B ="n est un multiple de 3", alors :*

1. *(non A)="n est impair"*
2. *(A ou B)="n est divisible soit par 2, soit par 3"*
3. *(A et B)="n est un multiple de 6" (par théorème de Gauss)*

Définition I.5. *On appelle* ***table de vérité*** *d'une assertion le tableau donnant sa valeur de vérité en fonction de celles des assertions utilisées pour la construire.*

Exemples I.6. *La négation, la disjonction et la conjonction ont pour tables de vérité :*

A	non A
V	F
F	V

A	B	A ou B
V	V	V
V	F	V
F	V	V
F	F	F

A	B	A et B
V	V	V
V	F	F
F	V	F
F	F	F

Propriété I.7. *Si A, B, C sont des assertions, on a les propriétés suivantes :*

1. $non\,(non\ A) \equiv A$;
2. $(A\ et\ B)\ et\ C \equiv A\ et\ (B\ et\ C)$;
3. $(A\ ou\ B)\ ou\ C \equiv A\ ou\ (B\ ou\ C)$;
4. $A\ et\ (B\ ou\ C) \equiv (A\ et\ B)\ ou\ (A\ et\ C)$;
5. $A\ ou\ (B\ et\ C) \equiv (A\ ou\ B)\ et\ (A\ ou\ C)$;
6. $non\,(A\ et\ B) \equiv [(non\ A)\ \ ou\ \ (non\ B)]$;
7. $non\,(A\ ou\ B) \equiv [(non\ A)\ \ et\ \ (non\ B)]$.

Démonstration. Par exemple, montrons la dernière. On procède par table de vérité :

A	B	A ou B	non(A ou B)	non A	non B	(non A) et (non B)
V	V	V	F	F	F	F
V	F	V	F	F	V	F
F	V	V	F	V	F	F
F	F	F	V	V	V	V

□

II Quantificateurs

Définition II.1. *Soit $A(x)$ une assertion dépendant de x, qui décrit un ensemble E :*

1. *Si, lorsque x décrit E, $A(x)$ est toujours vraie, on écrit :*

$$\forall x \in E,\ A(x)$$

qu'on lit "quel que soit x appartenant à E, $A(x)$". C'est le ***quantificateur universel****.*

2. *S'il existe x dans E tel que $A(x)$ est vraie, on écrit :*

$$\exists x \in E,\ A(x)$$

qu'on lit "il existe x appartenant à E tel que $A(x)$". C'est le ***quantificateur existentiel****.*

Propriété II.2. *Avec les mêmes notations, on a :*

1. $non\,(\forall x \in E,\ A(x)) \equiv \exists x \in E,\ (non\ A(x))$;
2. $non\,(\exists x \in E,\ A(x)) \equiv \forall x \in E,\ (non\ A(x))$;

Remarques II.3.

1. *S'il existe un unique x pour lequel $A(x)$ est vrai, on écrit : $\exists! x \in E,\ A(x)$.*
2. *L'ordre des quantificateurs est importante. Par exemple les assertions :*

$$[\forall x \in E,\ \exists y \in E,\ A(x,y)]\ \ et\ \ [\exists y \in E,\ \forall x \in E,\ A(x,y)]$$

ne sont pas les mêmes : dans la première, y dépend de x ; dans la seconde, y est indépendant de x.

Exemples II.4.

1. *L'assertion :*

$$\forall n \in \mathbb{N},\ \exists m \in \mathbb{N},\ n < m$$

veut dire que : pour tout entier naturel n, il existe un entier naturel m tel que $n < m$. Elle est vraie : pour n fixé, l'entier $m = n + 1$ convient.

2. *L'assertion :*

$$\exists m \in \mathbb{N},\ \forall n \in \mathbb{N},\ n < m$$

veut dire que : il existe un entier naturel m tel que, pour tout entier naturel m, $n < m$. Elle est fausse : si $n = m$ par exemple, on ne pourra avoir $n < m$.

III Implications, réciproques, contraposées et équivalences

Définition III.1. *Soient A, B sont deux assertions.*

1. *si, dès que A est vraie, alors B est aussi vraie : on dit que A **implique** B, que l'on note $A \Rightarrow B$ ou $B \Leftarrow A$ et que l'on lit "si A alors B"; on dit alors que : A est une condition **suffisante** pour B, ou que B est une condition **nécessaire** pour A.*
2. *si A implique B et que B implique A : on dit que A est **équivalent** à B, que l'on note $A \Leftrightarrow B$ ou $B \Leftrightarrow A$ et que l'on lit "A si et seulement si B"; on dit alors que : A est une condition **nécessaire et suffisante** pour B.*

Les tables de vérités correspondantes sont :

A	B	$A \Rightarrow B$
V	V	V
V	F	F
F	V	V
F	F	V

A	B	$A \Leftrightarrow B$
V	V	V
V	F	F
F	V	F
F	F	V

Exemples III.2.
1. *si n est un entier, alors "n est un multiple de 6" est une condition suffisante, mais non nécessaire, pour que n soit pair.*
2. *si x est un réel, alors "$x^2 = 1$" est une condition nécessaire, mais non suffisante, pour que x soit égal à 1 ;*
3. *si x est un réel, les assertions "$x^3 = -1$" et "$x = -1$" sont équivalentes.*

Proposition III.3. *Si A, B sont deux assertions, alors :*

1. $(A \Rightarrow B) \equiv [(non\ A)\ \ ou\ B]$;
2. $[non\ \ (A \Rightarrow B)] \equiv [A\ et\ \ (non\ B)]$;
3. $(A \Leftrightarrow B) \equiv (A\ et\ B)\ ou\ ((non\ A)\ et\ (non\ B))$;
4. $non\ (A \Leftrightarrow B) \equiv (A\ et\ (non\ B))\ ou\ ((non\ A)\ et\ B)$.

Démonstration. Par tables de vérité. □

Proposition-Définition III.4. *Si A et B sont deux assertions :*

1. *on appelle **réciproque** de l'implication $A \Rightarrow B$ l'implication $B \Rightarrow A$: il n'y a pas de lien de vérité entre une implication et sa réciproque ;*
2. *on appelle **contraposée** de l'implication $A \Rightarrow B$ l'implication $(non\ B) \Rightarrow (non\ A)$: une implication et sa contraposée ont même valeur de vérité, elles sont équivalentes.*

Démonstration.

A	B	$A \Rightarrow B$	$B \Rightarrow A$	non B	non A	(non B) $\Rightarrow$ (non A)
V	V	V	V	F	F	V
V	F	F	V	V	F	F
F	V	V	F	F	V	V
F	F	V	V	V	V	V

□

IV Méthodes de raisonnements

IV.1 Raisonnement par déduction

Propriété IV.1. *Pour montrer l'implication $A \Rightarrow B$, on peut supposer que A est vraie et montrer alors que B est vraie.*
Pour montrer l'équivalence $A \Leftrightarrow B$, on peut montrer séparément que les implications $A \Rightarrow B$ et $B \Rightarrow A$ sont vraies.
Pour prouver que A et B, on montre séparément que A et B sont vraies.
Pour prouver que A ou B, on peut supposer que A est fausse, et montrer alors que B est vraie.

Exemples IV.2.

1. *L'utilisation d'exemple repose sur l'implication :*

$$x \in E \text{ et } A(x) \Rightarrow \exists x \in E,\ A(x).$$

2. *Un contre-exemple repose sur l'implication :*

$$x \in E \text{ et non } A(x) \Rightarrow \text{non}\left(\forall x \in E,\ A(x)\right).$$

IV.2 Raisonnement par disjonction de cas

Propriété IV.3. *Lorsqu'une assertion $A(x)$ dépend d'une variable x qui prend des valeurs dans E ou dans F, pour montrer que $A(x)$ est vraie, on peut montrer que :*

1. *$A(x)$ est vraie pour x décrivant E ;*
2. *$A(x)$ est vraie pour x décrivant F.*

Remarque IV.4. *Les raisonnements par tables de vérités sont des raisonnements par disjonction de cas.*

Exemple IV.5. *Montrer que, pour tout entier naturel n, le nombre $\frac{n(n+1)}{2}$ est un entier.*

IV.3 Raisonnement par contraposition

Propriété IV.6. *Pour montrer l'implication $A \Rightarrow B$, on peut montrer sa contraposée $(\text{non } B) \Rightarrow (\text{non } A)$. On peut donc supposer que B est fausse, et montrer alors que A est fausse.*

Exemple IV.7. *Montrer que si n est un entier tel que n^2 est pair, alors n est pair.*

IV.4 Raisonnement par l'absurde

Propriété IV.8. *Pour montrer qu'une assertion est vraie, on peut montrer qu'elle n'est pas fausse. Pour cela, on suppose que l'assertion est fausse, et on cherche à aboutir à une contradiction, ou à une assertion dont on sait qu'elle est fausse.*

Remarque IV.9. *Beaucoup de raisonnements par l'absurde peuvent être remplacés par des raisonnements par contraposition (et inversement).*

Exemples IV.10. *Montrer que :*

1. *$\sqrt{2}$ est irrationnel ;*
2. *Montrer que si n est un entier tel que n^2 est pair, alors n est pair.*

IV.5 Raisonnement par analyse-synthèse

Propriété IV.11. *Pour montrer qu'un problème admet une unique solution, on peut procéder en deux temps :*

- *l'**analyse** : on montre qu'une hypothétique solution est nécessairement d'une certaine forme (ce qui réduit les solutions possibles) ;*
- *la **synthèse** : on regarde, parmi les solutions possibles de l'analyse, lesquelles sont bien des solutions.*

Exemple IV.12. *Résoudre dans $\mathbb{R}$ l'équation : $\sqrt{x+2} = x$.*

1. *analyse : on a les implications :*

$$\sqrt{x+2} = x \Rightarrow x+2 = x^2 \Rightarrow x^2 - x - 2 = 0$$

et on arrive donc à un trinôme du second degré que l'on sait résoudre. On a $\Delta = 1+8 = 9 = 3^2$, donc les solutions possibles sont $x_1 = \frac{1-3}{2} = -1$ et $x_2 = \frac{1+3}{2} = 2$.

2. *synthèse : $\sqrt{x_1+2} = 1 \neq -1 = x_1$ et $\sqrt{x_2+2} = 2 = x_2$, donc l'unique solution au problème est 2.*

Exemple IV.13. *Montrer que toute fonction réelle définie sur $\mathbb{R}$ s'écrit de manière unique comme somme d'une fonction paire et d'une fonction impaire.*
Soit $f : \mathbb{R} \to \mathbb{R}$.

1. *analyse : on suppose qu'il existe deux fonctions $g, h : \mathbb{R} \to \mathbb{R}$ telles que : g est paire, h est impaire et $f = g + h$. Si $x \in \mathbb{R}$, on a ainsi :*

$$\begin{cases} g(-x) = g(x) \\ h(-x) = -h(x) \\ f(x) = g(x) + h(x) \\ f(-x) = g(-x) + h(-x) \end{cases}$$

donc $g(x)$ et $h(x)$ sont solutions du système :

$$\begin{cases} g(x) & + & h(x) & = & f(x) \\ g(x) & - & h(x) & = & f(-x) \end{cases}$$

En prenant la somme et la différence des deux lignes du système, on trouve :

$$g(x) = \frac{f(x) + f(-x)}{2} \text{ et } h(x) = \frac{f(x) - f(-x)}{2}$$

*donc **nécessairement** g et h sont définies par les formules ci-dessus.*

2. *synthèse : considérons g, h définies par les formules ci-dessus. Alors, si $x \in \mathbb{R}$, on a :*
   - *$g(-x) = \frac{f(-x)+f(-(-x))}{2} = \frac{f(-x)+f(x)}{2} = g(x)$, donc g est paire ;*
   - *$h(-x) = \frac{f(-x)-f(-(-x))}{2} = \frac{f(-x)-f(x)}{2} = -h(x)$, donc h est impaire ;*
   - *$g(x) + h(x) = \frac{f(x)+f(-x)+f(x)-f(-x)}{2} = f(x)$, donc $f = g + h$.*

Ce qui montre bien l'existence et l'unicité d'une telle écriture.

IV.6 Raisonnement par récurrence

Théorème IV.14 (récurrence simple)**.** *Soit $A(n)$ une assertion dépendant de n décrivant $\mathbb{N}$. On suppose que :*

- *$A(0)$ est vraie ;*
- *pour tout $n \in \mathbb{N}$: $A(n) \Rightarrow A(n+1)$.*

Alors $A(n)$ est vraie pour tout $n \in \mathbb{N}$.

Théorème IV.15 (récurrence d'ordre k)**.** *Soit $A(n)$ une assertion dépendant de n décrivant $\mathbb{N}$, et $k \in \mathbb{N}^*$. On suppose que :*

— *$A(0), A(1), \ldots, A(k-1)$ sont vraies ;*

— *pour tout $n \in \mathbb{N}$: $(A(n-k+1)$ et $A(n-k+2)$ et $\ldots$ et $A(n)) \Rightarrow A(n+1)$.*

Alors $A(n)$ est vraie pour tout $n \in \mathbb{N}$.

Théorème IV.16 (récurrence forte)**.** *Soit $A(n)$ une assertion dépendant de n décrivant $\mathbb{N}$. On suppose que :*

— *$A(0)$ est vraie ;*

— *pour tout $n \in \mathbb{N}$: $(A(0)$ et $A(1)$ et $\ldots$ et $A(n)) \Rightarrow A(n+1)$.*

Alors $A(n)$ est vraie pour tout $n \in \mathbb{N}$.

Exemple IV.17. *Montrons par récurrence que pour tout $n \in \mathbb{N}$: $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.*

— *initialisation : si $n = 0$, on a :*

$$\frac{n(n+1)(2n+1)}{6} = 0 = \sum_{k=0}^{0} k^2.$$

— *hérédité : supposons que, pour un certain $n \in \mathbb{N}$, on ait $\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$. Alors :*

$$\begin{aligned}
\textstyle\sum_{k=0}^{n+1} k^2 &= \textstyle\sum_{k=0}^{n} k^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\
&= \frac{n(n+1)(2n+1)}{6} + \frac{6(n+1)^2}{6} = \frac{n+1}{6}[n(2n+1) + 6(n+1)] \\
&= \frac{n+1}{6}(2n^2+7n+6) = \frac{(n+1)(n+2)(2n+3)}{6} \\
&= \frac{(n+1)(n+1+1)(2(n+1)+1)}{6}
\end{aligned}$$

d'où la récurrence.

Exemple IV.18. *On montrera, avec un récurrence forte que tout entier naturel non nul s'écrit de manière unique comme produit de nombres premiers.*

Chapitre 2

Rappels et compléments de calculs

I Les ensembles de nombres usuels

Définition I.1. *On définit les ensembles de nombres suivants :*

1. $\mathbb{N} = \{0, 1, 2, \dots\}$ *l'ensemble des* ***entiers naturels*** *;*
2. $\mathbb{Z} = \mathbb{N} \cup -\mathbb{N} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ *l'ensemble des* ***entiers relatifs*** *;*
3. $\mathbb{Q} = \{\frac{p}{q} \,|\, p, q \in \mathbb{Z},\ q \neq 0\}$ *l'ensemble des* ***rationnels*** *;*
4. $\mathbb{R}$ *l'ensemble des abscisses d'une droite graduée, l'ensemble des* ***réels*** *;*
5. $\mathbb{C}$ *l'ensemble nombres de la forme* $a + ib$ *où* $a, b \in \mathbb{R}$ *et* $i^2 = -1$*, l'ensemble des* ***complexes***

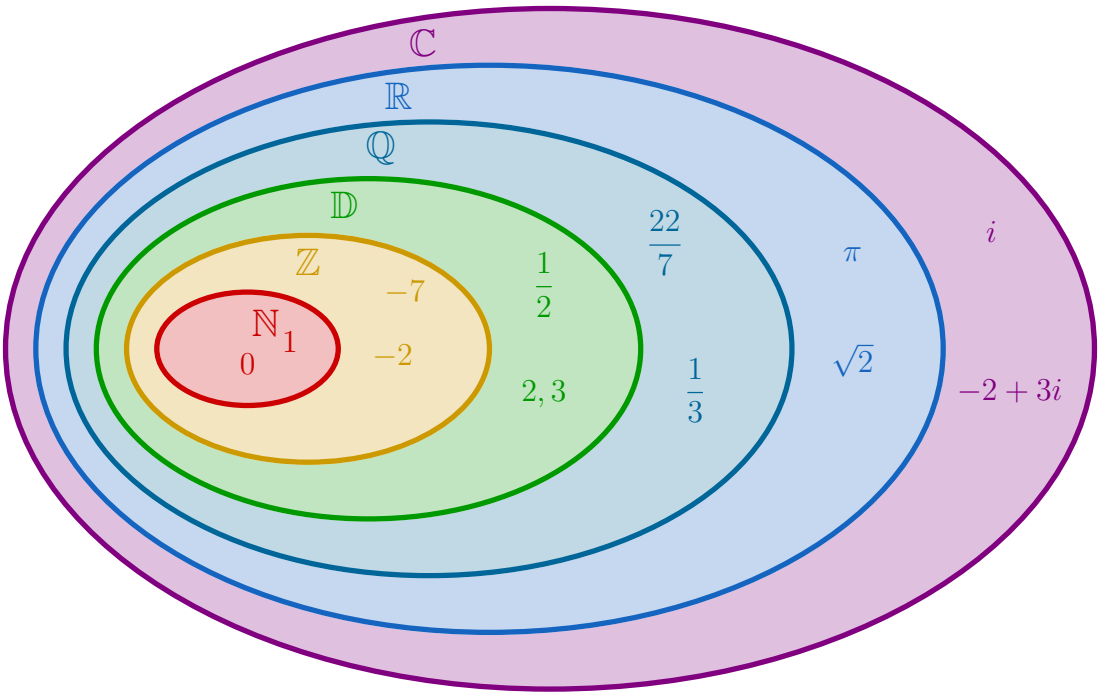
Et on note $\mathbb{N}^*, \mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ *les mêmes ensembles privés de* 0*.*
L'ensemble $\mathbb{R} \setminus \mathbb{Q}$ *est appelé l'ensemble des* ***irrationnels****.*

Remarque I.2. *On considère parfois aussi l'ensemble* $\mathbb{D}$ *des nombres* ***décimaux*** *:* $\mathbb{D} = \{\frac{n}{10^m} \,|\, n, m \in \mathbb{Z}\}$.

Proposition I.3. *On a les inclusions :*

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{D} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

et ces inclusions sont strictes.



II Intervalles et inégalités dans $\mathbb{R}$

Définition II.1. *Si $a, b \in \mathbb{R}$, on définit le* ***segment*** $[a; b]$ *comme :*

$$[a; b] = \{x \in \mathbb{R} \,|\, a \leq x \leq b\}.$$

On dit qu'un ensemble non vide I de $\mathbb{R}$ est un ***intervalle*** *s'il vérifie que :*

$$\forall a, b \in I,\ [a; b] \subset I.$$

Remarque II.2. *Cela revient à dire qu'un intervalle contient tous les réels entre ses éléments.*

Exemples II.3.

1. *si $a \in \mathbb{R}$, l'ensemble $I = \{a\}$ est un intervalle : il est non vide, et si $a, b \in I$, et $x \in [a; b]$, alors $a = b$ et ainsi : $a \leq x \leq a$, donc $x = a$ appartient bien à I ;*
2. *tout segment est un intervalle : si $I = [a; b]$ et $a', b' \in I$ alors :*

$$x \in [a'; b'] \Rightarrow a' \leq x \leq b' \Rightarrow a \leq a' \leq x \leq b' \leq b \Rightarrow a \leq x \leq b \Rightarrow x \in I.$$

3. *$\mathbb{N}$ n'est pas un intervalle car : $0 \in \mathbb{N}$ et $1 \in \mathbb{N}$ mais $\frac{1}{2} \in [0; 1]$ n'est pas dans $\mathbb{N}$, donc on n'a pas l'inclusion $[0; 1] \subset \mathbb{N}$.*

Proposition II.4. *Tout intervalle non vide de $\mathbb{R}$ est d'une (et une seule) des formes suivantes, où a, b désignent des réels tels que $a < b$:*

1. $\{a\}$;
2. $[a; b] = \{x \in \mathbb{R} \,|\, a \leq x \leq b\}$;
3. $[a; b[= \{x \in \mathbb{R} \,|\, a \leq x < b\}$;
4. $]a; b] = \{x \in \mathbb{R} \,|\, a < x \leq b\}$;
5. $]a; b[= \{x \in \mathbb{R} \,|\, a < x < b\}$;
6. $[a; +\infty[= \{x \in \mathbb{R} \,|\, a \leq x\}$;
7. $]a; +\infty[= \{x \in \mathbb{R} \,|\, a < x\}$;
8. $]-\infty; b] = \{x \in \mathbb{R} \,|\, x \leq b\}$;
9. $]-\infty; b[= \{x \in \mathbb{R} \,|\, x < b\}$;
10. $\mathbb{R}$.

Définition II.5. *Les intervalles précédents définis par des inégalités strictes sont appelés des* ***intervalles ouverts****.*
Plus généralement, si I est un intervalle, on appelle ***intérieur*** *de I, noté $\overset{\circ}{I}$, l'intervalle I privé de ses bornes.*

Remarque II.6. *Prendre l'intérieur, c'est "ouvrir" l'intervalle : $\overset{\circ}{I}$ est le pus grand intervalle ouvert inclus dans I.*

Proposition-Définition II.7. *Un ensemble non vide I de $\mathbb{R}$ est dit* ***convexe*** *si :*

$$\forall a, b \in I,\ \forall t \in [0; 1],\ ta + (1 - t)b \in I.$$

Les parties convexes de $\mathbb{R}$ sont exactement les intervalles.

Démonstration. Soit I un ensemble de $\mathbb{R}$

1. si I est un intervalle : soient $a, b \in I$ avec $a \leq b$, et $t \in [0;1]$; et posons $x = ta + (1-t)b$. Alors :

$$\begin{cases} x - a = (1-t)(b-a) \geq 0 \\ b - x = t(b-a) \geq 0 \end{cases}$$

donc $a \leq x \leq b$, donc $x \in I$ (comme I intervalle), donc I est convexe.
Si $a > b$, on se ramène au cas précédent en posant $t' = 1 - t \in [0;1]$, et alors $x = t'b + (1-t')a$ avec $b \leq a$.

2. si I est convexe : soient $a, b \in I$ et $x \in \mathbb{R}$ tel que $a \leq x \leq b$.
Si $a > b$: un tel x n'existe pas, donc il n'y a rien à dire.
Si $a = b$, alors $a = b = x$, donc $x \in I$.
Si $a < b$, posons $t = \dfrac{b-x}{b-a}$, de sorte que $1-t = \dfrac{x-a}{b-a}$. On a alors : $ta+(1-t)b = \dfrac{ab - ax + bx - ab}{b-a} = \dfrac{x(b-a)}{b-a} = x$. Mais $a \leq x \leq b$, donc $0 \leq x - a \leq b - a$ et ainsi : $0 \leq \dfrac{x-a}{b-a} = (1-t) \leq 1$. Et ainsi $(1-t)$ (et donc t) sont dans $[0;1]$. Par convexité de I, on a donc $x = ta + (1-t)b \in I$. Donc I est un intervalle.

□

III Racines et puissances

Définition III.1. *Si $x \geq 0$, on appelle sa **racine carrée**, notée $\sqrt{x}$, comme l'unique réel positif ou nul dont le carré vaut x.*

Remarque III.2. *Comme $x^2 = (-x)^2$, alors* $\sqrt{x^2} = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x \leq 0 \end{cases}$.

Proposition III.3. *Soient x, y positifs. Alors :*

$$\sqrt{xy} = \sqrt{x}\sqrt{y} \text{ et } \sqrt{\frac{x}{y}} = \frac{\sqrt{x}}{\sqrt{y}} \text{ (si } y \neq 0\text{).}$$

Démonstration. Par définition, on a $\sqrt{x}, \sqrt{y}$ sont positifs, donc leur produit aussi. Et :

$$\left(\sqrt{x}\sqrt{y}\right)^2 = (\sqrt{x})^2(\sqrt{y})^2 = xy$$

d'où la première égalité. On procède de même pour le quotient. □

Remarques III.4.

1. *on utilise les carrés parfaits pour simplifier les racines :* $1, 4, 9, 16, 25, 36, \ldots, 289, 324, 361, \ldots$;
2. *on évite de garder des racines au dénominateur dans un quotient. On simplifie une fraction en multipliant par $\sqrt{a}$, $\sqrt{a} - \sqrt{b}$ ou $\sqrt{a} + \sqrt{b}$ pour les faire disparaître.*

Exemples III.5.

1. $\sqrt{180} = \sqrt{36 \times 5} = 6\sqrt{5}$;
2. $\sqrt{\dfrac{3}{5}} = \dfrac{\sqrt{15}}{5}$;
3. $\dfrac{1}{\sqrt{11} - \sqrt{3}} = \dfrac{\sqrt{11} + \sqrt{3}}{8}$.

Définition III.6. *Si $x \in \mathbb{R}$ et $n \in \mathbb{N}$, on note :*

$$x^n = \begin{cases} 1 & si\ n = 0 \\ \underbrace{x \cdot \cdots \cdot x}_{n\ fois} & si\ n > 0 \end{cases}.$$

Si $x \neq 0$ et $n \in \mathbb{Z}_-$, on note :

$$x^n = \left(\frac{1}{x}\right)^{-n} = \frac{1}{\underbrace{x \cdot \cdots \cdot x}_{n\ fois}}.$$

Proposition III.7. *Si $x, y \in \mathbb{R}$ et $n, m \in \mathbb{N}$:*

$$x^{m+n} = x^m \cdot x^n,\ x^{mn} = (x^m)^n = (x^n)^m,\ (xy)^n = x^n y^n$$

et ces formules restent valables pour $n, m \in \mathbb{Z}$ si $x, y \neq 0$.

IV Manipuler des égalités et des inégalités

Proposition IV.1. *Si $a, b \in \mathbb{R}$, alors :*

1. *si $c \neq 0$: $a = b$ si, et seulement si, $ac = bc$;*
2. *si $a = b$, alors $a^2 = b^2$;*
3. *$ab = 0$ si, et seulement si, $a = 0$ ou $b = 0$;*
4. *pour tout fonction f définie en a et b : si $a = b$, alors $f(a) = f(b)$.*

Remarque IV.2. *La dernière proposition n'est en général pas une équivalence. Par exemple, pour une fonction constante, l'égalité $f(a) = f(b)$ est vérifiée peu importe la valeur de a et b.*
De manière moins extrême, on verra que : $\cos(a) = \cos(b) \Leftrightarrow a = \pm b + 2k\pi,\ k \in \mathbb{Z}$.
On a une équivalence si tout élément possède au plus un antécédent par f, comme dans l'exemple qui suit.

Exemple IV.3. *Soit $a, b \in \mathbb{R}$. Montrons que $a = b \Leftrightarrow e^a = e^b$:*
— *si $a = b$: alors en appliquant la fonction $\exp$: $e^a = e^b$;*
— *si $e^a = e^b$: alors en appliquant la fonction $\ln$: $\ln(e^a) = \ln(e^b)$, c'est-à-dire $a = b$.*
Ce qui montre l'équivalence voulue.

Proposition IV.4. *La relation $\leq$ est compatible avec l'addition et la multiplication de la manière suivante :*

1. *si $a, b, c, d \in \mathbb{R}$: $(a \leq b$ et $c \leq d) \Rightarrow a + b \leq c + d$;*
2. *si $a, b, c \in \mathbb{R}$ avec $c \geq 0$: $a \leq b \Rightarrow ac \leq bc$;*
3. *si $a, b, c \in \mathbb{R}$ avec $c \leq 0$: $a \leq b \Rightarrow bc \leq ac$;*
4. *si $a, b, c, d \in \mathbb{R}$: $(0 < a \leq b$ et $0 < c \leq d) \Rightarrow 0 < ac \leq bd$.*

Remarque IV.5. *On ne divise ni ne soustrait des inégalités. On se ramène à des additions ou des multiplications en utilisant :*
— *si $a, b \in \mathbb{R}$: $a \leq b \Leftrightarrow -b \leq -a$;*
— *si $a, b \in \mathbb{R}^*$ sont de même signe : $a \leq b \Leftrightarrow \dfrac{1}{b} \leq \dfrac{1}{a}$.*

Exemple IV.6. *Supposons que $a \in [1; 4]$ et $b \in [1/2; 3]$. Alors :*

1. *$-3 \leq -b \leq -1/2$ donc : $-2 \leq a - b \leq \frac{7}{2}$;*
2. *$\frac{1}{3} \leq \frac{1}{b} \leq 2$ donc : $\frac{1}{3} \leq \frac{a}{b} \leq 8$.*

Proposition IV.7. *Si $a, b \in \mathbb{R}$, alors :*
- *$ab > 0$ si, et seulement si, a et b sont non nuls de même signe ;*
- *si $ab < 0$ si, et seulement si, a et b sont non nuls de signes opposés.*

Démonstration. Par disjonction de cas. □

Proposition IV.8. *Si $a_1, \dots, a_n$ sont des réels de même signe, alors :*

$$a_1 + \cdots + a_n = 0 \Leftrightarrow a_1 = \cdots = a_n.$$

Démonstration. On montre séparément les deux implications :
- $\Leftarrow$ si $a_1 = \cdots = a_n = 0$, alors on a bien $a_1 + \cdots + a_n = 0$;
- $\Rightarrow$ Quitte à tout multiplier par -1 on peut supposer que les a_i sont positifs ou nuls.
  Raisonnons par contraposée : on suppose que l'un des a_i est non nul, c'est-à-dire qu'il existe $i_0 \in [\![1; n]\!]$ tel que $a_{i_0} > 0$.
  Mais comme tous les a_i sont positifs ou nuls, alors :

$$a_1 + a_2 + \cdots + a_n \geq a_{i_0} > 0$$

  donc $a_1 + \cdots + a_n \neq 0$.

□

V La valeur absolue

Définition V.1. *Si $x \in \mathbb{R}$, on appelle **valeur absolue** de x, notée $|x|$ le réel :*

$$|x| = \begin{cases} x & si\ x \geq 0 \\ -x & si\ x < 0 \end{cases}$$

Remarques V.2.
1. *Une valeur absolue est toujours positive ou nulle.*
2. *Si $x \in \mathbb{R}$: $-|x| \leq x \leq |x|$, et l'une des deux inégalités est une égalité.*

Proposition V.3. *Si $x, y \in \mathbb{R}$:*
1. $|x| = \sqrt{x^2}$;
2. $|x| = 0 \Leftrightarrow x = 0$;
3. $|xy| = |x| \times |y|$ *et* $\left|\dfrac{x}{y}\right| = \dfrac{|x|}{|y|}$ *(pour $y \neq 0$) ;*
4. $|x| = |y| \Leftrightarrow x^2 = y^2 \Leftrightarrow (x = y$ *ou* $x = -y)$;
5. $|x| \leq y \Leftrightarrow -y \leq x \leq y$ *et* $|x| \geq y \Leftrightarrow x \geq y$ *ou* $x \leq -y$.

Démonstration.
1. déjà vu avec les racines ;
2. clair ;
3. découle du *1.* ;
4. par le *1.*, on a déjà : $|x| = |y| \Leftrightarrow \sqrt{x^2} = \sqrt{y^2}$:
   — si $\sqrt{x^2} = \sqrt{y^2}$: en élevant au carré, on a : $x^2 = y^2$;
   — si $x^2 = y^2$: en prenant la racine carrée, on a : $\sqrt{x^2} = \sqrt{y^2}$.
   ce qui donne déjà que $|x| = |y| \Leftrightarrow x^2 = y^2$. Et on utilise enfin que :

$$x^2 = y^2 \Leftrightarrow x^2 - y^2 = 0 \Leftrightarrow (x - y)(x + y) = 0 \Leftrightarrow \begin{cases} x = y \\ \text{ou } x = -y \end{cases}.$$

5. On procède par disjonction de cas :
   — si $x \geq 0$: alors $|x| = x$ et donc :

$$|x \leq y \Leftrightarrow 0 \leq x \leq y \Leftrightarrow -y \leq 0 \leq x \leq y \Leftrightarrow -y \leq x \leq y.$$

   — si $x \leq 0$: alors $|x| = -x$ et donc :

$$|x| \leq y \Leftrightarrow 0 \leq -x \leq y \Leftrightarrow -y \leq x \leq 0 \Leftrightarrow -y \leq x \leq y.$$

□

Remarques V.4.

1. *si $y < 0$, alors les équivalences sont triviales (dans le sens où elles sont non seulement évidentes, mais qu'en plus elles n'apportent rien comme information) :*
   — *l'inégalité $|x| \leq y$ sera toujours fausse, de même que l'inégalité $-y \leq x \leq y$ (car elle impliquerait que $-y \leq y$, qui est évidemment fausse) ;*
   — *l'inégalité $|x| \geq y$ sera toujours vraie, comme le fait que $x \geq y$ ou que $x \leq -y$. On a en effet :*

$$\begin{cases} x \geq y & \Leftrightarrow & x \in [y; +\infty[\\ x \leq -y & \Leftrightarrow & x \in]-\infty; -y] \end{cases}$$

   et l'union de ces deux intervalles forme bien toute la droite des réels.
2. *Si $y \geq 0$, on a même : $|x| \leq y \Leftrightarrow x^2 \leq y^2$ et $|x| \leq y \Leftrightarrow x^2 \leq y^2$.*

Corollaire V.5. *Si $a, b \in \mathbb{R}$ avec $b > 0$, l'ensemble des réels x tels que $|x-a| \leq b$ est le segment $[a-b; a+b]$.*

Définition V.6. *Si $x, y \in \mathbb{R}$, la quantité $|x - y|$ est appelée **distance** entre x et y.*

Remarque V.7. *L'intervalle $[a - b; a + b]$ correspond à l'ensemble des réels à distance au plus b de a.*

Théorème V.8 (Inégalité triangulaire)**.** *Si $x, y \in \mathbb{R}$, alors :*

1. $|x + y| \leq |x| + |y|$;
2. $||x| - |y|| \leq |x - y|$.

De plus, il y a égalité dans les deux cas si, et seulement si, x et y sont de même signe.

Démonstration. 1. On utilise que $-|x| \leq x \leq |x|$ et $-|y| \leq y \leq |y|$.
Donc : $-(|x| + |y|) \leq x + y \leq |x| + |y|$.
D'où : $|x + y| \leq |x| + |y|$.

2. On utilise l'inégalité précédente :

$$|x| = |(x - y) + y| \leq |x - y| + |y|$$

donc $|x| - |y| \leq |x - y|$.
En échangeant les rôles de x et y, on trouve : $|y| - |x| \leq |y - x| = |x - y|$.
Donc : $-|x - y| \leq |x| - |y| \leq |x - y|$.
Et ainsi : $||x| - |y|| \leq |x + y|$.

Pour les égalités, on a :

$$|x + y| = |x| + |y| \Leftrightarrow (x + y)^2 = (|x| + |y|)^2 \Leftrightarrow xy = |x| \times |y| = |xy| \Leftrightarrow xy \geq 0.$$

$$||x| - |y|| = |x - y| \Leftrightarrow (|x| - |y|)^2 \leq (x - y)^2 \Leftrightarrow |xy| = xy \Leftrightarrow xy \geq 0$$

Dans un cas comme dans l'autre, on a égalité si, et seulement si, $xy \geq 0$, c'est-à-dire si, et seulement si, x et y sont de même signe. □

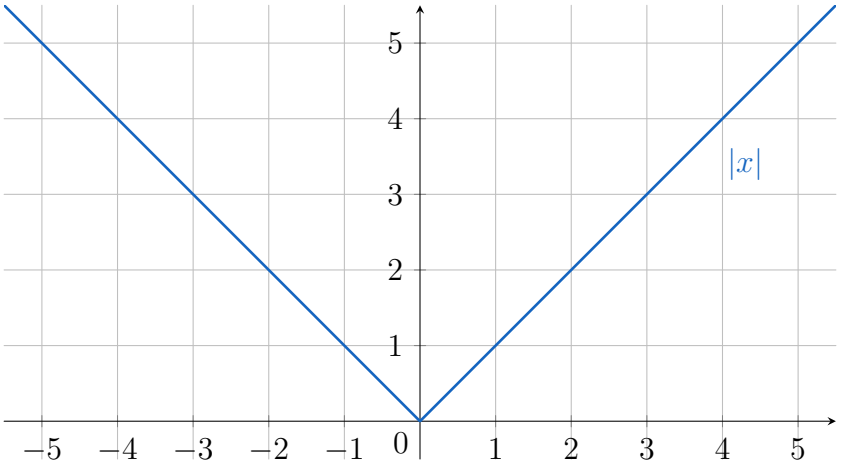
Corollaire V.9. *Si $x_1, \dots, x_n$ sont des réels, alors :*

$$\left|\sum_{k=1}^{n} x_k\right| = |x_1 + x_2 + \cdots + x_n| \leq |x_1| + |x_2| + \cdots + |x_n| = \sum_{k=1}^{n} |x_k|$$

avec égalité si, et seulement si, tous les x_i sont de même signe.

Démonstration. Par récurrence. □

Proposition V.10. *La fonction $x \mapsto |x|$ a pour courbe représentative :*



VI La partie entière

Théorème-Définition VI.1. *Si $x \in \mathbb{R}$, il existe un unique $n \in \mathbb{Z}$ tel que $n \leq x < n+1$.*
*L'entier n est appelé la **partie entière** de x, et est notée $\lfloor x \rfloor$.*

Démonstration. Voir dans un autre chapitre. □

Proposition VI.2. *Si $x \in \mathbb{R}$ et $n \in \mathbb{Z}$, alors $n = \lfloor x \rfloor$ si, et seulement si : $x - 1 < n \leq x$.*

Démonstration. Découle de la définition, en notant que : $x - 1 < n \Leftrightarrow x < n + 1$. □

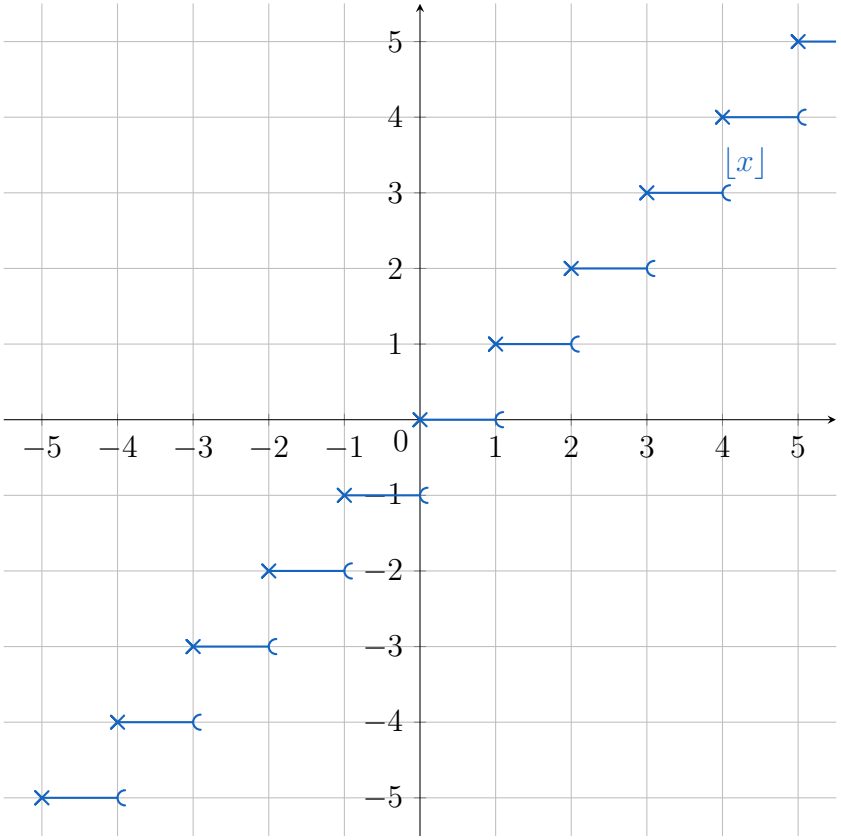
Remarque VI.3. *La partie entière se lit bien sur les décimales **pour les nombres positifs** : $\lfloor 1,32 \rfloor = 1$ mais $\lfloor -1,32 \rfloor = -2$.*

Exemple VI.4. *Si $n \in \mathbb{N}^*$ avec $n \geq 2$, alors : $\left(n + \frac{1}{n}\right)^2 = n^2 + 2 + \frac{1}{n^2}$.*
Donc : $n^2 + 2 \leq \left(n + \frac{1}{n}\right)^2 < n^2 + 3$.
Et ainsi : $\left\lfloor \left(n + \frac{1}{n}\right)^2 \right\rfloor = n^2 + 2$.

Proposition VI.5. *Si $x \in \mathbb{R}$ et $n \in \mathbb{N}$, alors : $\lfloor x + n \rfloor = n + \lfloor x \rfloor$.*

Démonstration. Par définition de $\lfloor x \rfloor$, on a : $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.
Donc, en rajoutant n : $\lfloor x \rfloor + n \leq x + n < \lfloor x \rfloor + n + 1$.
Et, comme $\lfloor x \rfloor + n$ est un entier, on a bien le résultat voulu. □

Proposition VI.6. *La fonction $x \mapsto |x|$ a pour courbe représentative :*



VII Techniques de résolutions d'équations et d'inéquations

Exemple VII.1. *Résolution de l'équation* $x = \sqrt{x+1}$.
À cause de la racine, on cherche les solution dans $[-1;+\infty[$. *Mais, comme on doit avoir* $x = \sqrt{x+1}$, *alors* x *aussi doit être positif. On cherche donc les solutions dans* $[0;+\infty[= \mathbb{R}_+$.
Pour $x \in \mathbb{R}_+$, *on a l'équivalence :*

$$x = \sqrt{x+1} \Leftrightarrow x^2 = \sqrt{x+1}^2 = x+1$$

donc on souhaite résoudre dans $\mathbb{R}_+$ *l'équation* $x^2 - x - 1 = 0$.
On a une équation du second degré de discriminant $\Delta = 1 - 4 \cdot (-1) \cdot 1 = 5$. *Donc les racines sont* $x_1 = \dfrac{1+\sqrt{5}}{2}$ *et* $x_2 = \dfrac{1-\sqrt{5}}{2}$.
On a bien que $x_1 \geq 0$, *mais* $x_2 < 0$ *n'est pas solution : donc l'équation admet pour unique solution* $x_1 = \dfrac{1+\sqrt{5}}{2}$.

Exemple VII.2. *Résolution de l'équation* $2x^2 + 2xy - 2x + y^2 + 1 = 0$.
On a : $y^2 + 2xy + x^2 = (y+x)^2$ *et* $x^2 - 2x + 1 = (x-1)^2$.
Donc l'équation est équivalente à : $(y+x)^2 + (x-1)^2 = 0$.
Comme un carré (de réel) est positif, on a donc :

$$(y+x)^2 + (x-1)^2 = 0 \Leftrightarrow \begin{cases} (y+x)^2 = 0 \\ (x-1)^2 = 0 \end{cases} \Leftrightarrow \begin{cases} x = 1 \\ y = -x = -1 \end{cases}$$

donc l'unique solution est $(x, y) = (1, -1)$.

Exemple VII.3. *Résolution de l'inéquation* $\sqrt{x-1} \leq \sqrt{2x^2 - 5}$.

On a l'équivalence :

$$\sqrt{x-1} \leq \sqrt{2x^2-5} \Leftrightarrow 0 \leq x-1 \leq 2x^2-5$$

On traite séparément les deux inéquations :

- $0 \leq x-1 \Leftrightarrow x \geq 1 \Leftrightarrow x \in [1;+\infty[= S_1$;
- $x-1 \leq 2x^2-5 \Leftrightarrow 0 \leq 2x^2-x-4$ *: on reconnaît un trinôme du second degré, de coefficient dominant positif, qui est donc positif à l'extérieur de ses racines.*

  Ses racines sont $x_1 = \dfrac{1+\sqrt{33}}{4}$ *et* $x_2 = \dfrac{1-\sqrt{33}}{4}$*. Donc la deuxième inéquation a pour ensemble solution* $S_2 =]-\infty; \frac{1-\sqrt{33}}{4}] \cup [\frac{1+\sqrt{33}}{4}; +\infty[$.

Comme $\frac{1-\sqrt{33}}{4} < 1$ *et que* $\frac{1+\sqrt{33}}{4} > 1$*, on déduit que l'équation admet pour ensemble solution :*

$$S_1 \cap S_2 = \left[\frac{1+\sqrt{33}}{4}; +\infty\right[.$$

Exemple VII.4. *Résolution de l'inéquation* $|x-1| \leq |2x-3|$.
Par propriétés des valeurs absolues, on a les équivalences :

$$|x-1| \leq |2x-3| \Leftrightarrow (x-1)^2 \leq (2x-3)^2 \Leftrightarrow 0 \leq (x-2)(3x-4) \Leftrightarrow 0 \leq 3(x-2)(x-4/3) \Leftrightarrow x \in]-\infty; \frac{4}{3}] \cup [2; +\infty[.$$

où, pour la dernière équivalence, on reconnaît à nouveau un trinôme du second degré, de coefficient dominant positif, dont les racines sont $\frac{4}{3}$ *et* 2.
Et donc l'ensemble solution est : $]-\infty; \dfrac{4}{3}] \cup [2; +\infty[$.

Autre méthode : on peut procéder par disjonction de cas pour éliminer les racines. On trouve alors les solutions selon les valeurs de x *:*

x	$]-\infty, 1]$	$[1, \frac{3}{2}]$	$[\frac{3}{2}, +\infty[$
$\lvert x-1\rvert$	$1-x$	$x-1$	$x-1$
$\lvert 2x-3\rvert$	$3-2x$	$3-2x$	$2x-3$
$\lvert x-1\rvert \leq \lvert 2x-3\rvert$	$1-x \leq 3-2x$ $\Leftrightarrow x \leq 2$	$x-1 \leq 3-2x$ $\Leftrightarrow x \leq \frac{4}{3}$	$x-1 \leq 2x-3$ $\Leftrightarrow x \geq 2$
S	$S_1 =]-\infty, 1]$	$S_2 = [1, \frac{4}{3}]$	$S_3 = [2, +\infty[$

Et on trouve finalement que : $S = S_1 \cup S_2 \cup S_3 =]-\infty; \dfrac{4}{3}] \cup [2; +\infty[$.

Exemple VII.5. *Résolution de l'équation* $\lfloor \frac{x^2}{3} - 2x + \frac{5}{3} \rfloor = -1$.
L'équation est équivalente à l'inéquation :

$$-1 \leq \frac{x^2}{3} - 2x + \frac{5}{3} < 0$$

dont on résout séparément les deux parties :

- *on procède par équivalences :*

$$\begin{array}{rcl} -1 \leq \frac{x^2}{3} - 2x + \frac{5}{3} & \Leftrightarrow & -3 \leq x^2 - 6x + 5 \\ & \Leftrightarrow & 0 \leq x^2 - 6x + 8 \end{array}$$

  On a donc un trinôme du second degré, de coefficient dominant positif, de discriminant $\Delta = 4 = 2^2$*, dont les racines sont :* $\dfrac{6-2}{2} = 2$ *et* $\dfrac{6+2}{2} = 4$*. Donc finalement la première inégalité est vérifiée pour* $x \in]-\infty; 2] \cup [4; +\infty[$.

— *on raisonne de la même manière :*

$$\tfrac{x^2}{3} - 2x + \tfrac{5}{3} < 0 \quad \Leftrightarrow \quad x^2 - 6x + 5 < 0$$

On a encore un trinôme du second degré, de coefficient dominant positif, de discriminant $\Delta = 16 = 4^2$*, dont les racines sont :* $\dfrac{6-4}{2} = 1$ *et* $\dfrac{6+4}{2} = 5$*. Donc finalement la seconde inégalité est vérifiée pour* $x \in]1;5[$.

Donc l'ensemble solution de l'équation est :

$$(]-\infty;2] \cup [4;+\infty[) \cap]1;5[=]1;2] \cup [4;5[.$$

Chapitre 3

Rappels et compléments sur les fonctions numériques

I Généralités sur les fonctions

I.1 Domaine de définition

Définition I.1. *Si $\mathcal{D}$ est une partie non vide de $\mathbb{R}$, **fonction numérique** f **définie sur** $\mathcal{D}$ est la donnée pour tout élément x d'un unique réel noté $f(x)$.*
*L'ensemble $\mathcal{D}$ est appelé **domaine de définition**.*
On notera alors : $f : \left\{ \begin{array}{ccc} \mathcal{D} & \to & \mathbb{R} \\ x & \mapsto & f(x) \end{array} \right.$.

Remarque I.2. *En général, une fonction sera donnée par une formule : auquel cas, son domaine de définition est là où la formule a bien un sens.*

Exemple I.3. *Considérons la fonction définie par $f(x) = \sqrt{4 - x^2}$.*
Alors la formule $f(x)$ n'a de sens que lorsque $4 - x^2 \geq 0$, c'est-à-dire que $\mathcal{D}_f = [-2; 2]$.

Définition I.4. *Si f est une fonction définie sur $\mathcal{D}$, et $A \subset \mathcal{D}$ un sous-ensemble de $\mathcal{D}$, on définit la **restriction de** f **à** A comme la fonction notée $f|_A$ définie sur A qui coïncide avec f :*

$$f|_A : \left\{ \begin{array}{ccc} A & \to & \mathbb{R} \\ x & \mapsto & f(x) \end{array} \right. .$$

*Inversement, on dit que f est un **prolongement** de $f|_A$.*

Exemple I.5. *La fonction $x \mapsto \sqrt{x^2}$ est la restriction de la fonction $x \mapsto x$ à $\mathbb{R}_+$.*

Définition I.6. *Si f est une fonction définie sur $\mathcal{D}$ et A est une partie de $\mathbb{R}$, on dit que f est **à valeurs dans** A si : pour tout $x \in \mathcal{D}$, $f(x) \in A$.*
On notera alors $f : \left\{ \begin{array}{ccc} \mathcal{D} & \to & A \\ x & \mapsto & f(x) \end{array} \right.$ *au lieu de* $f : \left\{ \begin{array}{ccc} \mathcal{D} & \to & \mathbb{R} \\ x & \mapsto & f(x) \end{array} \right.$.

Exemple I.7. *La fonction* sin *est à valeurs dans $[-1; 1]$. Sa restriction à $[0; \pi]$ est à valeurs dans $[0; 1]$.*

Définition I.8. *Soient f une fonction définie sur $\mathcal{D}$ et à valeurs dans A, et g une fonction définie sur A. On dit alors que g et f sont **composables**, et on définit la **composée de** g **et** f comme la fonction notée $g \circ f$, définie sur $\mathcal{D}$ par :*

$$g \circ f : \left\{ \begin{array}{ccc} \mathcal{D} & \to & \mathbb{R} \\ x & \mapsto & g\left(f(x)\right) \end{array} \right. .$$

Exemple I.9. *La fonction $f : x \mapsto x^2+1$ définie sur $\mathbb{R}$ est à valeurs dans $[1;+\infty[$. Donc elle est composable avec la fonction $g : x \mapsto \sqrt{x^2-1}$. Et on a :*

$$\forall x \in \mathbb{R},\ g \circ f(x) = \sqrt{(x^2+1)^2-1} = \sqrt{x^2(x^2+2)} = |x|\sqrt{x^2+2}.$$

Proposition I.10. *Si f, g sont deux fonctions définies sur un même ensemble $\mathcal{D}$, alors on peut définir les fonctions :*

1. ***somme*** *de f et g, notée $f+g$, définie par : $f+g : \left\{ \begin{array}{ccc} \mathcal{D} & \to & \mathbb{R} \\ x & \mapsto & f(x)+g(x) \end{array} \right.$;*
2. ***produit*** *de f et g, notée fg, définie par : $fg : \left\{ \begin{array}{ccc} \mathcal{D} & \to & \mathbb{R} \\ x & \mapsto & f(x) \times g(x) \end{array} \right.$.*

On définit de même, pour $\lambda \in \mathbb{R}$, la fonction λf.

Si g ne prend jamais de valeur nulle, on définit le ***quotient*** *de f et g, notée $\frac{f}{g}$, par : $\frac{f}{g} : \left\{ \begin{array}{ccc} \mathcal{D} & \to & \mathbb{R} \\ x & \mapsto & \frac{f(x)}{g(x)} \end{array} \right.$.*

I.2 Graphes, images et antécédents

Définition I.11. *Si f est une fonction définie sur $\mathcal{D}$, et $x \in \mathcal{D}$, $y \in \mathbb{R}$ tels que $f(x) = y$. On dit que :*

1. *y est* ***l'image*** *de x ;*
2. *x est* ***un antécédent*** *de y.*

Remarque I.12. *Une image est unique, tandis qu'un réel peut avoir aucun, un, plusieurs ou une infinité d'antécédents.*

Exemple I.13. *On considère la fonction* cos *définie sur $\mathbb{R}$. Alors :*

1. *l'image de $\frac{\pi}{2}$ est 0 ;*
2. *les antécédents de 0 sont les $\frac{\pi}{2} + k\pi$ pour $k \in \mathbb{Z}$;*
3. *tout y tel que $|y| > 1$ n'a pas d'antécédent.*

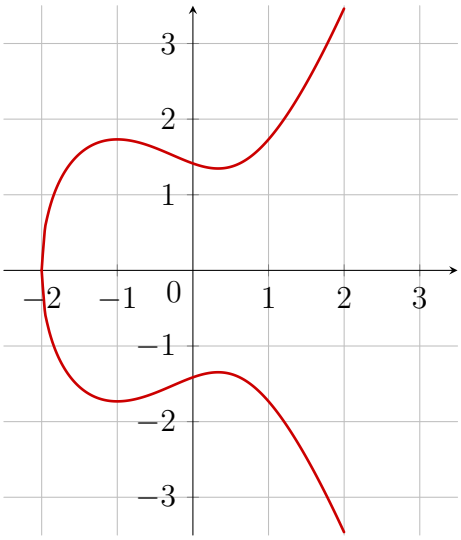
Définition I.14. *Si f est une fonction définie sur $\mathcal{D}$, son* ***graphe****, ou sa* ***représentation graphique****, est l'ensemble $\mathcal{C}_f$ défini par :*

$$\mathcal{C}_f = \{(x, f(x)) \,|\, x \in \mathcal{D}\}.$$

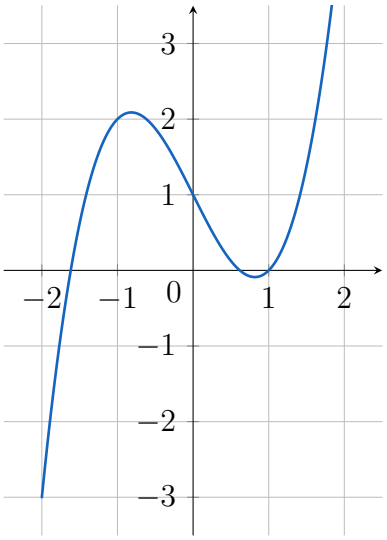
Remarque I.15. *Autrement dit, pour tout $x, y \in \mathbb{R}$, on a :*

$$(x, y) \in \mathcal{C}_f \Leftrightarrow x \in \mathcal{D} \text{ et } y = f(x)$$

donc, à abscisse donnée, il y a au plus un point sur le graphe.



Pas un graphe.



Un graphe.

I.3 Fonctions bornées

Définition I.16. *On dit qu'une fonction $f : \mathcal{D} \to \mathbb{R}$ est **majorée** par $M \in \mathbb{R}$ si :*

$$\forall x \in \mathcal{D},\ f(x) \leq M$$

*et on dit alors que M est un **majorant** de f.*
*On dit qu'elle est **minorée** par m si :*

$$\forall x \in \mathcal{D},\ f(x) \geq m$$

*et on dit alors que m est un **minorant** de f.*
On dit enfin que f est bornée si elle est majorée et minorée.

Définition I.17. *On dit qu'une fonction $f : \mathcal{D} \to \mathbb{R}$ possède un **maximum** (resp. **minimum**) en $x \in \mathcal{D}$ si $f(x)$ est un majorant (resp. un minorant) de f.*
*On dit plus généralement que f a un **extremum** en x si elle atteint son maximum ou son minimum en x.*

Exemples I.18.

1. *la fonction $x \mapsto x^2$ est minorée (elle admet même 0 pour minimum), mais n'est pas majorée ;*
2. *la fonction $x \mapsto e^x$ est minorée (par 0), mais non majorée ; et elle n'admet pas de minimum ;*
3. *la fonction $x \mapsto \sin(x)$ est bornée ; elle admet 1 comme maximum et -1 comme minimum, qui sont respectivement atteints en tous les $\frac{\pi}{2} + 2k\pi$ et $-\frac{\pi}{2} + 2k\pi$, pour $k \in \mathbb{Z}$.*

Remarque I.19. *Graphiquement, cela se voit : la courbe de f est limitée en ordonnée (vers le haut, vers le bas ou les deux).*

Proposition I.20. *La fonction $f : \mathcal{D} \to \mathbb{R}$ est bornée si, et seulement si, la fonction $|f| : \left\{ \begin{array}{ccc} \mathcal{D} & \to & \mathbb{R} \\ x & \mapsto & |f(x)| \end{array} \right.$ est majorée.*

Démonstration.
— si $|f|$ est majorée par M : alors pour tout $x \in \mathbb{R}$, on a : $|f(x)| \leq M$, et donc : $-M \leq f(x) \leq M$, donc f est bornée (minorée par $-M$ et majorée par M) ;
— réciproquement : si f est minorée par m et majorée par M, alors : $\forall x \in \mathcal{D},\ m \leq f(x) \leq M$. Et donc : $\left\{ \begin{array}{ccc} f(x) & \leq & M \\ -f(x) & \leq & -m \end{array} \right.$ donc $|f|$ est majorée par $\max(M, -m)$.

□

I.4 Monotonie

Définition I.21 (Fonction monotone)**.** *Si f est définie sur $\mathcal{D}$, on dit que f est :*

1. ***croissante** si pour tous $x, y \in \mathcal{D}$: $x \leq y \Rightarrow f(x) \leq f(y)$;*
2. ***strictement croissante** si pour tous $x, y \in \mathcal{D}$: $x < y \Rightarrow f(x) < f(y)$;*
3. ***décroissante** si pour tous $x, y \in \mathcal{D}$: $x \leq y \Rightarrow f(x) \geq f(y)$;*
4. ***strictement décroissante** si pour tous $x, y \in \mathcal{D}$: $x < y \Rightarrow f(x) > f(y)$;*
5. ***monotone** si elle est croissante ou décroissante ;*
6. ***strictement monotone** si elle est strictement croissante ou strictement décroissante.*

Exemples I.22.

1. *La fonction* exp *est croissante sur $\mathbb{R}$.*

2. *La fonction* $x \mapsto \dfrac{1}{x}$ *est décroissante sur* $\mathbb{R}_-^*$ *et sur* $\mathbb{R}_+^*$ *: elle n'est en revanche pas décroissante sur* $\mathbb{R}^*$ *car :*
$$-1 < 1 \text{ et } \frac{1}{-1} = -1 \leq 1 = \frac{1}{1}.$$
3. *La fonction* $x \mapsto x^2$ *est :*
   — *strictement décroissante sur* $\mathbb{R}_-$ *car :*
   $$x < y \leq 0 \Rightarrow 0 \leq -y < -x \Rightarrow 0 \leq y^2 < x^2$$
   — *strictement croissante sur* $\mathbb{R}_+$ *car :*
   $$0 \leq x < y \Rightarrow 0 \leq x^2 < y^2$$
   où dans chaque cas on a multiplié par elle-même une inégalité dont tous les termes étaient positifs (ce qui est parfaitement licite).

Proposition I.23. *Si* f *a pour graphe* $\mathcal{C}_f$*, alors :*

1. f *est croissante si, et seulement si,* $\mathcal{C}_f$ *"monte" quand on va vers la droite ;*
2. f *est décroissante si, et seulement si,* $\mathcal{C}_f$ *"descend" quand on va vers la droite.*

Remarque I.24. *La monotonie se comporte assez mal avec la somme, mais très mal avec les produits.*

Proposition I.25. *Si* f *et* g *sont deux fonctions composables monotones, alors* $g \circ f$ *est aussi monotone, et elle est :*

1. *croissante si* f *et* g *ont même monotonie ;*
2. *décroissante si* f *et* g *sinon.*

De plus, si f *et* g *sont strictement monotones, alors* $g \circ f$ *aussi.*

Remarque I.26. *Dans le cas de stricte monotonie, on a bien besoin de la stricte monotonie de* f *et de* g*. Par exemple, si* f *ou* g *est constante, alors* $f \circ g$ *est constante donc ne peut pas être strictement monotone.*

Démonstration.
Soient $x, y \in \mathcal{D}$ avec $x \leq y$:
— si f est croissante : alors : $f(x) \leq f(y)$ et donc :
  — si g est croissante : $g(f(x)) \leq g(f(y))$ donc $g \circ f$ est croissante ;
  — si g est décroissante : $g(f(x)) \geq g(f(y))$ donc $g \circ f$ est décroissante ;
— si f est décroissante : alors : $f(x) \geq f(y)$ et donc :
  — si g est croissante : $g(f(x)) \geq g(f(y))$ donc $g \circ f$ est décroissante ;
  — si g est décroissante : $g(f(x)) \leq g(f(y))$ donc $g \circ f$ est croissante ;

Ce qui montre bien les cas de monotonie.
La stricte monotonie de montre de la même manière, en considérant partout des inégalités strictes. □

I.5 Bijections

Définition I.27. *Si* I *et* J *sont deux parties de* $\mathbb{R}$*, on dit qu'une fonction* $f : I \to J$ *réalise* ***une bijection de*** I ***sur*** J *si tout élément de* J *admet* ***un unique antécédent*** *par* f *dans* I*.*
On note alors f^{-1} *la fonction définie sur* J *qui à tout* $y \in J$ *associe son unique antécédent par* f*.*
La fonction f^{-1} *est appelée* ***bijection réciproque*** *de* f*.*

Exemple I.28.

1. *La fonction $x \mapsto e^x$ réalise une bijection de $\mathbb{R}$ sur $\mathbb{R}_+^*$: sa réciproque est la fonction :*
$$\ln : \left\{ \begin{array}{ccc} \mathbb{R}_+^* & \to & \mathbb{R} \\ x & \mapsto & \ln(x) \end{array} \right. .$$
2. *La fonction* $\left\{ \begin{array}{ccc} \mathbb{R}_+ & \to & \mathbb{R}_+ \\ x & \mapsto & x^2 \end{array} \right.$ *est bijective, et sa bijection réciproque est la fonction racine carrée.*
3. *Soit* $f : \left\{ \begin{array}{ccc} \mathbb{R} \setminus \{2\} & \to & \mathbb{R} \\ x & \mapsto & \frac{x+1}{x-2} \end{array} \right.$.
Soit $y \in \mathbb{R}$. Déterminons les antécédents de y :
$$\begin{array}{rcl} y = f(x) & \Leftrightarrow & y = \dfrac{x+1}{x-2} \\ & \Leftrightarrow & (x-2)y = x+1 \\ & \Leftrightarrow & x(y-1) = 2y+1 \end{array}$$
et donc :
— *si $y = 1$: y n'a pas d'antécédent ;*
— *si $y \neq 1$: y a pour unique antécédent $x = \frac{2y+1}{y-1}$.*
Donc f n'est pas bijective de $\mathbb{R} \setminus \{2\}$ sur $\mathbb{R}$. Mais elle l'est de $\mathbb{R} \setminus \{2\}$ sur $\mathbb{R} \setminus \{1\}$, et sa bijection réciproque est :
$$f^{-1} : \left\{ \begin{array}{ccc} \mathbb{R} \setminus \{1\} & \to & \mathbb{R} \setminus \{2\} \\ y & \mapsto & \frac{2y+1}{y-1} \end{array} \right.$$

Définition I.29. *Si I est une partie de $\mathbb{R}$, on définit la* ***fonction identité sur*** *I, notée* id_I*, la fonction définie sur I par : $\forall x \in I,\ \mathrm{id}_I(x) = x$.*

Proposition I.30. *Si $f : I \to J$ est bijective, alors :*
1. *$f \circ f^{-1} = \mathrm{id}_J$;*
2. *$f^{-1} \circ f = \mathrm{id}_I$;*
3. *f^{-1} réalise une bijection de J sur I, avec $(f^{-1})^{-1} = f$.*

Démonstration.
1. si $y \in J$, comme $f^{-1}(y)$ est un antécédent de y par f (c'est même le seul), alors $f(f^{-1})(y) = y$;
2. si $x \in I$, alors $f(x)$ est l'image de x par f, donc x est l'unique antécédent de $f(x)$; mais $f^{-1}(f(x))$ aussi, donc $x = f^{-1}(f(x))$;
3. soit $x \in I$ et $y \in J$ un antécédent de x par f^{-1} : alors $f^{-1}(y) = x$. Et donc, en composant par f : $f(x) = y$, donc nécessairement $y = f(x)$, ce qui assure l'unicité d'un antécédent.
Mais $f^{-1}(f(x)) = x$, donc $f(x)$ est bien un antécédent de x, ce qui assure l'existence.
Donc f^{-1} est bien bijective, et comme $f(x)$ est l'unique antécédent de x par f^{-1}, alors $(f^{-1})^{-1} = f$.

□

Proposition I.31. *Si f est strictement monotone sur I, alors f réalise une bijection de I sur $J = f(I) = \{f(x) \,|\, x \in I\}$.*
De plus, sa réciproque f^{-1} a même monotonie que f.

Démonstration. Supposons par exemple que f est strictement croissante.
Soit $y \in J$: alors il existe $x \in I$ tel que $f(x) = y$ par définition de J, donc y a un antécédent.
Soient x_1, x_2 sont deux antécédents de y. Si $x_1 < x_2$, alors $y = f(x_1) < f(x_2) = y$ par monotonie, ce qui est impossible. Donc $x_1 = x_2$
Donc y a un unique antécédent, et f est bijective.

Soient $y_1, y_2 \in J$ tels que $y_1 < y_2$. Notons $y_1 = f(x_1)$ et $y_2 = f(x_2)$ pour $x_1, x_2 \in I$. Nécessairement on a : $x_1 < x_2$ (car $x_1 \geq x_2$ impliquerait que $y_1 \geq y_2$). Mais $x_1 = f^{-1}(y_1)$ et $x_2 = f^{-1}(y_2)$.
Donc f^{-1} est strictement croissante.
Le cas où f est strictement décroissante se montrer de la même manière. □

Remarque I.32. *Une bijection n'est pas nécessairement monotone. Mais si elle est monotone, elle l'est strictement.*

II Tracé d'une fonction

II.1 Symétries

Proposition II.1. *Soient f une fonction définie sur $\mathcal{D}$, de graphe $\mathcal{C}_f$ dans le plan muni du repère $(O, \vec{i}, \vec{j})$, et $a \in \mathbb{R}$. Alors :*

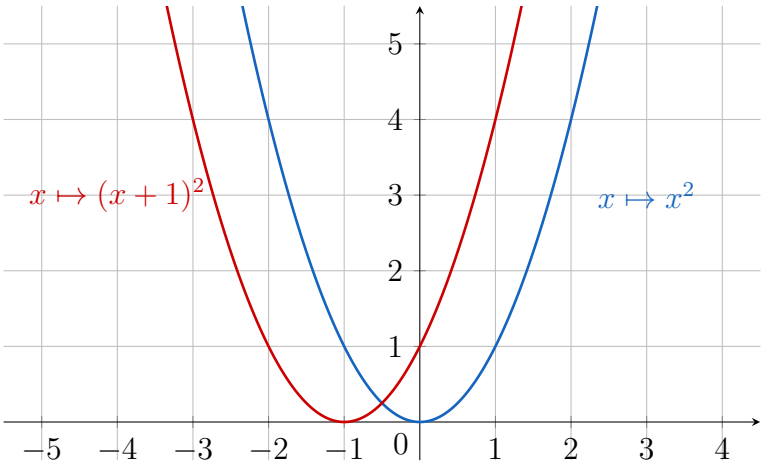
1. *le graphe de $x \mapsto f(x) + a$ est le translaté de $\mathcal{C}_f$ par le vecteur $a\vec{j}$;*
2. *le graphe de $x \mapsto f(x + a)$ est le translaté de $\mathcal{C}_f$ par le vecteur $-a\vec{i}$;*
3. *le graphe de $x \mapsto af(x)$ est le dilaté de $\mathcal{C}_f$ par l'affinité orthogonale $(x, y) \mapsto (x, ay)$;*
4. *si $a \neq 0$, le graphe de $x \mapsto f(ax)$ est le dilaté de $\mathcal{C}_f$ par l'affinité orthogonale $(x, y) \mapsto \left(\frac{x}{a}, y\right)$.*

Démonstration.

1. On note $g : x \mapsto f(x) + a$. Alors, si $x \in \mathcal{D}$, on a :
$$(x, y) \in \mathcal{C}_f \Leftrightarrow y = f(x) \Leftrightarrow y + a = f(x) + a \Leftrightarrow y + a = g(x) \Leftrightarrow (x, y + a) \in \mathcal{C}_g$$
2. On note $g : x \mapsto f(x + a)$. Alors, si $x \in \mathcal{D}$, on a :
$$(x, y) \in \mathcal{C}_f \Leftrightarrow y = f(x) \Leftrightarrow y = f\left((x - a) + a\right) \Leftrightarrow y = g(x - a) \Leftrightarrow (x - a, y) \in \mathcal{C}_g$$

3. et *4.* en exercices □

Remarque II.2. *Il faut bien faire attention au signe "−" et au fait qu'il faut diviser par a dans les cas 2 et 4. Par exemple, pour le cas 2, on représente ci-dessous la fonction $x \mapsto x^2$ et $x \mapsto (x + 1)^2$: la deuxième est bien l'image de la première par la translation de vecteur $-\vec{i}$.*



Définition II.3. *Soit $f : \mathbb{R} \to \mathbb{R}$. On dit que f est :*

1. ***paire*** *si : $\forall x \in \mathbb{R}, f(-x) = f(x)$;*

2. ***impaire*** *si :* $\forall x \in \mathbb{R}, f(-x) = -f(x)$ *;*
3. T***-périodique****, pour* $T \in \mathbb{R}$*, si :* $\forall x \in \mathbb{R}, f(x+T) = f(x)$*.*

Remarques II.4.

1. *On peut étendre les définitions à des fonctions définies sur* $\mathcal{D} \subset \mathbb{R}$ *: il faudra faire attention que* $-x \in \mathcal{D}$ *ou que* $x + T \in \mathcal{D}$*.*
2. *Une fonction* T*-périodique est aussi* (kT)*-périodique pour tout* $k \in \mathbb{Z}$*. Et il sera plus intéressant de chercher un* T *aussi petit que possible.*

Remarque II.5. *Si* f *est impaire, alors* $f(0) = 0$*.*

Proposition II.6. *Si* f *a pour graphe* $\mathcal{C}_f$ *:*

1. f *est paire si, et seulement si,* $\mathcal{C}_f$ *est symétrique par rapport à l'axe des ordonnées ;*
2. f *est impaire si, et seulement si,* $\mathcal{C}_f$ *est symétrique par rapport à l'origine du plan ;*
3. f *est* T*-périodique si, et seulement si,* $\mathcal{C}_f$ *est invariant par translation de vecteur* $T\overrightarrow{i}$*.*

Proposition II.7. *Toute fonction* f *définie sur* $\mathbb{R}$ *s'écrit de manière unique comme somme d'une fonction paire* g *et d'une fonction impaire* h*.*
Plus précisément, g *et* h *sont définie par :* $\forall x \in \mathbb{R},\ g(x) = \dfrac{f(x) + f(-x)}{2}$ *et* $h(x) = \dfrac{f(x) - f(-x)}{2}$*.*

Démonstration. Voir chapitre 1. □

Proposition II.8. *Soient* f *une fonction définie sur* $\mathbb{R}$ *de graphe* $\mathcal{C}_f$*, et* $a, b \in \mathbb{R}$ *:*

1. *si pour tout* $x \in \mathbb{R}$ *:* $f(a-x) = f(x)$*, alors* $\mathcal{C}_f$ *est symétrique par rapport à la droite verticale d'équation* $x = \dfrac{a}{2}$ *;*
2. *si pour tout* $x \in \mathbb{R}$ *:* $f(a-x) = b - f(x)$*, alors* $\mathcal{C}_f$ *est symétrique par rapport au point* $(\dfrac{a}{2}, \dfrac{b}{2})$*.*

Démonstration.

1. On considère $g : x \mapsto f(a-x)$. Alors :

$$\begin{array}{rcl} (x,y) \in \mathcal{C}_f & \Leftrightarrow & y = f(x) \\ & \Leftrightarrow & y = f(a-(a-x)) \\ & \Leftrightarrow & y = g(a-x) \\ & \Leftrightarrow & (a-x, y) \in \mathcal{C}_g \end{array}$$

   Et donc $\mathcal{C}_g$ est l'image par $\mathcal{C}_f$ de l'application $(x,y) \mapsto (a-x, y)$, qui n'est autre que la symétrie axiale considérée.
   Comme $f = g$, on déduit la symétrie pour f.

2. On considère $g : x \mapsto b - f(a-x)$. Alors :

$$\begin{array}{rcl} (x,y) \in \mathcal{C}_f & \Leftrightarrow & y = f(x) \\ & \Leftrightarrow & y = f(a-(a-x)) \\ & \Leftrightarrow & b - y = b - f(a-(a-x)) \\ & \Leftrightarrow & b - y = g(a-x) \\ & \Leftrightarrow & (a-x, b-y) \in \mathcal{C}_g \end{array}$$

   Et donc $\mathcal{C}_g$ est l'image par $\mathcal{C}_f$ de l'application $(x,y) \mapsto (a-x, b-y)$, qui n'est autre que la symétrie centrale considérée.
   Comme $f = g$, on déduit la symétrie pour f.

□

Proposition II.9. *Si f est bijective, alors le graphe de f^{-1} est l'image du graphe de f par la symétrie par rapport à la droite d'équation $y = x$.*

Démonstration. Découle de l'équivalence : $(x, y) \in \mathcal{C}_f \Leftrightarrow (y, x) \in \mathcal{C}_{f^{-1}}$. □

Remarque II.10. *Les symétries permettent de réduire l'**ensemble d'étude** de f (c'est-à-dire l'ensemble sur lequel on va étudier f pour pouvoir la connaître entièrement) :*
- *si f a une symétrie (axiale ou centrale), on peut "couper en deux" l'ensemble de définition ;*
- *si f est T-périodique : on peut restreindre l'ensemble sur un intervalle (quelconque) de longueur T.*

Exemple II.11. *Commençons l'étude de la fonction définie sur $\mathbb{R}$ par $f(x) = \cos(x)\sin(x)^3$. Alors f vérifie pour tout $x \in \mathbb{R}$:*
- *$f(2\pi + x) = \cos(2\pi + x)\sin(2\pi + x)^3 = \cos(x)\sin(x)^3 = f(x)$, donc f est 2π-périodique ;*
- *$f(-x) = \cos(-x)\sin(-x)^3 = -\cos(x)\sin(x)^3 = -f(x)$, donc f est impaire ;*
- *$f(\pi - x) = \cos(\pi - x)\sin(\pi - x)^3 = -\cos(x)\sin(x)^3 = -f(x)$, donc $\mathcal{C}_f$ est symétrique par rapport au point $(\frac{\pi}{2}, 0)$.*

Donc on peut se contenter d'étudier f sur l'intervalle $\left[0; \frac{\pi}{2}\right]$. On remonte alors à $\mathcal{C}_f$ sur $\mathbb{R}$ entier en faisant une symétrie centre par rapport à $(\frac{\pi}{2}, 0)$, puis une symétrie par rapport à l'axe des ordonnées, puis des translations de $\pm 2\pi \overrightarrow{i}$.

II.2 Asymptotes

Définition II.12. *Soit f définie sur un intervalle de la forme $]A; +\infty[$ (resp. $]-\infty; A[$).*
*On dit que la droite Δ d'équation $y = ax + b$ est **asymptote** à $\mathcal{C}_f$ en $+\infty$ (resp. en $-\infty$) si $\lim\limits_{x\to+\infty}(f(x) - (ax + b)) = 0$ (resp. $\lim\limits_{x\to-\infty}(f(x) - (ax + b)) = 0$).*
*On parle d'**asymptote horizontale** lorsque $a = 0$, et d'**asymptote oblique** sinon.*
*On dit que la droite $\mathcal{D}$ d'équation $x = A$ est **asymptote** à $\mathcal{C}_f$ si $\lim\limits_{x\to A^+} f(x) = \pm\infty$ (resp. $\lim\limits_{x\to A^-} f(x) = \pm\infty$).*
*On parle alors d'**asymptote verticale**.*

Proposition II.13. *La droite d'équation $y = ax + b$ est asymptote à $\mathcal{C}_f$ en $+\infty$ si, et seulement si :*

$$\begin{cases} \lim\limits_{x\to+\infty} \dfrac{f(x)}{x} = a \\ \lim\limits_{x\to+\infty} (f(x) - ax) = b \end{cases}$$

et pareil en $-\infty$.

Remarques II.14.
1. *ce résultat permet de chercher l'équation d'une asymptote en cherchant séparément (et dans cet ordre) le coefficient directeur (c'est-à-dire a) et l'ordonnée à l'origine (c'est-à-dire b).*
2. *Si jamais $\lim\limits_{x\to+\infty} \dfrac{f(x)}{x} = \pm\infty$ on a une branche parabolique d'axe vertical, comme c'est par exemple le cas pour les fonctions $x \mapsto e^x$ ou $x \mapsto x^2$.*

Démonstration. Supposons que la droite d'équation $y = ax + b$ est asymptote :
- comme $\frac{f(x)}{x} = \frac{f(x)-(ax+b)}{x} + \frac{ax+b}{x}$, alors :

$$\lim_{x\to+\infty} \frac{f(x)}{x} = \lim_{x\to+\infty} \left(\frac{f(x) - ax - b}{x} + \frac{ax + b}{x} \right) = \underbrace{\lim_{x\to+\infty} \frac{f(x) - ax - b}{x}}_{=0} + \underbrace{\lim_{x\to+\infty} \left(a + \frac{b}{x} \right)}_{=a} = a$$

— comme $(f(x)-ax) = (f(x)-(ax+b))+b$, alors de même :

$$\lim_{x\to+\infty}(f(x)-ax) = \lim_{x\to+\infty}(f(x)-(ax+b)+b) = \underbrace{\lim_{x\to+\infty}(f(x)-(ax+b))}_{=0} + \underbrace{\lim_{x\to+\infty}(b)}_{=b} = b$$

ce qui donne la première implication.
Pour la réciproque, il suffit de considérer la seconde limite. On a alors :

$$\lim_{x\to+\infty}(f(x)-(ax+b)) = \underbrace{\lim_{x\to+\infty}(f(x)-ax)}_{=b} + \underbrace{\lim_{x\to+\infty}(-b)}_{=-b} = b-b = 0.$$

□

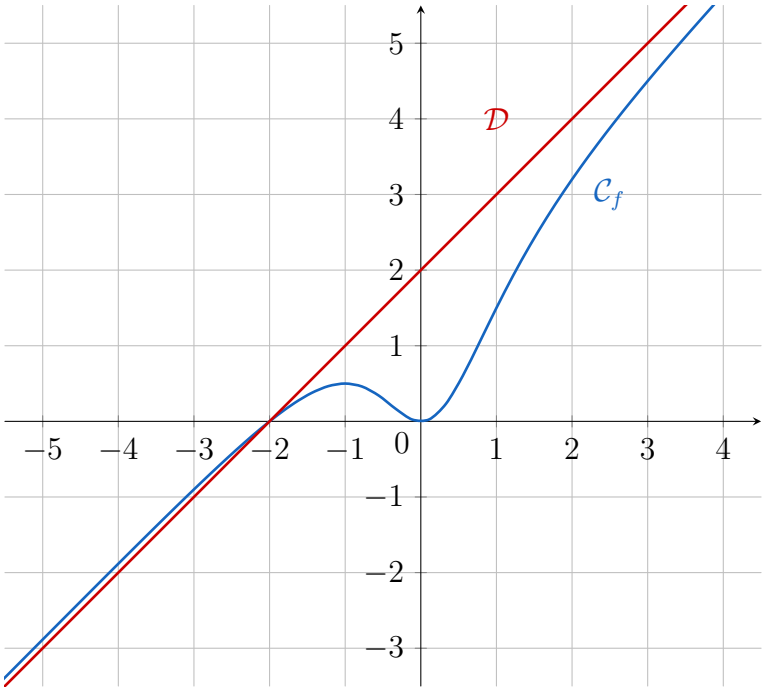
Remarque II.15. *Ce résultat assure l'unicité de l'asymptote. On l'utilise en pratique pour trouver une asymptote, en cherchant d'abord la limite de* $\dfrac{f(x)}{x}$*, puis celle de* $f(x)-ax$*.*
Si jamais $\lim\limits_{x\to+\infty}\dfrac{f(x)}{x} = a$ *mais que* $\lim\limits_{x\to+\infty}(f(x)-ax) = \pm\infty$*, on a alors un branche parabolique oblique d'axe* $\Delta : y = ax$*.*

Exemple II.16. *On considère la fonction* f *définie sur* $\mathbb{R}$ *par :* $f(x) = \dfrac{x^3+2x^2}{x^2+1}$.

— *pour* $x \neq 0$ *:* $\dfrac{f(x)}{x} = \dfrac{x^3+2x^2}{x^3+x} = \dfrac{1+\dfrac{2}{x}}{1+\dfrac{1}{x^2}} \underset{x\to\pm\infty}{\to} 1$;

— $f(x)-x = \dfrac{x^3+2x^2-x^3-x}{x^2+1} = \dfrac{2x^2-x}{x^2+1} = \dfrac{2-\dfrac{1}{x}}{1+\dfrac{1}{x^2}} \underset{x\to\pm\infty}{\to} 2$

donc la droite $\mathcal{D}$ *d'équation* $y = x+2$ *est asymptote à* $\mathcal{C}_f$ *en* $\pm\infty$*.*



III Continuité et dérivation

Les principaux résultats seront démontrés dans un autre chapitre.

III.1 Continuité

Définition III.1. *Si f est une fonction définie sur un intervalle I, et $a \in I$, on dit que f est* ***continue en*** *a si : $\lim_{x\to a} f(x) = f(a)$.*
Si f est continue en tout point $a \in I$, on dira qu'elle est ***continue sur*** *I.*

Proposition-Définition III.2. *Soient I est un intervalle, $a \in I$, et f définie sur $I\setminus\{a\}$ telle que : $\lim_{x\to a} f(x) = b \in \mathbb{R}$. Alors f est* ***prolongeable par continuité en*** *a.*
La fonction g définie sur I par :

$$\forall x \in I,\ g(x) = \begin{cases} f(x) & si\ x \neq a \\ b & si\ x = b \end{cases}$$

est un prolongement de f continu en a.

Exemple III.3. *La fonction $f : x \mapsto \dfrac{e^x - 1}{x}$ est prolongeable par continuité en 0, car : $\lim_{x\to 0} f(x) = 1$, en reconnaissant la limite du taux d'accroissement de la fonction exponentielle entre x et 0.*

Théorème III.4 (Théorème des valeurs intermédiaires)**.** *L'image d'un intervalle par une fonction continue est un intervalle.*

Remarque III.5. *C'est bien cohérent avec le théorème vu au lycée : considérons f continue sur un intervalle I, $x, y \in I$, et J l'ensemble des images.*
Alors $a = f(x), b = f(y) \in J$. Comme J est un intervalle, cela veut dire que tout élément entre a et b est dans J, donc a un antécédent dans I.
Autrement dit : pour tout k entre a et b, il existe z tel que $f(z) = k$.

III.2 Dérivabilité et dérivée

Définition III.6. *Si f est une fonction définie sur un intervalle I, et $a \in I$, on appelle* ***taux d'accroissement*** *de f en a la fonction :*

$$\tau_a : \begin{cases} I\setminus\{a\} & \to & \mathbb{R} \\ x & \mapsto & \dfrac{f(x) - f(a)}{x - a} \end{cases}.$$

Si $\lim_{x\to a} \tau_a(x)$ est existe et est finie, on dit que f est ***dérivable en*** *a, et on définit son* ***nombre dérivé*** *en a par : $f'(a) = \lim_{x\to a} \tau_a(x)$.*
Si f est dérivable en tout point $a \in I$, on dira qu'elle est ***dérivable sur*** *I, et la fonction $f' : x \mapsto f'(x)$ est appelée sa* ***fonction dérivée****.*

Remarques III.7.

1. *pour faciliter les calculs, on écrira plutôt : $f'(a) = \lim_{h\to 0} \dfrac{f(a+h) - f(a)}{h}$;*
2. *le nombre $\tau_a(x)$ est le coefficient directeur de la droite passant par les points de $\mathcal{C}_f$ d'abscisses a et x.*

Exemples III.8.

1. *la fonction $f : x \mapsto x^2$ est dérivable sur $\mathbb{R}$. Si $a, h \in \mathbb{R}$, on a :*

$$\frac{f(a+h) - f(a)}{h} = \frac{(a+h)^2 - a^2}{h} = 2a + h \underset{h\to 0}{\to} 2a$$

et ainsi $f' : \begin{cases} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & 2x \end{cases}$;

2. *la fonction* $f : x \mapsto |x|$ *n'est pas dérivable en* 0, *car son taux d'accroissement en* 0 *est :*

$$\tau_0(x) = \frac{|x| - |0|}{x - 0} = \frac{|x|}{x} = \begin{cases} 1 & si\ x > 0 \\ -1 & si\ x < 0 \end{cases}$$

qui n'admet pas de limite quand $x \to 0$.

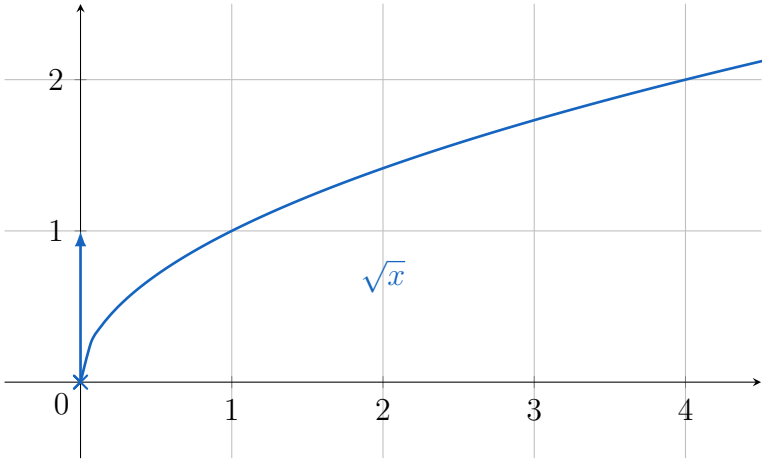
Théorème III.9. *Si* f *est dérivable en* a, *alors* f *est continue en* a.

Définition III.10. *Si* f *est dérivable en* a, *la* ***tangente à*** $\mathcal{C}_f$ ***au point d'abscisse*** a *est la droite passant* $(a, f(a))$ *de coefficient directeur* $f'(a)$, *c'est-à-dire la droite d'équation :* $y = f'(a)(x - a) + f(a)$.

Remarque III.11. *Si* f *n'est pas dérivable en* a, *mais que* $\lim\limits_{x \to a} \tau_a(x) = \pm\infty$, *alors* $\mathcal{C}_f$ *admet pour tangente en* a *la droite verticale passant par* $(a, f(a))$, *c'est-à-dire la droite d'équation :* $x = a$.
Par exemple, pour la fonction racine, le taux d'accroissement entre 0 *et* $h > 0$ *est :*

$$\tau_0(h) = \frac{\sqrt{h} - \sqrt{0}}{h - 0} = \frac{1}{\sqrt{h}} \underset{h \to 0}{\to} +\infty$$

donc la fonction racine admet une tangente horizontale en 0, *ce qu'on voit bien sur le tracé suivant :*



Proposition III.12. *Si* f, g *sont dérivables sur* I, *et* $\lambda \in \mathbb{R}$, *alors on a les fonctions dérivées suivantes :*

1. $(f + \lambda g)' = f' + \lambda g'$ *(la dérivation est linéaire) ;*
2. $(fg)' = f'g + fg'$ *;*
3. *si* g *ne s'annule pas :* $\left(\frac{1}{g}\right)' = -\frac{g'}{g^2}$ *;*
4. *si* g *ne s'annule pas :* $\left(\frac{f}{g}\right)' = \frac{f'g - fg'}{g^2}$.

Théorème III.13. *Soient* I, J *deux intervalles,* $f : I \to J$ *et* $g : J \to \mathbb{R}$ *deux fonctions dérivables.*
Alors la fonction $g \circ f$ *est dérivable, de dérivée :*

$$(g \circ f)' = f' \times g' \circ f : \begin{cases} I & \to & \mathbb{R} \\ x & \mapsto & f'(x) \times g'(f(x)) \end{cases}.$$

Corollaire III.14. *Si* u *est une fonction dérivable sur un intervalle* I, *alors :*

1. *si* $n \in \mathbb{N}$, *alors* $u^n : x \mapsto (u(x))^n$ *est dérivable sur* I *avec :* $(u^n)' = n \times u' \times u^{n-1}$ *;*
2. *si* u *ne s'annule pas et* $n \in \mathbb{Z}$, *alors* u^n *est dérivable sur* I *avec :* $(u^n)' = n \times u' \times u^{n-1}$ *;*
3. *la fonction* $e^u : x \mapsto e^{u(x)}$ *est dérivable sur* I *avec :* $(e^u)' = u' \times e^u$ *;*

4. si u est à valeurs strictement positives, $\ln(u) : x \mapsto \ln(u(x))$ est dérivable avec : $(\ln u)' = \dfrac{u'}{u}$.

Démonstration. On utilise la dérivée d'une composée. □

Remarque III.15. *On peut renforcer le dernier résultat : si u ne s'annule pas, alors $\ln(|u|)$ est dérivable avec* $(\ln(|u|))' = \dfrac{u'}{u}$.

Exemple III.16. *La fonction $f : x \mapsto (\ln(x^2+1))^2$ est dérivable sur $\mathbb{R}$:*
- *comme $u : x \mapsto x^2+1$ est dérivable et positive sur $\mathbb{R}$, alors $\ln(u)$ est dérivable sur $\mathbb{R}$, de dérivée :* $x \mapsto \dfrac{u'(x)}{u(x)} = \dfrac{2x}{x^2+1}$;
- *donc $f = (\ln(u))^2$ est dérivable sur $\mathbb{R}$, avec pour tout $x \in \mathbb{R}$:*

$$f'(x) = \frac{4x}{x^2+1} \times \ln(x^2+1).$$

III.3 Variations d'une fonction dérivable

Proposition III.17 (Monotonie et dérivée)**.** *Si f est dérivable sur un* ***intervalle*** *I, alors :*

1. *si f' est positive ou nulle, f est croissante ;*
2. *si f' est négative ou nulle, alors f est décroissante.*

Proposition III.18. *Si* ***de plus*** *f' ne s'annule qu'un nombre fini de fois sur I, alors f est strictement monotone.*

Remarque III.19. *Le résultat ne tient pas si I n'est pas un intervalle. Par exemple la fonction $f : x \mapsto \dfrac{1}{x}$ a pour dérivée $f' : x \mapsto -\dfrac{1}{x^2}$ qui est toujours négative, mais n'est pas décroissante sur $\mathbb{R}^*$.*

Exemple III.20. *Reprenons la fonction f définie sur $\mathbb{R}$ par $f(x) = \cos(x)\sin(x)^3$: elle est dérivable sur $\mathbb{R}$, de dérivée en x :*

$$f'(x) = -\sin(x)^4 + 3\cos(x)^2\sin(x)^2 = \sin(x)^2\left(4\cos(x)^2 - 1\right)$$

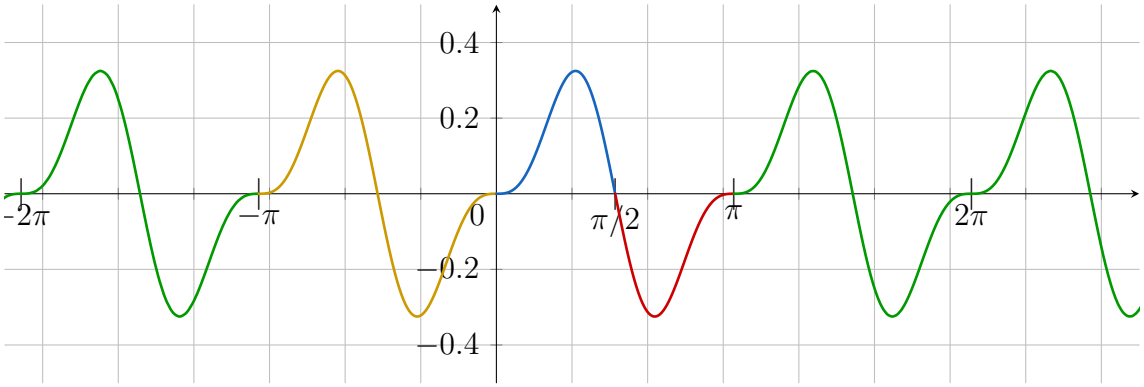
donc on déduit que sur $\left[0; \dfrac{\pi}{2}\right]$:
- *f' s'annule en 0 et $\dfrac{\pi}{3}$;*
- *f' est strictement positive sur $\left]0; \dfrac{\pi}{3}\right[$;*
- *f' est strictement négative sur $\left]\dfrac{\pi}{3}; \dfrac{\pi}{2}\right]$.*

D'où les variations suivantes :

x	0		$\pi/3$		$\pi/2$
f'	0	$+$	0	$-$	
f	0	↗	$\dfrac{3\sqrt{3}}{16}$	↘	0

On trouve le tracé ci-dessous, où on fait :
- *le tracé en bleu (par l'étude précédente) ;*

— *le tracé en rouge (par symétrie centrale) ;*
— *le tracé en orange (par symétrie axiale) ;*
— *le tracé en vert (par translation).*



Corollaire III.21. *Soit f une fonction dérivable sur un intervalle I. Alors f est constante si, et seulement si, f' est nulle.*

Démonstration. Si f est constante, son taux d'accroissement est toujours nul, donc sa dérivée aussi.
Si f' est nulle, alors f est à la fois croissante et décroissante. Ainsi, si $x, y \in I$ avec $x \leq y$, alors : $f(x) \leq f(y)$ et $f(x) \geq f(y)$, donc $f(x) = f(y)$ et f est constante. □

III.4 Dérivées d'ordre supérieur

Définition III.22. *Si f est définie sur I et $n \in \mathbb{N}$, on définit la **dérivée n-ème** de f (ou **dérivée d'ordre** n) comme :*

$$f^{(n)} = \begin{cases} f & si \quad n = 0 \\ \left(f^{(n-1)}\right)' & si \quad n \geq 1 \text{ et que } f^{(n-1)} \text{ est dérivable} \end{cases}$$

Si $f^{(n)}$ est bien définie, on dira que f est n-fois dérivable.
*Si f est n-fois dérivable pour tout entier naturel n, on dira que f est **infiniment dérivable**.*

Définition III.23. *On note $\mathcal{C}^0(I)$ l'ensemble des fonctions continues sur I.*
*Si $k \in \mathbb{N}^*$, on dira que f est **de classe $\mathcal{C}^k$ sur** I si f est k-fois dérivable sur I et que $f^{(k)}$ est continue sur I. On note $\mathcal{C}^k(I)$ l'ensemble des fonctions de classe $\mathcal{C}^k$ sur I.*
Enfin, on note $\mathcal{C}^\infty(I)$ l'ensemble des fonctions $\mathcal{C}^\infty$ sur I, c'est-à-dire des fonctions de classe $\mathcal{C}^k$ pour tout entier naturel k.

Remarque III.24. *Comme une fonction dérivable est continue, les fonctions de classe $\mathcal{C}^\infty$ sont exactement les fonctions infiniment dérivables.*

Exemple III.25. *La fonction $x \mapsto \begin{cases} x^2 \sin\left(\frac{1}{x}\right) & si\ x \neq 0 \\ 0 & si\ x = 0 \end{cases}$ est définie et dérivable sur $\mathbb{R}$, mais sa dérivée n'est pas continue en 0.*

III.5 Continuité et dérivabilité des fonctions réciproques

Théorème III.26 (de la bijection monotone)**.** *Si f est continue et strictement monotone sur un intervalle I, alors f réalise une bijection de I sur $J = f(I)$.*
De plus, J est un intervalle et f^{-1} est continue et de même monotonie que f sur J.

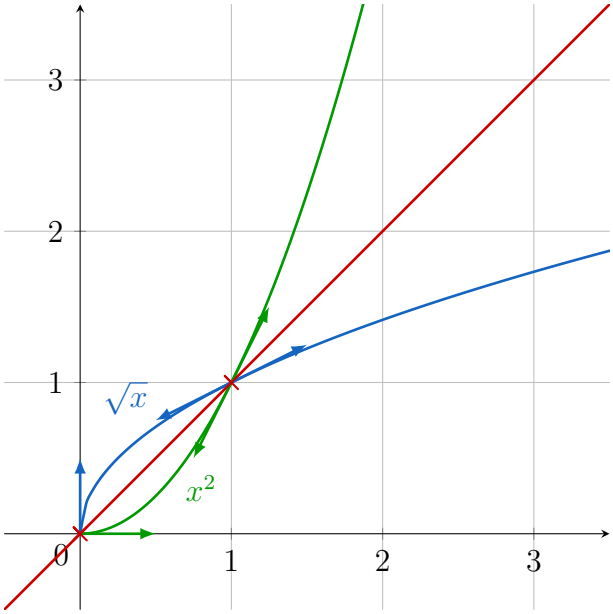
Exemple III.27. *Si $a, b \in \mathbb{R}$ avec $a < b$ et que f est continue strictement croissante sur $[a;b]$, alors $f([a;b]) = [f(a);f(b)]$. Et pour tout élément $c \in [f(a);f(b)]$, l'équation $f(x) = c$ admet une unique solution (dans $[a;b]$).*

Remarque III.28. *C'est en fait une amélioration du TVI, dans le sens où les antécédents sont uniques.*

Théorème III.29 (dérivabilité des fonctions réciproques)**.** *Soit f est continue strictement monotone sur un intervalle I et $x \in \overset{\circ}{I}$. On suppose que f est dérivable en x, et on pose $y = f(x)$. Alors :*

1. *si $f'(x) \neq 0$: f^{-1} est dérivable en y, avec $(f^{-1})'(y) = \dfrac{1}{f'(x)} = \dfrac{1}{f' \circ f^{-1}(y)}$;*
2. *si $f'(x) = 0$: f^{-1} n'est pas dérivable en y, et $\mathcal{C}_{f^{-1}}$ admet une tangente verticale en (y, x).*

Remarque III.30. *On retrouve graphiquement le résultat avec les tangentes : si D est une droite de pente $a \neq 0$, sa symétrique par rapport à la première bissectrice est une droite de pente $\dfrac{1}{a}$.*



Corollaire III.31. *Si I, J sont deux intervalles, f bijective de I sur J, dérivable sur I, et que f' ne s'annule pas sur I, alors f^{-1} est dérivable sur J avec : $(f^{-1})' = \dfrac{1}{f' \circ f^{-1}}$.*

Exemple III.32. *La fonction $f : x \mapsto x^2$ est dérivable sur $\mathbb{R}_+$ de dérivée : $x \mapsto 2x$.*
En particulier, f' est positive ou nulle sur $\mathbb{R}_+$, ne s'annulant qu'en 0, donc f réalise une bijection strictement croissante de $\mathbb{R}_+$ sur $f(\mathbb{R}_+) = \mathbb{R}_+$.
Sa bijection réciproque est la fonction racine : $f^{-1} : y \mapsto \sqrt{y}$, qui vérifie :

— *si $y \neq 0$: alors en notant $x = \sqrt{y}$, on a $f'(x) = 2x \neq 0$, donc f^{-1} est dérivable en y, avec :*

$$(f^{-1})'(y) = \frac{1}{f' \circ f^{-1}(y)} = \frac{1}{2\sqrt{y}}$$

— *si $y = 0$: comme $f'(0) = 0$, $\mathcal{C}_{f^{-1}}$ admet une tangente horizontale au point d'abscisse 0.*

ce qu'on avait déjà vu sur le graphe précédent.

Théorème III.33. *On a les dérivées usuelles suivantes :*

$f(x)$	D_f	$f'(x)$	$D_{f'}$
c $(c \in \mathbb{C})$	$\mathbb{R}$	0	$\mathbb{R}$
x^n $(n \in \mathbb{N}^*)$	$\mathbb{R}$	nx^{n-1}	$\mathbb{R}$
x^n $(n \in \mathbb{Z}_-^*)$	$\mathbb{R}^*$	nx^{n-1}	$\mathbb{R}^*$
cas particulier : $\dfrac{1}{x}$	$\mathbb{R}^*$	$-\dfrac{1}{x^2}$	$\mathbb{R}^*$
x^α $(\alpha \in]1;+\infty[\setminus \mathbb{N})$	$\mathbb{R}_+$	$\alpha x^{\alpha-1}$	$\mathbb{R}_+$
x^α $(\alpha \in]0;1[)$	$\mathbb{R}_+$	$\alpha x^{\alpha-1}$	$\mathbb{R}_+^*$
cas particulier : $\sqrt{x}$	$\mathbb{R}_+$	$\dfrac{1}{2\sqrt{x}}$	$\mathbb{R}_+^*$
x^α $(\alpha \in \mathbb{R}_-^* \setminus \mathbb{Z})$	$\mathbb{R}_+^*$	$\alpha x^{\alpha-1}$	$\mathbb{R}_+^*$
e^x	$\mathbb{R}$	e^x	$\mathbb{R}$
a^x $(a \in \mathbb{R}_+^*)$	$\mathbb{R}$	$\ln(a)a^x$	$\mathbb{R}$
$\ln(x)$	$\mathbb{R}_+^*$	$\dfrac{1}{x}$	$\mathbb{R}_+^*$
$\log_b(x)$ $(b \in \mathbb{R}_+^*)$	$\mathbb{R}_+^*$	$\dfrac{1}{x\ln(b)}$	$\mathbb{R}_+^*$
$\sin(x)$	$\mathbb{R}$	$\cos(x)$	$\mathbb{R}$
$\cos(x)$	$\mathbb{R}$	$-\sin(x)$	$\mathbb{R}$
$\tan(x)$	$\mathbb{R} \setminus \left(\dfrac{\pi}{2} + \pi\mathbb{Z}\right)$	$1 + \tan^2(x) = \dfrac{1}{\cos^2(x)}$	$\mathbb{R} \setminus \left(\dfrac{\pi}{2} + \pi\mathbb{Z}\right)$
$\arcsin(x)$	$[-1,1]$	$\dfrac{1}{\sqrt{1-x^2}}$	$]-1,1[$
$\arccos(x)$	$[-1,1]$	$-\dfrac{1}{\sqrt{1-x^2}}$	$]-1,1[$
$\arctan(x)$	$\mathbb{R}$	$\dfrac{1}{1+x^2}$	$\mathbb{R}$
$\mathrm{ch}(x)$	$\mathbb{R}$	$\mathrm{sh}(x)$	$\mathbb{R}$
$\mathrm{sh}(x)$	$\mathbb{R}$	$\mathrm{ch}(x)$	$\mathbb{R}$
$\mathrm{th}(x)$	$\mathbb{R}$	$1 - \mathrm{th}^2(x) = \dfrac{1}{\mathrm{ch}^2(x)}$	$\mathbb{R}$

Chapitre 4

Ensembles et relations

I Appartenance et inclusion

Définition I.1. *Un* ***ensemble*** *est une collection d'objets. Chacun des objets est appelé* ***élément****. Si x est un élément de l'ensemble E, on notera $x \in E$, qui se lit "x appartient à E". Inversement, si y n'est pas un élément de E, on notera $y \notin E$, qui se lit "y n'appartient pas à E".*

Définition I.2. *Si E et F sont deux ensembles, on dira que F est une* ***partie*** *(ou un* ***sous-ensemble****) de E, ou que F est inclus dans E, si tout élément de F est un élément de E. On notera alors : $F \subset E$.*

Remarque I.3. *Un ensemble E peut être décrit en* ***extension*** *(on énumère les éléments) ou en* ***compréhension*** *(on donne une propriété satisfaite par les éléments). Par exemple, l'ensemble E des entiers naturels plus petits que 3 peut s'écrire :*

- *en extension : $E = \{0; 1; 2\}$;*
- *en compréhension : $X = \{n \in \mathbb{N} \,|\, n < 3\}$.*

Définition I.4. *On dit que deux ensembles E et F sont* ***égaux*** *s'ils ont exactement les mêmes éléments, et on note alors $E = F$.*

Proposition I.5. *Les ensembles E et F sont égaux si, et seulement si, on a les inclusions $E \subset F$ et $F \subset E$.*

Proposition I.6. *L'inclusion est* ***transitive*** *: si $E \subset F$ et $F \subset G$, alors $E \subset G$.*

Proposition-Définition I.7. *On appelle* ***ensemble vide****, que l'on note $\emptyset$, l'ensemble ne contenant aucun élément.*
L'ensemble vide est sous-ensemble de tout autre ensemble, et il est unique.

Démonstration. Si A est un ensemble vide, et E un ensemble, comme A ne contient aucun élément, tout élément de A est dans E : donc $A \subset E$.
Si B est un autre ensemble vide, alors : $A \subset B$ et $B \subset A$, donc $A = B$. □

Définition I.8. *Un ensemble possédant un seul élément est appelé* ***singleton****, et on le note $\{a\}$.*

Définition I.9. *Si E est un ensemble, on notera $\mathcal{P}(E)$ l'ensemble de toute les parties de E, c'est-à-dire que :*

$$F \in \mathcal{P}(E) \Leftrightarrow F \subset E.$$

Remarque I.10. *Les ensembles $\emptyset$ et E sont toujours des éléments de $\mathcal{P}(E)$.*

Exemple I.11. *Si $E = \{1; 2; 3\}$, alors :*

$$\mathcal{P}(E) = \{\emptyset; \{1\}; \{2\}; \{3\}; \{1; 2\}; \{1; 3\}; \{2; 3\}; \{1; 2; 3\}\}.$$

II Opérations sur les ensembles

Définition II.1. *Si E est un ensemble, et A, B deux parties de E, on définit :*

1. *le* ***complémentaire*** *de A dans E, noté $E - A$, $E \setminus A$, A^C ou $\overline{A}$ par :*

$$\overline{A} = \{x \in E \,|\, x \notin A\};$$

2. *l'**intersection** de A et B est :*

$$A \cap B = \{x \in E \,|\, x \in A \text{ et } x \in B\};$$

3. *la **réunion** (ou l'**union**) de A et B est :*

$$A \cup B = \{x \in E \,|\, x \in A \text{ ou } x \in B\};$$

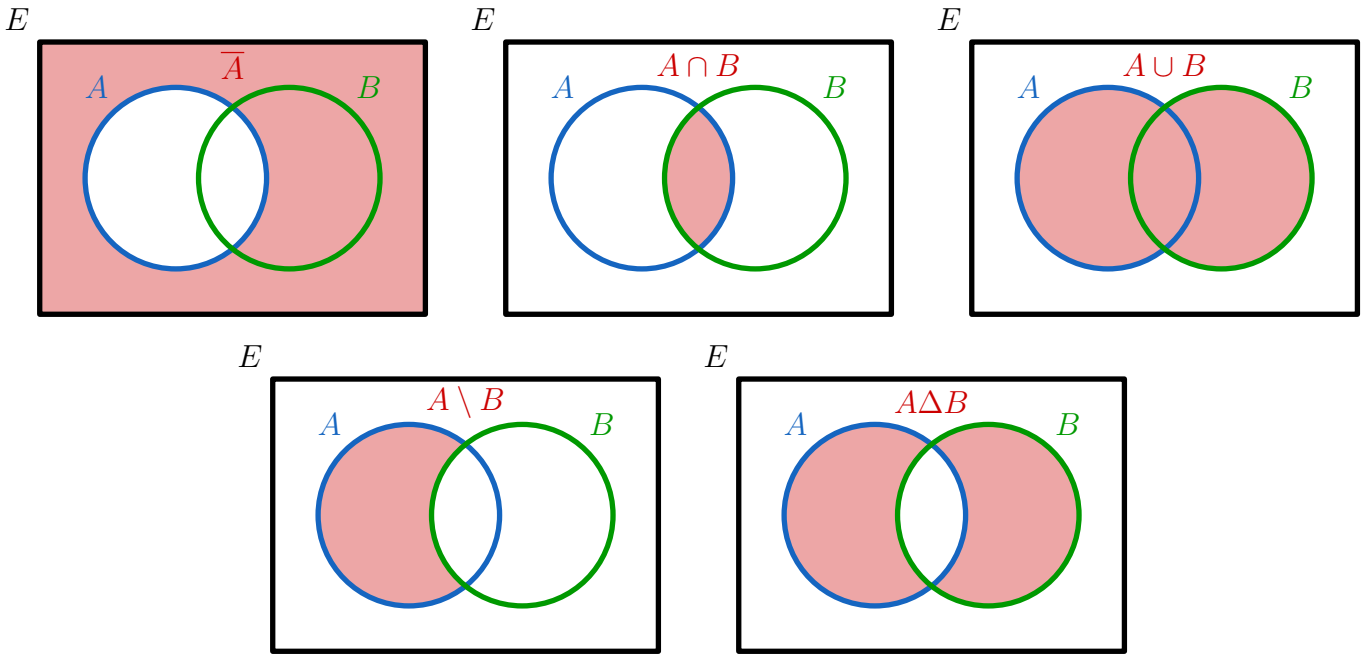
4. *la **différence** de A et B est :*

$$A - B = \{x \in E \,|\, x \in A \text{ et } x \notin B\} = A \cap \overline{B};$$

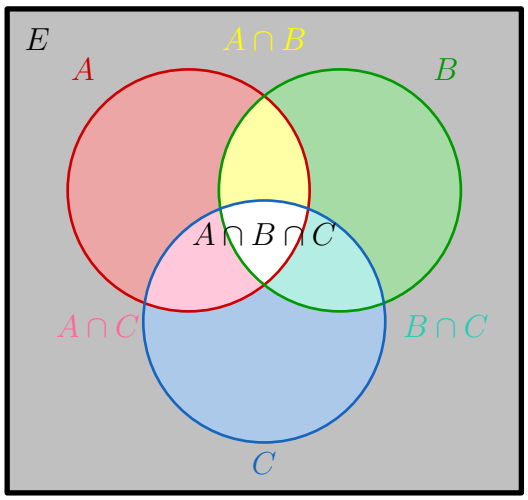
5. *la **différence symétrique** de A et B est :*

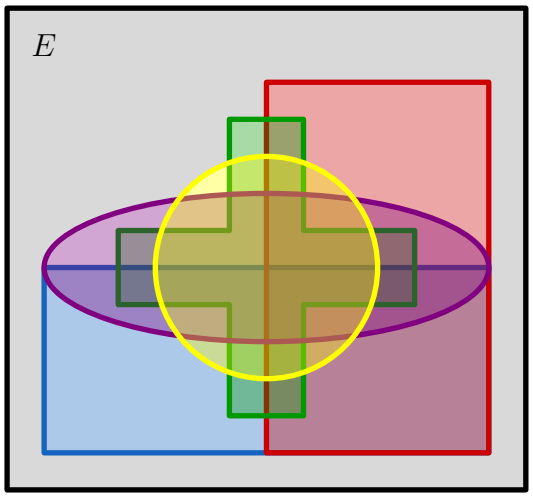
$$A \Delta B = \{x \in E \,|\, x \in A \cup B \text{ et } x \notin A \cap B\} = A \cup B - A \cap B = (A - B) \cup (B - A).$$

*On les représente par des **diagrammes de Venn** (ou diagramme patate) :*



Remarque II.2. *Plus généralement, les diagrammes de Venn permettent de mieux comprendre des ensembles, en permettant de visualiser séparément des différents éléments selon leur appartenance à chaque ensemble considéré. Cette méthode devient rapidement compliquée lorsque l'on prend beaucoup d'ensembles. Par exemple, on donne ci-dessous les diagrammes de Venn génériques pour 3 et 5 ensembles :*





Proposition II.3. *Si A, B, C sont trois parties d'un ensemble E, alors :*

1. *commutativité de la réunion et de l'intersection : $A \cup B = B \cup A$ et $A \cap B = B \cap A$;*
2. *associativité de la réunion et de l'intersection :*
   — $A \cup (B \cup C) = (A \cup B) \cup C = A \cup B \cup C$;
   — $A \cap (B \cap C) = (A \cap B) \cap C = A \cap B \cap C$.
3. *lois de de Morgan : $\overline{A \cap B} = \overline{A} \cup \overline{B}$ et $\overline{A \cup B} = \overline{A} \cap \overline{B}$;*
4. *distributivité de la réunion par rapport à l'intersection et réciproquement :*
   — $C \cup (A \cap B) = (C \cup A) \cap (C \cup B)$;
   — $C \cap (A \cup B) = (C \cap A) \cup (C \cap B)$.

Remarque II.4. *L'intersection et la réunion se généralisent à davantage de parties. Si $A_1, \dots, A_n$ sont des parties de E, on pose :*

$$\begin{array}{rcccl} A_1 \cap A_2 \cap \cdots \cap A_n & = & \cap_{i=1}^n A_i & = & \{x \in E \,|\, \forall i \in \{1, \dots, n\},\, x \in A_i\} \\ A_1 \cup A_2 \cup \cdots \cup A_n & = & \cap_{i=1}^n A_i & = & \{x \in E \,|\, \exists i \in \{1, \dots, n\},\, x \in A_i\} \end{array}.$$

Remarque II.5. *Il y a une correspondance entre logique et ensembles :*

Ensembliste	*Logique*
Ensemble : A	*Assertion : $x \in A$*
Inclusion : $A \subset B$	*Implication : $x \in A \Rightarrow x \in B$*
Égalité : $A = B$	*Équivalence : $x \in A \Leftrightarrow x \in B$*
Complémentaire : $\overline{A}$	*Négation : $\neg\,(x \in A)$*
Union : $A \cup B$	*Disjonction : $x \in A \vee x \in B$*
Intersection : $A \cap B$	*Conjonction : $x \in A \wedge x \in B$*

III Partitions

Définition III.1. *Si A, B sont deux ensembles, on dit qu'ils sont **disjoints** si : $A \cap B = \emptyset$.*

Définition III.2. *Soit P une partie de $\mathcal{P}(E)$. On dit que :*

1. *P est un **recouvrement** de E si : $\cup_{A \in P} A = E$;*
2. *P est une **partition** de E si P est un recouvrement dont tous les éléments sont deux-à-deux disjoints, c'est-à-dire que :*

$$\forall A, B \in P,\ A \neq B \Rightarrow A \cap B = \emptyset.$$

Remarque III.3. *Si P est un recouvrement de E, alors :*

$$\forall x \in E,\ \exists A \in P,\ x \in A$$

tandis que si P est une partition de E, alors :

$$\forall x \in E,\ \exists! A \in P,\ x \in A.$$

Exemples III.4. *L'ensemble $\{[n; n+1] \,|\, n \in \mathbb{Z}\}$ est un recouvrement de $\mathbb{R}$, mais pas une partition. On peut voir par exemple que $[0;1] \cap [1;2] = \{1\} \neq \emptyset$.*
En revanche, l'ensemble $\{[n; n+1[\,|\, n \in \mathbb{Z}\}$ est une partition de $\mathbb{R}$. Plus précisément, si $x \in \mathbb{R}$, on a :

$$x \in [n; n+1[\Leftrightarrow n = \lfloor x \rfloor.$$

IV Produits cartésiens

Définition IV.1. *Si E, F sont deux ensembles, on définit le* ***produit cartésien*** *de E par F par :*

$$E \times F = \{(x, y) \,|\, x \in E \text{ et } y \in F\}.$$

Plus généralement, si $E_1, \ldots, E_n$ sont des ensembles, on définit :

$$E_1 \times \cdots \times E_n = \{(x_1, \ldots, x_n) \,|\, x_1 \in E_1, \ldots, x_n \in E_n\}.$$

En particulier, si $E_1 = \cdots = E_n = E$, on note :

$$E \times \cdots \times E = E^n.$$

Remarque IV.2. *Il faut bien prendre garde aux notations, pour ne pas confondre le couple (x, y) avec la paire $\{x, y\}$.*

Exemple IV.3. *Un repère permet d'identifier chaque point du plan au couple de ses coordonnées, et ainsi d'identifier le plan à $\mathbb{R}^2$.*

V Relations binaires

V.1 Généralités sur les relations binaires

Définition V.1. *Si E est un ensemble, une* ***relation binaire*** *sur E est un sous ensemble $\mathcal{R}$ de $E \times E$. Si $(x, y) \in \mathcal{R}$, on notera alors : $x\mathcal{R}y$.*

Définition V.2. *Soit $\mathcal{R}$ une relation binaire sur E. On dit que $\mathcal{R}$ est :*

1. ***réflexive*** *si : $\forall x \in E,\ x\mathcal{R}x$;*
2. ***symétrique*** *si : $\forall x, y \in E,\ x\mathcal{R}y \Rightarrow y\mathcal{R}x$;*
3. ***antisymétrique*** *si : $\forall x, y \in E,\ \left\{ \begin{array}{l} x\mathcal{R}y \\ y\mathcal{R}x \end{array} \right. \Rightarrow x = y$;*
4. ***transitive*** *si : $\forall x, y, z \in E,\ \left\{ \begin{array}{l} x\mathcal{R}y \\ y\mathcal{R}z \end{array} \right. \Rightarrow x\mathcal{R}z.$*

Exemples V.3. *1. la relation de divisibilité sur $\mathbb{Z}$: $x\mathcal{R}y \Leftrightarrow x|y$. Elle est :*
- *réflexive : tout entier se divise lui-même ;*
- *transitive : si a divise b et b divise c, alors a divise c ;*

— *pas symétrique :* 1 *divise* 2 *mais* 2 *ne divise pas* 1 *;*
— *pas antisymétrique :* 1 *divise* -1 *et inversement, mais* $1 \neq -1$.

2. *la relation d'inclusion sur un ensemble* $\mathcal{P}(E)$*, pour* E *un ensemble non vide, est réflexive, antisymétrique et transitive (par les propriétés de l'inclusion). Elle n'est pas symétrique car on a :* $\emptyset \subset E$ *mais* $E \not\subset \emptyset$.
3. *si* E *est un ensemble possédant au moins deux éléments, la relation définie sur* $F = \mathcal{P}(E) \setminus \{\emptyset\}$ *par :* $A\mathcal{R}B \Leftrightarrow A \cap B \neq \emptyset$ *est :*
— *réflexive : car* $A \in F \Rightarrow A \neq \emptyset \Rightarrow A \cap A = A \neq \emptyset$ *;*
— *symétrique : par commutativité de l'intersection :* $A \cap B = B \cap A$ *;*
— *non transitive : prenons* $a \neq b \in E$*, et* $A = \{a\}, B = \{a; b\}, C = \{b\}$*. Alors* $A\mathcal{R}B$ *et* $B\mathcal{C}$ *mais pas* $A\mathcal{R}C$ *;*
— *non antisymétrique : avec les mêmes notations :* $A\mathcal{R}B$ *et* $B\mathcal{R}A$*, mais* $A \neq B$.

V.2 Relations d'équivalence

Définition V.4. *Une relation binaire* $\mathcal{R}$ *sur* E *est appelée* ***relation d'équivalence*** *si elle est : réflexive, symétrique et transitive.*
Si $x \in E$*, on définit la* ***classe d'équivalence*** *de* x*, notée* $\mathrm{cl}(x)$ *ou* $\overline{x}$*, comme l'ensemble :* $\overline{x} = \{y \in E \,|\, x\mathcal{R}y\}$.

Remarques V.5.

1. *On note souvent par* $\sim$ *ou* $\equiv$ *les relations d'équivalence.*
2. *Du fait de la symétrie, on a aussi :* $\overline{x} = \{y \in E \,|\, y\mathcal{R}y\}$.

Proposition V.6. *Soit* $\mathcal{R}$ *une relation d'équivalence sur* E*. Pour tous* $x, y \in E$ *:* $x\mathcal{R}y \Leftrightarrow \mathrm{cl}(x) = \mathrm{cl}(y)$.

Démonstration. Soient $x, y \in E$:

1. si $x\mathcal{R}y$: soit $z \in \mathrm{cl}(y)$. Alors $y\mathcal{R}z$, donc $x\mathcal{R}z$ (par transitivité). Donc $z \in \mathrm{cl}(x)$, et $\mathrm{cl}(y) \subset \mathrm{cl}(x)$. Par symétrie, on a aussi $y\mathcal{R}x$, et on trouve de même $\mathrm{cl}(x) \subset \mathrm{cl}(y)$. Donc : $\mathrm{cl}(x) = \mathrm{cl}(y)$.
2. si $\mathrm{cl}(x) = \mathrm{cl}(y)$: $x \in \mathrm{cl}(x)$ (par réflexivité), donc $x \in \mathrm{cl}(y)$, donc $x\mathcal{R}y$.

□

Proposition V.7. *L'ensemble des classes d'équivalences de* $\mathcal{R}$ *forme une partition de* E.

Démonstration.

1. si $x \in E$, alors $x \in \overline{x}$ donc tout élément de E appartient à une classe d'équivalence, et on a un recouvrement ;
2. si $x, y \in E$ tels que $\overline{x} \neq \overline{y}$. Montrons que $\overline{x} \cap \overline{y} = \emptyset$. Par l'absurde, si on avait $z \in \overline{x} \cap \overline{y}$, alors on aurait : $x\mathcal{R}z$ et $y\mathcal{R}z$. Donc, par symétrie et transitivité : $x\mathcal{R}y$, puis $\overline{x} = \overline{y}$, d'où la contradiction.

□

Remarque V.8. *On pouvait déjà vérifier que, par réflexivité, les classes d'équivalences sont non vides. En effet, si* $x \in E$*, alors* $x \in \overline{x}$.

Exemples V.9.

1. *La relation définie sur* E *par :* $x\mathcal{R}y \Leftrightarrow x = y$ *est une relation d'équivalence dont les classes sont les singletons de* E.
2. *Soit* $n \in \mathbb{N}^*$*. La relation définie sur* $\mathbb{Z}$ *par :* $x\mathcal{R}y \Leftrightarrow (x - y)$ *est un multiple de* n *est une relation d'équivalence, dont les classes sont appelée classes de congruences modulo* n*. Il y a* n *classes de congruences, à savoir* $\overline{0}, \overline{1}, \ldots, \overline{n-1}$*. On notera alors* $x \equiv y\,[n]$ *au lieu de* $x\mathcal{R}y$.
3. *Si* $\alpha \in \mathbb{R}^*$*, la relation de congruence modulo* α *sur* $\mathbb{R}$ *est la relation d'équivalence définie par :* $x\mathcal{R}y \Leftrightarrow (x - y)$ *est un multiple entier de* α*. Si* $x\mathcal{R}y$*, on notera alors :* $x \equiv y\,[\alpha]$.
4. *la relation d'équivalence dont les classes sont les* $[n; n+1[$ *est définie par :* $x\mathcal{R}y \Leftrightarrow \lfloor x \rfloor = \lfloor x \rfloor y$*. Plus généralement, si* f *est une fonction définie sur un ensemble* E*, la relation définie par :* $x\mathcal{R}y \Leftrightarrow f(x) = f(y)$ *est une relation d'équivalence.*

V.3 Relations d'ordre

Définition V.10. *Une relation binaire $\mathcal{R}$ sur E est appelée* ***relation d'ordre*** *si elle est : réflexive, antisymétrique et transitive.*
On parlera d'ordre ***total*** *si : $\forall x, y \in E,\ x\mathcal{R}y$ ou $y\mathcal{R}x$. Dans le cas contraire, on parle d'ordre partiel.*

Remarque V.11. *On note souvent par $\preceq$ ou $\succeq$ les relations d'ordre, où les écritures $x \preceq y$ et $y \succeq x$ sont équivalentes.*

Exemples V.12.

1. *sur $\mathbb{R}$, la relation usuelle $\leq$ est un ordre total ;*
2. *sur $\mathbb{N}$, la relation de divisibilité est une relation d'ordre partiel ;*
3. *si E est un ensemble quelconque, l'inclusion est une relation d'ordre sur $\mathcal{P}(E)$: elle est partielle si E contient au moins deux éléments.*

Définition V.13. *Soit E un ensemble muni d'une relation d'ordre $\leq$, et A une partie de E :*

1. *on dit qu'un élément M de E est un* ***majorant*** *de A si : $\forall a \in A,\ a \leq M$; on dit alors que E est* ***majorée*** *;*
2. *on dit qu'un élément m de E est un* ***minorant*** *de A si : $\forall a \in A,\ m \leq a$; on dit alors que E est* ***minorée****.*

Si E est majorée et minorée, on dit qu'elle est ***bornée****.*

Exemples V.14.

1. *pour $\mathbb{N}$ muni de la relation de divisibilité : 1 est un minorant (car tout entier est divisible par 1), tandis que 0 est un majorant (tout entier est un multiple de 0) ;*
2. *pour $\mathcal{P}(E)$ muni de l'inclusion : $\emptyset$ est un minorant et E est un majorant.*
3. *pour $\mathbb{R}$ muni de l'ordre $\leq$: il n'y a ni majorant ni minorant. En revanche on peut trouver des sous-parties majorées ou minorées. Par exemple $\mathbb{N}$ est une sous-partie minorée de $\mathbb{R}$, mais elle n'est pas majorée.*

Proposition-Définition V.15. *Avec les mêmes notations :*

1. *si $a \in A$ est un majorant de A, on l'appelle* ***maximum*** *(ou plus grand élément) de A, et il est unique ; on note $a = \max(A)$;*
2. *si $a \in A$ est un minorant de A, on l'appelle* ***minimum*** *(ou plus petit élément) de A, et il est unique ; on note $a = \min(A)$.*

Démonstration. Montrons l'unicité du maximum. Soient $a, a' \in A$ deux maximums :
— $a' \in A$ et a est un majorant de A donc : $a' \leq a$;
— $a \in A$ et a' est un majorant de A donc : $a \leq a'$.
Par antisymétrie, on a donc $a = a'$, d'où l'unicité. □

Remarque V.16. *L'unicité du maximum ou du minimum est* ***sous-réserve d'existence****. Par exemple sur $\mathbb{R}$, l'ensemble $]0;1[$ admet bien un minorant et un majorant, mais pas de maximum ni de minimum.*

Exemple V.17. *Sur $(\mathbb{R}, \leq)$, considérons l'intervalle $[-1;1[$. Il admet :*
— *comme minorant tout réel de $]-\infty;-1]$ et -1 comme minimum ;*
— *comme majorant tout réel de $[1;+\infty[$ mais pas de maximum.*
Montrons plus en détail le dernier point. Supposons par l'absurde que a soit un maximum de $[-1;1[$.
Comme $a \in [-1;1[$, alors : $-1 \leq a < 1$, donc :$0 \leq \frac{a+1}{2} < 1$.
Ainsi, $b = \frac{1+a}{2}$ est dans $[-1;1[$. Mais, comme a est un majorant de $[-1;1[$, on a donc : $b \leq a$.
Or, on a : $b \leq a \Leftrightarrow \frac{a+1}{2} \leq a \Leftrightarrow 1 \leq a$.
Donc on ne peut avoir $b \leq a$, d'où la contradiction.

Exemple V.18. *Sur* $(\mathbb{N}, |)$ *: l'ensemble* $\{2; 3; 6\}$ *admet :*
- *comme minorant uniquement* 1*, mais pas de minimum ;*
- *comme majorant tout multiple de* 6*, et* 6 *comme maximum.*

Théorème V.19. *Toute partie non vide de* $\mathbb{N}$ *possède un minimum.*

Démonstration. On procède par contraposée : soit A une partie de $\mathbb{N}$ ne possédant pas de minimum ; montrons alors que A est vide.
Par récurrence sur $n \in \mathbb{N}$, montrons que $n \notin A$:
- initialisation : $0 \notin A$, car sinon ce serait le plus petit élément de A ;
- hérédité : soit $n \in \mathbb{N}$ tel que aucun des entiers de $[\![0; n]\!]$ ne soit dans A. Alors $n+1 \notin A$, car sinon ce serait le plus petit élément de A.

D'où la récurrence, ce qui conclut la preuve. □

Remarque V.20. *En fait, ce résultat repose sur le principe de récurrence, qu'on a admis, mais on pourrait procéder dans l'autre sens : on admet ce théorème (on le pose comme un* ***axiome****), et on peut montrer alors que le principe de récurrence est vrai.*

Proposition V.21. *Toute partie non vide et majorée de* $\mathbb{N}$ *possède un plus grand élément.*

Démonstration. Soit A une partie non vide majorée de $\mathbb{N}$.
Alors l'ensemble $B = \{n \in n \,|\, \forall a \in A, a \leq n\}$ est une partie non vide de $\mathbb{N}$, donc possède un plus petit élément b.
Comme $b - 1 \notin B$, alors on a deux possibilités :
- soit $b - 1 \notin \mathbb{N}$: et donc $b = 0$, donc $A = \{0\}$ qui admet 0 comme maximum ;
- soit il existe $a \in A$ tel que : $b - 1 < a$. Et donc $a \geq b$. Mais, par définition de b, on a $a \leq b$, et donc $a = b$. Donc $b \in A$ et b est un majorant de A : c'est le maximum de A.

□

Corollaire V.22. *Toute partie non vide et majorée de* $\mathbb{Z}$ *possède un plus grand élément.*

Démonstration. Soit A un tel ensemble.
Si $A \cap \mathbb{N} \neq \emptyset$, alors le maximum de $A \cap \mathbb{N}$ convient.
Sinon, l'ensemble $-A = \{-a \,|\, a \in A\}$ est une partie non vide de $\mathbb{N}$, donc possède un minimum b. Et $-b$ convient. □

Chapitre 5

Applications

I Notion d'application

Définition I.1. *Si E, F sont deux ensembles, une **application** f de E vers F est la donnée, pour tout élément x de E, d'un **unique** élément y de F, que l'on note $f(x)$.*
On note alors l'application f par :

$$f : \left\{ \begin{array}{ccc} E & \to & F \\ x & \mapsto & f(x) \end{array} \right. \quad \text{ou } E \xrightarrow{f} F.$$

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

Proposition-Définition I.2. *Étant donnnée $f \in \mathcal{F}(E, F)$, on définit son **graphe** comme l'ensemble :*

$$\Gamma = \{(x, y) \in E \times F \mid f(x) = y\}.$$

Le graphe vérifie l'assertion :

$$\forall x \in E,\ \exists! y \in F,\ (x, y) \in \Gamma.$$

Et tout sous-ensemble de $E \times F$ vérifiant cette assertion définit une unique application de E dans F (autrement dit, une application est entièrement déterminée par son graphe).

Exemple I.3. *On considère l'application f de $\{A; B; C\}$ sur $\{a; b; c\}$ définie par : $f(A) = b$, $f(B) = a$ et $f(C) = b$. On peut représenter f par un diagramme sagittaire, ou par un diagramme cartésien :*

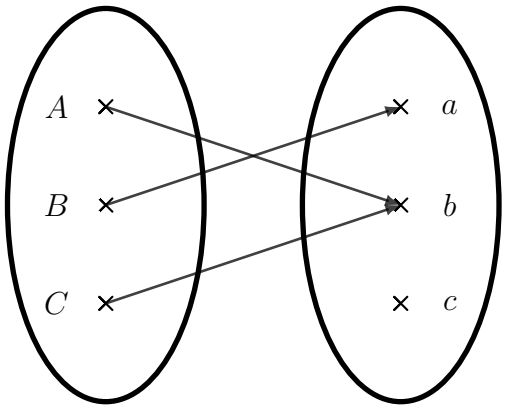


Diagramme sagittaire.

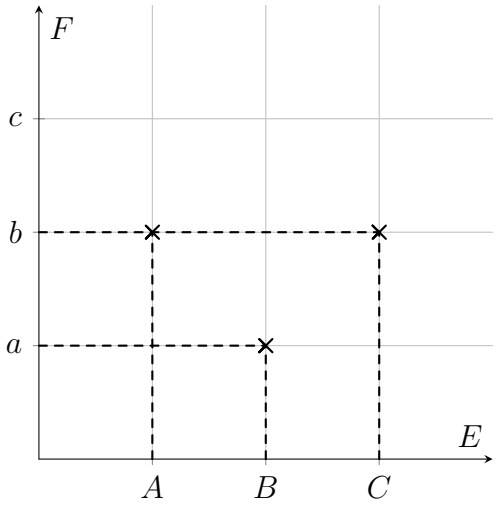


Diagramme cartésien.

Remarque I.4. *Une (même) application peut être définie de différentes manières. Par exemple, la fonction valeur absolue peut être définie sur $\mathbb{R}$:*

1. *explicitement :* $|x| = \sqrt{x^2}$;
2. *par disjonction de cas :* $|x| = \begin{cases} x & si\ x \geq 0 \\ -x & sinon \end{cases}$;
3. *implicitement :* $|x|$ *est l'unique solution positive ou nulle de l'équation :* $y^2 = x^2$.

Définition I.5. *Soit E un ensemble.*
On appelle application ***identité*** *de E l'application de E dans E définie par $x \mapsto x$, et on la note Id_E.*
Si A est une partie de E, on définit la ***fonction indicatrice*** *de A comme l'application de E dans $\{0;1\}$, notée $\mathbb{1}_A$, et définie par :*

$$\mathbb{1}_A : x \mapsto \begin{cases} 0 & si \quad x \notin A \\ 1 & si \quad x \in A \end{cases}$$

Proposition I.6. *Soit E un ensemble et A, B deux parties de E :*

1. $\mathbb{1}_{A\cap B} = \mathbb{1}_A \cdot \mathbb{1}_B$;
2. $\mathbb{1}_{\overline{A}} = 1 - \mathbb{1}_A$;
3. $\mathbb{1}_{A\cap B} = \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_{A\cup B}$.
4. $A \subset B \Leftrightarrow \mathbb{1}_A \leq \mathbb{1}_B$.

Démonstration. Par disjonction de cas. □

Définition I.7. *Si $f : E \to F$ est une application, et $(x, y) \in E \times F$ tel que $f(x) = y$. On dit que :*

1. *y est* ***l'image*** *de x par f ;*
2. *x est* ***un antécédent*** *de x par f*

Remarque I.8. *L'image d'un élément de E est toujours unique. En revanche, un élément de F peut très bien ne posséder aucun antécédent, ou un seul, ou même une infinité.*

Définition I.9. *Si E et I sont des ensembles, on appelle* ***famille*** *d'éléments de E indexés par I une application x de I sur E. On notera alors x_i pour désigner $x(i)$. Et la famille x sera notée $(x_i)_{i\in I}$.*

Exemple I.10. *Une suite réelle $(u_n)_{n\in\mathbb{N}}$ est une famille de réels indexés par $\mathbb{N}$.*

Définition I.11. *Si $f \in \mathcal{F}(E, F)$, et A une partie non vide de E, on définit la* ***restriction*** *de f à A comme l'application de A sur F coïncidant avec f, c'est-à-dire :*

$$f|_A : \begin{cases} A & \to & F \\ x & \mapsto & f(x) \end{cases}.$$

Inversement, si $f \in \mathcal{F}(E, F)$ et $g \in \mathcal{F}(A, F)$ vérifient que $f|_A = g$, on dit que f est un ***prolongement*** *de g.*
Enfin, si B est une partie de F telle que f est à valeurs dans B, on appelle ***corestriction*** *comme l'application de E sur B coïncidant avec f, c'est-à-dire :*

$$f|^B : \begin{cases} E & \to & B \\ x & \mapsto & f(x) \end{cases}.$$

Définition I.12. *Si E, F, G sont trois ensembles, $f \in \mathcal{F}(E, F)$ et $g \in \mathcal{F}(F, G)$, on définit la* ***composée*** *de g et f, notée $g \circ f$, comme l'application de E dans G définie par :*

$$\forall x \in E,\ (g \circ f)(x) = g\left(f(x)\right).$$

Remarque I.13. *Si $f \in \mathcal{F}(E, E)$ et $n \in \mathbb{N}$, on notera $f^n = \underbrace{f \circ f \circ \cdots \circ f}_{n\ fois}$ (avec la convention que $f^0 = \mathrm{id}_E$).*

Proposition I.14. *La composition est* ***associative*** *: si $f \in \mathcal{F}(E, F)$, $g \in \mathcal{F}(F, G)$ et $h \in \mathcal{F}(G, H)$, alors : $(h \circ g) \circ f = h \circ (g \circ f)$.*

II Image directe et image réciproque

Définition II.1. *Soit $f \in \mathcal{F}(E,F)$, A une partie de E et B une partie de F.*

1. *On appelle* ***image directe*** *de A l'ensemble :*

$$f(A) = \{f(x) \,|\, x \in A\}.$$

2. *On appelle* ***image réciproque*** *de B l'ensemble :*

$$f^{-1}(B) = \{x \in E \,|\, f(x) \in B\}.$$

Remarque II.2. *Les images directes et réciproques correspondent aux assertions suivantes :*

$$y \in f(A) \Leftrightarrow \exists x \in A,\ f(x) = y$$

$$x \in f^{-1}(B) \Leftrightarrow f(x) \in B$$

Définition II.3. *Si $f \in \mathcal{F}(E,F)$, on appelle* ***image*** *de f, notée $\mathrm{Im}(f)$, l'image directe de E par f :*

$$\mathrm{Im}(f) = f(E) = \{f(x) \,|\, x \in E\}.$$

Si $\mathrm{Im}(f) \subset B$, pour une partie B de F, on dira que f est ***à valeurs*** *dans B.*

Remarque II.4. *On n'a pas toujours $f(E) = F$, en revanche on a toujours $f^{-1}(F) = E$.*

Exemples II.5. *Soit $f : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^2 \end{array} \right.$. Alors :*

1. $f([0;1]) = [0;1]$;
2. $f(]-1;2]) = [0;4]$;
3. $f^{-1}([0;2]) = [-\sqrt{2};\sqrt{2}]$;
4. $f^{-1}([-4;1]) = [-1;1]$;
5. $f^{-1}(\{9\}) = \{-3;3\}$;
6. $f^{-1}(]-12;-1]) = \emptyset$.

Définition II.6. *Si $f \in \mathcal{F}(E,F)$ et $A \subset E$, on dira que A est* ***stable*** *par f si $f(A) \subset A$.*

Proposition II.7. *Soient $f \in \mathcal{F}(E,F)$, A, B deux parties de E et C, D deux parties de F. Alors :*

1. $A \subset B \Rightarrow f(A) \subset f(B)$;
2. $f(A \cup B) = f(A) \cup f(B)$;
3. $f(A \cap B) \subset f(A) \cap f(B)$ (***Attention :*** *on n'a pas égalité en général)*
4. $C \subset D \Rightarrow f^{-1}(C) \subset f^{-1}(D)$;
5. $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$;
6. $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$;
7. $f^{-1}(C - D) = f^{-1}(C) - f^{-1}(D)$.

Démonstration. 1. Supposons que $A \subset B$:

$$\begin{array}{rcl} y \in f(A) & \Rightarrow & \exists x \in A,\ f(x) = y \\ & \Rightarrow & \exists x \in B,\ f(x) = y \\ & \Rightarrow & y \in f(B) \end{array}$$

Donc $f(A) \subset f(B)$.

2. Montrons les deux inclusions :
   (a) $f(A \cup B) \subset f(A) \cup f(B)$:

$$\begin{array}{rcl} y \in f(A \cup B) & \Rightarrow & \exists x \in A \cup B,\ f(x) = y \\ & \Rightarrow & \left\{ \begin{array}{l} \exists x \in A, \quad f(x) = y \\ \text{ou } \exists x \in B, \quad f(x) = y \end{array} \right. \\ & \Rightarrow & \left\{ \begin{array}{l} y \in f(A) \\ \text{ou } y \in f(B) \end{array} \right. \\ & \Rightarrow & y \in (f(A) \cup f(B)) \end{array}$$

   (b) $f(A) \cup f(B) \subset f(A \cup B)$: On applique le résultat précédent à $A \subset (A \cup B)$ et $B \subset (A \cup B)$. On a donc : $f(A) \subset f(A \sup B)$ et $f(B) \subset f(A \cup B)$, et donc : $f(A) \cup f(B) \subset f(A \cup B)$.

3. soit $y \in f(A \cap B)$. Alors il existe $x \in A \cap B$ tel que $y = f(x)$. Mais :
   — comme $x \in A$: alors $y \in f(A)$;
   — comme $x \in B$: alors $y \in f(B)$.
   Et donc $y \in f(A) \cap f(B)$, ce qui prouve l'inclusion. L'autre inclusion est fausse en général, comme le montre la remarque qui suit, donc il n'est pas nécessaire de s'y attarder.

4. Supposons que $C \subset D$:

$$\begin{array}{rcl} x \in f^{-1}(C) & \Rightarrow & f(x) \in C \\ & \Rightarrow & f(x) \in D \\ & \Rightarrow & x \in f^{-1}(D) \end{array}$$

   Donc $f^{-1}(C) \subset f^{-1}(D)$.

5. Procédons par équivalences :

$$\begin{array}{rcl} x \in f^{-1}(C \cup D) & \Leftrightarrow & f(x) \in C \cup D \\ & \Leftrightarrow & \left\{ \begin{array}{l} f(x) \in C \\ \text{ou } f(x) \in D \end{array} \right. \\ & \Leftrightarrow & \left\{ \begin{array}{l} x \in f^{-1}(C) \\ \text{ou } x \in f^{-1}(D) \end{array} \right. \\ & \Leftrightarrow & x \in (f^{-1}(C) \cup f^{-1}(D)) \end{array}$$

6. Procédons par équivalences :

$$\begin{array}{rcl} x \in f^{-1}(C \cap D) & \Leftrightarrow & f(x) \in C \cap D \\ & \Leftrightarrow & \left\{ \begin{array}{l} f(x) \in C \\ \text{et } f(x) \in D \end{array} \right. \\ & \Leftrightarrow & \left\{ \begin{array}{l} x \in f^{-1}(C) \\ \text{et } x \in f^{-1}(D) \end{array} \right. \\ & \Leftrightarrow & x \in (f^{-1}(C) \cap f^{-1}(D)) \end{array}$$

7. Procédons par équivalences :

$$\begin{array}{rcl} x \in f^{-1}(C - D) & \Leftrightarrow & f(x) \in C - D \\ & \Leftrightarrow & \left\{ \begin{array}{l} f(x) \in C \\ \text{et } f(x) \notin D \end{array} \right. \\ & \Leftrightarrow & \left\{ \begin{array}{l} x \in f^{-1}(C) \\ \text{et } x \notin f^{-1}(D) \end{array} \right. \\ & \Leftrightarrow & x \in (f^{-1}(C) - f^{-1}(D)) \end{array}$$

□

Remarque II.8. *La plupart des implications précédentes sont en fait des équivalences, et donc les quelques raisonnements par double inclusion pourraient se traiter par équivalence.*
Il faut tout de même faire attention aux quantificateurs qui ne passent pas toujours très bien aux équivalences, comme justement au point 3 où l'implication suivante n'est pas une équivalence :

$$[\exists x \in A \cap B,\ f(x) = y] \Rightarrow \left\{ \begin{array}{rl} \exists x \in A, & f(x) = y \\ et\ \exists x \in B, & f(x) = y \end{array} \right. .$$

Remarque II.9. *Pour le cas d'inclusion seule, on peut reprendre* $f : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^2 \end{array} \right.$ *. Avec* $A = \mathbb{R}_-^*$ *et* $B = \mathbb{R}_+^*$*, on a* $f(A) = f(B) = \mathbb{R}_+^*$*, et donc :*

$$f(A \cap B) = f(\emptyset) = \emptyset \text{ et } f(A) \cap f(B) = \mathbb{R}_+^*.$$

III Injections, surjections, bijections

Définition III.1. *Soit* $f \in \mathcal{F}(E, F)$*. On dit que* f *est :*

1. ***injective*** *si tout élément de* F *admet* ***au plus*** *un antécédent par* f *;*
2. ***surjective*** *si tout élément de* F *admet* ***au moins*** *un antécédent par* f *;*
3. ***bijective*** *si elle est injective et surjective, c'est-à-dire si tout élément de* F *admet* ***un unique*** *antécédent par* f*.*

Proposition III.2. *Si* $f \in \mathcal{F}(E, F)$*, on a équivalence entre :*

1. f *est injective ;*
2. $\forall x, y \in E,\ x \neq y \Rightarrow f(x) \neq f(y)$ *;*
3. $\forall x, y \in R,\ f(x) = f(y) \Rightarrow x = y$*.*

Proposition III.3. *De même, on a équivalence entre :*

1. f *est surjective ;*
2. $\mathrm{Im}(f) = F$ *;*
3. $\forall y \in F,\ \exists x \in E,\ f(x) = y$*.*

Proposition-Définition III.4. *L'application* $f \in \mathcal{F}(E, F)$ *est bijective si, et seulement si, elle vérifie :*

$$\forall y \in F,\ \exists! x \in E,\ f(x) = y.$$

*On peut alors définir l'****application réciproque*** *de* f*, notée* f^{-1}*, qui est l'unique application définie par :*

$$f^{-1} : \left\{ \begin{array}{ccl} F & \to & E \\ y & \mapsto & x \text{ l'unique antécédent de } y \text{ par } f \end{array} \right. .$$

Et on a alors : $f \circ f^{-1} = \mathrm{id}_F$*,* $f^{-1} \circ f = \mathrm{id}_E$*, et* f^{-1} *est bijective avec* $(f^{-1})^{-1} = f$*.*

Exemples III.5.

1. *la fonction* $\mathrm{id}_E : E \to E$ *est bijective, d'inverse elle-même ;*
2. *si* $a, b \in \mathbb{R}$*, la fonction* $f : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & ax + b \end{array} \right.$ *est bijective si, et seulement si,* $a \neq 0$*, et son inverse est alors la fonction définie sur* $\mathbb{R}$ *par :* $f^{-1}(y) = \frac{y-b}{a}$*. On a en fait le résultat plus fort suivant :*

$$a \neq 0 \Leftrightarrow f \text{ injective} \Leftrightarrow f \text{ surjective} \Leftrightarrow f \text{ surjective.}$$

Pour le montrer, on peut voir que toutes les assertions sont équivalentes au fait que $a \neq 0$ *:*

— *si $a \neq 0$: alors f est bijective (on a même donné sa réciproque précédemment), donc f est injective et surjective ;*
— *si $a = 0$: alors :*
  — *$f(\mathbb{R}) = \{b\} \neq \mathbb{R}$ donc f n'est pas surjective ;*
  — *$f(0) = b = f(1)$ donc f n'est pas injective.*
  et ainsi f n'est ni surjective ni injective, et ne peut donc pas être bijective.

Proposition III.6. *Soient $f \in \mathcal{F}(E, F)$ et $g \in \mathcal{F}(E, F)$. Alors :*

1. *si $g \circ f$ est injective, alors f est injective ;*
2. *si $g \circ f$ est surjective, alors g est surjective.*

Démonstration. 1. si $x, y \in E$, alors :

$$f(x) = f(y) \Rightarrow g(f(x)) = g(f(y)) \Rightarrow g \circ f(x) = g \circ f(y) \Rightarrow x = y$$

donc f est injective ;

2. soit $z \in G$. Il existe $x \in E$ tel que : $z = g \circ f(x) = g\,(f(x))$, donc $y = f(x) \in F$ vérifie $g(y) = z$. Donc g est surjective.

□

Théorème III.7. *Soit $f \in \mathcal{F}(E, F)$. Alors f est bijective si, et seulement si, il existe une application $g : F \to E$ telle que $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$.*
Dans ces conditions, on a : $g = f^{-1}$.

Démonstration. On montre séparément les deux implications :
— nécessité : si f est bijective, alors l'application $g = f^{-1}$ convient ;
— suffisance : si un tel g existe, alors :
  — $g \circ f = \mathrm{id}_E$ est injective, donc f aussi ;
  — $f \circ g = \mathrm{id}_F$ est surjective, donc f aussi.
  Donc f est bijective. Comme $g \circ f = \mathrm{id}_E$, alors : $g \circ f \circ f^{-1} = f^{-1}$, donc $g = f^{-1}$.

□

Proposition III.8. *Soient $f \in \mathcal{F}(E, F)$ et $g \in \mathcal{F}(F, G)$. Alors :*

1. *si f et g sont injectives, alors $g \circ f$ est injective ;*
2. *si f est g sont surjectives, alors $g \circ f$ est surjective ;*
3. *si f et g sont bijectives, alors $g \circ f$ est bijective, et : $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Démonstration. 1. si $x, y \in E$, alors :

$$g \circ f(x) = g \circ f(y) \Rightarrow g(f(x)) = g(f(y)) \Rightarrow f(x) = f(y) \Rightarrow x = y$$

2. si $z \in G$, il existe $y \in F$ tel que $g(y) = z$. De même, il existe $x \in E$ tel que $f(x) = y$. Et donc : $z = g \circ f(x)$.
3. Posons $h = f^{-1} \circ g^{-1}$. Alors :
  — $h \circ (g \circ f) = f^{-1} \circ g^{-1} \circ g \circ f = f^{-1} \circ f = \mathrm{id}_E$;
  — $(g \circ f) \circ h = g \circ f \circ f^{-1} \circ g^{-1} = g \circ g^{-1} = \mathrm{id}_G$
  ce qui donne bien le résultat.

□

Exemples III.9. 1. *Si E est un ensemble, l'application $f : \left\{ \begin{array}{ccc} \mathcal{P}(E) & \to & \mathcal{P}(E) \\ A & \mapsto & \overline{A} \end{array} \right.$ est une bijection dont c'est la propre réciproque. On dit que f est **involutive**.*
2. *Si E est un ensemble, l'application $f : \left\{ \begin{array}{ccc} \mathcal{P}(E) & \to & \mathcal{F}(E, \{0;1\}) \\ A & \mapsto & \mathbb{1}_A \end{array} \right.$ est une bijection, dont la réciproque est donnée par : $f^{-1} : \left\{ \begin{array}{ccc} \mathcal{F}(E, \{0;1\}) & \to & \mathcal{P}(E) \\ \chi & \mapsto & \chi^{-1}(\{1\}) \end{array} \right.$.*

IV Les ensembles finis

Lemme IV.1. *Soient $n, m \in \mathbb{N}^*$ et $f : [\![1; n]\!] \to [\![1; m]\!]$. Alors :*

1. *si f est injective, alors $n \leq m$;*
2. *si f est surjective, alors $n \geq m$;*
3. *si f est bijective, alors $n = m$.*

Démonstration.

1. si f est injective : $f(1), f(2), \ldots, f(n)$ sont des entiers distincts de $[\![1; m]\!]$ donc $n \leq m$;
2. si f est surjective : $f(1), f(2), \ldots, f(n)$ constituent les m entiers de $[\![1; m]\!]$, donc $n \geq m$.
3. découle des deux premiers points.

□

Définition IV.2. *On dit qu'un ensemble E est **fini** s'il existe un entier $n \in \mathbb{N}$ et une bijection $f : [\![1; n]\!] \to E$. On dit alors que E est de **cardinal** n, que l'on note :* $\mathrm{Card}(E) = n$ *ou* $|E| = n$.

Proposition IV.3. *Le cardinal d'un ensemble fini est **unique**.*

Démonstration. Découle du lemme. □

Proposition IV.4. *Si E et F sont deux ensembles. Si E est fini, et qu'il existe une bijection entre E et F, alors F est fini de même cardinal que E.*

Démonstration. Notons $n = \mathrm{Card}(E)$ et donnons-nous $f : E \to [\![1; n]\!]$ et $g : E \to F$ bijectives. Alors $g \circ f$ est une bijection de $[\![1; n]\!]$ sur F, donc F est fini de cardinal n. □

Proposition IV.5. *Soit E un ensemble fini, et F une partie de E. Alors F est fini, avec* $\mathrm{Card}(F) \leq \mathrm{Card}(E)$.
De plus, si $\mathrm{Card}(E) = \mathrm{Card}(F)$, *alors $E = F$.*

Démonstration. On procède par récurrence sur $n = \mathrm{Card}(E) \in \mathbb{N}$:

- (initialisation) si $n = 0$: alors E est vide, donc F aussi, et on a bien le résultat ;
- (hérédité) soit $n \in \mathbb{N}^*$, et supposons le résultat acquis pour tous les ensembles finis de cardinal au plus $n - 1$:
  - si $F = E$: alors F est fini, avec $\mathrm{Card}(F) = \mathrm{Card}(E)$;
  - si $F \neq E$: comme $F \subset E$, il existe $x \in E \setminus F$. Considérons $f : [\![1; n]\!] \to E$ bijective, et notons $k \in [\![A; n]\!]$ l'antécédent de x par f. Construisons la fonction g suivante :

$$\begin{array}{rcl} g : [\![1; n-1]\!] & \to & E \setminus \{x\} \\ i & \mapsto & \left\{ \begin{array}{l} f(i) \text{ si } i < k \\ f(i+1) \text{ si } i \geq k \end{array} \right. \end{array}$$

    qui est construite à partir de f en "retirant" k ainsi que son image.
    L'application g est bijective puisque :
  - elle est injective : puisque f l'est ; en effet, si $i, j \in [\![1; n-1]\!]$ tels que $g(i) = g(j)$, alors :
    - si $i, j < k$: $g(i) = f(i)$ et $g(j) = f(j)$, donc $f(i) = f(j)$, donc $i = j$ (par injectivité) ;
    - si $i < k$ et $j \geq k$: $g(i) = f(i)$ et $g(j) = f(j+1)$, alors $f(i) = f(j+1)$ puis $i = j + 1$, ce qui est impossible car : $i < k$ et $j + 1 > k$; donc ce cas est impossible ;
    - si $j < k$ et $i \geq k$: on montre de même que ce cas est impossible ;
    - si $i, j \geq k$: alors on trouve $f(i+1) = f(j+1)$, donc $i + 1 = j + 1$, donc $i = j$.

    ce qui assure bien l'injectivité ;
  - elle est surjective : soit $y \in E \setminus \{x\}$. Alors $y \in E$, donc y possède un unique antécédent par f dans $[\![1; n]\!]$, que l'on note i. Comme $f(k) = x \neq y$, alors $i \neq k$. Et ainsi :

— si $i < k$: alors $f(i) = g(i) = y$;
— si $i > k$: alors $f(i) = g(i-1) = y$.
ce qui assure bien la surjectivité.
D'où la bijectivité. Donc $E \setminus \{x\}$ est fini de cardinal $n-1$.
Comme $x \notin F$, alors $F \subset E \setminus \{x\}$: par récurrence on déduit donc que F est fini, de cardinal au plus $n-1$. Et ainsi, si $F \neq E$, on a bien $\mathrm{Card}(F) < \mathrm{Card}(E)$.
ce qui conclut l'hérédité.
D'où la récurrence. □

Proposition IV.6. *Soit E un ensemble. On a équivalence entre les propriétés suivantes :*

1. *E est fini ;*
2. *il existe une **surjection** d'un ensemble fini F vers E ;*
3. *il existe une **injection** de E vers un ensemble fini F.*

De plus, dans les deux derniers cas on a : $\mathrm{Card}(E) \leq \mathrm{Card}(F)$.

Démonstration. Découle du point précédent, en choisissant des restrictions et correstrictions adaptées. □

Proposition IV.7. *Si A et B sont deux ensembles finis disjoints, alors $A \cup B$ est fini, avec :* $\mathrm{Card}(A \cup B) = \mathrm{Card}(A) + \mathrm{Card}(B)$.
Plus généralement :

1. *si $A_1, \ldots, A_n$ sont des ensembles finis deux-à-deux disjoints, alors $A_1 \cup \cdots \cup A_n$ est fini avec :* $\mathrm{Card}(A_1 \cup \cdots \cup A_k) = \mathrm{Card}(A_1) + \cdots + \mathrm{Card}(A_n)$;
2. *si A et B sont finis, alors $A \cup B$ et $A \cap B$ sont finis avec :* $\mathrm{Card}(A \cup B) = \mathrm{Card}(A) + \mathrm{Card}(B) - \mathrm{Card}(A \cap B)$.

Démonstration. Posons $n = \mathrm{Card}(A)$ et $m = \mathrm{Card}(B)$, et prenons deux bijections $f : [\![1; n]\!] \to A$, $g : [\![1; m]\!] \to B$.
On définit alors la bijection :

$$h : \left\{ \begin{array}{ccc} [\![1; n+m]\!] & \to & A \cup B \\ i & \mapsto & \left\{ \begin{array}{ll} f(i) & \text{si } i \leq n \\ g(i-n) & \text{si } i > n \end{array} \right. \end{array} \right. .$$

Ce qui donne le premier résultat.
Le deuxième résultat se montre par récurrence sur n.
Le dernier résultat en découle, à l'aide des unions disjointes : $A \cup B = A \cup (B \setminus A \cap B)$ et $B = (A \cap B) \cup (B \setminus A \cap B)$. □

Corollaire IV.8. *Si E est fini et $A \subset E$, alors $\overline{A}$ est fini avec :* $\mathrm{Card}(\overline{A}) = \mathrm{Card}(E) - \mathrm{Card}(A)$.
Plus généralement, si $A, B \subset E$, alors $A \setminus B$ est fini avec : $\mathrm{Card}(A \setminus B) = \mathrm{Card}(A) - \mathrm{Card}(A \cap B)$.

Proposition IV.9. *Si E et F sont des ensembles finis, alors $E \times F$ est fini, et :* $\mathrm{Card}(E \times F) = \mathrm{Card}(E) \times \mathrm{Card}(F)$.

Démonstration. Notons $n = \mathrm{Card}(E)$, et $m = \mathrm{Card}(F)$ avec $F = \{y_1, \ldots, y_m\}$.
On pose pour $i \in [\![1; m]\!]$: $E_i = \{(x, y_i) \,|\, x \in E\}$.
Alors :
— chaque E_i est en bijection avec E, et est donc fini de cardinal n ;
— les E_i sont deux-à-deux disjoints ;
— $E \times F = \cup_{i \in [\![1;m]\!]} E_i$.
Donc $\mathrm{Card}(E \times F) = \mathrm{Card}(E_1) + \cdots + \mathrm{Card}(E_m) = \underbrace{n + \cdots + n}_{m \text{ fois}} = n \times m$. □

Proposition IV.10. *Soient E, F deux ensembles finis, et f une application de E vers F :*

1. *si f est **injective**, alors* $\mathrm{Card}(E) \leq \mathrm{Card}(F)$ *;*
2. *si f est **surjective**, alors* $\mathrm{Card}(E) \geq \mathrm{Card}(F)$ *;*
3. *si f est **bijective**, alors* $\mathrm{Card}(E) = \mathrm{Card}(F)$.

Démonstration. 1. la corestriction de f à $f(E)$ fournit une bijection de E vers une partie de F ;

2. l'application qui à tout élément de F lui associe un antécédent dans E par F est une injection de E sur F ;
3. évident.

□

Théorème IV.11. *Soient E, F de ensembles finis de même cardinal, et $f : E \to F$. On a équivalence entre :*

1. *f injective ;*
2. *f surjective ;*
3. *f bijective.*

Démonstration. Posons $n = \mathrm{Card}(E) = \mathrm{Card}(F)$, et notons $g : [\![1; n]\!] \to F$ bijective, de sorte que $F = \{g(1), \ldots, g(n)\}$.
Notons pour tout $i \in [\![1; n]\!] : E_i = f^{-1}(\{g(i)\})$ (l'ensemble des antécédents de $g(i)$) et $e_i = |E_i|$ (le nombre d'antécédents de $g(i)$). Alors les E_i :

— sont deux-à-deux disjoints : si $x \in E_i \cap E_j$, alors $f(x) = g(i) = g(j)$, donc par injectivité de g on a $i = j$;
— forment un recouvrement de E : si $x \in E$, par surjectivité de g il existe $i \in [\![1; n]\!]$ tel que $g(i) = f(x)$, et donc $x \in E_i$.

donc par cardinal d'une union on déduit que : $\mathrm{Card}(E) = \mathrm{Card}(E_1) + \cdots + \mathrm{Card}(E_n)$, c'est-à-dire :

$$n = e_1 + \cdots + e_n.$$

Posons pour tout i : $x_i = e_i - 1$. Alors : $x_1 + \cdots + x_n = 0$. Et ainsi :

$$(\forall i,\ x_i \leq 0) \Leftrightarrow (\forall i,\ x_i = 0) \Leftrightarrow (\forall i,\ x_i \geq 0)$$

ce qui traduit bien que :

$$f \text{ injective} \Leftrightarrow f \text{ bijective} \Leftrightarrow f \text{ surjective.}$$

□

Proposition IV.12. *Si E, F sont deux ensembles finis avec* $\mathrm{Card}(E) = n$ *et* $\mathrm{Card}(F) = m$*, alors $\mathcal{F}(E, F)$ est fini de cardinal m^n.*

Démonstration. On procède par récurrence sur n :

— si $n = 1$: il y a bien m applications ;
— supposons le résultat acquis pour un certain $n \geq 1$, et supposons que $|E| = n + 1$: on fixe $a \in E$, et on pose $E' = E \setminus \{a\}$. On considère l'application de restriction :

$$\begin{array}{rcl} \varphi : \mathcal{F}(E, F) & \to & \mathcal{F}(E', F) \\ f & \mapsto & f|_{E'} \end{array}$$

Tout élément de $\mathcal{F}(E', F)$ possède exactement m antécédents, qui correspondent aux m choix possibles pour $f(a)$. On a donc : $|\mathcal{F}(E, F)| = m \times |\mathcal{F}(E', F)| = m \times m^n = m^{n+1}$, ce qui conclut la récurrence.

□

Corollaire IV.13. *Si E est fini avec* $\mathrm{Card}(E) = n$*, alors $\mathcal{P}(E)$ est fini de cardinal 2^n.*

Démonstration. On considère l'application : $\varphi : \left\{ \begin{array}{ccc} \mathcal{P}(E) & \to & \mathcal{F}(E, \{0;1\}) \\ A & \mapsto & \mathbb{1}_A \end{array} \right.$. Alors φ est bijective :

— injectivité : si $\mathbb{1}_A = \mathbb{1}_B$ alors pour tout $x \in E$:

$$x \in A \Leftrightarrow \mathbb{1}_A(x) = 1 \Leftrightarrow \mathbb{1}_B(x) = 1 \Leftrightarrow x \in B.$$

— surjectivité : si $f \in \mathcal{F}(E, \{0;1\})$, alors : $f = \mathbb{1}_{f^{-1}(\{1\})}$.

Donc $\mathrm{Card}(\mathcal{P}(E)) = \mathrm{Card}(\mathcal{F}(E, \{0;1\})) = 2^n$. □

Chapitre 6

Sommes, produits et systèmes

I Les notations $\sum$ et $\prod$

Définition I.1. *Soient $I = \{i_1, \dots, i_n\}$ un ensemble fini, et $(a_i)_{i\in I}$ une famille de complexes indexée par I. On définit alors :*

1. *la **somme** de tous les éléments a_i, notée $\sum_{i\in I} a_i$, comme :*

$$\sum_{i\in I} a_i = a_{i_1} + \cdots + a_{i_n};$$

2. *le **produit** de tous les éléments a_i, notée $\prod_{i\in I} a_i$, comme :*

$$\prod_{i\in I} a_i = a_{i_1} \times \cdots \times a_{i_n}.$$

Si $I = [\![n; m]\!]$, pour $n \leq m$ deux entiers, on notera :

$$\sum_{i\in[\![n;m]\!]} a_i = \sum_{i=n}^{m} a_i \text{ et } \prod_{i\in[\![n;m]\!]} a_i = \prod_{i=n}^{m} a_i.$$

Remarque I.2. *Par convention, si $I = \emptyset$, on pose :*

$$\sum_{i\in I} a_i = 0 \text{ et } \prod_{i\in I} a_i = 1.$$

Exemples I.3.
1. $\sum_{k=2}^{5} k^3 = 2^3 + 3^3 + 4^3 + 5^3 = 224$;
2. $\prod_{k=2}^{5} k^3 = 2^3 \times 3^3 \times 4^3 \times 5^3 = 1\,728\,000$.

Remarques I.4. *Les indices qui apparaissent dans une somme n'existent que dans une somme, et leur dénomination est arbitraire. Ainsi :*

1. $k \times \sum_{k=3}^{12} a_k$ *n'est pas défini, mais* $\sum_{k=3}^{12} k \times a_k$ *l'est ;*
2. $\sum_{k=4}^{8} k^3 = \sum_{l=4}^{8} l^3 = 1260$.

Proposition I.5. *Avec les mêmes notations, si $a_i = \alpha$ ne dépend pas de $i \in I$, alors :*

$$\sum_{i\in I} \alpha = \alpha \times \mathrm{Card}(I) \text{ et } \prod_{i\in I} \alpha = \alpha^{\mathrm{Card}(I)}.$$

En particulier, si $n \leq m$ sont deux entiers :

$$\sum_{k=n}^{m} \alpha = (m-n+1)\alpha \text{ donc } \sum_{k=1}^{n} \alpha = n\alpha \text{ et } \sum_{k=0}^{n} \alpha = (n+1)\alpha$$

$$\prod_{k=n}^{m} \alpha = \alpha^{(m-n+1)} \text{ donc } \prod_{k=1}^{n} \alpha = \alpha^{n} \text{ et } \prod_{i=0}^{n} \alpha = \alpha^{n+1}.$$

Proposition I.6 (Relation de Chasles)**.** *Si I_1, I_2 sont deux ensembles disjoints, alors :*

$$\sum_{i \in I_1 \cup I_2} a_i = \sum_{i \in I_1} a_i + \sum_{i \in I_2} a_i \text{ et } \prod_{i \in I_1 \cup I_2} a_i = \prod_{i \in I_1} a_i \times \prod_{i \in I_2} a_i.$$

En particulier, si $n \leq m$ sont deux entiers :

$$\sum_{k=1}^{m} a_k = \sum_{k=1}^{n} a_k + \sum_{k=n+1}^{m} a_k \text{ et } \prod_{k=1}^{m} a_k = \prod_{k=1}^{n} a_k \times \prod_{k=n+1}^{m} a_k.$$

Remarque I.7. *Si I_1 et I_2 ne sont pas disjoints, on peut écrire :*

$$\sum_{i \in I_1 \cup I_2} a_i = \sum_{i \in I_1} a_i + \sum_{i \in I_2} a_i - \sum_{i \in I_1 \cap I_2} a_i \text{ et } \prod_{i \in I_1 \cup I_2} a_i = \frac{\prod_{i \in I_1} a_i \times \prod_{i \in I_2} a_i}{\prod_{i \in I_1 \cap I_2} a_i}.$$

Exemple I.8. *En partitionnant $[\![0; 2n-1]\!]$, on peut calculer : $\displaystyle\sum_{k=0}^{2n-1} \left\lfloor \frac{k}{2} \right\rfloor$. En effet, pour $k \in [\![0; 2n-1]\!]$:*

- *si k est pair : on écrit $k = 2i$, avec $i \in [\![0; n-1]\!]$, et alors : $\left\lfloor \frac{k}{2} \right\rfloor = \lfloor i \rfloor = i$;*
- *si k est impair : on écrit $k = 2j+1$, avec $j \in [\![0; n-1]\!]$, et alors : $\left\lfloor \frac{k}{2} \right\rfloor = \left\lfloor j + \frac{1}{2} \right\rfloor = j$.*

Et finalement :

$$\sum_{k=0}^{2n-1} \left\lfloor \frac{k}{2} \right\rfloor = \sum_{i=0}^{n-1} i + \sum_{j=0}^{n-1} j = 2 \cdot \sum_{i=0}^{n-1} i = 2 \cdot \frac{n(n-1)}{2} = n(n-1).$$

Proposition I.9 (Linéarité de la somme)**.** *Si $\lambda, \mu \in \mathbb{C}$, et $(a_i), (b_i)$ deux familles indexées par I fini :*

$$\sum_{i \in I} (\lambda a_i + \mu b_i) = \lambda \left(\sum_{i \in I} a_i \right) + \mu \left(\sum_{i \in I} b_i \right).$$

Remarque I.10. *Si $\lambda = \mu = 1$, ou si $\mu = 0$, ceci nous donne les cas particuliers :*

$$\sum_{i \in I} (a_i + b_i) = \left(\sum_{i \in I} a_i \right) + \left(\sum_{i \in I} b_i \right) \text{ et } \sum_{i \in I} (\lambda a_i) = \lambda \left(\sum_{i \in I} a_i \right).$$

Proposition I.11. *Avec les mêmes notations :*

1. $\prod_{i \in I} (a_i^\lambda \times b_i^\mu) = \left(\prod_{i \in I} a_i^\lambda \right) \times \left(\prod_{i \in I} b_i^\mu \right) = \left(\prod_{i \in I} a_i \right)^\lambda \times \left(\prod_{i \in I} b_i \right)^\mu$;
2. $\prod_{i \in I} (\lambda a_i) = \lambda^{\mathrm{Card}(I)} \left(\prod_{i \in I} a_i \right)$.

Remarque I.12. *Attention à l'exposant pour le produit !*

Proposition I.13 (Changement d'indice)**.** *Si I, J sont deux ensembles, $f : I \to J$ une bijection et $(a_j)_{j\in J}$ une famille de complexes indexée par J, alors :*

$$\sum_{j\in J} a_j = \sum_{i\in I} a_{f(i)}.$$

Inversement, si $(b_i)_{i\in I}$ est une famille de complexes indexée par I, alors :

$$\sum_{i\in J} b_i = \sum_{j\in J} b_{f^{-1}(j)}.$$

En particulier :

$$\sum_{j=n}^{m} a_j = \sum_{i=0}^{m-n} a_{i+n}.$$

Remarque I.14. *On a la même chose avec les produits.*

II Sommes classiques

Proposition II.1 (Sommes télescopiques)**.** *Si $n \leq m$ sont des entiers et $(a_i)_{i\in[\![n;m+1]\!]}$ est une famille de complexes alors :*

$$\sum_{k=n}^{m}(a_{k+1} - a_k) = a_{m+1} - a_n.$$

Si de plus les a_i sont non-nuls :

$$\prod_{k=n}^{m} \frac{a_{k+1}}{a_k} = \frac{a_{m+1}}{a_n}.$$

Exemples II.2. *Soit $n \in \mathbb{N}^*$, on a :*

1. *si $k \in [\![1; n]\!]$, alors : $\dfrac{1}{k} - \dfrac{1}{k+1} = \dfrac{1}{k(k+1)}$, et donc :*

$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = 1 - \frac{1}{n+1};$$

2. *si $k \in [\![1; n]\!]$, alors : $1 + \dfrac{1}{k} = \dfrac{k+1}{k}$, et donc :*

$$\prod_{k=1}^{n} \left(1 + \frac{1}{k}\right) = n + 1.$$

Proposition II.3 (Somme géométrique)**.** *Si q est un complexe et $n \in \mathbb{N}$, alors :*

$$\sum_{k=0}^{n} q^k = \begin{cases} \dfrac{1-q^{n+1}}{1-q} & \text{si } q \neq 1 \\ n+1 & \text{si } q = 1 \end{cases}.$$

Démonstration. Si $q = 1$, alors : $\sum_{k=0}^{n} q^k = \sum_{k=0}^{n} 1 = n + 1$.
Si $q \neq 1$, alors :

$$\begin{array}{rcl} (1-q) \times \sum_{k=0}^{n} q^k & = & \sum_{k=0}^{n}(q^k - q^{k+1}) \text{ par linéarité} \\ & = & 1 - q^{n+1} \text{ par télescopage} \end{array}$$

D'où le résultat. □

Corollaire II.4. *Si $q \neq 1$ est un complexe, $n \leq m$ deux entiers, et (a_k) est une suite **géométrique** de raison q (c'est-à-dire que pour tout entier k : $a_{k+1} = q \times a_k$), alors :*

$$\sum_{k=n}^{m} a_k = \frac{a_n - a_{m+1}}{1-q} = a_n \times \frac{1-q^{m-n+1}}{1-q} = (\textit{Premier terme}) \times \frac{1 - \textit{raison}^{\textit{nombre de termes}}}{1 - \textit{raison}}.$$

Démonstration. Une récurrence immédiate montre que, pour tout $k \in \mathbb{N}$: $a_{n+k} = a_n \times q^k$.
Le résultat découle par linéarité du point précédent. □

Proposition II.5 (Sommes arithmétiques)**.** *Soit $n \in \mathbb{N}$, alors :*

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}.$$

Démonstration. Par changement d'indice, on a : $\sum_{k=0}^{n} k = \sum_{l=0}^{n}(n-l)$. Et ainsi :

$$2 \times \sum_{k=0}^{n} k = \sum_{k=0}^{n} k + \sum_{k=0}^{n}(n-k) = \sum_{k=0}^{n} n = n(n+1)$$

ce qui donne le résultat voulu. □

Corollaire II.6. *Si r est un complexe, $n \leq m$ deux entiers, et (a_k) est une suite **arithmétique** de raison r (c'est-à-dire que pour tout entier k : $a_{k+1} = a_k + r$), alors :*

$$\begin{array}{rcl} \sum_{k=n}^{m} a_k & = & (m-n+1) \times a_n + \dfrac{(m-n)(m-n+1)}{2} \times r = \dfrac{a_n + a_m}{2} \times (m-n+1) \\ & = & \dfrac{\textit{Premier terme} + \textit{Dernier terme})}{2} \times \textit{nombre de termes} \end{array}.$$

Démonstration. Une récurrence immédiate montre que, pour tout $k \in \mathbb{N}$: $a_{n+k} = a_n + k \times r$.
Le résultat découle par linéarité du point précédent. □

Proposition II.7. *Si a, b sont deux complexes, et $n \in \mathbb{N}^*$, alors :*

$$\begin{array}{rcl} a^n - b^n & = & (a-b) \times (a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) \\ & = & (a-b) \times \sum_{k=0}^{n-1} a^{n-1-k}b^k = (a-b) \times \sum_{k=1}^{n} a^{n-k}b^{k-1} \end{array}.$$

Démonstration. On développe directement la somme :

$$\begin{array}{rcl} (a-b) \times \sum_{k=0}^{n-1} a^{n-1-k}b^k & = & \sum_{k=0}^{n-1}(a^{n-k}b^k - a^{n-k-1}b^{k+1}) \\ & = & \sum_{k=0}^{n-1}(a^{n-k}b^k - a^{n-(k+1)}b^{k+1} \\ & = & a^n - b^n \text{ par télescopage} \end{array}$$

□

Remarques II.8.

1. *pour $n = 2$, on retrouve l'identité remarquable : $a^2 - b^2 = (a-b)(a+b)$;*
2. *on pouvait aussi reconnaître une somme géométrique de raison $\dfrac{b}{a}$, mais cela demanderai des disjonctions de cas suivant les valeurs de a et b ;*
3. *inversement, on retrouve la somme géométrique en prenant $a = 1$ et $b = q$.*

Corollaire II.9. *Si de plus n est impair, alors :*

$$a^n + b^n = (a+b) \times \left(a^{n-1} - a^{n-2}b + \cdots - ab^{n-2} + b^{n-1}\right) = (a+b) \times \sum_{k=0}^{n-1}(-1)^k a^{n-1-k}b^k.$$

Démonstration. Comme n est impair, alors $(-1)^n = -1$, et donc : $a^n + b^n = a - (-b)^n$. Et on applique le résultat précédent. □

Proposition II.10 (Sommes quadratique et cubique)**.** *Pour $n \in \mathbb{N}^*$, on a :*

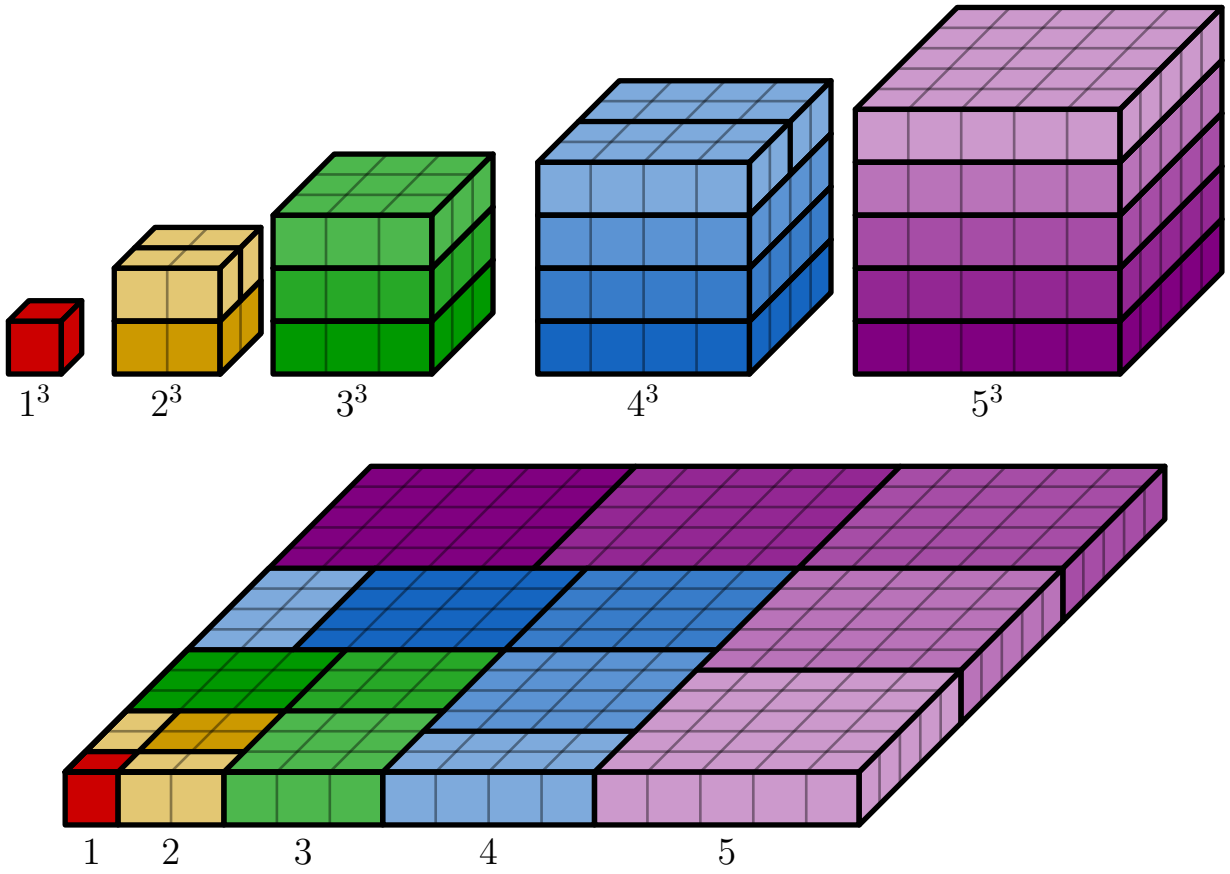
1. $\displaystyle\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$;
2. $\displaystyle\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$.

Démonstration. Le premier résultat a été montré au chapitre 1.
Le second est laissé en exercice. □

Remarque II.11. *Le second résultat peut aussi se lire comme :*

$$\sum_{k=1}^{n} k^3 = \left(\sum_{k=1}^{n} k\right)^2$$

ce que l'on peut voir géométriquement. L'idée étant que l'aire d'un carré de côté $1 + 2 + \cdots + n$ doit être égale à $1 + 2^3 + \cdots + n^3$.
Pour cela, on peut voir que, au moment d'augmenter la longueur du carré de n, on rajoute une bande dont l'aire peut être découpée en n carrés de taille $n \times n$. C'est-à-dire qu'on augment l'aire totale de $n \times n^2 = n^3$. Ce dernier point est illustrée sur la figure ci-dessous :



III Sommes et produits doubles

Tous les résultats suivants s'étendent à des produits.

Proposition III.1. *Si I, J sont deux ensembles finis, et $(a_{i,j})$ est une famille de complexes indexée par $I \times J$, alors :*

$$\sum_{(i,j)\in I\times J} a_{i,j} = \sum_{i\in I}\left(\sum_{j\in J} a_{i,j}\right) = \sum_{j\in J}\left(\sum_{i\in I} a_{i,j}\right)$$

c'est-à-dire que l'on peut sommer sur un pavé dans l'ordre que l'on veut.

Corollaire III.2.

$$\left(\sum_{i\in I} a_i\right)\left(\sum_{j\in J} b_j\right) = \sum_{i\in I}\sum_{j\in J} a_i b_j = \sum (i,j) \in I \times J a_i b_j.$$

Remarque III.3. *Si (a_k) est indexée par $[\![1;n]\!]$, on trouve :*

$$\left(\sum_{k=1}^{n} a_k\right)^2 = \sum_{k=1}^{n} a_k^2 + 2\sum_{1\le i<j\le n} a_i a_j$$

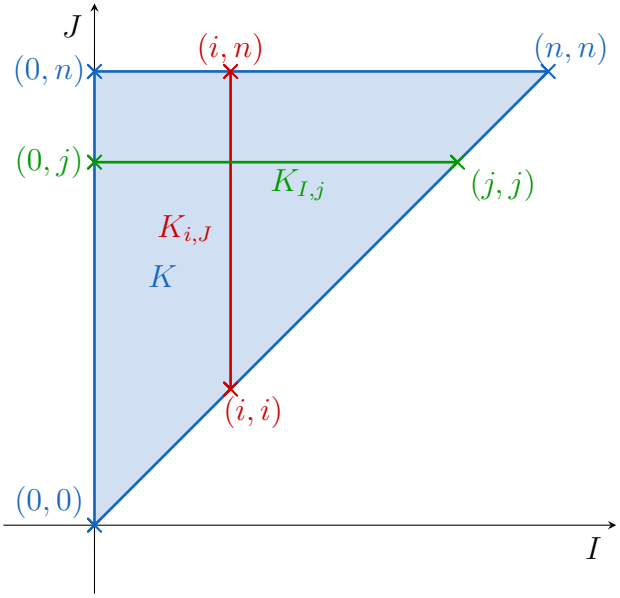
qui correspond quand $n = 2$ à l'identité remarquable : $(a_1 + a_2)^2 = a_1^2 + a_2^2 + 2a_1a_2$.

Définition III.4. *Si I, J sont deux ensembles, et $K \subset I \times J$, on définit :*

1. *pour tout $i \in I$, la coupe de K suivant i comme : $K_{i,J} = \{j \in J \,|\, (i,j) \in K\}$;*
2. *pour tout $j \in J$, la coupe de K suivant j comme : $K_{I,j} = \{i \in I \,|\, (i,j) \in K\}$.*

Exemple III.5. *Si $I = J = [\![0;n]\!]$ et $K = \{(i,j) \in I \times J \,|\, i \le j\}$, alors pour tous $0 \le i, j \le n$:*

$$K_{i,J} = \{j \in J \,|\, i \le j \le n\} = [\![i;n]\!] \text{ et } K_{I,j} = \{i \in I \,|\, 0 \le i \le j\} = [\![0;j]\!]$$



Proposition III.6. *Avec les mêmes notations, on a les recouvrements disjoints :*

$$K = \bigcup_{i\in I}(\{i\} \times K_{i,J}) = \bigcup_{j\in J}(K_{I,j} \times \{j\})$$

et donc, si $(a_{i,j})$ est une famille indexée par $I \times J$:

$$\sum_{(i,j)\in K} a_{i,j} = \sum_{i\in I}\sum_{j\in K_{i,J}} a_{i,j} = \sum_{j\in J}\sum_{i\in K_{I,j}} a_{i,j}.$$

Corollaire III.7. *Si $(a_{i,j})$ est indexée par $[\![0,n]\!]^2$, alors :*

$$\sum_{0\leq i\leq j\leq n} a_{i,j} = \sum_{i=0}^{n}\sum_{j=i}^{n} a_{i,j} = \sum_{j=0}^{n}\sum_{i=0}^{j} a_{i,j}$$

$$\sum_{0\leq i< j\leq n} a_{i,j} = \sum_{i=0}^{n}\sum_{j=i+1}^{n} a_{i,j} = \sum_{j=0}^{n}\sum_{i=0}^{j-1} a_{i,j}$$

Exemple III.8. *Calculer pour tout $n\in\mathbb{N}^*$ la somme : $\sum_{k=1}^{n} k2^{k-1}$:*

$$\begin{aligned}
\sum_{k=1}^{n} k2^{k-1} &= \sum_{k=1}^{n}\sum_{l=1}^{k} 2^{k-1}\\
&= \sum_{l=1}^{n}\sum_{k=l}^{n} 2^{k-1}\\
&= \sum_{l=1}^{n} \frac{2^{l-1}-2^n}{1-2}\\
&= \sum_{l=1}^{n} (2^n - 2^{l-1})\\
&= n\times 2^n - \frac{1-2^n}{1-2}\\
&= (n-1)\times 2^n + 1
\end{aligned}$$

IV Factorielle et coefficients binomiaux

Définition IV.1. *Si $n\in\mathbb{N}^*$, on définit la **factorielle** de n par :*

$$n! = n\times(n-1)\times\cdots\times 2\times 1 = \prod_{k=1}^{n} k$$

et on pose par convention $0!=1$.

Définition IV.2. *Si $n,k\in\mathbb{N}$, on définit le **coefficient binomial** "k parmi n" par :*

$$\binom{n}{k} = \begin{cases} \dfrac{n!}{k!(n-k)!} & \text{si } k\leq n \\ 0 & \text{si } k>n \end{cases}.$$

Remarque IV.3. *La quantité $\binom{n}{k}$ correspond aux nombres de parties à k éléments dans un ensemble à n éléments.*

Proposition IV.4. *Si $k,n\in\mathbb{N}$:*

$$\binom{n}{k} = \binom{n}{n-k}.$$

Exemple IV.5. *On a les valeurs particulières suivantes :*

1. $\binom{n}{0} = \binom{n}{n} = 1$;
2. $\binom{n}{1} = \binom{n}{n-1} = n$;
3. $\binom{n}{2} = \binom{n}{n-2} = \dfrac{n(n-1)}{2}$.

Proposition IV.6 (Triangle de Pascal)**.** *Si $k, n \in \mathbb{N}$, alors :*

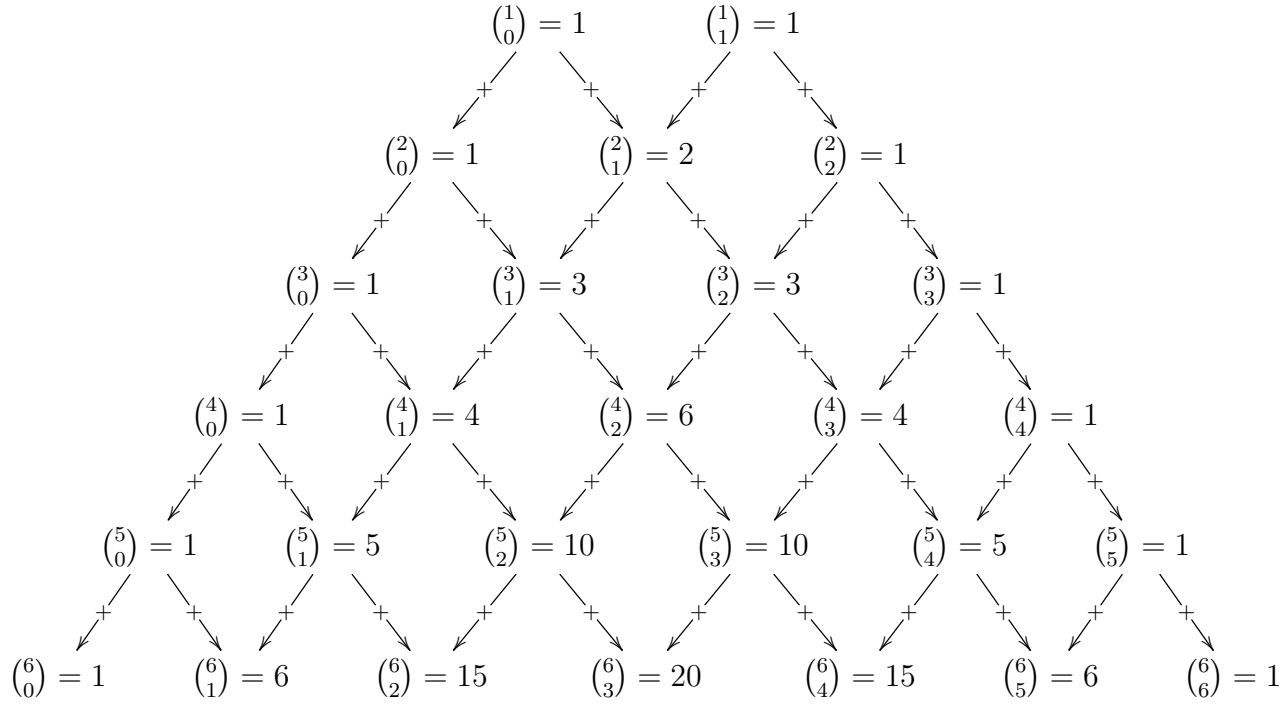
$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

Démonstration. On procède par disjonction de cas.
Si $k > n$: toutes les sommes sont nulles.
Si $k = n$: on trouve : $1 + 0 = 1$.
Si $k \in [\![0; n-1]\!]$:

$$\begin{aligned}\tbinom{n}{k} + \tbinom{n}{k+1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-(k+1))!} \\ &= \frac{n! \times (k+1)}{(k+1)!(n-k)!} + \frac{n! \times (n-k)}{(k+1)!(n-k)!} = \frac{n! \times (k+1+n-k)}{(k+1)!(n-k)!} \\ &= \frac{(n+1)!}{(k+1)!((n+1)-(k+1))!} = \tbinom{n+1}{k+1}\end{aligned}.$$

□

Remarque IV.7. *Le triangle de Pascal permet de calculer de proche en proche tous les coefficients binomiaux. On représente sur la n-ème ligne les coefficients $\binom{n}{k}$ pour $0 \leq k \leq n$:*



Corollaire IV.8. *Pour tous $n, k \in \mathbb{N}$: $\binom{n}{k} \in \mathbb{N}$.*

Démonstration. En utilisant le triangle de Pascal, on montre par récurrence sur $n \in \mathbb{N}$ la proposition :

$$\forall k \in \mathbb{N},\ \binom{n}{k} \in \mathbb{N}.$$

□

Proposition IV.9. *Si $n, k \in \mathbb{N}^*$, alors :*

$$k\binom{n}{k} = n\binom{n-1}{k-1}$$

Démonstration. Le cas $k > n$ est immédiat.
Si $k \leq n$:

$$k\binom{n}{k} = k\frac{n!}{k!(n-k)!} = \frac{n!}{(k-1)!(n-k)!} = \frac{n \times (n-1)!}{(k-1)!((n-1)-(k-1))!} = n\binom{n-1}{k-1}.$$

□

Théorème IV.10 (Formule du binôme de Newton)**.** *Si $a, b \in \mathbb{C}$ et $n \in \mathbb{N}$, alors :*

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

Démonstration. On procède par récurrence sur $n \in \mathbb{N}$.
Si $n = 0$: $(a+b)^n = (a+b)^0 = 1$ et $\sum_{k=0}^{0} \binom{0}{k} a^k b^{n-k} = \binom{0}{0} a^0 b^0 = 1$.
Hérédité : supposons que $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ pour un certain $n \in \mathbb{N}$. Alors :

$$\begin{array}{rcl}
(a+b)^{n+1} & = & (a+b) \times (a+b)^n = (a+b) \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\
& = & \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} \\
& = & \sum_{l=1}^{n+1} \binom{n}{l-1} a^l b^{n+1-l} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} \\
& = & a^{n+1} + \sum_{k=1}^{n} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=1}^{n} \binom{n}{k} a^k b^{n+1-k} + b^{n+1} \\
& = & b^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k b^{n+1-k} + a^{n+1} \\
& = & \binom{n+1}{0} a^0 b^{n+1-0} + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n+1-k} + \binom{n+1}{n+1} a^{n+1} b^0 \\
& = & \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}
\end{array}$$

ce qui conclut la récurrence. □

Exemples IV.11. *Soit $n \in \mathbb{N}^*$. Alors :*

1. $\displaystyle\sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} = (1+1)^n = 2^n$;
2. $\displaystyle\sum_{k=0}^{n} (-1)^k \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} (-1)^k 1^{n-k} = (-1+1)^n = 0$;
3. $\displaystyle\sum_{k=0}^{n} \binom{n}{k} n^k = \sum_{k=0}^{n} \binom{n}{k} n^k \cdot 1^{n-k} = (n+1)^n$;
4. *en revanche, on ne peut pas faire apparaître une formule du binôme dans la somme $\displaystyle\sum_{k=0}^{n} \binom{n}{k} k^k$, car le nombre que l'on met à la puissance (à sa voir k ici) change lors de la sommation.*
5. *Posons :*

$$A_n = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} \text{ et } A_n = \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2k+1}.$$

Alors, par changement d'indice, on trouve :
— si $k \in \lfloor \frac{n}{2} \rfloor$, alors $l = 2k$ parcourt tous les entiers pairs de $[\![0; n]\!]$; donc :

$$A_n = \sum_{\substack{\in [\![0;n]\!] \\ l \text{ pair}}} \binom{n}{l};$$

— *si* $k \in \lfloor \frac{n-1}{2} \rfloor$, *alors* $l = 2k+1$ *parcourt tous les entiers impairs de* $[\![0;n]\!]$ *; donc :*

$$B_n = \sum_{\substack{\in [\![0;n]\!] \\ l \text{ impair}}} \binom{n}{l}.$$

Et ainsi, on trouve :

$$A_n + B_n = \sum_{l=0}^{n} \binom{n}{l} = 2^n \text{ et } A_n - B_n = \sum_{l=0}^{n} \binom{n}{l}(-1)^l = 0.$$

Et finalement :

$$A_n = B_n = 2^{n-1}.$$

V Résolution de systèmes linéaires

On fixe $\mathbb{K}$ comme étant $\mathbb{R}$ ou $\mathbb{C}$. On appelle **scalaires** les éléments de $\mathbb{K}$.

Définition V.1. *Un* ***système linéaire à*** n ***équations et*** p ***inconnues*** *est un système de la forme :*

$$(\mathcal{S}) : \left\{ \begin{array}{ccccccccc} a_{1,1}x_1 & + & a_{1,2}x_2 & + & \dots & + & a_{1,p}x_p & = & b_1 \\ a_{2,1}x_1 & + & a_{2,2}x_2 & + & \dots & + & a_{n,p}x_p & = & b_2 \\ \vdots & & \vdots & & \vdots & & \vdots & \vdots & \vdots \\ a_{n,1}x_1 & + & a_{n,2}x_2 & + & \dots & + & a_{n,p}x_p & = & b_n \end{array} \right.$$

où $x_1, \dots, x_p$ *sont des inconnues (que l'on cherche dans* $\mathbb{K}$*), et où les* $(a_{i,j})$ *et les* b_i *sont des scalaires fixé.*
Les $a_{i,j}$ *sont appelés les* ***coefficients*** *du système.*
Le n*-uplet* $(b_1, \dots, b_n)$ *est appelé le* ***second membre*** *du système.*
Le système obtenu en remplaçant le second membre par $(0, \dots, 0)$ *est appelé* ***système homogène associé à*** $\mathcal{S}$*.*
On dit que $(\mathcal{S})$ *est* ***incompatible*** *s'il n'a pas de solutions, et* ***compatible*** *sinon.*

Remarque V.2. *Un système homogène est toujours compatible.*

Proposition V.3. *Si* $(n,p) = (2,2)$*, résoudre le système*

$$(\mathcal{S}) : \left\{ \begin{array}{ccc} ax + by & = & e \\ cx + dy & = & f \end{array} \right.$$

où $(a,b), (c,d) \neq (0,0)$*, revient à chercher l'intersection des droites* $\mathcal{D}_1 : ax + by = e$ *et* $\mathcal{D}_2 : cx + dy = f$ *:*

1. *si les droites sont confondues : il y a une infinité de solutions (tous les points de* $\mathcal{D}_1 = \mathcal{D}_2$*) ;*
2. *si les droites sont parallèles distinctes : il n'y a pas de solutions ;*
3. *si les droites sont sécantes : il y a une seule solution.*

Proposition-Définition V.4. *Avec les mêmes notations appelle* ***déterminant du système*** $(\mathcal{S})$ *la quantité* $ad - bc$*. Alors* $(\mathcal{S})$ *admet une unique solution si, et seulement si,* $ad - bc \neq 0$*.*

Démonstration. Le système admet une unique solution si, et seulement si, $\mathcal{D}_1$ et $\mathcal{D}_2$ sont sécantes.
Les vecteurs (a,b) et (c,d) sont des vecteurs normaux à $\mathcal{D}_1$ et $\mathcal{D}_2$. Donc les droites $\mathcal{D}_1$ et $\mathcal{D}_2$ sont sécantes si, et seulement si : $\det((a,b),(c,d)) \neq 0$, c'est-à-dire $ad - bc \neq 0$. □

Proposition V.5. *Si $(n,p)=(3,2)$, résoudre le système :*

$$(\mathcal{S}):\left\{\begin{array}{rcl} ax+by+cz &=& g\\ dx+ey+fz &=& h\end{array}\right.$$

où $(a,b,c),(d,e,f)\neq(0,0,0)$, revient à chercher l'intersection des plans $\mathcal{P}_1 : ax+by+cz=g$ et $\mathcal{P}_2 : dx+ey+fz=h$:

1. *si les plans sont confondues : il y a une infinité de solutions (tous les points de $\mathcal{P}_1=\mathcal{P}_2$) ;*
2. *si les plans sont parallèles distincts : il n'y a pas de solutions ;*
3. *si les plans sont sécants : il y a une infinité de solutions (tous les points de la droite $\mathcal{P}_1\cap\mathcal{P}_2$).*

Définition V.6. *Un système est dit **échelonné** si le premier coefficient non nul de chaque ligne, qu'on appelle **pivot**, est situé strictement à gauche des pivots des lignes suivantes.*

Remarque V.7. *Si on note j_i l'indice du pivot de la ligne L_i, cela revient à dire qu'il existe $k\in[\![1;n]\!]$ tel que : les lignes $L_{k+1},\dots,L_n$ du système homogène sont nulles, et que :$j_1<j_2<\cdots<j_k$.*

$$(\mathcal{S}):\left\{\begin{array}{ccccccccccccccc} a_{1,j_1}x_{j_1} & + & \dots & + & \dots & + & \dots & & \dots & & \dots & & \dots & = & b_1\\ 0 & + & 0 & + & a_{2,j_2}x_{j_2} & + & \dots & + & \dots & & \dots & & \dots & = & b_2\\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots\\ 0 & + & 0 & + & 0 & + & 0 & + & 0 & + & a_{k,j_k} & + & \dots & = & b_k\end{array}\right.$$

Exemple V.8. *Le système suivant est échelonné :*

$$\left\{\begin{array}{ccccccc} x_1 & + & 3x_2 & + & 2x_3 & = & 0\\ & & 2x_2 & + & 4x_3 & = & 2\\ & & & - & x_3 & = & 1\end{array}\right. .$$

Définition V.9. *Les **opérations élémentaires** sur les lignes d'un système sont :*

1. *la **permutation** : on échange les lignes L_i et L_j, codée par $L_i\leftrightarrow L_j$;*
2. *la **dilatation** : multiplication d'une ligne par un scalaire λ non nul, codée par $L_i\leftarrow\lambda L_i$;*
3. *la **transvection** : ajout à la ligne L_i d'un multiple de la ligne L_j, codée $L_i\leftarrow L_i+\lambda L_j$.*

Remarques V.10.

1. *Il faut bien considérer **toute** la ligne à chaque fois (y compris b_i).*
2. *L'ordre des opérations a une importance, et on les fait **successivement**.*

Définition V.11. *On dit que deux systèmes linéaires sont **équivalents** si l'on peut passer de l'un à l'autre par un succession finie d'opérations élémentaires.*

Remarque V.12. *On peut "revenir en arrière" après avoir fait un opération élémentaire, et ceci à l'aide d'une autre opération élémentaire. Plus précisément :*

— *une permutation est annulée par elle-même ;*
— *une dilatation de rapport λ est annulée par la dilatation de la même ligne de rapport $\frac{1}{\lambda}$;*
— *une transvection de coefficient λ est annulée par la dilatation des mêmes lignes de coefficient $-\lambda$.*

En conséquence, la relation "être équivalent" sur les systèmes est une relation d'équivalence.

Théorème V.13. *Deux systèmes équivalents ont même ensemble solution.*

Démonstration. Constatons déjà que chaque opération élémentaire ne peut qu'agrandir l'ensemble solution du système initial. Ceci est clair car un système d'égalité est bien préservé quand on les combine par les opérations élémentaires.
Comme on peut revenir en arrière par d'autres opérations élémentaires, le résultat découle par double inclusion. □

Théorème V.14 (Algorithme du pivot de Gauss–Jordan)**.** *Tout système est équivalent à un système échelonné. La succession d'opérations élémentaires est donnée par la méthode de Gauss-Jordan.*

Remarque V.15. *L'intérêt est qu'un système échelonné est très facile à résoudre par méthode de remontée : on résout les équations avec le moins d'inconnues, puis les réinjecte dans les précédentes.*

Méthode V.16. *La méthode se fait récursivement selon le nombre d'inconnues du système. On considère le système :*

$$(\mathcal{S}) : \begin{cases} a_{1,1}x_1 & + & a_{1,2}x_2 & + & \dots & + & a_{1,p}x_p & = & b_1 \\ a_{2,1}x_1 & + & a_{2,2}x_2 & + & \dots & + & a_{n,p}x_p & = & b_2 \\ \vdots & & \vdots & & \vdots & & \vdots & \vdots & \vdots \\ a_{n,1}x_1 & + & a_{n,2}x_2 & + & \dots & + & a_{n,p}x_p & = & b_n \end{cases}$$

- *si tous les $a_{i,1}$ sont nuls : alors la première colonne du système est nulle, et on continue à échelonner suivant les colonnes suivantes ;*
- *sinon : quitte à permuter deux lignes, on a $a_{1,1} \neq 0$. On fait pour tout $i \in [\![2; n]\!]$ la transvection : $L_i \leftarrow L_i - \dfrac{a_{i,1}}{a_{1,1}} L_1$. La première colonne du système a seulement son premier coefficient non nul. Le système obtenu est de la forme :*

$$\begin{cases} a_{1,1}x_1 & + & a_{1,2}x_2 & + & \dots & + & a_{1,p}x_p & = & b_1 \\ 0 & + & a'_{2,2}x_2 & + & \dots & + & a_{n,p}x_p & = & b'_2 \\ \vdots & & \vdots & & \vdots & & \vdots & \vdots & \vdots \\ 0 & + & a'_{n,2}x_2 & + & \dots & + & a_{n,p}x_p & = & b'_n \end{cases}$$

où, pour tout $i \in [\![2; n]\!]$ et tout $j \in [\![2; p]\!]$ on a :

$$a'_{i,j} = a_{i,j} - \frac{a_{i,1}}{a_{1,1}} a_{1,j} \text{ et } b'_j = b_j - \frac{a_{i,1}}{a_{1,1}} b_1.$$

et il suffit alors d'échelonner le système :

$$(\mathcal{S}') : \begin{cases} a'_{2,2}x_2 & + & \dots & + & a_{n,p}x_p & = & b_2 \\ \vdots & & \vdots & & \vdots & \vdots & \vdots \\ a'_{n,2}x_2 & + & \dots & + & a_{n,p}x_p & = & b_n \end{cases}$$

Remarque V.17. *En pratique, on prendra un pivot qui facilite les expression $\dfrac{a_{i,1}}{a_{1,1}}$ (par exemple un pivot égal à 1).*

Corollaire V.18. *Un système **homogène** à n équations et p inconnues possède une infinité de solutions dès lors que $p > n$.*
En particulier, il admet une solution non nulle.

Démonstration. On échelonne le système homogène, ce qui donne un système homogène, échelonné, à n équations.
Comme $p > n$, alors l'une des inconnues n'apparaît pas comme pivot, donc peut être choisie librement dans $\mathbb{K}$.
Pour chacune des valeurs choisie, la remontée permet de trouver une solution au système. L'infinité de l'ensemble solution découle alors de l'infinité de $\mathbb{K}$. □

Exemple V.19. *Résoudre le système à 3 équations et 3 inconnues :*

$$(\mathcal{S}) : \begin{cases} x_1 & + & x_2 & - & x_3 & = & 2 \\ 2x_1 & - & x_2 & + & x_3 & = & 1 \\ 4x_1 & + & x_2 & + & 3x_3 & = & 3 \end{cases}$$

$$(\mathcal{S}) \Leftrightarrow \left\{\begin{array}{rcrcrcl} x_1 & + & x_2 & - & x_3 & = & 2 \\ & - & 3x_2 & + & 3x_3 & = & -3 \\ & - & 3x_2 & + & 7x_3 & = & -5 \end{array}\right. \quad \text{avec } \left\{\begin{array}{rcl} L_2 & \leftarrow & L_2 - 2L_1 \\ L_3 & \leftarrow & L_3 - 4L_1 \end{array}\right.$$

$$\Leftrightarrow \left\{\begin{array}{rcrcrcl} x_1 & + & x_2 & - & x_3 & = & 2 \\ & - & 3x_2 & + & 3x_3 & = & -3 \\ & & & + & 4x_3 & = & -2 \end{array}\right. \quad \text{avec } \left\{\begin{array}{rcl} L_3 & \leftarrow & L_3 - 2L_2 \end{array}\right.$$

$$\Leftrightarrow \left\{\begin{array}{rcl} x_3 & = & -1/2 \\ x_2 & = & 1 + x_3 = 1/2 \\ x_1 & = & 2 - x_2 + x_3 = 1 \end{array}\right.$$

Donc le système admet pour unique solution $(1, 1/2, -1/2)$.

Exemple V.20. *Résoudre le système à* 4 *équations et* 4 *inconnues :*

$$(\mathcal{S}) : \left\{\begin{array}{rcrcrcrcl} 2x_1 & + & 3x_2 & - & x_3 & + & x_4 & = & 2 \\ x_1 & - & x_2 & + & x_3 & - & x_4 & = & 1 \\ 3x_1 & + & 2x_2 & + & x_3 & + & x_4 & = & -1 \\ x_1 & + & x_2 & - & 2x_3 & + & 2x_4 & = & 1 \end{array}\right.$$

$$(\mathcal{S}) \Leftrightarrow \left\{\begin{array}{rcrcrcrcl} x_1 & - & x_2 & + & x_3 & - & x_4 & = & 1 \\ 2x_1 & + & 3x_2 & - & x_3 & + & x_4 & = & 2 \\ 3x_1 & + & 2x_2 & + & x_3 & + & x_4 & = & -1 \\ x_1 & + & x_2 & - & 2x_3 & + & 2x_4 & = & 1 \end{array}\right. \quad \text{avec } L_1 \leftrightarrow L_2$$

$$\Leftrightarrow \left\{\begin{array}{rcrcrcrcl} x_1 & - & x_2 & + & x_3 & - & x_4 & = & 1 \\ & & 5x_2 & - & 3x_3 & + & 3x_4 & = & 0 \\ & & 5x_2 & - & 2x_3 & + & 4x_4 & = & -4 \\ & & 2x_2 & - & 3x_3 & + & 3x_4 & = & 0 \end{array}\right. \quad \text{avec } \left\{\begin{array}{rcl} L_2 & \leftarrow & L_2 - 2L_1 \\ L_3 & \leftarrow & L_3 - 3L_1 \\ L_4 & \leftarrow & L_4 - L_1 \end{array}\right.$$

$$\Leftrightarrow \left\{\begin{array}{rcrcrcrcl} x_1 & - & x_2 & + & x_3 & - & x_4 & = & 1 \\ & & 2x_2 & - & 3x_3 & + & 3x_4 & = & 0 \\ & & 5x_2 & - & 2x_3 & + & 4x_4 & = & -4 \\ & & 5x_2 & - & 3x_3 & + & 3x_4 & = & 0 \end{array}\right. \quad \text{avec } L_2 \leftrightarrow L_4$$

$$\Leftrightarrow \left\{\begin{array}{rcrcrcrcl} x_1 & - & x_2 & + & x_3 & - & x_4 & = & 1 \\ & & 2x_2 & - & 3x_3 & + & 3x_4 & = & 0 \\ & & & & \frac{11}{2}x_3 & - & \frac{7}{2}x_4 & = & -4 \\ & & & & \frac{9}{2}x_3 & - & \frac{9}{2}x_4 & = & 0 \end{array}\right. \quad \text{avec } \left\{\begin{array}{rcl} L_3 & \leftarrow & L_3 - \frac{5}{2}L_2 \\ L_4 & \leftarrow & L_4 - \frac{5}{2}L_2 \end{array}\right.$$

$$\Leftrightarrow \left\{\begin{array}{rcrcrcrcl} x_1 & - & x_2 & + & x_3 & - & x_4 & = & 1 \\ & & 2x_2 & - & 3x_3 & + & 3x_4 & = & 0 \\ & & & & \frac{11}{2}x_3 & - & \frac{7}{2}x_4 & = & -4 \\ & & & & & - & \frac{18}{11}x_4 & = & \frac{36}{11} \end{array}\right. \quad \text{avec } L_4 \leftarrow L_4 - \tfrac{9}{11}L_3$$

Et on trouve par L_4 *que* $x_4 = -2$*, qu'on réinjecte dans* L_3 *pour déduire que* $x_3 = -2$*, qu'on réinjecte dans* L_2 *pour déduire* $x_2 = 0$*, qu'on réinjecte dans* L_1 *pour trouver* $x_1 = 1$.
Donc le système admet pour unique solution $(1, 0, -2, -2)$.

Chapitre 7

Les fonctions usuelles

I Logarithmes, exponentielles et puissances

I.1 La fonction logarithme

Définition I.1. *On appelle* ***fonction logarithme népeirien*** *l'unique primitive de la fonction* $x \mapsto \dfrac{1}{x}$ *sur* $\mathbb{R}_+^*$ *qui s'annule en* 1. *On la note* ln *ou* Log.

Théorème I.2. *Si* $a, b \in \mathbb{R}_+^*$ *et* $n \in \mathbb{Z}$, *alors :*

1. $\ln(ab) = \ln(a) + \ln(b)$;
2. $\ln\left(\dfrac{1}{a}\right) = -\ln(a)$;
3. $\ln\left(\dfrac{a}{b}\right) = \ln(a) - \ln(b)$;
4. $\ln(a^n) = n\ln(a)$.

Démonstration.

1. Si $a, b > 0$, on considère la fonction $f_b : x \mapsto \ln(xb) - \ln(x)$
   Alors f_b est dérivable sur $\mathbb{R}_+^*$, avec : $\forall x \in \mathbb{R}_+^*,\ f'(x) = \dfrac{b}{xb} - \dfrac{1}{x} = 0$.
   Donc f_b est constante, donc : $f(a) = f(1)$, donc : $\ln(ab) - \ln(a) = \ln(b)$.
2. On déduit : $0 = \ln(1) = \ln\left(a\dfrac{1}{a}\right) = \ln(a) + \ln\left(\dfrac{1}{a}\right)$.
3. De même : $\ln\left(\dfrac{a}{b}\right) = \ln(a) + \ln\left(\dfrac{1}{b}\right) = \ln(a) - \ln(b)$.
4. Par récurrence : $\forall n \in \mathbb{N},\ \ln(a^n) = n\ln(a)$. Puis : $\forall n \in \mathbb{N},\ \ln(a^{-n}) = \ln\left(\dfrac{1}{a^n}\right) = -n\ln(a)$.

□

Proposition I.3. *La fonction* ln *est strictement croissante sur* $\mathbb{R}_+^*$, *telle que :*

$$\lim_{x\to+\infty} \ln(x) = +\infty \text{ et } \lim_{x\to 0^+} \ln(x) = -\infty.$$

Démonstration. — $\forall x \in \mathbb{R}_+^*,\ \ln'(x) = \dfrac{1}{x} > 0$ donc ln est strictement croissante ;

— montrons que $\lim_{x\to+\infty} \ln(x) = +\infty$, c'est-à-dire que :

$$\forall A > 0,\ \exists B > 0,\ x > B \Rightarrow \ln(x) > A.$$

Soit $A > 0$. Par stricte croissante : $\ln(2) > \ln(1) = 0$.
Posons $N = \left\lfloor \frac{A}{\ln(2)} \right\rfloor + 1$ (qui est un entier naturel). Alors :

$$\ln(2^N) = N \cdot \ln(2) \geq \frac{A}{\ln(2)} \cdot \ln(2) = A.$$

Par croissance de ln, $B = 2^N$ convient.

— $\lim_{x\to0^+} \ln(x) = \lim_{x\to+\infty} \ln\left(\frac{1}{x}\right) = -\lim_{x\to+\infty} \ln(x) = -\infty$.

□

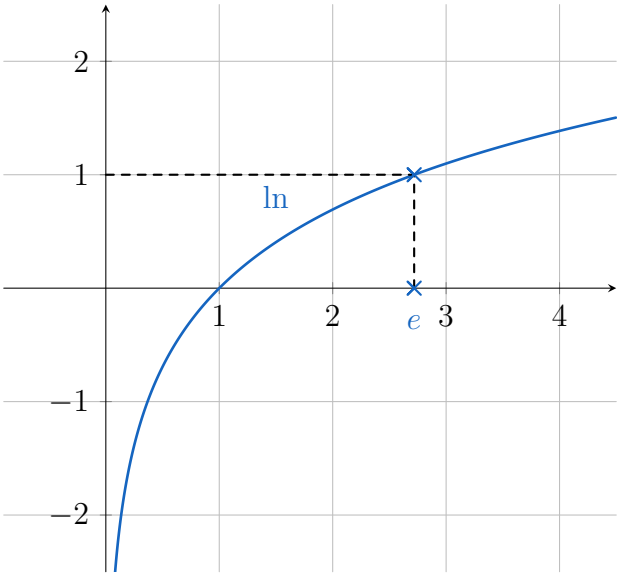
Corollaire I.4. *La fonction* ln *réalise une bijection strictement croissante de* $\mathbb{R}_+^*$ *sur* $\mathbb{R}$.

Démonstration. Découle de la continuité de ln. □

Proposition I.5. *L'équation* $\ln(x) = 1$ *possède une unique solution : on la note* e, *et on a* $e \simeq 2,71828$.

Proposition I.6. *On a le tableau de variations et la représentation graphique suivants :*

x	0		$+\infty$
$\ln'$	‖	$+$	
ln	‖	$-\infty$ ↗	$+\infty$



Définition I.7. *Si* $a \in \mathbb{R}_+^* \setminus \{1\}$, *on lui associe la fonction* ***logarithme de base*** *a, notée* $\log_a$, *comme la fonction définie sur* $\mathbb{R}_+^*$ *par :* $\forall x \in \mathbb{R}_+^*,\ \log_a(x) = \dfrac{\ln(x)}{\ln(a)}$.

Remarques I.8.

1. *On utilise beaucoup le logarithme en base* 2*, aussi appelé* ***logarithme binaire****, et le logarithme en base* 10*, aussi appelé* ***logarithme décimal****, et noté parfois* log*..*
2. *Le logarithme népeirien est le logarithme de base* e*.*

Proposition I.9. *La fonction* $\log_a$ *réalise une bijection strictement monotone de* $\mathbb{R}_+^*$ *sur* $\mathbb{R}$ *telle que* $\log_a(1) = 0$ *et* $\log_a(a) = 1$*.*
Elle est strictement croissante si $a > 1$ *et strictement décroissante si* $0 < a < 1$*, et vérifie les formules du théorème I.2.*

I.2 La fonction exponentielle

Théorème-Définition I.10. *On définit la fonction* ***exponentielle (népeirienne)****, notée* exp*, comme la réciproque de la fonction* ln*.*
Elle est définie sur $\mathbb{R}$ *par :*

$$\forall x \in \mathbb{R},\ \forall y \in \mathbb{R}_+^*,\ y = \exp(x) \Leftrightarrow x = \ln(y).$$

La fonction exp *est continue, strictement croissante et dérivable sur* $\mathbb{R}$*, de dérivée elle-même.*

Démonstration. L'existence, la continuité et la monotonie découlent des propriétés de ln.
Comme $\ln' = x \mapsto \dfrac{1}{x}$ ne s'annule pas sur $\mathbb{R}_+^*$, alors exp est dérivable sur $\ln(\mathbb{R}_+^*) = \mathbb{R}$.
Si $x \in \mathbb{R}$, on a :

$$\exp'(x) = \frac{1}{\ln'(\exp(x))} = \frac{1}{\dfrac{1}{\exp(x)}} = \exp(x).$$

□

Remarque I.11. *On notera plutôt* e^x *au lieu de* $\exp(x)$*.*
La raison étant que, si $n \in \mathbb{Z}$*, on a :* $\ln(e^n) = n\ln(e) = n$*, donc* $\exp(n) = e^n$*.*

Théorème I.12. *Si* $a, b \in \mathbb{R}$ *et* $n \in \mathbb{Z}$*, alors :*

1. $e^{a+b} = e^a e^b$;
2. $e^{-a} = \dfrac{1}{e^a}$;
3. $e^{a-b} = \dfrac{e^a}{e^b}$;
4. $e^{na} = (e^a)^n$.

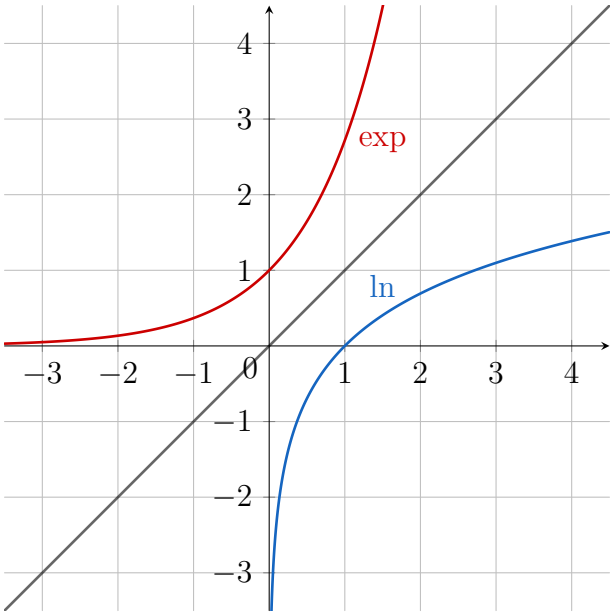
Démonstration. Découle des propriétés du ln. Montrons par exemple la première.
Par injectivité de ln, on a :

$$e^{a+b} = e^a e^b \Leftrightarrow \ln(e^{a+b}) = \ln(e^a e^b)$$

Et on a :
— $\ln(e^{a+b}) = a + b$ (par définition de exp qui est la réciproque de ln) ;
— $\ln(e^a e^b) = \ln(e^a) + \ln(e^b) = a + b$ (où la première égalité découle des propriétés de ln, et la seconde de la définition de exp).
et ainsi on a bien $e^{a+b} = e^a \cdot e^b$. □

Proposition I.13. *On a le tableau de variations et la représentation graphique suivants :*

x	$-\infty$	$+\infty$
$\exp'$	$+$	
$\exp$	0	$+\infty$



I.3 Les fonctions puissances et exponentielles

Définition I.14. *Si $a \in \mathbb{R}_+^*$ et $\alpha \in \mathbb{R}$, on définit le nombre a **puissance** α comme : $a^\alpha = \exp(\alpha \ln(a))$.*

Remarque I.15. *La notation x^n, pour $x < 0$, n'a de sens que si $n \in \mathbb{Z}$.*

Proposition I.16. *Si $a, b \in \mathbb{R}_+^*$ et $\alpha, \beta \in \mathbb{R}$, alors :*

1. $a^{\alpha+\beta} = a^\alpha \cdot a^\beta$ *et* $a^{\alpha-\beta} = \dfrac{a^\alpha}{a^\beta}$;
2. $(a^\alpha)^\beta = \left(a^{\alpha\beta}\right) = \left(a^\beta\right)^\alpha$;
3. $(ab)^\alpha = a^\alpha b^\alpha$ *et* $\left(\dfrac{a}{b}\right)^\alpha = \dfrac{a^\alpha}{b^\alpha}$.

Définition I.17. *Si $a \in \mathbb{R}_+^*$, on appelle fonction **exponentielle de base** a la fonction $\exp_a$ définie sur $\mathbb{R}$ par : $\exp_a(x) = a^x = e^{x\ln(a)}$.*

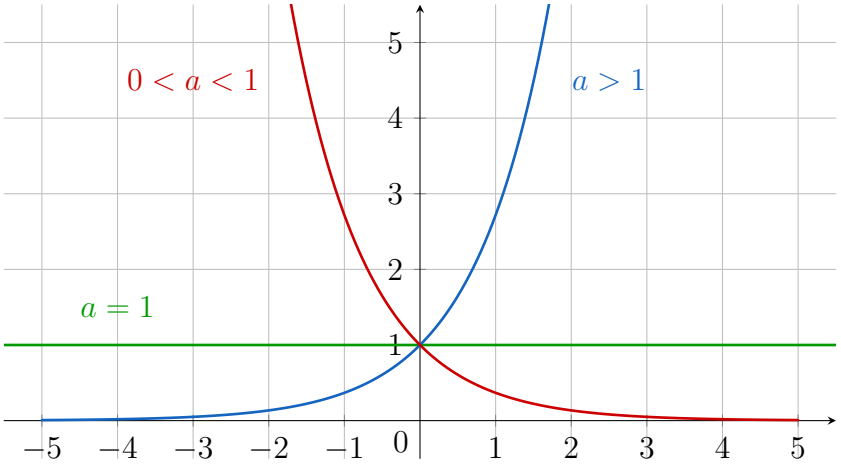
Proposition I.18. *La fonction $\exp_a$ est dérivable sur $\mathbb{R}$ avec : $\forall x \in \mathbb{R}$, $(\exp_a)'(x) = \ln(a) \cdot a^x$:*

1. *si $a = 1$: elle est constante de valeur 1 ;*
2. *si $a > 1$: elle réalise une bijection strictement croissante de $\mathbb{R}$ sur $\mathbb{R}_+^*$;*
3. *si $a < 1$: elle réalise une bijection strictement décroissante de $\mathbb{R}$ sur $\mathbb{R}_+^*$.*

Proposition I.19. *On a les tableaux de variations et les courbes représentatives "génériques" suivantes :*

x	$-\infty$		0		$+\infty$
$\exp_a$ $a>1$	0	↗	1	↗	$+\infty$

x	$-\infty$		0		$+\infty$
$\exp_a$ $a<1$	$+\infty$	↘	1	↘	0



Définition I.20. *Si $\alpha \in \mathbb{R}$, on appelle fonction **puissance** α la fonction f_α définie sur $\mathbb{R}_+^*$ par : $f_\alpha(x) = x^\alpha = e^{\alpha \ln(x)}$.*

Proposition I.21. *La fonction f_α est dérivable sur $\mathbb{R}_+^*$ avec : $\forall x \in \mathbb{R}_+^*,\ f'_\alpha(x) = \alpha \cdot x^{\alpha-1}$:*

1. *si $\alpha = 0$: elle est constante de valeur 1, et prolongeable par continuité en 0 ;*
2. *si $\alpha < 0$: elle réalise une bijection strictement décroissante de $\mathbb{R}_+^*$ dans lui même, avec pour asymptotes les axes du repère ;*
3. *si $\alpha > 0$: elle réalise une bijection strictement croissante de $\mathbb{R}_+^*$ dans lui-même.*

Démonstration. Par dérivabilité des fonctions composées, f_α est dérivable sur $\mathbb{R}_+^*$ avec :

$$\forall x \in \mathbb{R}_+^*,\ f'_\alpha(x) = \alpha \frac{1}{x} e^{\alpha \ln(x)} = \alpha x^{-1} x^\alpha = \alpha x^{\alpha-1}.$$

Ainsi, f'_α est du signe de α, ce qui donne la monotonie cherchée.
Pour l'image de f_α, on a :

— si $\alpha > 0$: $\lim\limits_{x\to 0} x^\alpha = \lim\limits_{x\to 0} e^{\alpha \ln(x)} = 0$ et $\lim\limits_{x\to+\infty} x^\alpha = \lim\limits_{x\to+\infty} e^{\alpha\ln(x)} = +\infty$;
— si $\alpha < 0$: $\lim\limits_{x\to 0} x^\alpha = \lim\limits_{x\to 0} e^{\alpha \ln(x)} = +\infty$ et $\lim\limits_{x\to+\infty} x^\alpha = \lim\limits_{x\to+\infty} e^{\alpha\ln(x)} = 0$.

Et le dernier point donne les asymptotes. □

Proposition I.22. *Si $\alpha \neq 0$, alors : $f_\alpha^{-1} = f_{\frac{1}{\alpha}}$.*

Démonstration. Soit $\alpha \neq 0$ et $x \in \mathbb{R}_+^*$: $f_\alpha\left(f_{\frac{1}{\alpha}}(x)\right) = \left(x^{\frac{1}{\alpha}}\right)^\alpha = x^{\frac{\alpha}{\alpha}} = x$. □

Proposition I.23. *Si $\alpha > 0$, la fonction f_α est prolongeable par continuité en 0 en une fonction g telle que $g(0) = 0$.*
Son prolongement est :

1. *non dérivable en 0, avec une tangente verticale, si $0 < \alpha < 1$;*
2. *dérivable en 0, de dérivée 1, si $\alpha = 1$;*
3. *dérivable en 0, de dérivée nulle, si $\alpha > 1$.*

Démonstration. Le prolongement continu découle des limites calculées précédemment. Pour $x > 0$, le taux d'accroissement de f_α entre 0 et x est donné par :

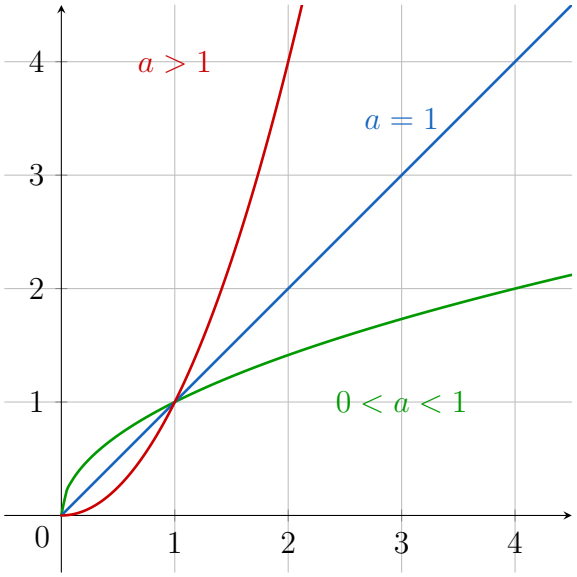
$$\tau_0(x) = \frac{f_\alpha(x) - f_\alpha(0)}{x - 0} = x^{\alpha-1} = f_{\alpha-1}(x)$$

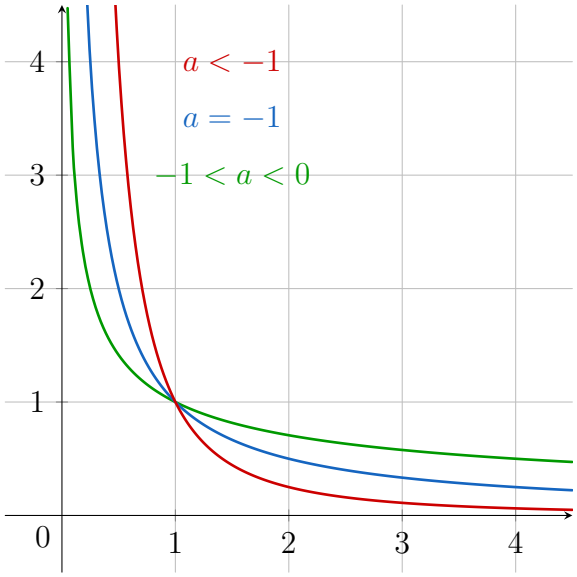
et on peut alors utiliser les limites calculées précédemment.
On trouve bien le résultat voulu, où la disjonction suivant le signe de $\alpha - 1$ nous donne bien les trois cas de la proposition. □

Proposition I.24. *On a les tableaux de variations et les courbes représentatives "génériques" suivantes :*

x	0		1		$+\infty$
f_a $a > 0$	0	↗	1	↗	$+\infty$

x	0		1		$+\infty$
f_a $a < 0$	$+\infty$	↘	1	↘	0





I.4 Comparaisons et limites

Théorème I.25 (Croissances comparées)**.** *Si $\alpha > 0$:*

1. $\lim\limits_{x\to+\infty} \dfrac{\ln(x)}{x} = \lim\limits_{x\to+\infty} \dfrac{\ln(x)}{x^\alpha} = 0$;
2. $\lim\limits_{x\to0} x\ln(x) = \lim\limits_{x\to0} x^\alpha \ln(x) = 0$;
3. $\lim\limits_{x\to+\infty} \dfrac{e^x}{x} = \lim\limits_{x\to+\infty} \dfrac{e^x}{x^\alpha} = +\infty$;
4. $\lim\limits_{x\to-\infty} xe^x = \lim\limits_{x\to-\infty} |x|^\alpha e^x = 0$.

Démonstration.

1. Considérons $\varphi : \left\{ \begin{array}{ccc} [1;+\infty[& \to & \mathbb{R} \\ t & \mapsto & \ln(t) - 2\sqrt{t} \end{array} \right.$.

   Alors φ est dérivable sur $[1;+\infty[$, de dérivée en t : $\varphi'(t) = \dfrac{1}{t} - \dfrac{1}{\sqrt{t}} = \dfrac{1-\sqrt{t}}{t} \leq 0$.

Donc φ est décroissante sur $[1;+\infty[$: comme $\varphi(1) = -2 < 0$, alors φ est strictement négative sur $[1;+\infty[$.

Si $x \geq 1$, on a donc : $0 \leq \ln(x) \leq 2\sqrt{x}$, donc : $0 \leq \dfrac{\ln(x)}{x} \leq \dfrac{2}{\sqrt{x}}$.

Par encadrement : $\lim\limits_{x\to+\infty} \dfrac{\ln(x)}{x} = 0$.

En posant $y = x^\alpha$, donc $x = y^{\frac{1}{\alpha}}$, on trouve :

$$\lim_{x\to+\infty} \frac{\ln(x)}{x^\alpha} = \lim_{y\to+\infty} \frac{\ln(y^{\frac{1}{\alpha}})}{y} = \lim_{y\to+\infty} \frac{1}{\alpha}\frac{\ln(y)}{y} = 0.$$

2. On pose $y = \dfrac{1}{x}$, donc $x = \dfrac{1}{y}$. Alors :

$$\lim_{x\to0} x^\alpha \ln(x) = \lim_{y\to+\infty} \frac{\ln\left(\frac{1}{y}\right)}{y^\alpha} = \lim_{y\to+\infty} -\frac{\ln(y)}{y^\alpha} = 0.$$

3. $\ln\left(\dfrac{e^x}{x^\alpha}\right) = x - \alpha\ln(x) = x \times \left(1 - \alpha\dfrac{\ln(x)}{x}\right) \underset{x\to+\infty}{\to} +\infty$

   donc en composant avec la fonction exponentielle : $\lim\limits_{x\to+\infty} \dfrac{e^x}{x^\alpha} = +\infty$.

4. $\ln\left(|x|^\alpha e^x\right) = \alpha\ln(|x|) + x = x \times \left(1 + \alpha\dfrac{\ln|x|}{x}\right) \underset{x\to-\infty}{\to} -\infty$

   donc en composant avec la fonction exponentielle : $\lim\limits_{x\to-\infty} |x|^\alpha e^x = 0$.

□

Remarque I.26. *L'exponentielle croît infiniment plus vite que les puissances, qui croissent infiniment plus vite que le logarithme. Cela se manifeste dans les limites précédentes en notant que, dans le cas de formes indéterminées, c'est la partie "dominante" qui donne la limite.*

Proposition I.27 (Limites classiques)**.**

1. $\lim\limits_{x\to0} \dfrac{\ln(1+x)}{x} = 1$;
2. $\lim\limits_{x\to0} \dfrac{e^x - 1}{x} = 1$

Démonstration.

1. $\lim\limits_{x\to0} \dfrac{\ln(1+x)}{x} = \lim\limits_{x\to0} \dfrac{\ln(1+x) - \ln(1)}{(1+x) - 1} = \ln'(1) = 1$;
2. $\lim\limits_{x\to0} \dfrac{e^x - 1}{x} = \lim\limits_{x\to0} \dfrac{e^x - e^0}{x - 0} = \exp'(0) = 1.$

□

Exemples I.28. *Pour déterminer une limite, on commence par regarder si les limites classiques et les opérations sur les limites suffisent. Sinon, c'est qu'on obtient une forme indéterminée : il faut alors transformer l'expression habilement pour faire disparaître ces formes indéterminées.*

1. $\lim\limits_{x\to+\infty} \frac{\ln(x^3+1)}{x^4-5}$:

$$\frac{\ln(x^3+1)}{x^4-5} = \frac{\ln(x^3+1)}{x^3+1} \times \frac{x^3+1}{x^4-5} = \underbrace{\frac{\ln(x^3+1)}{x^3+1}}_{\to0} \times \underbrace{\frac{1}{x}}_{\to0} \times \underbrace{\frac{1+\frac{1}{x^3}}{1-\frac{5}{x^4}}}_{\to1} \underset{x\to+\infty}{\longrightarrow} 0.$$

2. $\lim\limits_{x\to+\infty} \frac{\ln(x^4+1)}{x^2+3}$ *:*

$$\frac{\ln(x^4+1)}{x^2+3} = \frac{\ln(x^4+1)}{x^4+1} \times \frac{x^4+1}{x^2+3} = \underbrace{\frac{\ln(x^4+1)}{(x^4+1)^{1/2}}}_{\to 0} \times \underbrace{\frac{(1+\frac{1}{x^4})^{1/2}}{1+\frac{3}{x^2}}}_{\to 1} \underset{x\to+\infty}{\longrightarrow} 0.$$

3. $\lim\limits_{x\to+\infty} \frac{e^{3x}}{x+2}$ *:*

$$\frac{e^{3x}}{x+2} = \underbrace{\frac{e^{3x}}{3x}}_{\to+\infty} \times \underbrace{\frac{3x}{x+2}}_{\to 3} \underset{x\to+\infty}{\longrightarrow} +\infty.$$

4. $\lim\limits_{x\to+\infty} \frac{e^{3x}}{x^3+1}$ *:*

$$\frac{e^{3x}}{x^3+1} = \underbrace{\frac{e^{3x}}{(3x)^3}}_{\to+\infty} \times \underbrace{\frac{(3x)^3}{x^3+1}}_{\to 27} \underset{x\to+\infty}{\longrightarrow} +\infty.$$

5. $\lim\limits_{x\to+\infty} \frac{x^3-3x\ln x+\ln x}{e^x+x\sin x}$ *:*

$$\frac{x^3-3x\ln x+\ln x}{e^x+x\sin x} = \underbrace{\frac{x^3}{e^x}}_{\to 0} \times \underbrace{\frac{1-\frac{3\ln x}{x^2}+\frac{\ln x}{x^3}}{1+\frac{x}{e^x}\sin x}}_{\to 1} \underset{x\to+\infty}{\longrightarrow} 0.$$

Proposition I.29 (Inégalités classiques)**.**

1. *si* $x > -1$*, alors* $\ln(1+x) \leq x$ *;*
2. *si* $x \in \mathbb{R}$*, alors* $e^x \geq 1+x$*.*

Démonstration.

1. posons φ définie sur $]-1;+\infty[$ par :$\varphi(x) = \ln(1+x) - x$.
   Alors φ est dérivable avec : $\varphi'(x) = \dfrac{1}{1+x} - 1 = -\dfrac{x}{1+x}$.
   D'où les variations :

x	-1		0		$+\infty$
φ'	‖	$+$	0	$-$	
φ	‖	↗	0	↘	

   Donc φ est négative sur $]1;+\infty[$, ce qui donne l'inégalité voulue.
2. posons ψ définie sur $\mathbb{R}$ par :$\psi(x) = e^x - x - 1$.
   Alors ψ est dérivable avec : $\psi'(x) = e^x - 1$.
   D'où les variations :

x	$-\infty$		0		$+\infty$
ψ'	‖	$-$	0	$+$	
ψ	‖	↘	0	↗	

Donc ψ est positive sur $\mathbb{R}$, ce qui donne l'inégalité voulue.

□

I.5 Puissances de fonctions par des fonctions

Proposition I.30. *Si u, v sont des fonctions définies sur un intervalle I et dérivables sur I, avec u à valeurs dans $\mathbb{R}_+^*$. Alors la fonction $f : x \mapsto u(x)^{v(x)}$ est bien définie sur I. De plus, elle est dérivable sur I, de dérivée $x \mapsto \ln(u(x))v'(x)u(x)^{v(x)} + v(x)u'(x)u(x)^{v(x)-1}$.*

Démonstration. Comme u est à valeurs dans $\mathbb{R}_+^*$, alors f est bien définie.
Pour analyser en détail f, on préfère écrire : $f : x \mapsto \exp\left(v(x) \cdot \ln(u(x))\right)$.
Par composition et produits, la fonction f est dérivable sur I, et sa dérivée en $x \in I$ est donnée par :

$$f'(x) = (v \cdot \ln(u))'(x) \cdot \exp\left(v(x)\ln(u(x))\right) = (v \cdot \ln(u))'(x) \cdot u(x)^{v(x)}$$

qui donne bien la formule précédente en constatant que :

$$(v \cdot \ln(u))'(x) = \ln(u(x))v'(x) + \frac{v(x)u'(x)}{u(x)}.$$

□

Remarque I.31. *Cette formule n'est pas à connaître : elle est là pour illustrer comment étudier ce type de fonctions, ce qui se fait par passage par l'écriture exponentielle d'une puissance.*

Exemple I.32. *Étudions la fonction $f : x \mapsto x^x$.*
À cause de la puissance quelconque qui apparaît, f est définie sur $\mathbb{R}_+^*$.
De plus, elle est dérivable. On calcule sa dérivée en écrivant que $x^x = \exp(x\ln(x))$, ce qui donne pour tout $x \in \mathbb{R}_+^*$:

$$f'(x) = (\ln(x) + 1)x^x.$$

Par stricte croissance de ln*, on déduit le signe de f' sur $\mathbb{R}_+^*$, et donc les variations de f.*
Étudions les limites de f aux bornes de $\mathbb{R}_+^*$:

— *en 0 : par croissances comparées, on a :* $\lim\limits_{x\to 0} x\ln(x) = 0$ *; et donc par composition de limites :*

$$\lim_{x\to 0} f(x) = \lim_{x\to 0} \exp(x\ln(x)) = \lim_{x\to 0} \exp(x) = 1$$

donc $\lim\limits_{x\to 0} f(x) = 1$ *; ceci nous dit que f est prolongeable par continuité en 0 ; on notera g son prolongement, qui est donc défini sur $\mathbb{R}_+$ par :*

$$g(x) = \begin{cases} x^x & si \quad x > 0 \\ 1 & si \quad x = 0 \end{cases}.$$

— *en $+\infty$:* $\lim\limits_{x\to+\infty} x\ln(x) = +\infty$ *(par calcul direct), et donc par composition :*

$$\lim_{x\to+\infty} f(x) = \lim_{x\to+\infty} \exp(x\ln(x)) = \lim_{x\to+\infty} \exp(x) = +\infty$$

donc $\lim\limits_{x\to+\infty} f(x) = +\infty$.

On déduit donc le tableau de variations suivant :

x	0		$\frac{1}{e}$		$+\infty$
f'	‖	$-$	0	$+$	
f	‖ 1	↘	$\frac{1}{e}^{\frac{1}{e}}$	↗	$+\infty$

Étudions plus en détail f en 0 et en $+\infty$:

— *en 0 : on a déjà le prolongement par continuité ; étudions la dérivabilité du prolongement. Pour $x > 0$, le taux d'accroissement de g entre 0 et x est donné par :*

$$\tau_0(x) = \frac{x^x - 1}{x} = \frac{\exp(x\ln(x)) - 1}{x} = \frac{\exp(x\ln(x)) - 1}{x\ln(x)} \cdot \ln(x)$$

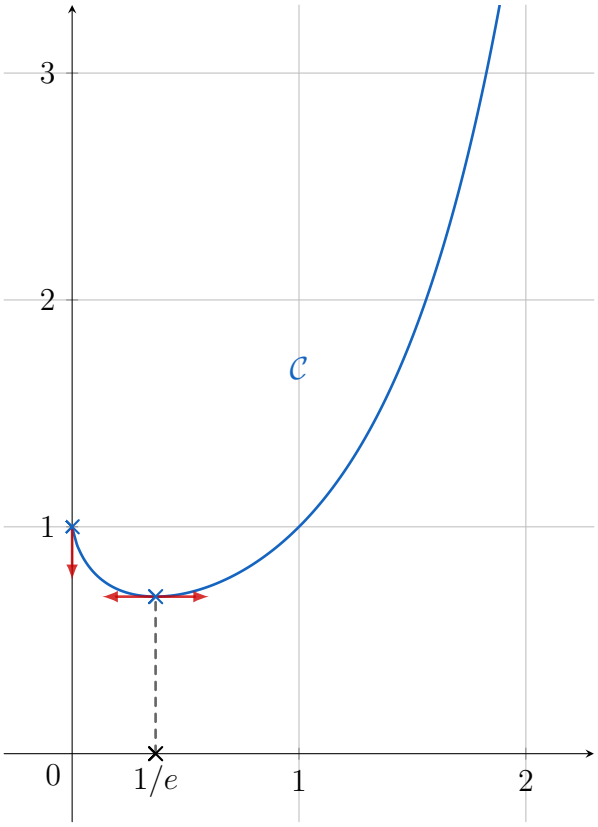
et par limite classique et produit de limites, on a ainsi : $\lim\limits_{x\to 0} \tau_0(x) = -\infty$. Donc g n'est pas dérivable en 0, mais sa courbe y admet une tangente verticale.

— *en $+\infty$: pour $x > 0$, on a :*

$$\frac{f(x)}{x} = x^{x-1} = \exp((x-1)\ln(x))$$

et donc $\lim\limits_{x\to+\infty} \frac{f(x)}{x} = +\infty$ (par calcul direct). Donc la courbe de f admet en $+\infty$ une branche parabolique d'axe vertical.

On a donc le tracé suivant :



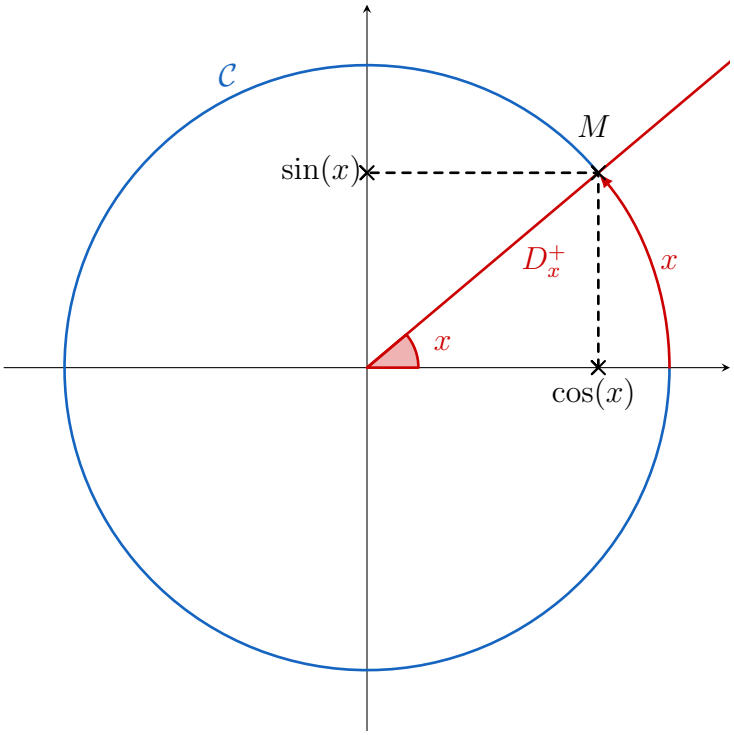
II Les fonctions circulaires

II.1 Le cercle trigonométrique

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

Définition II.1. *Le* ***cercle trigonométrique*** *est le cercle $\mathcal{C}$ de centre O et de rayon 1 : $\mathcal{C} = \{(x,y) \in \mathbb{R}^2,\ x^2+y^2=1\}$.*

Définition II.2. *Pour $t \in \mathbb{R}$, on considère la demi-droite D_t^+ issue de O faisant un angle x avec l'axe des abscisses. Elle coupe $\mathcal{C}$ en un unique point M.*
On appelle ***cosinus*** *de t, noté $\cos(t)$, l'abscisse de M. On appelle* ***sinus*** *de t, noté $\sin(t)$, l'ordonnée de M.*



Définition II.3. *Si $t \in \mathbb{R} \setminus \left\{\frac{\pi}{2}+k\pi,\ k\in,\mathbb{Z}\right\} = \bigcup_{k\in\mathbb{Z}}\left]-\frac{\pi}{2}+k\pi;\frac{\pi}{2}+k\pi\right[$, on définit sa* ***tangente****, notée $\tan(t)$, comme : $\tan(t) = \frac{\sin(t)}{\cos(t)}$.*

Proposition II.4 (Paramétrisation du cercle trigonométrique)**.** *Si $M(x,y)$ est un point du cercle, il existe un réel t tel que $(x,y) = (\cos(t),\sin(t))$. Ce réel est unique à 2π près.*

Démonstration. La demi-droite $[OM)$ fournit l'existence, en prenant pour t l'angle qu'elle fait avec l'axe des abscisses.
L'unicité provient de la définition même de π : deux valeurs de t doivent différer d'un nombre de tours entier du cercle, donc d'un multiple entier de 2π. □

Remarque II.5. *En pratique, on utilisera la paramétrisation pour dire qu'il existe un unique t dans $]\pi;pi]$ ou dans $[0;2\pi[$.*

Corollaire II.6. *Si $r>0$, et que $M(x,y)$ est un point du cercle de centre O de rayon r, il existe un unique réel t (à 2π près) tel que : $(x,y) = (r\cos(t), r\sin(t))$.*

Démonstration. Pour un tel (x,y), on a : $x^2+y^2=r^2$.
Donc, en posant $(x',y') = \left(\frac{x}{r},\frac{y}{r}\right)$, on a : $x'^2+y'^2=1$.
Donc $(x',y') = (\cos(t),\sin(t))$, puis $(x,y) = (r\cos(t), r\sin(t))$. □

Proposition II.7. *Si $t\in\mathbb{R}$, alors :*

1. $\cos^2(t)+\sin^2(t)=1$;
2. $\cos(t+2\pi)=\cos(t)$ *et* $\sin(t+2\pi)=\sin(t)$;

3. $\cos(-t) = \cos(t)$ *et* $\sin(-t) = -\sin(t)$;
4. $\cos(\pi - t) = -\cos(t)$ *et* $\sin(\pi - t) = \sin(t)$;
5. $\cos\left(\frac{\pi}{2} - t\right) = \sin(t)$ *et* $\sin\left(\frac{\pi}{2} - t\right) = \cos(t)$;
6. *si* $t \neq \frac{\pi}{2} + k\pi,\ k \in \mathbb{Z}$ *:* $\tan(t + \pi) = \tan(\pi)$.

Démonstration. 1. théorème de Pythagore ;
2. définition de π ;
3. la symétrie d'axe horizontal transforme D_t^+ en D_{-t}^+ ; donc envoie $(x, y) = (\cos(t), \sin(t))$ sur $(x, -y) = \cos(-t), \sin(-t))$;
4. pareil avec la symétrie d'axe vertical ;
5. pareil avec la symétrie d'axe oblique ;
6. découle de *3.* et *4.*.

□

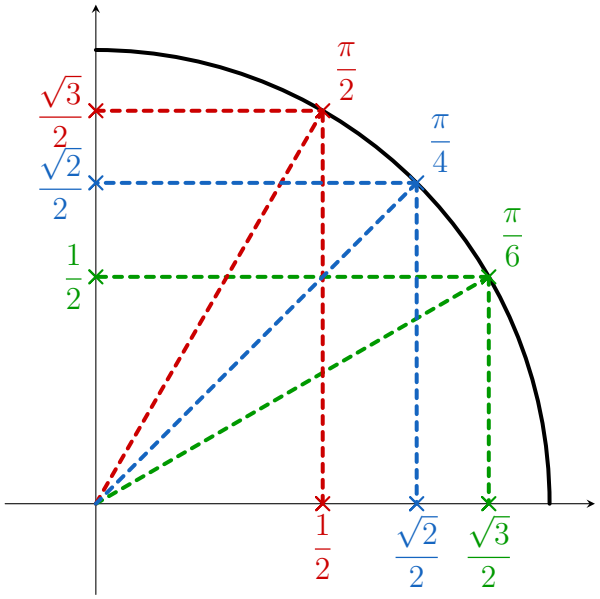
Proposition II.8. *Les fonctions* cos *et* sin *sont* 2π*-périodiques.*
De plus, cos *est paire,* sin *est impaire et pour tout* $t \in \mathbb{R}$ *on a :*

$$\cos(x + \pi) = -\cos(x) \text{ et } \sin(x + \pi) = -\sin(x).$$

Proposition II.9. *La fonction* tan *est* π*-périodique et impaire.*

Proposition II.10 (Valeurs remarquables)**.** *On a le tableau de valeurs :*

t	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$
$\sin(t)$	0	$\frac{1}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1
$\cos(t)$	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0
$\tan(t)$	0	$\frac{\sqrt{3}}{3}$	1	$\sqrt{3}$	*pas défini*



Démonstration. Les valeurs pour 0 ou $\frac{\pi}{2}$ sont immédiates. Pour les autres valeurs, on utilise le théorème de Pythagore dans des triangles particuliers (isocèle-rectangle ou équilatéral). □

Proposition II.11. *Si* $a, b \in \mathbb{R}$*, alors :*

1. $\cos(a + b) = \cos(a)\cos(b) - \sin(a)\sin(b)$;
2. $\cos(a - b) = \cos(a)\cos(b) + \sin(a)\sin(b)$;
3. $\sin(a + b) = \sin(a)\cos(b) + \cos(a)\sin(b)$;
4. $\sin(a - b) = \sin(a)\cos(b) - \cos(a)\sin(b)$;

5. *si* $a, b, a+b \neq \frac{\pi}{2} + k\pi,\ k \in \mathbb{Z}$ *:* $\tan(a+b) = \dfrac{\tan(a)+\tan(b)}{1-\tan(a)\tan(b)}$ *;*
6. *si* $a, b, a-b \neq \frac{\pi}{2} + k\pi,\ k \in \mathbb{Z}$ *:* $\tan(a-b) = \dfrac{\tan(a)-\tan(b)}{1+\tan(a)\tan(b)}$.

Démonstration. On se contente de montrer la deuxième (les autres en découlent).
On pose $M, N \in \mathcal{C}$ avec $M(x,y) = (\cos(a), \sin(a))$ et $N(x', y') = (\cos(b), \sin(b))$.
Alors : $(\overrightarrow{ON}, \overrightarrow{OM}) = (a-b)$.
Donc : $\overrightarrow{ON}.\overrightarrow{OM} = OM \cdot ON \cdot \cos(a-b) = \cos(a-b)$.
Mais on a aussi : $\overrightarrow{ON}.\overrightarrow{OM} = xx' + yy' = \cos(a)\cos(b) + \sin(a)\sin(b)$.
Ce qui donne bien l'égalité cherchée. □

Corollaire II.12. *Pour tout* $a \in \mathbb{R}$ *:*

1. $\cos(2a) = \cos^2(a) - \sin^2(a) = 2\cos^2(a) - 1 = 1 - 2\sin^2(a)$ *;*
2. $\sin(2a) = 2\sin(a)\cos(a)$ *;*
3. *si* $a, 2a \neq \frac{\pi}{2} + k\pi,\ k \in \mathbb{Z}$ *:* $\tan(2a) = \dfrac{2\tan(a)}{1-\tan^2(a)}$.

Et ainsi :

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

Corollaire II.13. *Si* $a \neq k\pi,\ k \in \mathbb{Z}$*, on pose* $t = \tan\left(\frac{a}{2}\right)$*. Alors :*

1. $\sin(a) = \frac{2t}{1+t^2}$ *;*
2. $\cos(a) = \frac{1-t^2}{1+t^2}$ *;*
3. $\tan(a) = \frac{2t}{1-t^2}$ *(si* $a \neq k\frac{\pi}{2},\ k \in \mathbb{Z}$*)*

Démonstration. Montrons par exemple la première. À l'aide du résultat précédent, on trouve :

$$\frac{2t}{1+t^2} = \frac{2\tan(a/2)}{1+\tan^2(a/2)} = 2\frac{\sin(a/2)}{\cos(a/2)}\cos^2(a/2) = 2\sin(a/2)\cos(a/2) = \sin(a)$$

ce qui donne bien le résultat cherché.
Les autres égalités se montrent de même. □

Corollaire II.14 (Formules de développement)**.** *Si* $a, b \in \mathbb{R}$ *:*

1. $\cos(a)\cos(b) = \dfrac{1}{2}\left(\cos(a+b) + \cos(a-b)\right)$ *;*
2. $\sin(a)\sin(b) = \dfrac{1}{2}\left(\cos(a-b) - \cos(a+b)\right)$ *;*
3. $\sin(a)\cos(b) = \dfrac{1}{2}\left(\sin(a+b) + \sin(a-b)\right)$.

Corollaire II.15 (Formules de factorisation)**.** *Si* $a, b \in \mathbb{R}$ *:*

1. $\cos(a) + \cos(b) = 2\cos\left(\dfrac{a+b}{2}\right)\cos\left(\dfrac{a-b}{2}\right)$ *;*
2. $\cos(a) - \cos(b) = -2\sin\left(\dfrac{a+b}{2}\right)\sin\left(\dfrac{a-b}{2}\right)$ *;*
3. $\sin(a) + \sin(b) = 2\sin\left(\dfrac{a+b}{2}\right)\cos\left(\dfrac{a-b}{2}\right)$ *;*

4. $\sin(a) - \sin(b) = 2\cos\left(\frac{a+b}{2}\right)\sin\left(\frac{a-b}{2}\right)$.

Corollaire II.16 (Factorisation générale)**.** *Si $a, b \in \mathbb{R}$, il existe un réel φ tel que :*

$$\forall t \in \mathbb{R},\ a\cos(t) + b\sin(t) = \sqrt{a^2+b^2}\cos(t-\phi).$$

Démonstration. Si $a = b = 0$, alors tout réel φ convient.
Sinon, comme $\left(\frac{a}{\sqrt{a^2+b^2}}\right)^2 + \left(\frac{b}{\sqrt{a^2+b^2}}\right)^2 = 1$, alors il existe φ tel que : $\cos(\varphi) = \frac{a}{\sqrt{a^2+b^2}}$ et $\sin(\varphi) = \frac{b}{\sqrt{a^2+b^2}}$.
Et un tel φ convient d'après les formules d'addition. □

Exemple II.17. *Considérons pour $t \in \mathbb{R}$ l'expression :*

$$\cos(t) + \sqrt{3}\sin(t).$$

On a :

$$\frac{1}{\sqrt{1^2+\sqrt{3}^2}} = \frac{1}{2} \text{ et } \frac{\sqrt{3}}{\sqrt{1^2+\sqrt{3}^2}} = \frac{\sqrt{3}}{2}$$

et ainsi on $\varphi = \frac{\pi}{3}$ convient. Ce qui donne finalement :

$$\forall t \in \mathbb{R},\ \cos(t) + \sqrt{3}\sin(t) = 2\cos\left(t - \frac{\pi}{3}\right).$$

Remarques II.18.

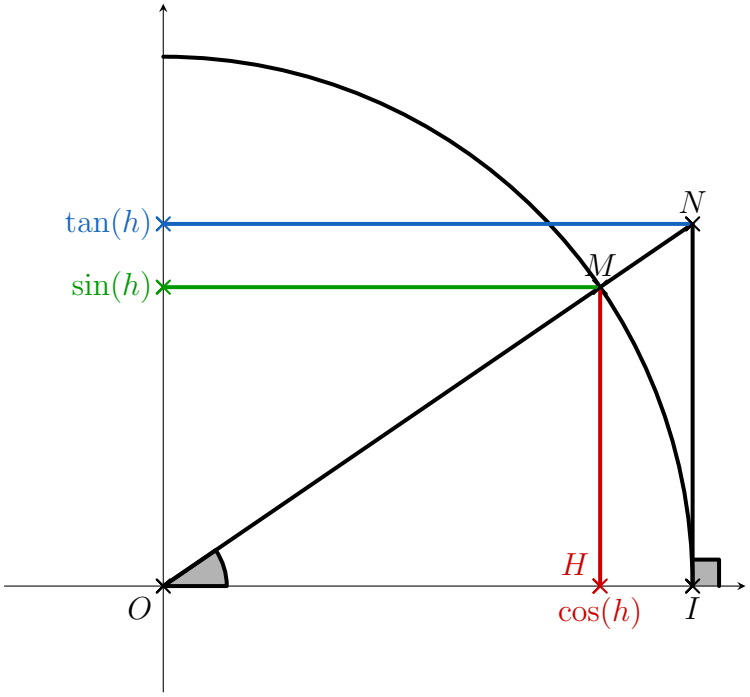
1. *En pratique, on commence par regarder* $\cos(\varphi)$ *(ce qui donneφ au signe près), et* $\sin(\varphi)$ *permet de lever l'ambiguïté sur le signe.*
2. *Ce résultat permet de mieux comprendre les valeurs prises par une combinaison linéaire de* sin *et* cos*. Par exemple, dans l'exemple précédent, on voit que l'expression prend toutes les valeurs entre -2 et 2.*

II.2 Propriétés des fonctions circulaires

Lemme II.19. *On a les limites :*

1. $\lim\limits_{t\to 0} \sin(t) = 0$;
2. $\lim\limits_{t\to 0} \cos(t) = 1$;
3. $\lim\limits_{t\to 0} \frac{\sin(t)}{t} = 1$.

Démonstration. Soit $h \in \left]0; \frac{\pi}{2}\right[$:



On a les aires suivantes :
- le triangle OMI est d'aire $\frac{\sin(h)}{2}$;
- le secteur angulaire entre $[OI]$ et $[OM]$ est d'aire $\frac{h}{2}$;
- le triangle ONI est d'aire $\frac{\tan(h)}{2}$.

Et donc :

$$0 < \sin(h) \leq h \leq \tan(h).$$

1. par encadrement : on trouve $\lim\limits_{h\to 0^+} \sin(h) = 0$;
   Par parité, on a : $\lim\limits_{h\to 0^-} \sin(h) = 0$.
   Donc : $\lim\limits_{t\to 0} \sin(t) = 0$
2. D'où : $\lim\limits_{t\to 0} \cos(t) = \lim\limits_{t\to 0} \left(1 - 2\sin^2(\frac{t}{2})\right) = 1$;
3. En divisant par $\sin(h)$:
$$1 \leq \frac{h}{\sin(h)} \leq \frac{1}{\cos(h)}$$
   d'où par encadrement : $\lim\limits_{h\to 0^+} \dfrac{\sin(h)}{h} = 1$.
   Et par parité : $\lim\limits_{h\to 0^-} \dfrac{\sin(h)}{h} = 1$.
   Donc : $\lim\limits_{t\to 0} \dfrac{\sin(t)}{t} = 1$.

□

Proposition II.20. *Pour tout $x \in \mathbb{R}$, on a :* $|\sin(x)| \leq |x|$.

Démonstration. On procède par disjonction de cas :
- si $x = 0$: ok ;
- si $x \in]0; \frac{\pi}{2}[$: c'est fait dans la démonstration précédente ;
- si $x \in]-\frac{\pi}{2}; 0[$: c'est vrai par parité ;
- si $x \notin]-\frac{\pi}{2}; \frac{\pi}{2}[$: alors $|x| \geq \frac{\pi}{2} > 1 \geq |\sin(x)|$.

□

Théorème II.21. *Les fonction* sin *et* cos *sont continues et dérivables sur* $\mathbb{R}$*, avec* $\sin' = \cos$ *et* $\cos' = -\sin$.

Démonstration. On utilise le lemme et les formules d'addition.
Continuité : Si $x, y \in \mathbb{R}$:

$$|\sin(x) - \sin(y)| = \left|2\cos\left(\frac{x+y}{2}\right)\sin\left(\frac{x-y}{2}\right)\right| \leq 2\left|\sin\left(\frac{x-y}{2}\right)\right| \leq |x-y|$$

donc $\lim\limits_{y\to x}(\sin(x) - \sin(y)) = 0$: sin est continue en x, donc sur $\mathbb{R}$.
Comme $\forall x \in \mathbb{R},\ \cos(x) = \sin\left(x + \frac{\pi}{2}\right)$, alors cos est la composée des fonctions continues sin et $x \mapsto x + \frac{\pi}{2}$, donc cos est continue sur $\mathbb{R}$.
Dérivabilité : Si $x, y \in \mathbb{R}$ avec $x \neq y$:

$$\frac{\sin(x) - \sin(y)}{x - y} = \cos\left(\frac{x+y}{2}\right)\frac{\sin\left(\frac{x-y}{2}\right)}{\frac{x-y}{2}}$$

et :

— par continuité de cos : $\lim\limits_{y\to x}\cos\left(\frac{x+y}{2}\right) = \cos(x)$;

— par le lemme : $\lim\limits_{y\to x}\frac{\sin\left(\frac{x-y}{2}\right)}{\frac{x-y}{2}} = \lim\limits_{t\to 0}\frac{\sin(t)}{t} = 1$.

Donc : $\lim\limits_{y\to x}\dfrac{\sin(x) - \sin(y)}{x - y} = \cos(x)$.
Donc sin est dérivable sur $\mathbb{R}$, avec : $\sin' = \cos$.
Par dérivée d'une composée, cos est dérivable et pour tout $x \in \mathbb{R}$:

$$\cos'(x) = 1 \times \sin'\left(x + \frac{\pi}{2}\right) = \cos\left(x + \frac{\pi}{2}\right) = -\sin(x)$$

donc $\cos' = -\sin$. □

Corollaire II.22. *Les fonctions* cos *et* sin *sont de classe* $\mathcal{C}^\infty$ *sur* $\mathbb{R}$.

Démonstration. On prouve par récurrence sur $n \in \mathbb{N}$ que :

$$\forall n \in \mathbb{N},\ \cos^{(n)} = \cos\left(x + \frac{n\pi}{2}\right) \text{ et } \sin^{(n)} = \sin\left(x + \frac{n\pi}{2}\right).$$

□

Corollaire II.23. *La fonction* tan *est continue et dérivable sur* $\mathbb{R}\setminus\{\frac{\pi}{2} + k\pi,\ k \in \mathbb{Z}\}$*, avec :* $\tan' = 1 + \tan^2 = \frac{1}{\cos^2}$.

II.3 Réciproques des fonctions circulaires

Proposition-Définition II.24. *La restriction de la fonction* sin *à* $\left[-\frac{\pi}{2}; \frac{\pi}{2}\right]$ *est une bijection strictement croissante de* $\left[-\frac{\pi}{2}; \frac{\pi}{2}\right]$ *sur* $[-1; 1]$.
Sa réciproque, appelée ***arc sinus****, notée* Arcsin*, réalise une bijection de* $[-1; 1]$ *sur* $\left[-\frac{\pi}{2}; \frac{\pi}{2}\right]$*. Elle est continue, strictement croissante et impaire sur* $[-1; 1]$.
Elle est dérivable sur $]-1; 1[$ *avec :* $\forall x \in]-1; 1[,\ \text{Arcsin}'(x) = \frac{1}{\sqrt{1-x^2}}$.
Elle admet en -1 *et en* 1 *des demi-tangentes verticales.*

Démonstration. On utilise que $\sin' = \cos$, qui est positive sur $\left[-\frac{\pi}{2}; \frac{\pi}{2}\right]$, s'annulant uniquement en $\pm\frac{\pi}{2}$.
Les propriétés (croissance, continuité, dérivabilité, tangentes verticales) découlent des propriétés de sin par théorème de la bijection monotone.

Montrons l'imparité de Arcsin : soit $y \in [-1;1]$. Notons $x = \text{Arcsin}(y)$, et donc $x \in [-\frac{\pi}{2};\frac{\pi}{2}]$ vérifie $\sin(x) = y$. Ainsi :

$$-y = -\sin(x) = \sin(-x).$$

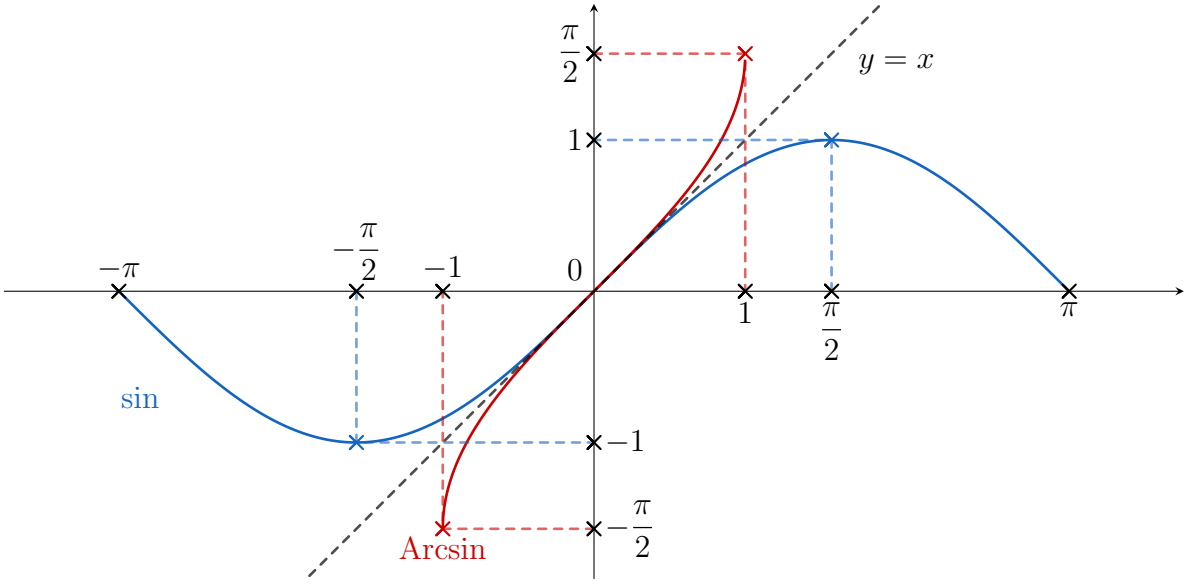
Comme $(-x) \in [-\frac{\pi}{2};\frac{\pi}{2}]$, alors on a : $\text{Arcsin}(-y) = -x = -\text{Arcsin}(y)$, ce qui montre bien que Arcsin est impaire.
Montrons la formule de la dérivée de Arcsin. Soit $y \in]-1;1[$, et notons $x = \text{Arcsin}(y)$. Par définition, on a : $x \in \left[-\frac{\pi}{2};\frac{\pi}{2}\right]$, donc $\cos(x) \geq 0$. Donc : $\cos(x) = \sqrt{\cos^2(x)} = \sqrt{1-\sin^2(x)} = \sqrt{1-y^2}$. Et ainsi :

$$\text{Arcsin}'(y) = \frac{1}{\cos(x)} = \frac{1}{\sqrt{1-\sin^2(x)}} = \frac{1}{\sqrt{1-y^2}}.$$

□

Remarque II.25. *Si $y \in [-1;1]$, alors :* $\sin(\text{Arcsin}(y)) = y$.
En revanche, si $x \in \mathbb{R}$, alors : $\text{Arcsin}(\sin(x)) \neq x$, *à moins que* $x \in \left[-\frac{\pi}{2};\frac{\pi}{2}\right]$.

Proposition II.26. *On a les représentations graphiques suivantes :*

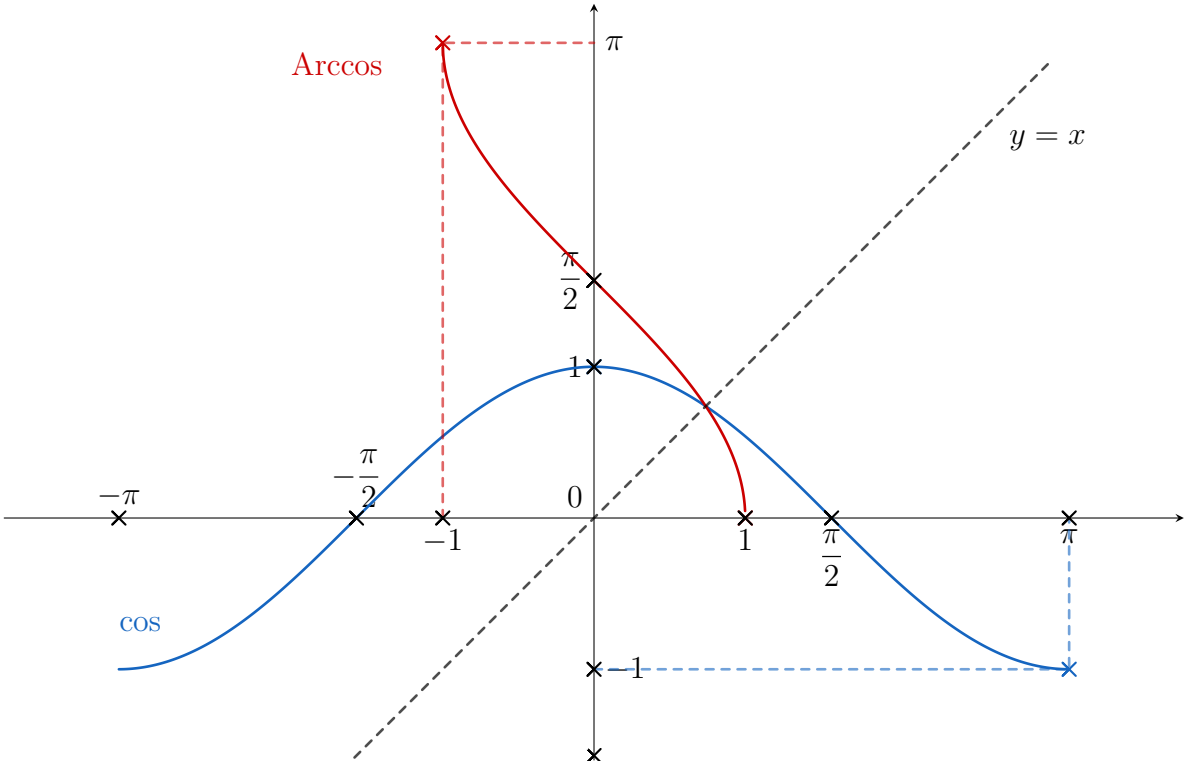


Proposition-Définition II.27. *La restriction de la fonction* cos *à* $[0;\pi]$ *est une bijection strictement décroissante de* $[0;\pi]$ *sur* $[-1;1]$.
Sa réciproque, appelée ***arc cosinus****, notée* Arccos, *réalise une bijection de* $[-1;1]$ *sur* $[0;\pi]$. *Elle est continue et strictement croissante sur* $[-1;1]$.
Elle est dérivable sur $]-1;1[$ *avec :* $\forall x \in]-1;1[,\ \text{Arccos}'(x) = \frac{-1}{\sqrt{1-x^2}}$.
Elle admet en -1 *et en* 1 *des demi-tangentes verticales.*

Démonstration. Comme pour Arcsin. □

Remarque II.28. *Si $y \in [-1;1]$, alors :* $\cos(\text{Arccos}(y)) = y$.
En revanche, si $x \in \mathbb{R}$, alors : $\text{Arccos}(\cos(x)) \neq x$, *à moins que* $x \in [0;\pi]$.

Proposition II.29. *On a les représentations graphiques suivantes :*



Proposition-Définition II.30. *La restriction de la fonction* tan *à* $]-\frac{\pi}{2};\frac{\pi}{2}[$ *est une bijection strictement croissante de* $]-\frac{\pi}{2};\frac{\pi}{2}[$ *sur* $\mathbb{R}$.
Sa réciproque, appelée ***arc tangente****, notée* Arctan, *réalise une bijection de* $\mathbb{R}$ *sur* $]-\frac{\pi}{2};\frac{\pi}{2}[$. *Elle est continue, strictement croissante et impaire sur* $\mathbb{R}$.
Elle est dérivable sur $\mathbb{R}$ *avec :* $\forall x \in]-1;1[,\ \text{Arctan}'(x) = \frac{1}{1+x^2}$.

Démonstration. La stricte monotonie de tan sur $]-\frac{\pi}{2};\frac{\pi}{2}[$ découle de l'expression de sa dérivée :

$$\forall x \in]-\frac{\pi}{2};\frac{\pi}{2}[,\ \tan'(x) = 1+\tan^2(x) \geq 1 > 0.$$

L'imparité de Arctan découle de l'imparité de tan (et se démontre comme pour Arcsin).
Reste à déterminer l'image de $]-\frac{\pi}{2};\frac{\pi}{2}[$ par tan. Pour cela, on étudie les limites de tan en $\pm\frac{\pi}{2}$:

— en $-\frac{\pi}{2}^+$: on a les limites suivantes :

$$\lim_{x\to-\frac{\pi}{2}^+} \sin(x) = -1 \text{ et } \lim_{x\to-\frac{\pi}{2}^+} \cos(x) = 0^+$$

et donc : $\lim\limits_{x\to-\frac{\pi}{2}^+} \tan(x) = -\infty$;

— en $\frac{\pi}{2}^-$: on a les limites suivantes :

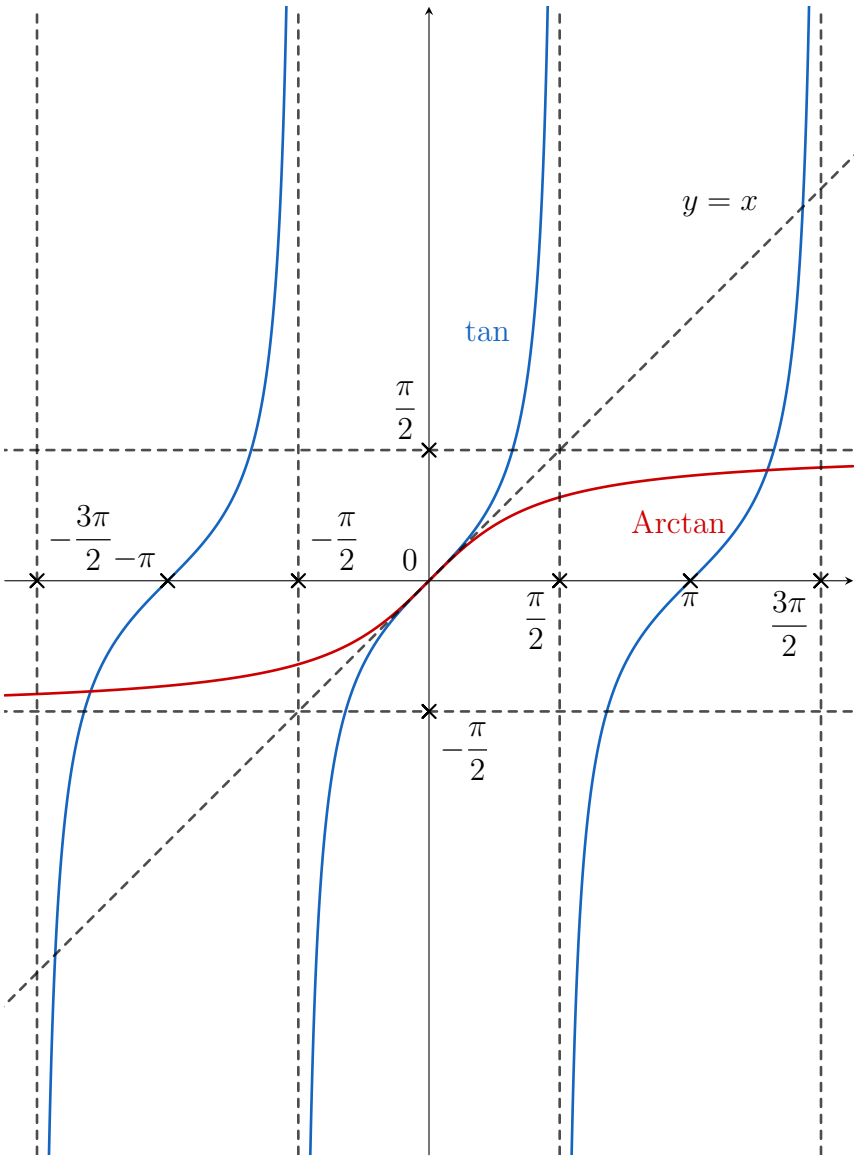
$$\lim_{x\to\frac{\pi}{2}^-} \sin(x) = 1 \text{ et } \lim_{x\to\frac{\pi}{2}^-} \cos(x) = 0^+$$

et donc : $\lim\limits_{x\to\frac{\pi}{2}^-} \tan(x) = +\infty$;

ce qui donne bien la bijectivité de tan de $]-\frac{\pi}{2};\frac{\pi}{2}[$ sur $\mathbb{R}$. □

Remarque II.31. *Si* $y \in \mathbb{R}$, *alors :* $\tan(\text{Arctan}(y)) = y$.
En revanche, si $x \in \mathbb{R} \setminus \{\frac{\pi}{2} + k\pi,\ k \in \mathbb{Z}\}$, *alors :* $\text{Arctan}(\tan(x)) \neq x$, *à moins que* $x \in]-\frac{\pi}{2};\frac{\pi}{2}[$.

Proposition II.32. *On a les représentations graphiques suivantes :*



Proposition II.33. *On a :*

1. $\cos(a) = \cos(b) \Leftrightarrow (a \equiv b\ [2\pi]$ *ou* $a \equiv -b\ [2\pi]\ )$;
2. $\sin(a) = \sin(b) \Leftrightarrow (a \equiv b\ [2\pi]$ *ou* $a \equiv \pi - b\ [2\pi]\ )$;
3. $\tan(a) = \tan(b) \Leftrightarrow (a \equiv b\ [\pi]\ )$

Démonstration.

1. Par 2π-périodicité, on peut supposer $a, b \in]-\pi;\pi]$.
   Comme cos est strictement croissante sur $[-\pi;0]$, strictement décroissante sur $[0;\pi]$, avec $\cos(-\pi) = \cos(\pi) = -1$ et $\cos(0) = 1$, alors :
   — si $\cos(a) \neq \pm 1$: alors $\cos(a)$ possède deux antécédents par cos dans $]-\pi;\pi]$, qui sont a et $-a$;
   — si $\cos(a) = \pm 1$: alors $a = 0$ ou π, et a est l'unique antécédent de $\cos(a)$ par cos sur $]-\pi;\pi]$.
   Ce qui donne bien l'équivalence cherchée.
2. Le cas de sin se traite de la même manière en regardant les variations de sin sur $]-\frac{\pi}{2};\frac{3\pi}{2}]$.
3. Le cas de tan découle de la π-périodique et de la bijectivité de tan de $\left]-\frac{\pi}{2};\frac{\pi}{2}\right[$ sur $\mathbb{R}$.

□

Proposition II.34. *Si* $x \in [-1;1]$, *alors :*

$$\mathrm{Arcsin}(x) + \mathrm{Arccos}(x) = \frac{\pi}{2}.$$

Démonstration. Soit $x \in [-1;1]$. Posons : $a = \text{Arccos}(x)$ et $b = \frac{\pi}{2} - \text{Arcsin}(x)$.
Alors $a, b \in [0;\pi]$ et la fonction cos est injective sur $[0;\pi]$.
Mais $\cos(a) = x$ et $\cos(b) = \sin(\text{Arcsin}(x)) = x$.
Donc $a = b$. □

Proposition II.35. *Si $x \in \mathbb{R}^*$, alors :*

$$\text{Arctan}(x) + \text{Arctan}\left(\frac{1}{x}\right) = \begin{cases} \frac{\pi}{2} & si\ x > 0 \\ -\frac{\pi}{2} & si\ x < 0 \end{cases}$$

Démonstration. On définit la fonction f sur $\mathbb{R}^*$ par $f(x) = \text{Arctan}(x) + \text{Arctan}\left(\frac{1}{x}\right)$.
Alors f est dérivable sur $\mathbb{R}^*$, avec :

$$\forall x \in \mathbb{R}^*,\ f'(x) = \frac{1}{1+x^2} + \frac{-1}{x^2} \cdot \frac{1}{1+\frac{1}{x^2}} = 0$$

donc f est constante sur chaque intervalle de $\mathbb{R}^*$, donc sur $\mathbb{R}_+^*$ et sur $\mathbb{R}_-^*$.
On a : $f(1) = 2\text{Arctan}(1) = \frac{\pi}{2}$ et $f(-1) = 2\text{Arctan}(-1) = -\frac{\pi}{2}$.
D'où le résultat. □

III Les fonctions hyperboliques

Définition III.1. *On définit sur $\mathbb{R}$ les fonctions :*

1. ***cosinus hyperbolique**, notée* ch, *par :* $\text{ch}(x) = \dfrac{e^x + e^{-x}}{2}$;
2. ***sinus hyperbolique**, notée* sh, *par :* $\text{sh}(x) = \frac{e^x - e^{-x}}{2}$;
3. ***tangente hyperbolique**, notée* th, *par :* $\text{th}(x) = \frac{\text{sh}(x)}{\text{ch}(x)} = \frac{e^x - e^{-x}}{e^x + e^{-x}}$.

Proposition III.2. *Pour tout $x \in \mathbb{R}$, on a :* $\text{ch}^2(x) - \text{sh}^2(x) = 1$.

Démonstration. Soit $x \in \mathbb{R}$. On a :

$$\text{ch}^2(x) - \text{sh}^2(x) = \left(\frac{e^x + e^{-x}}{2}\right)^2 - \left(\frac{e^x - e^{-x}}{2}\right)^2 = \frac{1}{4}\left(e^{2x} + 2 + e^{-2x} - (e^{2x} - 2 + e^{-2x})\right) = 1.$$

□

Proposition III.3. *La fonction* ch *et paire, dérivable sur $\mathbb{R}$ de dérivée* sh.
Elle vérifie : $\lim\limits_{x\to+\infty} \text{ch}(x) = \lim\limits_{x\to-\infty} \text{ch}(x) = +\infty$.

Démonstration. Si $x \in \mathbb{R}$, alors : $\text{ch}(-x) = \frac{e^{-x}+e^x}{2} = \text{ch}(x)$ donc ch est paire.
Elle est dérivable avec, pour tout $x \in \mathbb{R}$:

$$\text{ch}'(x) = \frac{e^x - e^{-x}}{2} = \text{sh}(x).$$

Comme $\lim\limits_{x\to+\infty} e^x = +\infty$ et $\lim\limits_{x\to-\infty} e^x = 0$, on trouve les limites voulues. □

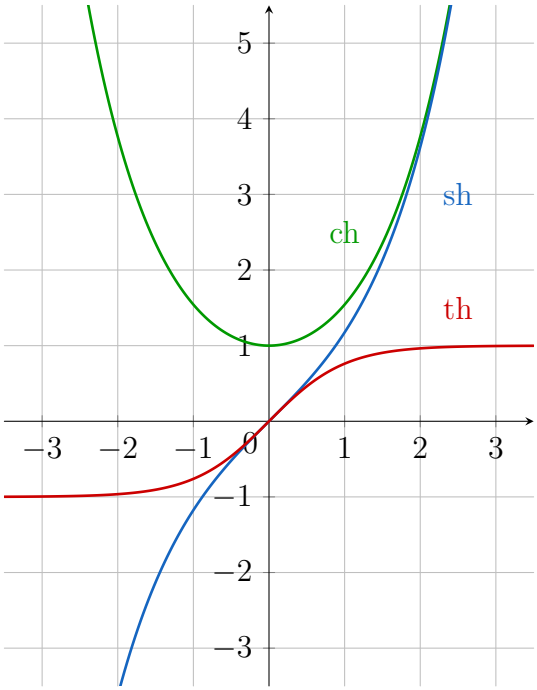
Proposition III.4. *La fonction* sh *et impaire, dérivable sur $\mathbb{R}$ de dérivée* ch.
Elle vérifie : $\lim\limits_{x\to+\infty} \text{sh}(x) = +\infty$ *et* $\lim\limits_{x\to-\infty} \text{sh}(x) = -\infty$.

Proposition III.5. *La fonction* th *et impaire, dérivable sur $\mathbb{R}$ de dérivée* $\frac{1}{\text{ch}^2} = 1 - \text{th}^2$.
Elle vérifie : $\lim\limits_{x\to+\infty} \text{th}(x) = 1$ *et* $\lim\limits_{x\to-\infty} \text{th}(x) = -1$.

x	$-\infty$		0		$+\infty$
ch'		$-$	0	$+$	
ch	$+\infty$	$\searrow$	1	$\nearrow$	$+\infty$

x	$-\infty$		0		$+\infty$
sh'		$+$	1	$+$	
sh	$-\infty$	$\nearrow$	0	$\nearrow$	$+\infty$

x	$-\infty$		0		$+\infty$
th'		$+$	1	$+$	
th	-1	$\nearrow$	0	$\nearrow$	1



Proposition III.6. *Pour tous $a, b \in \mathbb{R}$, on a :*

1. $\mathrm{ch}(a+b) = \mathrm{ch}(a)\mathrm{ch}(b) + \mathrm{sh}(a)\mathrm{sh}(b)$;
2. $\mathrm{sh}(a+b) = \mathrm{sh}(a)\mathrm{ch}(b) + \mathrm{ch}(a)\mathrm{sh}(b)$;
3. $\mathrm{th}(a+b) = \frac{\mathrm{th}(a)+\mathrm{th}(b)}{1+\mathrm{th}(a)\mathrm{th}(b)}$.

Proposition-Définition III.7.

1. *La fonction* ch *réalise une bijection strictement croissante de* $[0;+\infty[$ *sur* $[1;+\infty[$. *Sa réciproque, notée* argch *est dérivable sur* $]1;+\infty[$ *avec :* $\forall x \in]1;+\infty[,\ \mathrm{argch}'(x) = \dfrac{1}{\sqrt{x^2-1}}$.
2. *La fonction* sh *réalise une bijection strictement croissante de* $\mathbb{R}$ *dans lui-même. Sa réciproque, notée* argsh *est dérivable sur* $\mathbb{R}$ *avec :* $\forall x \in \mathbb{R},\ \mathrm{argsh}'(x) = \dfrac{1}{\sqrt{x^2+1}}$.
3. *La fonction* th *réalise une bijection strictement croissante de* $\mathbb{R}$ *sur* $]-1;1[$. *Sa réciproque, notée* argth *est dérivable sur* $]-1;1[$ *avec :* $\forall x \in]-1;1[,\ \mathrm{argth}'(x) = \dfrac{1}{1-x^2}$.

Démonstration. L'existence et la dérivabilité découle des points précédents.
Si $x \in]1;+\infty[$. On note $y \in \mathbb{R}_+^*$ tel que $\mathrm{ch}(y) = x$. Alors : $\mathrm{argch}'(x) = \frac{1}{\mathrm{sh}(y)}$.
Comme $\mathrm{ch}^2(y) - \mathrm{sh}^2(y) = 1$, alors $\mathrm{sh}(y) = \pm\sqrt{x^2-1}$. Mais $y \in \mathbb{R}_+^*$, donc $\mathrm{sh}(y) > 0$, et : $\mathrm{sh}(y) = \sqrt{x^2-1}$.
Et finalement : $\mathrm{argch}'(x) = \frac{1}{\sqrt{x^2-1}}$.
Et pareil pour les autres. □

Remarque III.8. *Les réciproques des fonctions circulaires hyperboliques s'expriment explicitement de la manière suivante :*

$$\mathrm{Argch}(x) = \ln\left(x + \sqrt{x^2-1}\right),\ \mathrm{Argsh}(x) = \ln\left(x + \sqrt{x^2+1}\right)\ \textit{et}\ \mathrm{Argth}(x) = \frac{1}{2}\ln\left(\frac{1+x}{1-x}\right).$$

Chapitre 8

Les complexes

I L'ensemble $\mathbb{C}$

Définition I.1. *On note i une solution de l'équation $x^2+1=0$.*
On définit alors l'ensemble $\mathbb{C}$ des ***complexes*** *comme :*

$$\mathbb{C} = \{a+ib \,|\, a,b \in \mathbb{R}\}.$$

Si $a,b \in \mathbb{R}$ et $z=a+ib$, on dit que a est la ***partie réelle*** *de z, notée $\mathrm{Re}(z)$, et que b est la* ***partie imaginaire****, notée $\mathrm{Im}(z)$. Et l'écriture $z=a+ib$ est appelée* ***écriture algébrique*** *de z.*

Remarque I.2. *Un nombre complexe est entièrement déterminé par ses parties réelles et imaginaires, c'est-à-dire que :*

$$\forall a,a',b,b' \in \mathbb{R},\ a+ib=a'+ib' \Leftrightarrow \left\{ \begin{array}{rcl} a & = & a' \\ b & = & b' \end{array} \right. .$$

Remarques I.3.

1. *L'ensemble des réel est l'ensemble des complexes de partie imaginaire nulle.*
2. *On appelle* ***imaginaires purs*** *l'ensemble $i\mathbb{R}$ des complexes de partie réelle nulle.*

Proposition I.4. *Si $a,a',b,b' \in \mathbb{R}$, on a les écritures algébriques :*

1. $(a+ib)+(a'+ib') = (a+a')+i(b+b')$;
2. $(a+iy)\times(a'+ib') = (aa'-bb')+i(xy'+yx')$.

Proposition-Définition I.5 (Inverse)**.** *Si $z \in \mathbb{C}^*$, alors il existe un unique $\omega \in \mathbb{C}^*$ tel que $z\omega = 1$: on l'appelle* ***l'inverse*** *de z, et on note $\omega = \frac{1}{z}$.*

Démonstration. On procède par analyse-synthèse. On pose $z=a+ib$ et $\omega = x+iy$.
Alors :

$$\begin{array}{rcl} z\omega = 1 & \Rightarrow & (ax-by)+i(bx+ay)=1 \\ & \Rightarrow & \left\{ \begin{array}{rcl} ax-by & = & 1 \\ bx+ay & = & 0 \end{array} \right. \\ & \Rightarrow & \left\{ \begin{array}{rcl} a^2x-aby & = & a \\ aby+b^2x & = & 0 \\ abx-b^2y & = & b \\ abx+a^2y & = & 0 \end{array} \right. \\ & \Rightarrow & \left\{ \begin{array}{rcl} x & = & \dfrac{a}{a^2+b^2} \\ y & = & -\dfrac{b}{a^2+b^2} \end{array} \right. \end{array}$$

où $a^2+b^2 \neq 0$ comme $z \neq 0$.
Réciproquement : $\omega = \dfrac{a-ib}{a^2+b^2}$ vérifie bien $\omega z = 1$. □

Définition I.6. *Étant donné $(O, \overrightarrow{i}, \overrightarrow{j})$ un repère du plan, on associe à tout point $M(x, y)$ le complexe $z = x + iy$. On dit alors que z est **l'affixe** de M, ou que M est **l'image** du complexe z.*
On dira également que $z = x + iy$ est l'affixe du vecteur $\overrightarrow{u} = x\overrightarrow{i} + y\overrightarrow{j}$.

II Conjugaison et module

Définition II.1 (Conjugué complexe)**.** *Si $z = a + ib$ (forme algébrique), le complexe $\overline{z} = a - ib$ est appelé **conjugué (complexe)** de z.*

Proposition II.2. *Si $z \in \mathbb{C}$, alors $\mathrm{Re}(z) = \dfrac{1}{2}(z + \overline{z})$ et $\mathrm{Im}(z) = \dfrac{1}{2i}(z - \overline{z})$.*

Corollaire II.3. *On déduit les équivalences suivantes :*

1. *$z \in \mathbb{R} \Leftrightarrow \mathrm{Im}(z) \Leftrightarrow z = \overline{z}$;*
2. *$z \in i\mathbb{R} \Leftrightarrow \mathrm{Re}(z) \Leftrightarrow z = -\overline{z}$;*

Proposition II.4. *Si $z, z' \in \mathbb{C}$ et $\lambda \in \mathbb{R}^*$, alors :*

1. *$\overline{z + z'} = \overline{z} + \overline{z'}$;*
2. *$\overline{\lambda z} = \lambda \overline{z}$;*
3. *$\overline{zz'} = \overline{z}\,\overline{z'}$;*
4. *si $z \neq 0$: $\dfrac{\overline{z'}}{z} = \dfrac{\overline{z'}}{\overline{z}}$ et $\dfrac{\overline{1}}{z} = \dfrac{\overline{1}}{\overline{z}}$;*
5. *$\overline{(\overline{z})} = z$.*

Remarque II.5. *En particulier, on déduit que l'application $z \mapsto \overline{z}$ est une application $\mathbb{R}$-linéaire sur $\mathbb{C}$ qui est involutive (et elle est donc bijective)*

Définition II.6 (Module)**.** *Si $z = a + ib$ (forme algébrique), on appelle **module de** z le réel positif ou nul défini par :*

$$|z| = \sqrt{a^2 + b^2}.$$

Proposition II.7. *Si $z \in \mathbb{C}$, alors : $|z| = \sqrt{z\overline{z}} = |\overline{z}|$. Et ainsi :*

1. *Si $z \in \mathbb{C}$: $|\mathrm{Re}(z)| \leq |z|$ et $|\mathrm{Im}(z)| \leq |z|$;*
2. *$|z| = 0 \Leftrightarrow z = 0$;*
3. *si $z \neq 0$: $z^{-1} = \dfrac{\overline{z}}{|z|^2}$;*
4. *si $z, z' \in \mathbb{C}$: $|zz'| = |z| \cdot |z'|$ et $\left|\dfrac{z}{z'}\right| = \dfrac{|z|}{|z'|}$ (si $z' \neq 0$).*

Démonstration. Notons $z = a + ib$. Alors :

$$z\overline{z} = (a + ib)(a - ib) = a^2 + b^2$$

Le reste en découle. □

Remarque II.8. *On déduit que, si $z \in \mathbb{C}$ et $\lambda \in \mathbb{R}$: $|\lambda z| = |\lambda| \cdot |z|$.*

Corollaire II.9. *Pour $z \in \mathbb{C}^*$, on a l'équivalence : $|z| = 1 \Leftrightarrow \dfrac{1}{z} = \overline{z}$.*

Théorème II.10 (Inégalité triangulaire)**.** *Si $z, z' \in \mathbb{C}$, alors :*

1. *$|z + z'| \leq |z| + |z'|$;*

2. $||z| - |z'|| \leq |z - z'|$.

De plus, il y a égalité dans les deux cas si, et seulement si, z et z' sont positivement liés : $z' = 0$ ou il existe $\lambda \in \mathbb{R}_+$ tel que $z = \lambda z'$.

Démonstration. Si $z, z' \in \mathbb{C}$, alors :
- $|z + z'|^2 = |z|^2 + |z'|^2 + 2\mathrm{Re}(z\overline{z'})$;
- $|z - z'|^2 = |z|^2 + |z'|^2 - 2\mathrm{Re}(z\overline{z'})$;
- $(|z| + |z'|)^2 = |z|^2 + |z'|^2 + 2|z\overline{z'}|$;
- $||z| - |z'||^2 = |z|^2 + |z'|^2 - 2|z\overline{z'}|$.

Les inégalités découlent de : $-2|z\overline{z'}| \leq \pm 2\mathrm{Re}(z\overline{z'}) \leq 2\|z\overline{z'}|$.
On a égalité dans la première si, et seulement si : $\mathrm{Re}(z\overline{z'}) = |zz'|$, c'est-à-dire $z\overline{z'} \in \mathbb{R}_+$. Tout va bien si $z' = 0$. Sinon, on a :

$$z = \frac{z\overline{z'}}{\overline{z'}} = \frac{z\overline{z'}}{\underbrace{z'\overline{z'}}_{\in \mathbb{R}_+}} z' = \lambda z'.$$

Et pareil pour la seconde inégalité. □

Remarque II.11. *On les regroupe dans la double inégalité :*

$$||z| - |z'|| \leq |z \pm z'| \leq |z| + |z'|.$$

Corollaire II.12. *Si $z_1, \ldots, z_n$ sont des complexes, alors :*

$$\left|\sum_{k=1}^{n} z_k\right| = |z_1 + z_2 + \cdots + z_n| \leq |z_1| + |z_2| + \cdots + |z_n| = \sum_{k=1}^{n} |z_k|$$

avec égalité si, et seulement si, tous les z_k sont deux-à-deux positivement liés.

Démonstration. Par récurrence. □

III Trigonométrie et exponentielle complexe

III.1 Argument d'un complexe

Définition III.1. *On note $\mathbb{U}$ l'ensemble des nombres complexes de module 1 :*

$$\mathbb{U} = \{z \in \mathbb{C} \,|\, |z| = 1\}.$$

Proposition III.2. *L'ensemble $\mathbb{U}$ est stable par produit, quotient et conjugaison :*

$$\forall z, z' \in \mathbb{U},\ zz' \in \mathbb{U},\ \frac{z}{z'} \in \mathbb{U} \text{ et } \overline{z} \in \mathbb{U}.$$

Démonstration. Découle des propriétés du module. □

Définition III.3 (Exponentielle complexe)**.** *On définit **l'exponentielle complexe** sur les imaginaires purs par :*

$$\forall \theta \in \mathbb{R},\ e^{i\theta} = \cos(\theta) + i\sin(\theta).$$

Exemples III.4. *On a les valeurs particulières :*

$$e^{i0} = e^{2i\pi} = 1,\ e^{i\pi} = e^{-i\pi} = -1,\ e^{i\frac{\pi}{2}} = i \text{ et } e^{-i\frac{\pi}{2}} = -i.$$

Proposition III.5. *Si $\theta_1, \theta_2 \in \mathbb{R}$ et $k \in \mathbb{Z}$, alors :*

1. $e^{i(\theta_1+2k\pi)} = e^{i\theta_1}$;
2. $e^{i(\theta_1+\theta_2)} = e^{i\theta_1}e^{i\theta_2}$;
3. $e^{i(\theta_1-\theta_2)} = \dfrac{e^{i\theta_1}}{e^{i\theta_2}}$;
4. $\overline{e^{i\theta_1}} = e^{-i\theta_1}$;
5. $|e^{i\theta_1}| = 1$.

Démonstration. Découle des propriétés de cos et sin. Montrons par exemple l'exponentielle complexe d'une somme. On a :

$$\begin{aligned} e^{i(\theta_1+\theta_2)} &= \cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2) \\ &= \cos(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2) + i\left(\cos(\theta_1)\sin(\theta_2) + \sin(\theta_1)\cos(\theta_2)\right) \\ &= \left(\cos(\theta_1) + i\sin(\theta_1)\right)\left(\cos(\theta_2) + i\sin(\theta_2)\right) \\ &= e^{i\theta_1}e^{i\theta_2} \end{aligned}$$

□

Proposition III.6. *L'identification de $\mathbb{C}$ au plan $\mathbb{R}^2$ identifie l'ensemble $\mathbb{U}$ au cercle trigonométrique $\mathcal{C}$. Ainsi, pour tout $z \in \mathbb{U}$, il existe $\theta \in \mathbb{R}$ (unique à 2π près) tel que : $z = \cos(\theta) + i\sin(\theta) = e^{i\theta}$.*

Démonstration. Si z est l'affixe de $M(x, y)$, alors :

$$z \in \mathbb{U} \Leftrightarrow x^2 + y^2 = 1 \Leftrightarrow M \in \mathcal{C}.$$

Le reste découle de la paramétrisation de $\mathcal{C}$. □

Corollaire III.7. *La fonction définie de $\mathbb{R}_+^* \times]-\pi;\pi]$ sur $\mathbb{C}^*$ par : $(r, \theta) \mapsto re^{i\theta}$ est bijective.*

Démonstration.

— surjectivité : si $z \in \mathbb{C}^*$, alors $\frac{z}{|z|} \in \mathbb{U}$ et on applique la proposition ;

— injectivité : si $z = r_1e^{i\theta_1} = r_2e^{i\theta_2}$, alors : $r_1 = r_2$ car $|z| = r_1 = r_2$; et $\theta_1 \equiv \theta_2\ [2\pi]$, donc $\theta_1 = \theta_2$.

□

Définition III.8 (forme trigonométrique)**.** *Tout nombre complexe non nul z s'écrit sous la forme $z = re^{i\theta}$, pour $r > 0$ et $\theta \in \mathbb{R}$. Cette écriture s'appelle* ***forme trigonométrique****.*
Le réel r est unique, et est le module de z.
Le réel θ est unique à 2π près, et est ***un argument*** *de z.*
L'unique argument de z dans $]-\pi;\pi]$ est appelé ***argument principal*** *de z, et est noté* $\arg(z)$.

Proposition III.9. *Si $z, z' \in \mathbb{C}^*$ et $\lambda \in \mathbb{R}^*$, alors :*

1. $\arg(zz') \equiv \arg(z) + \arg(z')\ [2\pi]$;
2. $\arg\left(\dfrac{z}{z'}\right) \equiv \arg(z) - \arg(z')\ [2\pi]$;
3. $\arg(\overline{z}) = \arg\left(\dfrac{1}{z}\right) \equiv -\arg(z)\ [2\pi]$;
4. $\arg(\lambda z) = \arg\left(\dfrac{z}{\lambda}\right) \equiv \begin{cases} \arg(z) & si\ \lambda > 0 \\ \arg(z) + \pi & si\ \lambda < 0 \end{cases}$.

Démonstration. Les résultats découlent des propriétés de l'exponentielle complexe. Détaillons la dernière. Soit $z = re^{i\theta}$ (forme trigonométrique) et $\lambda \in \mathbb{R}^*$. Alors :

$$\lambda z = \begin{cases} (\lambda r)e^{i\theta} & \text{si } \lambda > 0 \text{ avec } \lambda r > 0 \\ (-\lambda r)e^{i(\theta+\pi)} & \text{si } \lambda < 0 \text{ avec } (-\lambda r) > 0 \end{cases}$$

donc les écritures précédentes sont bien des formes trigonométriques, ce qui donne bien l'argument voulu. □

Remarque III.10. *On déduit que $z, z' \in \mathbb{C}^*$ sont positivement liés si, et seulement si, ils ont même argument.*

III.2 Formules classiques

Proposition III.11 (Formules d'Euler)**.** *Si $\theta \in \mathbb{R}$, alors :*

$$\cos(\theta) = \frac{e^{i\theta} + e^{-i\theta}}{2} \text{ et } \sin(\theta) = \frac{e^{i\theta} - e^{-i\theta}}{2i}.$$

Méthode III.12. *Les formules d'Euler permettent de* ***linéariser*** $\cos^n(\theta)$ *ou* $\sin^n(\theta)$ *:*

1. *on applique les formules d'Euler ;*
2. *on développe la puissance avec le binôme ;*
3. *on regroupe les termes pour faire apparaître des* $\cos(k\theta)$ *ou* $\sin(k\theta)$ *avec la formule d'Euler.*

Exemple III.13. *Linéariser* $\cos^4(\theta)$ *:*

$$\begin{aligned}
\cos^4(\theta) &= \left(\frac{e^{i\theta} + e^{-i\theta}}{2}\right)^4 = \frac{1}{2^4}\sum_{k=0}^{4}\binom{4}{k}e^{ik\theta}e^{-i(4-k)\theta} \\
&= \frac{1}{16}\left(e^{-4i\theta} + 4e^{-2i\theta} + 6 + 4e^{2i\theta} + e^{4i\theta}\right) \\
&= \frac{1}{16}\left[e^{-4i\theta} + e^{4i\theta}) + 4(e^{-2i\theta} + e^{2i\theta}) + 6\right] \\
&= \frac{1}{16}\left(2\cos(4\theta) + 8\cos(2\theta) + 6\right) \\
&= \frac{1}{8}\cos(4\theta) + \frac{1}{2}\cos(2\theta) + \frac{3}{8}
\end{aligned}$$

Proposition III.14 (Formules de l'angle moitié)**.** *Si $\theta_1, \theta_2 \in \mathbb{R}$, alors :*

1. $1 + e^{i\theta_1} = e^{i\frac{\theta_1}{2}}\left(e^{-i\frac{\theta_1}{2}} + e^{-\frac{\theta_1}{2}}\right) = 2\cos\left(\frac{\theta_1}{2}\right)e^{i\frac{\theta_1}{2}}$;
2. $1 - e^{i\theta_1} = e^{i\frac{\theta_1}{2}}\left(e^{-i\frac{\theta_1}{2}} - e^{-\frac{\theta_1}{2}}\right) = -2i\sin\left(\frac{\theta_1}{2}\right)e^{i\frac{\theta_1}{2}}$;
3. $e^{i\theta_1} + e^{i\theta_2} = e^{i\theta_1}\left(1 + e^{i(\theta_2-\theta_1)}\right) = 2\cos\left(\frac{\theta_1-\theta_2}{2}\right)e^{i\frac{\theta_1+\theta_2}{2}}$;
4. $e^{i\theta_1} - e^{i\theta_2} = e^{i\theta_1}\left(1 - e^{i(\theta_2-\theta_1)}\right) = 2i\sin\left(\frac{\theta_1-\theta_2}{2}\right)e^{i\frac{\theta_1+\theta_2}{2}}$.

Remarque III.15. *On retrouve les formules de factorisation de sommes de* sin *ou* cos*.*

Méthode III.16. *Ces formules permettent de factoriser ou d'exprimer plus simplement des sommes d'exponentielles complexes, de* sin *ou de* cos*.*

Exemple III.17. *Calculer* $C = 1 + \cos(\theta) + \cos(2\theta) + \cdots + \cos((n-1)\theta) = \sum_{k=0}^{n-1}\cos(k\theta)$*.*
Posons $S = \sum_{k=0}^{n-1}\sin(k\theta)$ *et* $E = C + iS$ *(de sorte que* $C = \mathrm{Re}(E)$ *et* $S = \mathrm{Im}(E)$*).*
Alors : $E = \sum_{k=0}^{n-1}\left(\cos(k\theta) + i\sin(k\theta)\right) = \sum_{k=0}^{n-1}e^{ik\theta} = \sum_{k=0}^{n-1}(e^{i\theta})^k$*.*

— *si* $\theta \equiv 0\ [2\pi]$ *: alors* $E = n$*, donc* $C = n$ *et* $S = 0$ *;*

— *si* $\theta \not\equiv 0\ [2\pi]$ *: alors on a une somme géométrique de raison* $e^{i\theta} \neq 1$ *:*

$$\begin{aligned}
E &= 1 \times \frac{1 - e^{in\theta}}{1 - e^{i\theta}} \\
&= \frac{-2i\sin\left(\frac{n\theta}{2}\right)e^{i\frac{n\theta}{2}}}{-2i\sin\left(\frac{\theta}{2}\right)e^{i\frac{\theta}{2}}} \\
&= \frac{\sin\left(\frac{n\theta}{2}\right)}{\sin\left(\frac{\theta}{2}\right)}e^{i(n-1)\frac{\theta}{2}}
\end{aligned}$$

Et donc :

$$C = \mathrm{Re}(E) = \frac{\sin\left(\frac{n\theta}{2}\right)}{\sin\left(\frac{\theta}{2}\right)}\cos\left(\frac{(n-1)\theta}{2}\right) \text{ et } S = \mathrm{Re}(E) = \frac{\sin\left(\frac{n\theta}{2}\right)}{\sin\left(\frac{\theta}{2}\right)}\sin\left(\frac{(n-1)\theta}{2}\right).$$

Proposition III.18 (Formules de Moivre)**.** *Si $\theta \in \mathbb{R}$ et $n \in \mathbb{N}$, alors : $e^{in\theta} = \left(e^{i\theta}\right)^n$. Et ainsi :*

$$\cos(n\theta) + i\sin(n\theta) = (\cos(\theta) + \sin(\theta))^n .$$

Méthode III.19. *Les formules de Moivre permettent d'exprimer $\cos(n\theta)$ ou $\sin(n\theta)$ comme des polynômes en $\cos(\theta)$ et/ou $\sin(\theta)$.*

Exemple III.20. *Exprimer $\cos(3\theta)$ comme un polynôme en $\cos(\theta)$:*

$$\begin{array}{rcl} \cos(3\theta) + i\sin(3\theta) & = & (\cos(\theta) + i\sin(\theta))^3 \\ & = & \cos^3(\theta) + 3i\cos^2(x)\sin(\theta) + 3i^2\cos(\theta)\sin^2(\theta) + i^3\sin^3(\theta) \\ & = & \left(\cos^3(\theta) - 3\cos(\theta)\sin^2(\theta)\right) + i\left(3\cos^2(\theta)\sin(\theta) - \sin^3(\theta)\right) \end{array}$$

Et en identifiant les parties réelle et imaginaire, on trouve :

$\cos(3\theta) = \cos^3(\theta) - 3\cos(\theta)\sin^2(\theta) = 4\cos^3(\theta) - 3\cos(\theta)$ *et* $\sin(3\theta) = 3\cos^2(\theta)\sin(\theta) - \sin^3(\theta) = -4\sin^3(\theta) + 3\sin(\theta)$.

Remarque III.21. *On peut toujours exprimer $\cos(n\theta)$ comme un polynôme en $\cos(\theta)$. On peut seulement exprimer $\sin(n\theta)$ comme un polynôme en $\sin(\theta)$ si n est impair.*

Définition III.22 (Exponentielle complexe)**.** *Si $z = x + iy$ (forme algébrique), on définit* ***l'exponentielle*** *de z par :*

$$\exp(z) = e^z = e^x \cdot e^{iy} = e^x \left(\cos(y) + i\sin(y)\right).$$

Remarque III.23. *Comme : $\forall x \in \mathbb{R},\ e^x > 0$, alors $e^x \cdot e^{iy}$ est la forme trigonométrique de e^z. De sorte que : $|e^z| = e^{\mathrm{Re}(z)}$ et $\arg(e^z) \equiv \mathrm{Im}(z)\ [2\pi]$.*

Proposition III.24. *Si $z, z' \in \mathbb{C}$, alors :*

1. $e^{z+z'} = e^z e^{z'}$;
2. $e^{z-z'} = \dfrac{e^z}{e^{z'}}$;
3. $\overline{e^z} = e^{\overline{z}}$;
4. $e^z = e^{z'} \Leftrightarrow \left\{ \begin{array}{c} \mathrm{Re}(z) = \mathrm{Re}(z') \\ \mathrm{Im}(z) \equiv \mathrm{Im}(z')\ [2\pi] \end{array} \right. \Leftrightarrow (z - z') \in 2i\pi\mathbb{Z}.$

Proposition III.25. *Si $a \in \mathbb{C}$, alors l'équation $e^z = a$:*

— *n'a pas de solution si $a = 0$;*
— *a une infinité de solutions si $a \neq 0$, à savoir : $\{\ln|a| + i(\arg(a) + 2k\pi) \mid k \in \mathbb{Z}\}$.*

IV Résolution d'équations algébriques

IV.1 Racines n-èmes

Définition IV.1. *Si $n \in \mathbb{N}^*$, et $a \in \mathbb{C}$, on dit que z est* ***une racines n-ème de*** *a si $z^n = a$.*
Lorsque $a = 1$, on parle de ***racine n-ème de l'unité****, et on note $\mathbb{U}_n$ l'ensemble des racines n-ème de l'unité.*

Proposition IV.2. *L'ensemble $\mathbb{U}_n$ possède n éléments :*

$$\mathbb{U}_n = \left\{\omega_k = e^{\frac{2ik\pi}{n}} \mid k \in \mathbb{Z}\right\} = \left\{\omega_k = e^{\frac{2ik\pi}{n}} \mid k \in [\![0; n-1]\!]\right\}.$$

Démonstration. Comme $0^n = 0$, alors $0 \notin \mathbb{U}_n$.
Soit $z \neq 0$. On écrit $z = re^{i\theta}$ (forme trigonométrique) :

$$\begin{array}{rcl} z \in \mathbb{U}_n & \Leftrightarrow & z^n = 1 \\ & \Leftrightarrow & r^n e^{in\theta} = 1 \cdot e^{i0} \\ & \Leftrightarrow & r^n = 1 \text{ et } n\theta \equiv 0\ [2\pi] \\ & \Leftrightarrow & r = \sqrt[n]{1} = 1 \text{ (car } r > 0) \text{ et } n\theta = 2k\pi,\ k \in \mathbb{Z} \\ & \Leftrightarrow & z = e^{\frac{2ik\pi}{n}},\ k \in \mathbb{Z} \end{array}$$

ce qui donne la première égalité.
La seconde se déduit par 2π-périodicité de $\theta \mapsto e^{i\theta}$. □

Exemples IV.3.

1. $\mathbb{U}_2 = \{\pm 1\}$;
2. $\mathbb{U}_4 = \{\pm 1,\ \pm i\}$;
3. $\mathbb{U}_3 = \{1, e^{\frac{2i\pi}{3}}, e^{\frac{4i\pi}{3}}\} = \{1, j, j^2\}$ *avec* $j = e^{\frac{2i\pi}{3}}$.

Corollaire IV.4. *Si $n \in \mathbb{N}^*$ et $a \in \mathbb{C}^*$, alors a possède exactement n racines n-èmes. Si l'on note $a = re^{i\theta}$, leur ensemble est :*

$$\left\{ \sqrt[n]{r} e^{i\frac{\theta+2k\pi}{n}} \,|\, k \in [\![0; n-1]\!] \right\} = \{z_0 \times \omega \,|\, \omega \in \mathbb{U}_n\}$$

où z_0 est une racine n-ème quelconque de a.

Démonstration. Il est immédiat que les $\sqrt[n]{r} e^{i\frac{\theta+2k\pi}{n}}$ sont des racines de a.
Réciproquement, si z_0 est une racine n-ème de a, alors $z_0 \neq 0$ et :

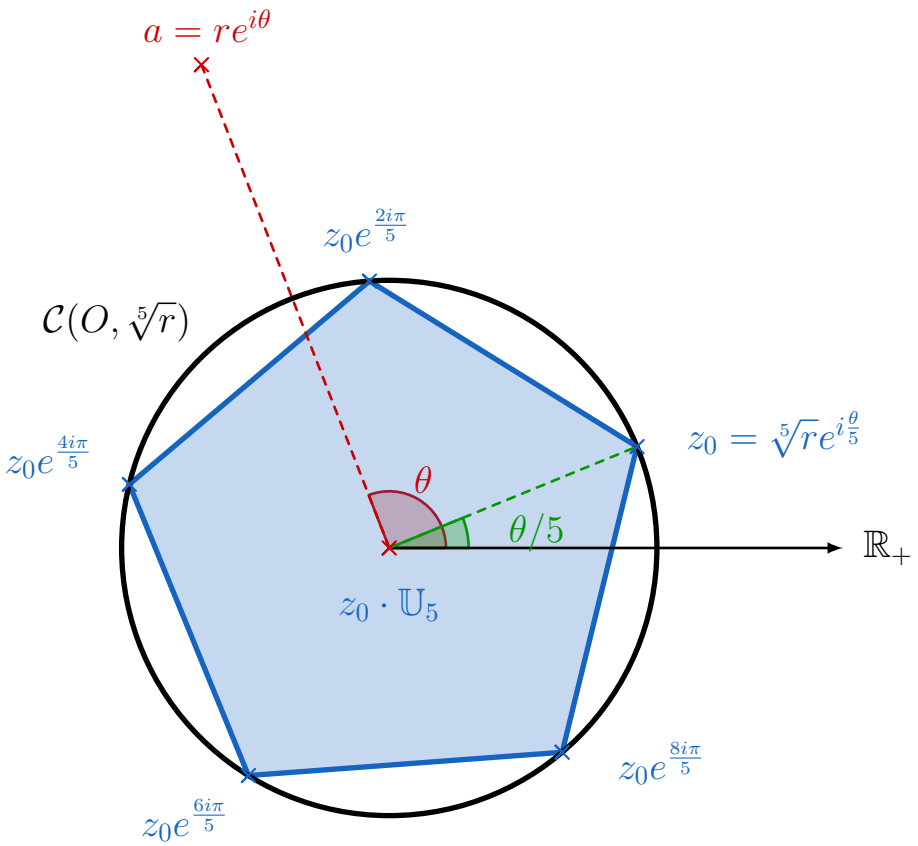
$$z^n = a \Leftrightarrow z^n = z_0^n \Leftrightarrow \left(\frac{z}{z_0}\right)^n = 1 \Leftrightarrow \frac{z}{z_0} \in \mathbb{U}_n$$

ce qui donne le résultat. □

Proposition IV.5. *Si $n \in \mathbb{N}^*$ et $a \in \mathbb{C}^*$, alors la somme des racines n-èmes de a vaut 0.*

Démonstration. On fait apparaître une somme géométrique de raison $e^{\frac{2i\pi}{n}}$. □

Remarque IV.6. *Les racines n-ème de a sont les sommets d'un polygone régulier à n côtés, inscrit dans le cercle de centre O de rayon $\sqrt[n]{|a|}$:*



Le barycentre de ces points est l'origine du plan, ce qui illustre :

$$\sum_{z\in\mathbb{C},\ z^n=a} z = 0.$$

Exemple IV.7. *Calculons le cosinus et le sinus de* $\frac{2\pi}{5}$.
Considérons les racines 5-èmes de l'unité : $1, e^{\pm\frac{2i\pi}{5}}, e^{\pm\frac{4i\pi}{5}}$. *Comme leur somme vaut* 0, *on déduit que :*

$$1 + 2\cos\left(\frac{2\pi}{5}\right) + 2\cos\left(\frac{4\pi}{5}\right) = 0.$$

Par formule de duplication, on a : $\cos\left(\frac{4\pi}{5}\right) = 2\cos^2\left(\frac{2\pi}{5}\right) - 1$, *et donc* $\cos\left(\frac{2\pi}{5}\right)$ *est solution de l'équation :*

$$4x^2 + 2x - 1 = 0.$$

Les solutions sont $\dfrac{-2 \pm \sqrt{20}}{8} = \dfrac{\pm\sqrt{5} - 1}{4}$.

Comme $\frac{2\pi}{5} \in [0; \frac{\pi}{2}]$, *alors* $\cos\left(\frac{2\pi}{5}\right) > 0$, *et donc :* $\cos\left(\frac{2\pi}{5}\right) = \dfrac{\sqrt{5}-1}{4}$.
Comme $\frac{2\pi}{5} \in [0; \frac{\pi}{2}]$, *alors* $\sin\left(\frac{2\pi}{5}\right) > 0$, *et donc :*

$$\sin\left(\frac{2\pi}{5}\right) = \sqrt{1 - \cos^2\left(\frac{2\pi}{5}\right)} = \sqrt{1 - \left(\frac{\sqrt{5}-1}{4}\right)^2} = \sqrt{\frac{5+\sqrt{5}}{8}}.$$

IV.2 Racines carrées

Méthode IV.8. *On note* $z = x + iy$ *une racine carrée de* $a + ib$ *(c'est-à-dire* $z^2 = a + ib$*). Trouver* z *revient à résoudre (dans* $\mathbb{R}$*) le système :*

$$\begin{cases} x^2 + y^2 &= \sqrt{a^2 + b^2} & \text{(en regardant le module)} \\ x^2 - y^2 &= a & \text{(en regardant la partie réelle)} \\ 2xy &= b & \text{(en regardant la partie imaginaire)} \end{cases}.$$

On trouve x et y (au signe près) avec les deux premières égalités. On trouve le signe avec la dernière.

Exemple IV.9. *Trouver les racines carrées de $-5+12i$: on les cherche sous la forme $z=x+iy$. On a :*

$$\begin{cases} x^2+y^2 &= \sqrt{5^2+12^2}=13 \\ x^2-y^2 &= -5 \\ 2xy &= 12 \end{cases}.$$

Et ainsi :

$$\begin{cases} x^2 &= 4 \\ y^2 &= 9 \\ xy &> 0 \text{ donc } x,y \text{ de même signe} \end{cases}.$$

Donc les deux racines carrées de $-5+12i$ sont $2+3i$ et $-2-3i$.

Proposition IV.10. *Soient $a,b,c\in\mathbb{C}$ avec $a\neq 0$, $\Delta=b^2-4ac$ et δ une racine carrée de Δ. Alors l'équation $az^2+bz+c=0$ admet :*

1. *une seule solution si $\Delta=0$, à savoir $z_0=\dfrac{-b}{2a}$;*
2. *deux solution si $\Delta\neq 0$, à savoir : $z_{1,2}=\dfrac{-b\pm\delta}{2a}$.*

Démonstration.

$$\begin{aligned} az^2+bz+c=0 &\Leftrightarrow a\left[z^2+\frac{b}{a}z+\frac{c}{a}\right]=0 \Leftrightarrow \left(z+\frac{b}{2a}\right)^2-\frac{\Delta}{4a^2}=0 \\ &\Leftrightarrow \left(z+\frac{b}{2a}\right)^2=\left(\frac{\delta}{2a}\right)^2 \Leftrightarrow z+\frac{b}{2a}=\pm\frac{\delta}{2a} \\ &\Leftrightarrow z=\frac{-b\pm\delta}{2a} \end{aligned}$$

□

Proposition IV.11 (Relations coefficients-racines)**.** *Si $a,b,c\in\mathbb{C}$ avec $a\neq 0$, et que z_1,z_2 sont les solutions (éventuellement confondues) de l'équation $az^2+bz+c=0$, alors :*

$$z_1z_2=\frac{c}{a} \text{ et } z_1+z_2=-\frac{b}{a}.$$

De plus, on a : $az^2+bz+c=a(z-z_1)(z-z_2)$.

Corollaire IV.12 (Systèmes somme-produit)**.** *Si $s,p\in\mathbb{C}$, les solutions du système :*

$$\begin{cases} x+y &= s \\ xy &= p \end{cases}$$

sont les couples de solutions de l'équation $z^2-sz+p=0$, formés de complexes différents si l'équation précédente possède deux solutions distinctes.

Exemple IV.13. *On considère le système :*

$$\begin{cases} x+y &= 3+3i \\ xy &= 5i \end{cases}$$

On lui associe l'équation : $z^2-(3+3i)z+5i$.
On a : $\Delta=-2i$, donc $\delta=1-i$ est une racine carrée de Δ.
Donc $z_{1,2}=\dfrac{3+3i\pm(1-i)}{2}=2+i$ ou $1+2i$.
Et les solutions du système sont $(2+i,1+2i)$ et $(1+2i,2+i)$.

IV.3 Équations polynomiales

Définition IV.14. *Pour $n \in \mathbb{N}$, on appelle* ***fonction polynomiale à coefficients complexes de degré*** *n une fonction $P : \mathbb{C} \to \mathbb{C}$ définie par : $\forall z \in \mathbb{C},\ P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$, où $a_0, \ldots, a_n \in \mathbb{C}$ et $a_n \neq 0$.*
Une ***racine*** *de P est une solution de l'équation $P(z) = 0$.*

Proposition IV.15 (Factorisation des polynômes)**.** *Si $n \geq 1$ et si z_0 est une racine de P, alors il existe une fonction polynomiale Q de degré $n-1$ telle que :*

$$\forall z \in \mathbb{C},\ P(z) = (z - z_0)Q(z).$$

Théorème IV.16 (d'Alembert–Gauss)**.** *Toute fonction polynomiale à coefficients complexes de degré ≥ 1 possède une racine dans $\mathbb{C}$.*

Remarque IV.17. *Il faut être dans $\mathbb{C}$: la fonction $x \mapsto x^2 + 1$ n'a pas de racine dans $\mathbb{R}$ par exemple.*

Corollaire IV.18. *Si P est une fonction polynomiale à coefficients complexes de degré $n \geq 1$, alors il existe $a \in \mathbb{C}^*$ et $z_1, \ldots, z_n \in \mathbb{C}$ tels que :*

$$\forall z \in \mathbb{C},\ P(z) = a(z - z_1)(z - z_2)\ldots(z - z_n).$$

V Interprétation géométrique des nombres complexes

Proposition V.1. *Si A, B sont deux points du plan d'affixes respectives z_A et z_B, alors le vecteur $\overrightarrow{AB}$ a pour affixe $z_B - z_A$. Sa norme vaut $|z_B - z_A|$ et son angle avec l'axe (O, x) est* $\arg(z_B - z_A)$.
Plus généralement, si C est un autre point d'affixe z_C, alors l'angle $\widehat{BAC} = \left(\overrightarrow{AB}, \overrightarrow{AC}\right)$ est égal à $\arg(z_C - z_A) - \arg(z_B - z_A) = \arg\left(\dfrac{z_C - z_A}{z_B - z_A}\right)$.

Proposition V.2. *On a les équivalences :*

1. *A, B, C alignés* $\Leftrightarrow \left(\arg\left(\dfrac{z_C - z_A}{z_B - z_A}\right) = 0\ [\pi]\right) \Leftrightarrow \left(\dfrac{z_C - z_A}{z_B - z_A} \in \mathbb{R}\right)$;
2. *(AB) et (CD) sont perpendiculaires* $\Leftrightarrow \left(\arg\left(\dfrac{z_C - z_D}{z_B - z_A}\right) = \dfrac{\pi}{2}\ [\pi]\right) \Leftrightarrow \left(\dfrac{z_C - z_D}{z_B - z_A} \in i\mathbb{R}\right)$.

Définition V.3. *Une* ***transformation du plan*** *est une bijection $f : \mathbb{R}^2 \to \mathbb{R}^2$, ou $f : \mathbb{C} \to \mathbb{C}$ (en assimilant le plan à $\mathbb{C}$).*

Proposition V.4. *On a les transformations suivantes du plan :*

1. *l'application $z \mapsto \overline{z}$ est la* ***symétrie*** *d'axe (Ox) ;*
2. *si $b \in \mathbb{C}$, l'application $z \mapsto z + b$ est la* ***translation*** *du vecteur d'affixe b ;*
3. *si $\lambda \in \mathbb{R}$ et $z_A \in \mathbb{C}$, l'application $z \mapsto \lambda(z - z_A) + z_A$ est* ***l'homothétie*** *de centre A (d'affixe z_A) et de rapport r ;*
4. *si $\theta \in \mathbb{R}$ et $\omega \in \mathbb{C}$, l'application $z \mapsto e^{i\theta}(z - \omega) + \omega$ est la* ***rotation*** *de centre Ω (d'affixe ω) et d'angle $e^{i\theta}$.*

Théorème-Définition V.5. *Une* ***similitude directe*** *est une transformation du plan qui préserve les angles orientés.*
Vue comme une application de $\mathbb{C}$ dans $\mathbb{C}$, toute similitude s'écrit sous la forme $z \mapsto az + b$, où $a, b \in \mathbb{C}$ avec $a \neq 0$.
Si $a \neq 1$, f possède un unique ***point fixe*** *Ω (un point qui est sa propre image par f) : on dit alors que f est la similitude directe de* ***centre*** *Ω, de* ***rapport*** *$|a|$, et d'****angle*** *$\arg(a)$.*

Démonstration. Toute application $z \mapsto az+b$ avec $a \neq 0$ est bien un similitude directe (il suffit de regarder les arguments).
Réciproquement : soit f un similitude.

Lemme V.6. *Une similitude préserve les rapports de longueurs.*

Preuve du lemme : Soient A, B, M, N quatre points du plan distincts, d'images respectives A', B', M', N'. Comme les angles sont conservés, alors les triangles ABM et $A'B'M'$ sont semblables. Donc : $\dfrac{AB}{A'B'} = \dfrac{AM}{A'M'} = \dfrac{BM}{B'M'}$.
De même, avec les triangles AMN et $A'M'N'$: $\dfrac{AM}{A'M'} = \dfrac{AN}{A'N'} = \dfrac{MN}{M'N'}$.
Et donc : $\dfrac{AB}{MN} = \dfrac{A'B'}{M'N'}$. □

Considérons O, A, M d'affixes respectives $0, 1, z$. Notons O', A', M' leurs images par f, et b, c, z' leurs affixes. La conservation des angles et des rapports de longueur donne :

$$\frac{O'M'}{O'A'} = \frac{OM}{OA} \text{ et } \widehat{A'O'M'} = \widehat{AOM}$$

donc, par égalité des modules et arguments :

$$\frac{z'-b}{c-b} = \frac{z-0}{1-0}$$

et donc : $z' = az + b$, avec $a = c - b \neq 0$.
L'existence et l'unicité du point fixe si $a \neq 1$ vient du fait que pour un tel a :

$$z = az + b \Leftrightarrow z - az = b \Leftrightarrow z = \frac{b}{1-a}.$$

□

Remarque V.7. *Parmi les transformations précédentes, seule la conjugaison n'est pas une similitude directe : elle change tout angle en son opposé.*

Proposition V.8. *La composé de deux similitudes est une similitude.*

Proposition V.9. *On considère la similitude directe $f : z \mapsto az + b$. Alors :*

1. *si $a = 1$: alors il s'agit d'une translation ;*
2. *si $a \neq 1$: si Ω est son point fixe, f est la composée de la rotation de centre Ω d'angle $\arg(a)$ et de l'homothétie de centre Ω de rapport $|a|$.*

Démonstration.

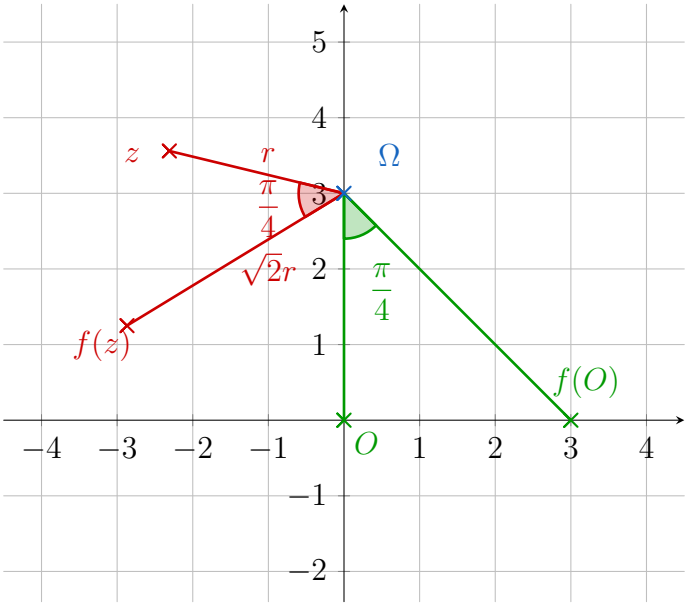
1. si $a = 1$: alors $f : z \mapsto z + b$ est la translation de vecteur d'abscisse b ;
2. si $a \neq 1$: alors $\omega = \dfrac{b}{1-a}$ vérifie $f(\omega) = \omega$. On note : $a = \lambda e^{it}$, $h : z \mapsto \lambda(z - \omega) + \omega$ l'homothétie de centre Ω de rapport λ, et $r : z \mapsto e^{it}(z - \omega) + \omega$ la rotation de centre Ω d'angle t. Alors :

$$(h \circ r)(z) = \frac{b}{1-a} + \underbrace{\lambda e^{it}}_{=a}\left(z - \frac{b}{1-a}\right) = az + \frac{b - ab}{1-a} = az + b = f(z)$$

□

Exemple V.10. *On considère l'application* $f : z \mapsto (1+i)z+3$. *Alors :*

- *l'unique point fixe de* f *est le point* Ω *d'affixe* $\dfrac{3}{1-(1+i)} = \dfrac{3}{-i} = 3i$;
- f *est la composée de l'homothétie de centre* Ω *de rapport* $|1+i| = \sqrt{2}$ *et de la rotation de centre* Ω *d'angle* $\arg(1+i) = \frac{\pi}{4}$.



VI Fonction complexe d'une variable réelle

Définition VI.1. *Soit* I *un intervalle de* $\mathbb{R}$, *et* $\varphi : I \to \mathbb{C}$. *On note* φ_1 *et* φ_2 *les parties réelle et imaginaire de* φ, *c'est-à-dire les fonctions définies de* I *sur* $\mathbb{R}$ *par :* $\forall t \in I,\ \varphi_1(t) = \mathrm{Re}(\varphi(t))$ *et* $\varphi_2(t) = \mathrm{Im}(\varphi(t))$ *(de sorte que* $\varphi = \varphi_1 + i\varphi_2$*).*
On dit que φ *est continue (resp. dérivable) en* $t_0 \in I$ *si* φ_1 *et* φ_2 *le sont. Et pour la dérivabilité, on pose :*

$$\varphi'(t_0) = \varphi_1'(t_0) + i\varphi_2'(t_0).$$

Proposition VI.2. *Si* f, g *sont des fonctions dérivables sur* I *à valeurs dans* $\mathbb{C}$, *et* $\lambda \in \mathbb{C}$, *alors on a les fonctions dérivées suivantes :*

1. $(f+\lambda g)' = f' + \lambda g'$ *(la dérivation est linéaire) ;*
2. $(fg)' = f'g + fg'$;
3. *si* g *ne s'annule pas :* $\left(\dfrac{1}{g}\right)' = -\dfrac{g'}{g^2}$;
4. *si* g *ne s'annule pas :* $\left(\dfrac{f}{g}\right)' = \dfrac{f'g - fg'}{g^2}$.

Démonstration. Toutes les formules découlent de la dérivabilité des fonctions à valeurs réelles, en ramenant le calcul à des dérivées de combinaisons linéaires, produits ou quotient de fonctions réelles. Montrons par exemple la formule pour le produit.
Soient f, g deux fonctions à valeurs complexes dérivables sur I, et notons $f_1 = \mathrm{Re}(f)$, $f_2 = \mathrm{Im}(f)$, $g_1 = \mathrm{Re}(g)$ et $g_2 = \mathrm{Im}(g)$. De sorte que :

$$fg = (f_1 + if_2)\cdot(g_1 + ig_2) = (f_1g_1 - f_2g_2) + i(f_1g_2 + f_2g_1).$$

Par dérivée d'un produit (pour les fonctions à valeurs réelles), on déduit que $\mathrm{Re}(fg)$ et $\mathrm{Im}(fg)$ sont dérivables, donc fg aussi, de dérivée :

$$(fg)' = (f_1'g_1 + f_1g_1' - f_2'g_2 - f_2g_2') + i\,(f_1'g_2 + f_1g_2' + f_2'g_1 + f_2g_1')$$

tandis que l'on a :

$$\begin{array}{rcl} f'g & = & (f_1' + if_2') \cdot (g_1 + ig_2) \\ & = & (f_1'g_1 - f_2'g_2) + i \cdot (f_1'g_2 + f_2'g_1) \\ fg' & = & (f_1 + if_2) \cdot (g_1' + ig_2') \\ & = & (f_1g_1' - f_2g_2') + i \cdot (f_1g_2' + f_2g_1') \end{array}$$

ce qui donne bien l'égalité voulue. □

Proposition VI.3. *Soit* $\varphi : I \to \mathbb{C}$ *dérivable. Alors la fonction* $\psi : \left\{ \begin{array}{ccc} I & \to & \mathbb{C} \\ t & \mapsto & e^{\varphi(t)} \end{array} \right.$ *est dérivable sur* I*, avec :* $\forall t \in I,\ \psi'(t) = \varphi'(t)e^{\varphi(t)}$.

Démonstration. On pose $\varphi_1 = \mathrm{Re}(\varphi)$ et $\varphi_2 = \mathrm{Im}(\varphi)$.
Si $x \in I$:

$$\psi(t) = e^{\varphi_1(t)}e^{i\varphi_2(t)} = e^{\varphi_1(t)}\left(\cos(\varphi_2(t)) + i\sin(\varphi_2(t))\right).$$

D'où :

$$\left\{ \begin{array}{rcl} \psi_1(t) & = & \mathrm{Re}(\psi(t)) \\ \psi_2(t) & = & \mathrm{Im}(\psi(t)) \end{array} \right. = \left\{ \begin{array}{l} e^{\varphi_1(t)}\cos(\varphi_2(t)) \\ e^{\varphi_1(t)}\sin(\varphi_2(t)) \end{array} \right. .$$

Comme φ est dérivable, φ_1 et φ_2 aussi, donc ψ_1 et ψ_2 aussi. Et on a :

$$\forall t \in I,\ \left\{ \begin{array}{rcl} \psi_1'(t) & = & e^{\varphi_1(t)}\left[\varphi_1'(t)\cos(\varphi_2(t)) - \varphi_2'(t)\sin(\varphi_2(t))\right] \\ \psi_2'(t) & = & e^{\varphi_1(t)}\left[\varphi_1'(t)\sin(\varphi_2(t)) + \varphi_2'(t)\cos(\varphi_2(t))\right] \end{array} \right. .$$

Donc ψ est dérivable, avec pour tout $t \in I$:

$$\begin{array}{rcl} \psi'(t) & = & \psi_1(t) + i\psi_2(t) \\ & = & e^{\varphi_1(t)}\left[(\varphi_1'(t) + i\varphi_2'(t))\cos(\varphi_2(t)) + (-\varphi_2'(t) + i\varphi_1'(t))\sin(\varphi_2(t))\right] \\ & = & e^{\varphi_1(t)}(\varphi_1'(t) + i\varphi_2'(t))e^{i\varphi_2(t)} \\ & = & \varphi'(t)e^{\varphi(t)} \end{array}$$

□

Exemple VI.4. *Si* $\alpha \in \mathbb{C}$*, la fonction* $f : t \mapsto \exp\left(\alpha\ln(t)\right)$ *est dérivable sur* $\mathbb{R}_+^*$*. Si* $t \in \mathbb{R}_+^*$*, alors :*

$$f'(t) = \frac{\alpha}{\ln(t)}\exp\left(\alpha\ln(t)\right) = \alpha\exp\left((\alpha - 1)\ln(t)\right)$$

c'est-à-dire que, avec l'abus de notation $f(t) = t^\alpha$*, on trouve :* $f'(t) = \alpha t^{\alpha-1}$.

Chapitre 9

Primitives

I Primitives et intégrales

I.1 Généralités sur les primitives

Définition I.1. *Si f est définie sur un intervalle I, on dit qu'une fonction F dérivable sur I est une* ***primitive*** *de f si $F' = f$.*

Exemples I.2.

1. *$x \mapsto x^3$ ou $x \mapsto x^3 - 4$ sont des primitives de $x \mapsto 3x^2$ sur n'importe quel intervalle de $\mathbb{R}$;*
2. *$x \mapsto \text{signe}(x)\frac{x^2}{2} = \begin{cases} \frac{x^2}{2} & si\ x \geq 0 \\ -\frac{x^2}{2} & si\ x \leq 0 \end{cases}$ est une primitive de $x \mapsto |x|$ sur $\mathbb{R}$.*

Proposition I.3. *Si I est un intervalle, $f : I \to \mathbb{R}$ et F une primitive de f sur I, alors les primitives de f sur I sont exactement les fonctions $F + \lambda$, pour $\lambda \in \mathbb{R}$.*

Démonstration. Si F est une primitive de f, et G une fonction dérivable sur I, alors :

$$G \text{ primitive de } f \Leftrightarrow G' = F' \Leftrightarrow (G - F)' = 0 \Leftrightarrow G - F \text{ est constante.}$$

□

Remarques I.4.

1. *Ce résultat dit que, s'il existe une primitive, il en existe un infinité. Mais il ne dit pas qu'il en existe.*
2. *Le résultat est faux si I n'est plus un intervalle. Par exemple, les fonctions $\mathbb{1}_{\mathbb{R}_+^*}$ et $\mathbb{1}_{\mathbb{R}_-^*}$ sont des primitives de la fonction nulle sur $\mathbb{R}^*$, mais ne diffèrent pas d'une constante. Mais il permet quand même de chercher des primitives : par exemple pour chercher une primitive de $x \mapsto |x|$, on peut regarder les primitives de $x \mapsto x$ sur $\mathbb{R}_+$ et de $x \mapsto -x$ sur $\mathbb{R}_-$, puis chercher à recoler ces primitives en une fonction dérivable sur $\mathbb{R}$.*

Théorème I.5 (Théorème fondamental de l'analyse)**.** *Si f est continue sur un intervalle I, alors f admet une primitive.*

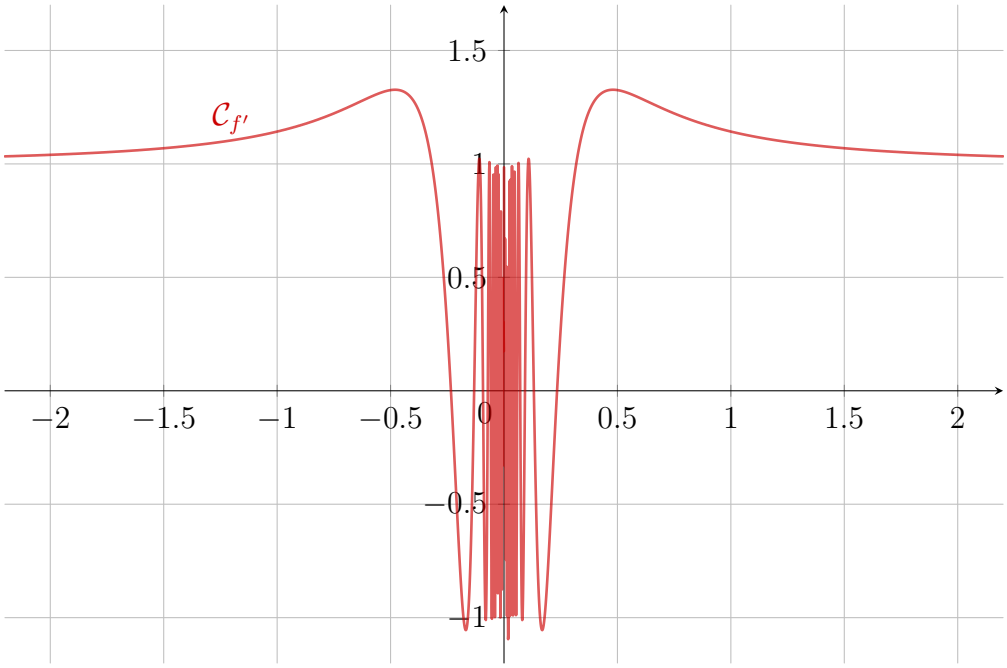
Démonstration. Admis (pour le moment). □

Corollaire I.6. *Si f est continue sur un intervalle I et $(x_0, y_0) \in I \times \mathbb{R}$, alors il existe une unique primitive F de f sur I telle que $F(x_0) = y_0$.*

Remarque I.7. *Il existe des fonctions non continues qui ont des primitives. Considérons par exemple la fonction $f : x \mapsto \begin{cases} x^2 \sin\left(\frac{1}{x}\right) & si\ x \neq 0 \\ 0 & si\ x = 0 \end{cases}$.*
La fonction f est dérivable sur $\mathbb{R}$:

— *sur* $\mathbb{R}^*$ *: par composée et produit,* f *est dérivable sur* $\mathbb{R}^*$ *avec :* $\forall x \in \mathbb{R}^*, f'(x) = 2x\sin\left(\frac{1}{x}\right) - \cos\left(\frac{1}{x}\right)$.
— *en* 0 *:* $\frac{f(x)-f(0)}{x-0} = x\sin\left(\frac{1}{x}\right) \underset{x\to 0}{\longrightarrow} 0$ *par encadrement. Donc* f *est dérivable en* 0 *avec* $f'(0) = 0$

Mais f *est une primitive de* f' *(qui est bien définie), c'est-à-dire que* f' *admet une primitive sur* $\mathbb{R}$*. Mais* f' *n'est pas continue en* 0 *car* $f'(x)$ *n'a pas de limite quand* x *tend vers* 0.
En effet : $2x\sin\left(\frac{1}{x}\right)$ *tend vers* 0 *en* 0 *(par encadrement) mais* $\cos\left(\frac{1}{x}\right)$ *n'a pas de limite en* 0 *(car* cos *n'a pas de limite en* $+\infty$*).*



I.2 Intégrale d'une fonction continue

Proposition-Définition I.8. *Soit* f *une fonction continue sur un intervalle* I*, et* F *une primitive de* f *sur* I*. Si* $a, b \in I$*, on définit* ***l'intégrale de*** f ***entre*** a ***et*** b *comme :*

$$\int_a^b f(t)\mathrm{d}t = [F(t)]_a^b = F(b) - F(a).$$

Cette quantité est bien définie, et ne dépend pas du choix de F*.*

Démonstration. Il suffit de voir que cette quantité ne dépend pas du choix de F. Soient G, F deux primitives de f sur I, et $\lambda \in \mathbb{R}$ tel que $G = F + \lambda$.
Alors : $G(b) - G(a) = F(b) + \lambda - F(a) - \lambda = F(b)F(a)$. □

Remarques I.9.

1. *On donnera une autre définition de l'intégrale (pour des fonctions plus générales que les fonctions continues). Et on verra que les deux définitions coïncident.*
2. *Une intégrale est un peu comme une somme : la variable d'intégration correspond à l'indice de sommation. On peut donc changer sa dénomination, et il n'a pas de sens hors de l'intégrale.*
3. *Cette définition n'a de sens que si* f *est continue (donc* f *doit avoir une primitive de classe* $\mathcal{C}^1$*).*

Proposition I.10. *Si* f, g *sont deux fonctions continues sur le segment* $[a; b]$*, et* $\lambda, \mu \in \mathbb{R}$*, alors :*

1. $\int_a^b (\lambda f(t) + \mu g(t))\,\mathrm{d}t = \lambda\left(\int_a^b f(t)\mathrm{d}t\right) + \mu\left(\int_a^b g(t)\mathrm{d}t\right)$ *(linéarité de l'intégrale) ;*
2. *si* $c \in [a; b]$ *:* $\int_a^b f(t)\mathrm{d}t = \int_a^c f(t)\mathrm{d}t + \int_c^b f(t)\mathrm{d}t$ *(relation de Chasles) ;*

3. $\int_a^b f(t)\mathrm{d}t = -\int_a^b f(t)\mathrm{d}t$;
4. *si* $f \geq 0$ *sur* $[a;b]$: $\int_a^b f(t)\mathrm{d}t \geq 0$ *(positivité de l'intégrale) ;*
5. *si* $f \geq g$ *sur* $[a;b]$: $\int_a^b f(t)\mathrm{d}t \geq \int_a^b g(t)\mathrm{d}t$ *(croissance de l'intégrale).*

Démonstration.

1. par linéarité de la dérivation, $\lambda F + \mu G$ est une primitive de $\lambda f + \mu G$, et donc :
$$\begin{array}{rcl}\int_a^b (\lambda f(t) + \mu g(t))\,\mathrm{d}t & = & \lambda F(b) + \mu G(b) - \lambda F(a) - \mu G(a) = \lambda\left(F(b) - F(a)\right) + \mu\left(G(b) - G(a)\right) \\ & = & \lambda\left(\int_a^b f(t)\mathrm{d}t\right) + \mu\left(\int_a^b g(t)\mathrm{d}t\right)\end{array}$$
2. $\int_a^b f(t)\mathrm{d}t = F(b) - F(a) = (F(c) - F(a)) + (F(b) - F(c)) = \int_a^c f(t)\mathrm{d}t + \int_c^b f(t)\mathrm{d}t$;
3. $\int_a^b f(t)\mathrm{d}t = F(b) - F(a) = -\left(F(a) - F(b)\right) = -\int_b^a f(t)\mathrm{d}t$;
4. si $f \geq 0$, alors F est croissante, donc $F(b) \geq F(a)$ et ainsi : $\int_a^b f(t)\mathrm{d}t = F(b) - F(a) \geq 0$;
5. on applique le résultat précédent à $f - g$.

□

Remarque I.11. *La croissance de l'intégrale se comprend en terme d'application sur des ensembles ordonnés. Cela revient en fait à dire que l'application :*
$$\varphi : \left\{\begin{array}{rcl}\mathcal{F}([a,b],\mathbb{R}) & \to & \mathbb{R} \\ f & \mapsto & \int_a^b f(t)\mathrm{d}t\end{array}\right.$$
est croissante, en munissant $\mathcal{F}([a,b],\mathbb{R})$ *de l'ordre partiel défini par* $g \preceq f$ *si, et seulement si,* $\forall t \in [a,b]$, $g(t) \leq f(t)$, *et qu'on munit* $\mathbb{R}$ *de son ordre usuel* $\leq$.

Proposition I.12. *Si* f *est continue de signe constant sur* $[a;b]$, *alors :*
$$f = 0 \Leftrightarrow \int_a^b f(t)\mathrm{d}t = 0.$$

Démonstration. La première implication découle de la linéarité car alors $f = 0 \cdot f$.
Réciproquement, si $\int_a^b f(t)\mathrm{d}t = 0$: on peut supposer $f \geq 0$ sur $[a;b]$ (quitte à changer f en $-f$). On a donc : $F(b) = F(a)$. Mais F est croissante sur $[a;b]$, comme $F' = f \geq 0$, donc F est constante. Et donc $f = F' = 0$. □

Théorème I.13. *Si* f *est une fonction continue sur un intervalle* I, *et* $a \in I$, *alors l'application* $F : x \mapsto \int_a^x f(t)\mathrm{d}t$ *est l'unique primitive de* f *sur* I *qui s'annule en* a.

Démonstration. Notons G une primitive de f. Alors, si $x \in I$: $F(x) = G(x) - G(a)$. Et donc $F'(x) = G'(x) = f(x)$ et $F(a) = G(a) - G(a) = 0$. L'unicité provient du théorème fondamental de l'analyse. □

Remarque I.14. *Toutes les primitives de* f *sont de la forme* $x \mapsto \int_a^x f(t)\mathrm{d}t + \lambda$. *Pour éviter un choix arbitraire pour* a *et* λ, *on notera* $\int^x f(t)\mathrm{d}t$ *une* ***primitive générique*** *de* f

Proposition I.15 (Intégrales dépendant de leurs bornes)**.** *Si* I, J *sont deux intervalles,* u, v *deux fonctions dérivables sur* I *à valeurs dans* J, *et* f *continue sur* J.
Alors la fonction φ *définie sur* I *par :* $\varphi(x) = \int_{u(x)}^{v(x)} f(t)\mathrm{d}t$ *est dérivable sur* I, *avec :*
$$\forall x \in I,\ \varphi'(x) = v'(x) \cdot f(v(x)) - u'(x) \cdot f(u(x).$$

Démonstration. Si F est une primitive de f sur J, alors : $\varphi(x) = F(v(x)) - F(u(x))$, qu'on peut dériver comme une composée. □

Corollaire I.16. *Si f est une fonction continue sur $\mathbb{R}$, et $x \in \mathbb{R}$:*

1. *si f est impaire, alors : $\int_{-x}^{x} f(t)\mathrm{d}t = 0$;*
2. *si f est T-périodique, alors : $\int_{x}^{x+T} f(t)\mathrm{d}t = \int_{0}^{T} f(t)\mathrm{d}t$.*

Démonstration. On dérive par rapport à x :

1. si $\varphi(x) = \int_{-x}^{x} f(t)\mathrm{d}t$, alors $\varphi'(x) = f(x) + f(-x) = 0$, donc φ est constante, de valeur $\varphi(0) = 0$;
2. si $\varphi(x) = \int_{x}^{T+x} f(t)\mathrm{d}t$, alors $\varphi'(x) = f(T+x) - f(x) = 0$, donc φ est constante, de valeur $\varphi(0) = \int_{0}^{T} f(t)\mathrm{d}t$.

□

Remarque I.17. *Le deuxième résultat dit en fait que toute primitive d'une fonction continue impaire est paire.*

Exemple I.18. *Calculons $I = \int_{0}^{\pi} \cos^2(t)\mathrm{d}t$. Par π-périodicité de $t \mapsto \sin^2(t)$:*

$$I = \int_{0}^{\pi} \sin^2(\pi/2 + t)\mathrm{d}t = \int_{\pi/2}^{3\pi/2} \sin^2(t)\mathrm{d}t = \int_{0}^{\pi} \sin^2(t)\mathrm{d}t$$

et donc $I + I = \int_{0}^{\pi} \left(\cos^2(t) + \sin^2(t)\right) \mathrm{d}t = \int_{0}^{2\pi} 1 \cdot \mathrm{d}t = \pi$. Donc $I = \frac{\pi}{2}$.

II Calcul de primitives et d'intégrales

II.1 Calcul direct

Théorème II.1. *On a les primitives usuelles suivantes :*

$f(x)$	D_f	$F(x)$
0	$\mathbb{R}$	0
c $(c \in \mathbb{C}^*)$	$\mathbb{R}$	cx
x^n $(n \in \mathbb{N})$	$\mathbb{R}$	$\dfrac{x^{n+1}}{n+1}$
$\dfrac{1}{x}$	$\mathbb{R}^*$	$\ln(\lvert x\rvert)$
x^n $(n \in \mathbb{Z},\ n \leq -2)$	$\mathbb{R}^*$	$\dfrac{x^{n+1}}{n+1}$
x^α $(\alpha \in \mathbb{R} \setminus \{-1\})$	$\mathbb{R}_+^*$	$\dfrac{x^{\alpha+1}}{\alpha+1}$
cas particulier : $\frac{1}{\sqrt{x}}$	$\mathbb{R}_+^*$	$2\sqrt{x}$
e^x	$\mathbb{R}$	e^x
$\ln(\lvert x\rvert)$	$\mathbb{R}^*$	$x\ln(\lvert x\rvert) - x$
$\cos(x)$	$\mathbb{R}$	$\sin(x)$
$\sin(x)$	$\mathbb{R}$	$-\cos(x)$
$\tan(x)$	$\mathbb{R} \setminus \left\{\frac{\pi}{2} + k\pi \mid k \in \mathbb{Z}\right\}$	$-\ln(\lvert\cos(x)\rvert)$
$1 + \tan^2(x) = \dfrac{1}{\cos^2(x)}$	$\mathbb{R} \setminus \left\{\frac{\pi}{2} + k\pi \mid k \in \mathbb{Z}\right\}$	$\tan(x)$
$\dfrac{1}{\sqrt{1-x^2}}$	$]-1,1[$	$\mathrm{Arcsin}(x)$
$-\dfrac{1}{\sqrt{1-x^2}}$	$]-1,1[$	$\mathrm{Arccos}(x)$
$\dfrac{1}{1+x^2}$	$\mathbb{R}$	$\mathrm{Arctan}(x)$
$\mathrm{sh}(x)$	$\mathbb{R}$	$\mathrm{ch}(x)$
$\mathrm{ch}(x)$	$\mathbb{R}$	$\mathrm{sh}(x)$
$\mathrm{th}(x)$	$\mathbb{R}$	$\ln(\mathrm{ch}(x))$
$1 - \mathrm{th}^2(x) = \dfrac{1}{\mathrm{ch}^2(x)}$	$\mathbb{R}$	$\mathrm{th}(x)$

Remarque II.2. *En pratique, on n'aura pas dès le départ les écritures précédentes : on utilisera la linéarité de l'intégrale et la proposition suivante.*

Proposition II.3. *Si $u : I \to J$ et φ définie sur J sont deux fonctions de classe $\mathcal{C}^1$, alors la fonction $u' \cdot (\varphi' \circ u)$ est continue, et admet pour primitive $\varphi \circ u$.*

Démonstration. Par dérivée d'une composée. □

Corollaire II.4. *Si u est de classe $\mathcal{C}^1$ sur un intervalle I :*

1. *pour $n \in \mathbb{N}$, une primitive de $u' \cdot u^n$ sur I est $\dfrac{1}{n+1}u^{n+1}$;*
2. *une primitive de $u' \cdot e^u$ sur I est e^u ;*
3. *si u ne s'annule pas sur I, une primitive de $\dfrac{u'}{u}$ sur I est $\ln(|u|)$;*
4. *si $u > 0$ sur I et que $\alpha \neq -1$, alors une primitive de $u' \cdot u^\alpha$ est $\dfrac{1}{\alpha+1}u^{\alpha+1}$.*

Exemples II.5.

1. *$xe^{-x^2} = \frac{-1}{2} \cdot (-2x)e^{-x^2}$, donc une primitive de $x \mapsto xe^{-x^2}$ est $x \mapsto -\frac{1}{2}e^{-x^2}$;*
2. *$\tan(x) = \dfrac{\sin(x)}{\cos(x)} = -\dfrac{-\sin(x)}{\cos(x)}$, donc une primitive de $\tan$ est $x \mapsto -\ln(|\cos(x)|)$;*
3. *$\dfrac{e^x}{1+e^{2x}} = e^x \cdot \dfrac{1}{1+(e^x)^2}$, donc une primitive de $x \mapsto \dfrac{e^x}{1+e^{2x}}$ est $\mathrm{Arctan} \circ \exp$.*

Remarque II.6. *On peut créer d'autres formules du même type, mais qu'on rencontre moins souvent. Comme par exemple qu'une primitive de $u' \cdot \cos(u)$ est $\sin(u)$. Par rapport au tableau, cela revient à changer tous les x en $u(x)$ et de multiplier la colonne de gauche par $u'(x)$.*

Corollaire II.7. *Soient F est une primitive d'une fonction continue f, et $a, b \in \mathbb{R}$ avec $a \neq 0$. Alors, là où elle est définie, la fonction $x \mapsto f(ax+b)$ est continue et admet pour primitive $x \mapsto \frac{1}{a}F(ax+b)$.*

Exemples II.8.

1. *Si on note F une primitive de $t \mapsto \sin^2(t)$ sur $\mathbb{R}$, alors $t \mapsto F(\frac{\pi}{2}+t)$ est une primitive de $t \mapsto \sin^2(t)$. Ainsi on retrouve que :*

$$\int_0^\pi \sin^2(\pi/2+t)\mathrm{d}t = F(\frac{3\pi}{2}) - F(\frac{\pi}{2}) = \int_{\pi/2}^{3\pi/2} \sin^2(t)\mathrm{d}t$$

   qu'on avait énoncé précédemment sans le justifier.

2. *Si $a, b \in \mathbb{R}$ avec $a \neq 0$, alors une primitive sur $\mathbb{R}$ de $x \mapsto \dfrac{1}{(ax+b)^2+1}$ est $x \mapsto \dfrac{1}{a}\mathrm{Arctan}(ax+b)$.*

   Calculons une primitive de $x \mapsto \dfrac{1}{x^2+2x+2}$. On a : $\dfrac{1}{x^2+2x+2} = \dfrac{1}{(x+1)^2+1}$. Donc une primitive est : $x \mapsto \mathrm{Arctan}(x+1)$.

II.2 Intégration par parties

Théorème II.9 (Intégration par parties)**.** *Si u, v sont deux fonctions de classes $\mathcal{C}^1$ sur $[a;b]$, alors :*

$$\int_a^b u'(t)v(t)\mathrm{d}t = [u(t)v(t)]_a^b - \int_a^b u(t)v'(t)\mathrm{d}t.$$

Démonstration. Par dérivée d'un produit, une primitive de $u'v + v'u$ est uv. Et ainsi :

$$[u(t)v(t)]_a^b = \int_a^b \left(u'(t)v(t) + u(t)v'(t)\right)\mathrm{d}t = \int_a^b u'(t)v(t)\mathrm{d}t + \int_a^b u(t)v'(t)\mathrm{d}t.$$

□

Remarque II.10. *En pratique, pour être que cette formule soit utile, il faudra que v' soit facile à primitiver, tandis que le fait de dériver u ne rende pas la fonction à intégrer plus compliquée.*

Corollaire II.11. *Si u, v sont deux fonctions de classe $\mathcal{C}^1$ sur I, et $x \in I$, alors :*

$$\int^x u'(t)v(t)\mathrm{d}t = u(x)v(v) - \int^x u(t)v'(t)\mathrm{d}t.$$

Exemples II.12.

1. $\int_0^1 \underbrace{t}_{v}\underbrace{e^t}_{u'}\mathrm{d}t = [te^t]_0^1 - \int_0^1 \underbrace{1}_{v'}\underbrace{e^t}_{u}\mathrm{d}t = e^1 - 0 - (e^1 - 1) = 1$;
2. $\int_0^{\pi/2} \underbrace{t^2}_{v}\underbrace{\sin(t)}_{u'}\mathrm{d}t = \cancel{[-t^2\cos(t)]_0^{\pi/2}} - \int_0^{\pi/2} \underbrace{2t}_{v'}\underbrace{(-\cos(t))}_{u}\mathrm{d}t = [2t\sin(t)]_0^{\pi/2} - \int_0^{\pi/2} 2\sin(t)\mathrm{d}t = \pi - 2$ *(en faisant deux intégrations par parties successives)* ;
3. *si $I = \int_0^1 \mathrm{Arctan}(t)\mathrm{d}t$: on pose $u'(t) = 1$ et $v(t) = \mathrm{Arctan}(t)$ (donc $u(t) = t$ et $v'(t) = \frac{1}{1+t^2}$). On trouve :*

$$I = [t\mathrm{Arctan}(t)]_0^1 - \int_0^1 \frac{t}{1+t^2}\mathrm{d}t = \mathrm{Arctan}(1) - \left[\frac{1}{2}\ln(1+t^2)\right]_0^1 = \frac{\pi}{4} - \ln(2).$$

Exemples II.13.

1. *avec $u'(x) = 1$ et $v(x) = \ln(x)$, donc $u(x) = x$ et $v'(x) = \frac{1}{x}$, on trouve :*

$$\int^x \ln(t)\mathrm{d}t = x\ln(x) - \int^x 1\mathrm{d}t = x\ln(x) - x.$$

2. *avec $u'(x) = \cos(x)$ et $v(x) = x$, donc $u(x) = \sin(x)$ et $v'(x) = 1$, on trouve :*

$$\int^x t\cos(t)\mathrm{d}t = x\sin(x) - \int^x \sin(t)\mathrm{d}t = x\sin(x) + \cos(x).$$

II.3 Changement de variable

Théorème II.14 (Changement de variable)**.** *Si φ est une fonction de classe $\mathcal{C}^1$ sur $[a;b]$, et que f est continue sur $\varphi([a;b])$, alors :*

$$\int_a^b \varphi'(t)\cdot f\left(\varphi(t)\right)\mathrm{d}t = \int_{\varphi(a)}^{\varphi(b)} f(t)\mathrm{d}t.$$

Démonstration. Par dérivée d'une composée, si F est une primitive de F, alors $F\circ\varphi$ est une primitive de $\varphi'\cdot(f\circ\varphi)$. Et ainsi :

$$\int_a^b \varphi'(x)\cdot f\left(\varphi(x)\right)\mathrm{d}x = [F(\varphi(t))]_a^b = F\left(\varphi(b)\right) - F\left(\varphi(a)\right) = [F(t)]_{\varphi(a)}^{\varphi(b)} = \int_{\varphi(a)}^{\varphi(b)} f(t)\mathrm{d}t.$$

□

Remarque II.15. *Ce théorème peut s'utiliser dans les deux sens (comme on va le voir dans les exemples).*

Exemple II.16. *Calculons $I = \int_0^1 \frac{e^{2x}}{1+e^x}\mathrm{d}x$.*

On fait le changement de variable $\varphi(x) = e^x$, avec $f : t \mapsto \frac{t}{1+t}$. Alors φ est $\mathcal{C}^1$ sur $[0;1]$, avec $\varphi([0;1]) = [1;e]$, et f est continue sur $[1;e]$. On déduit :

$$I = \int_0^1 \varphi'(x)f\left(\varphi(x)\right)\mathrm{d}x = \int_1^e \frac{t}{1+t}\mathrm{d}t = \int_1^e \left(1 - \frac{1}{1+t}\right)\mathrm{d}t = (e-1) - \ln(e-1) + \ln(2).$$

Remarque II.17. *En pratique, on ne fait pas apparaître φ. On procède en trois étapes en posant directement $t = \varphi(x)$:*

1. *on dérive t en fonction de x : $\mathrm{d}t = \varphi'(x)\mathrm{d}x$;*
2. *on exprime toute l'expression dans l'intégrale en fonction de t (et plus x) ;*
3. *on change les bornes.*

Pour l'exemple précédent, cela donne avec $t = e^x$:

1. $\mathrm{d}t = e^x \mathrm{d}x$;
2. $\dfrac{e^{2x}}{1+e^x}\mathrm{d}x = \dfrac{t}{1+t}\mathrm{d}t$;
3. $\int_0^1 \dfrac{e^{2x}}{1+e^x}\mathrm{d}x = \int_1^e \dfrac{t}{1+t}\mathrm{d}t$.

Exemple II.18. *Calculons $\int_{-1}^1 \sqrt{1-t^2}\mathrm{d}t$.*
On va faire le changement de variable $t = \cos(x)$. Pour $x = 0$, on a $t = 1$ et pour $x = \pi$, on a $t = -1$. La fonction cos *est bien $\mathcal{C}^1$. Et on a $\mathrm{d}t = -\sin(x)\mathrm{d}x$. Et donc :*

$$\int_{-1}^1 \sqrt{1-t^2}\mathrm{d}t = \int_{\pi}^0 \sqrt{1-\cos^2(x)}\,(-\sin(x))\,\mathrm{d}x = \int_0^{\pi} \sin^2(x)\mathrm{d}x = \frac{\pi}{2}$$

en inversant les bornes, et en reconnaissant que $\sqrt{1-\cos^2(x)} = \sin(x)$ pour $x \in [0;\pi]$.

Exemple II.19. *Calculons l'intégrale $\int_0^1 \frac{e^{2x}}{1+e^x}\mathrm{d}x$.*
On pose $x = \ln(t)$, où la fonction ln *est $\mathcal{C}^1$. On a $t = 1$ pour $x = 0$ et $t = e$ pour $x = 1$. Et $\mathrm{d}x = \frac{\mathrm{d}t}{t}$. Et donc :*

$$\int_0^1 \frac{e^{2x}}{1+e^x}\mathrm{d}x = \int_1^e \frac{e^{2\ln(t)}}{1+e^{\ln(t)}}\frac{\mathrm{d}t}{t} = \int_1^e \frac{t^2}{1+t}\frac{\mathrm{d}t}{t} = \int_1^e \frac{t}{1+t}\mathrm{d}t.$$

Méthode II.20 (Règles de Bioche)**.** *Pour simplifier le calcul d'une fraction rationnelle f en* cos *et* sin*, on peut utiliser les* ***règles de Bioche*** *: si $f(t)\mathrm{d}t$ est invariant par le changement $t \mapsto -t$ (resp. $t \mapsto \pi - t$, $t \mapsto \pi + t$), alors on peut faire le changement de variable $u = \cos(t)$ (resp. $u = \sin(t)$, $u = \tan(t)$).*

Remarques II.21.

1. *Les changements de variables correspondent aux fonctions invariantes utilisées :* $\cos(-t) = \cos(t)$, $\sin(\pi - t) = \sin(t)$ *et* $\tan(\pi + t) = \tan(t)$.
2. *Si tous les changements fonctionnent, on peut poser $u = \cos(2t)$.*
3. *Si aucun des changements ne fonctionne, on peut poser $u = \tan\left(\frac{t}{2}\right)$.*

Exemple II.22. *Déterminons une primitive de $f : t \mapsto \dfrac{\tan(t)}{1+\cos(t)}$ à l'aide des règles de Bioche :*

— *avec $t \mapsto -t$: $f(-t)\mathrm{d}(-t) = \dfrac{-\tan(t)}{1+\cos(t)} \cdot (-\mathrm{d}t) = f(t)\mathrm{d}t$;*

— *avec $t \mapsto \pi - t$: $f(\pi - t)\mathrm{d}(\pi - t) = \dfrac{\tan(t)}{1-\cos(t)}\mathrm{d}t \neq f(t)\mathrm{d}t$;*

— *avec $t \mapsto \pi + t$: $f(\pi + t)\mathrm{d}(\pi + t) = \dfrac{\tan(t)}{1-\cos(t)}\mathrm{d}t \neq f(t)\mathrm{d}t$.*

Donc on fait le changement de variable $u = \cos(t)$, avec donc $\mathrm{d}u = -\mathrm{sint})\mathrm{d}t$, ce qui donne :

$$\int^x \frac{\tan(t)}{1+\cos(t)}\mathrm{d}t = \int^x \frac{\sin(t)}{\cos(t)(1+\cos(t))}\mathrm{d}t = -\int^{\cos(x)} \frac{\mathrm{d}u}{u(u+1)}$$

Or, on a : $-\dfrac{1}{u(u+1)} = -\dfrac{1}{u} + \dfrac{1}{u+1}$. *Et finalement :*

$$\int^x \frac{\tan(t)}{1+\cos(t)}\mathrm{d}t = \ln\left(|1+\cos(x)|\right) - \ln\left(|\cos(x)|\right) = \ln\left|\frac{1+\cos(x)}{\cos(x)}\right| = \ln\left|1+\frac{1}{\cos(x)}\right|.$$

Exemple II.23. *Pour primitiver, pour* $p, q \in \mathbb{N}$, *la fonction* $t \mapsto \sin^p(t)\cos^q(t)$, *on trouve ainsi que :*

1. *si* p *et* q *sont impairs : on fait le changement de variable* $u = \cos(2t)$;
2. *si* p *est impair et* q *est impair : on fait le changement de variable* $u = \cos(t)$;
3. *si* q *est pair et* q *est impair, on fait le changement de variable* $u = \sin(t)$.

Si p *et* q *sont pairs, il est plus efficace de linéariser.*
Par exemple, pour calculer une primitive de $t \mapsto \sin^5(t)$, *les règles de Bioche montrent que l'on peut faire le changement de variable* $u = \cos(t)$, *et donc* $\mathrm{d}u = -\sin(t)\mathrm{d}t$, *ce qui donne :*

$$\begin{aligned}\int^x \sin^5(t)\mathrm{d}t &= -\int^x \underbrace{\sin^4(t)}_{=(1-\cos^2(t))^2}\cdot(-\sin(t))\mathrm{d}t \\ &= -\int^{\cos(x)}(1-u^2)^2\mathrm{d}u \\ &= -\frac{1}{5}\cos^5(x) + \frac{2}{3}\cos^3(x) - \cos(x)\end{aligned}$$

II.4 Intégrales complexes et fonctions trigonométriques

Proposition II.24. *Si* φ *est une fonction dérivable de classe* $\mathcal{C}^1$ *à valeurs complexes, alors* $\exp\circ\varphi$ *est une primitive de* $\varphi'\cdot(\exp\circ\varphi)$.

Corollaire II.25. *Si* $\alpha \in \mathbb{C}^*$, *alors une primitive de* $x \mapsto e^{\alpha x}$ *est* $x \mapsto \frac{1}{\alpha}e^{\alpha x}$.

Exemple II.26. *Cherchons une primitive de* $x \mapsto e^{3x}\sin(4x)$. *On a :* $e^{3x}\sin(4x) = \mathrm{Im}(e^{3x}e^{4ix}) = \mathrm{Im}(e^{(3+4i)x})$.
Mais $x \mapsto \dfrac{1}{3+4i}e^{(3+4i)x}$ *est une primitive de* $x \mapsto e^{(3+4i)x}$. *Donc En prenant la partie imaginaire, on aura une primitive de* $x \mapsto e^{3x}\sin(4x)$ *:*

$$\frac{1}{3+4i}e^{(3+4i)x} = \frac{3-4i}{25}e^{3x}\left(\cos(4x)+i\sin(4x)\right)$$

donc : $x \mapsto \dfrac{e^{3x}}{25}\left(3\sin(4x) - 4\cos(4x)\right)$ *est une primitive de* $x \mapsto e^{3x}\sin(4x)$.

Exemple II.27. *Cherchons une primitive de* $x \mapsto \cos(2\ln(x))$.
On a : $\cos(2\ln(x)) = \mathrm{Re}(e^{2i\ln(x)})$.
Mais $x \mapsto \frac{1}{2i+1}\cdot e^{(2i+1)\ln(x)}$ *est une primitive de* $x \mapsto e^{2i\ln(x)}$.
Donc : $x \mapsto \mathrm{Re}\left(\frac{1}{2i+1}\cdot e^{(2i+1)\ln(x)}\right) = \frac{x\cos(2\ln(x))}{5} + \frac{2x\sin(2\ln(x))}{5}$.

Méthode II.28. *Outre les règles de Bioche, on peut chercher à primitiver une puissance de* cos *ou de* sin, *ou un produit de telles puissances, par linéarisation.*

Exemple II.29. *Cherchons une primitive de* $x \mapsto \cos^4(x)$.
Par linéarisation, on a : $\cos^4(x) = \frac{1}{8}\cos(4x) + \frac{1}{2}\cos(2x) + \frac{3}{8}$.
Donc une primitive est : $x \mapsto \frac{1}{32}\sin(4x) + \frac{1}{4}\sin(2x) + \frac{3x}{8}$.

Remarque II.30. *On voit que la primitive d'une fonction périodique n'est pas nécessairement périodique.*

II.5 Intégrales de fonctions du type $\frac{1}{ax^2+bx+c}$

Proposition II.31. *Soient $a, b, c \in \mathbb{R}$, avec $a > 0$, et posons $f : x \mapsto \frac{1}{ax^2+bx+c}$, $P = ax^2 + bx + c$ et $\Delta = b^2 - 4ac$:*

1. *si $\Delta > 0$: en notant r_1, r_2 les racines de P, on a $P = a(x - r_1)(x - r_2)$. Ainsi :*

$$f(x) = \frac{1}{a(x-r_1)(x-r_2)} = \frac{1}{a(r_2-r_1)}\left(\frac{1}{x-r_2} - \frac{1}{x-r_1}\right)$$

donc une primitive de f est $x \mapsto \frac{1}{a(r_2-r_1)}\ln\left|\frac{x-r_2}{x-r_1}\right|$;

2. *si $\Delta = 0$: en notant r l'unique racine de P, on a $P = a(x - r)^2$. Ainsi :*

$$f(x) = \frac{1}{a}\frac{1}{(x-r)^2}$$

donc une primitive de f est $x \mapsto -\frac{1}{a(x-r)}$;

3. *si $\Delta < 0$: en notant $p = \frac{b}{2a}$ et $q = -\frac{\Delta}{4a}$, on a la forme canonique $P = a(x + p)^2 + q$. Ainsi :*

$$f(x) = \frac{1}{q}\frac{1}{\frac{a}{q}(x+p)^2 + 1}$$

donc une primitive de f est $x \mapsto \frac{1}{\sqrt{aq}}\mathrm{Arctan}\left(\sqrt{\frac{a}{q}}(x+p)\right)$.

Exemple II.32. *Si $a, b \in \mathbb{R}$, avec $b \neq 0$, et $\alpha = a + ib$, alors pour tout $x \in \mathbb{R}$:*

$$\frac{1}{x-\alpha} = \frac{(x-a)-ib}{(x-a)^2+b^2} = \frac{x-a}{(x-a)^2+b^2} - i\frac{b}{(x-a)^2+b^2}$$

et donc une primitive sur $\mathbb{R}$ de $x \mapsto \frac{1}{x-(a+ib)}$ est :

$$x \mapsto \frac{1}{2}\ln\left((x-a)^2+b^2\right) + i\mathrm{Arctan}\left(\frac{x-a}{b}\right).$$

Chapitre 10

Équations différentielles linéaires

Pour toute la suite, on note $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, et I un intervalle de $\mathbb{R}$.

I Généralités

Définition I.1. *Si $n \in \mathbb{N}^*$, une **équation différentielle linéaire d'ordre** n est une équation, dont l'inconnue y est une fonction de I dans $\mathbb{K}$, et de la forme :*

$$(E) \ : \ a_n y^{(n)} + \cdots + a_1 y' + a_0 y = b$$

*où b et les a_i sont des fonctions définies sur I à valeur dans $\mathbb{K}$, et a_n ne s'annulant pas sur I. Les fonctions a_i s'appellent les **coefficients**.*
*Son **équation homogène associée** est l'équation différentielle obtenue en remplaçant b par la fonction nulle.*

Remarque I.2. *En général, l'intervalle I sur lequel on résout l'équation est donné dans l'énoncé. Sinon, on le cherchera le plus grand possible comme intervalle de $\mathbb{R}$.*

Exemples I.3.

1. *la fonction* cos *est une solution sur $\mathbb{R}$ de l'équation différentielle linéaire d'ordre 1 : $y' = -\sin$, ou des équations différentielles $y'' + y = 0$ et $y^(4) - y = 0$;*
2. *la fonction $x \mapsto -\frac{1}{x}$ est une solution sur $\mathbb{R}_+^*$ ou sur $\mathbb{R}_-^*$ de l'équation différentielle linéaire homogène d'ordre 1 : $xy' + y = 0$.*

Définition I.4. *Un **problème de Cauchy** est un système formé :*
— *d'une équation différentielle (E) d'ordre n ;*
— *des n équations : $y^{(k)}(x_0) = y_k$ (avec $0 \leq k \leq n-1$), pour un $x_0 \in I$ et $y_0, \ldots, y_{n-1} \in \mathbb{K}$.*
*La donnée de x_0 et des y_k est appelée **condition initiale**.*

Exemple I.5. *En mécanique classique du point, le principe fondamental de la dynamique fournit une équation différentielle linéaire d'ordre 2 en la position de l'objet étudié. Une condition initiale correspond à la donnée de la position et de la vitesse à un instant donné.*

Proposition I.6. *Si $(E_0) : a_n y^{(n)} + \cdots + a_1 y' + a_0 y = 0$ est une équation différentielle linéaire homogène. Alors l'ensemble $\mathcal{S}_0$ de ses solutions est non vide et stable par combinaisons linéaires, c'est-à-dire que :*

$$\forall f, g \in \mathcal{S}_0, \ \forall \lambda, \mu \in \mathbb{K}, \ \lambda f + \mu g \in \mathcal{S}_0.$$

Démonstration. La fonction nulle est infiniment dérivable, de dérivées successives nulles, et est bien solution du système homogène.
Si $f, g \in \mathcal{S}_0$ et $\lambda, \mu \in \mathbb{K}$, alors $h = \lambda f + \mu g$ est n-fois dérivable (par linéarité de la dérivation), avec : $\forall k \in [\![1; n]\!],\ h^{(k)} = \lambda f^{(k)} + \mu g^{(k)}$. Et donc $h \in \mathcal{S}_0$ car :

$$a_n h^{(n)} + \cdots + a_1 h' + a_0 h = \lambda \underbrace{\left(a_n f^{(n)} + \cdots + a_1 f' + a_0 f\right)}_{=0 \text{ car } f \in \mathcal{S}_0} + \mu \underbrace{\left(a_n g^{(n)} + \cdots + a_1 g' + a_0 g\right)}_{=0 \text{ car } g \in \mathcal{S}_0} = 0.$$

□

Théorème I.7 (Ensemble des solutions)**.** *Soit (E) une équation différentielle linéaire d'ordre n. On note $\mathcal{S}$ l'ensemble de ses solutions, et $\mathcal{S}_0$ l'ensemble des solutions de l'équation homogène associée.*
Alors, si f est une solution de (E), on a :

$$\mathcal{S} = f + \mathcal{S}_0 = \{f + g \,|\, g \in \mathcal{S}_0\}.$$

Démonstration. Posons $f \in \mathcal{S}$ et considérons h une fonction n-fois dérivable sur I.
Alors :

$$\begin{array}{rcl} h \in \mathcal{S} & \Leftrightarrow & a_n h^{(n)} + \cdots + a_1 h' + a_0 h = b = a_n f^{(n)} + \cdots + a_1 f' + a_0 f \\ & \Leftrightarrow & a_n (h-f)^{(n)} + \cdots + a_1 (h-f)' + a_0 (h-f) = 0 \\ & \Leftrightarrow & (h-f) \in \mathcal{S}_0 \end{array} .$$

□

Remarque I.8. *Cet énoncé ne dit pas qu'il existe des solutions. Il dit en revanche que, si on sait résoudre l'équation homogène et que l'on possède **une** solution à l'équation, alors on a toutes les solutions.*

Proposition I.9 (Principe de superposition)**.** *Soient b_1, b_2 deux fonctions définies sur I, $\lambda, \mu \in \mathbb{K}$, et $b = \lambda b_1 + \mu b_2$. On considère les équations différentielles*

$$\begin{array}{rl} (E) & : a_n y^{(n)} + \cdots + a_1 y' + a_0 y = b \\ (E_1) & : a_n y^{(n)} + \cdots + a_1 y' + a_0 y = b_1 \\ (E_2) & : a_n y^{(n)} + \cdots + a_1 y' + a_0 y = b_2 \end{array}$$

Si f est une solution de (E_1) et g est une solution de (E_2), alors $\lambda f + \mu g$ est une solution de (E).

II Équations différentielles linéaires du premier ordre

On considère ici l'équation différentielle : $(E) : y' + ay = b$, définie sur un intervalle I, où a, b sont deux fonctions continues sur I à valeurs dans $\mathbb{K}$.
On note $(E_0) : y' + ay = 0$ l'équation homogène associée.

II.1 Solutions de l'équation homogène

Proposition II.1. *Les solutions de (E_0) sont les fonctions de la forme $x \mapsto \lambda e^{-A(x)}$, pour $\lambda \in \mathbb{K}$, où A est une primitive de a sur I.*

Démonstration. Montrons déjà que les fonction $f_\lambda : x \mapsto \lambda e^{-A(x)}$, pour $\lambda \in \mathbb{K}$, sont bien solutions de (E_0). Par dérivation de l'exponentielle complexe, on a que f_λ est dérivable sur I, avec : $\forall x \in I,\ f'_\lambda(x) = -a(x)e^{-A(x)}$. Et ainsi :

$$\forall x \in I,\ f'_\lambda(x) + a(x) f_\lambda(x) = -a(x)e^{-A(x)} + a(x)e^{-A(x)} = 0.$$

Réciproquement, si f est une solution de (E_0), qui vérifie donc : $f' + af = 0$. Posons : $g : x \mapsto f(x)e^{A(x)}$. Alors g est dérivable sur I, avec : $\forall x \in I,\ g'(x) = f'(x)e^{A(x)} + f(x)a(x)e^{A(x)} = 0$. Donc g est constante sur I : en posant $\lambda \in K$ comme étant l'unique valeur prise par g, on trouve bien que : $f : x \mapsto \lambda e^{-A(t)}$ est de la forme voulue. □

Remarque II.2. *On peut retrouver partiellement ce résultat : si une solution f de (E_0) ne s'annule pas, elle vérifie que $\frac{f'}{f} = -a(x)$, donc : $(\ln(|f|))' = -a(x)$. En primitivant, puis en prenant l'exponentielle, on retrouve que $f = e^{-A(x)+C} = \lambda e^{-A(x)}$, avec $\lambda = e^C$ une constante.*

Corollaire II.3 (Équation à coefficients constants)**.** *Si $a \in \mathbb{C}$, les solutions de l'équation homogène (E_a) : $y' + ay = 0$ sont les fonctions $x \mapsto \lambda e^{-ax}$ pour $\lambda \in \mathbb{K}$.*

Exemples II.4.

1. *si $a(x) = x$: alors $A(x) = \frac{x^2}{2}$ donc les solutions sur $\mathbb{R}$ sont de la forme $x \mapsto \lambda e^{-\frac{x^2}{2}}$;*
2. *si $a(x) = -\frac{1}{x}$: alors $A(x) = -\ln(|x|)$ donc les solutions sur $\mathbb{R}_+^*$ ou $\mathbb{R}_-^*$ sont de la forme $x \mapsto \lambda e^{\ln(|x|)} = \lambda|x|$. Mais, quitte à changer λ en son opposé, on déduit que les solutions sur $\mathbb{R}_+^*$ ou $\mathbb{R}_-^*$ sont de la forme $x \mapsto \lambda x$.*

Remarque II.5. *Dans le deuxième exemple, on peut recoller les solutions sur $\mathbb{R}_+^*$ et $\mathbb{R}_-^*$ pour obtenir des solutions qui sont des restrictions de fonctions dérivables sur $\mathbb{R}$ entier. Mais ce n'est pas toujours le cas.*

II.2 Solutions de l'équation complète

Méthode II.6 (Méthode de variation de la constante)**.** *Pour trouver une solution de (E), on peut la chercher sous la forme $f(x) = \lambda(x)e^{-A(x)}$, où λ est une fonction dérivable.*
On obtient alors que f est solution de (E) si, et seulement si, λ est une primitive de la fonction $x \mapsto b(x)e^{A(x)}$.

Démonstration. La fonction f est bien dérivable, de dérivée : $f' = \lambda' e^{-A} - \lambda a e^{-A}$. Et ainsi :

$$\begin{array}{rcl} f \in \mathcal{S} & \Leftrightarrow & f' + af = \lambda' e^{-A} - \lambda a e^{-A} + a\lambda e^{-A} = b \\ & \Leftrightarrow & \lambda' \cdot e^{-A} = b \\ & \Leftrightarrow & \lambda' = be^{A} \end{array} .$$

□

Remarque II.7. *Pour simplifier la recherche d'une solution, on pourra décomposer b en sommes de fonctions plus simples, et utiliser le principe de superposition.*

Exemples II.8.

1. *On considère l'équation $(E) : y' + xy = x$ sur $\mathbb{R}$. Les solutions de l'équation homogène sont les $x \mapsto \lambda e^{-\frac{x^2}{2}}$, pour $\lambda \in \mathbb{K}$.*
   Prenons donc λ dérivable sur $\mathbb{R}$ et posons $f : x \mapsto \lambda(x)e^{-\frac{x^2}{2}}$. Alors :
   $$f \in \mathcal{S} \Leftrightarrow \lambda'(x) = xe^{\frac{x^2}{2}} \Leftrightarrow \lambda'(x) = \left(e^{\frac{x^2}{2}}\right)'$$
   donc : $f : x \mapsto e^{\frac{x^2}{2}}e^{-\frac{x^2}{2}} = 1$ est une solution de (E).
   Et finalement : $\mathcal{S} = \{x \mapsto 1 + \lambda e^{-\frac{x^2}{2}} \mid \lambda \in \mathbb{K}\}$.
2. *On considère l'équation $(E) : y' - \frac{1}{x}y = x$ sur $\mathbb{R}_+^*$. Les solutions de l'équation homogène sont les $x \mapsto \lambda x$, pour $\lambda \in \mathbb{K}$.*
   Prenons donc λ dérivable sur $\mathbb{R}_+^*$ et posons $f : x \mapsto \lambda(x) \cdot x$. Alors :
   $$f \in \mathcal{S} \Leftrightarrow \lambda'(x) = \frac{x}{x} = 1 = (x)'$$
   donc : $f : x \mapsto x^2$ est une solution de (E).
   Et finalement : $\mathcal{S} = \{x \mapsto x^2 + \lambda x \mid \lambda \in \mathbb{K}\}$.

Proposition II.9 (Formulation intégrale)**.** *Si on fixe $x_0 \in I$, l'ensemble des solutions de (E) est :*

$$\mathcal{S} = \left\{ x \mapsto e^{-A(x)} \left(\lambda + \int_{x_0}^{x} b(t)e^{A(t)}\mathrm{d}t \right) \mid \lambda \in \mathbb{K} \right\}.$$

II.3 Problèmes de Cauchy et recollement de solutions

Théorème II.10 (Théorème de Cauchy–Lipschitz)**.** *Si $x_0 \in I$ et $y_0 \in \mathbb{K}$, alors il existe une unique solution au problème de Cauchy :*

$$\left\{ \begin{array}{rcl} y' + ay & = & b \\ y(x_0) & = & y_0 \end{array} \right. .$$

Démonstration. Toute solution de (E) est de la forme $f : x \mapsto e^{-A(x)} \left(\lambda + \int_{x_0}^{x} b(t) e^{A(t)} \right)$, pour un $\lambda \in \mathbb{K}$.
Et donc pour un tel f on a : $f(x_0) = y_0 \Leftrightarrow \lambda = y_0 e^{A(x_0)}$.
Ce qui assure l'existence et l'unicité de la solution au problème de Cauchy. □

Remarque II.11. *Le fait que a et b soient continues est essentiel : on peut perdre aussi bien l'existence que l'unicité sinon.*

Remarque II.12. *On peut reformuler le résultat en terme d'applications. Cela veut dire que, pour tout $x_0 \in I$, l'application :*

$$\varphi : \left\{ \begin{array}{rcl} \mathcal{S} & \to & \mathbb{K} \\ f & \mapsto & f(x_0) \end{array} \right.$$

est bijective (peu importe la valeur de x_0).

Corollaire II.13. *Si f, g sont deux solutions de (E), alors : soit $f = f$, soit leurs courbes ne se croisent jamais. C'est-à-dire que :*

$$\forall f, g \in \mathcal{S},\ (\forall x \in I,\ f(x) = g(x)) \Leftrightarrow (\exists x \in I,\ f(x) = g(x)) .$$

Démonstration. S'il existe $x_0 \in I$ tel que $f(x_0) = g(x_0)$, alors f et g sont solutions du même problème de Cauchy (associé aux conditions initiales x_0 et $f(x_0) = y_0 = g(x_0)$), donc $f = g$. □

Remarque II.14. *On peut reformuler le résultat en terme de relations : cela veut dire que la relation définie sur $I \times \mathbb{K}$ par :*

$$(x_1, y_1) \mathcal{R} (x_2, y_2) \Leftrightarrow \exists f \in \mathcal{S},\ f(x_1) = y_1 \text{ et } f(x_2) = y_2$$

est une relation d'équivalence (la symétrie et la réflexivité sont immédiates, et c'est la transitivité qui découle du résultat précédent).

Méthode II.15 (Problème de recollement)**.** *Si a et b sont continues sur un intervalle I privé des points $x_1, \ldots, x_m$, on peut chercher une solution sur I de (E) en :*

1. *cherchant une solution de (E) sur chaque intervalle ouvert inclus dans $I \setminus \{x_1, \ldots, x_n\}$;*
2. *choisir **si possible** les paramètres λ sur chaque intervalle de telle sorte que la solution obtenue soit prolongeable par continuité en les x_i ;*
3. *vérifier que la solution obtenue est dérivable.*

Exemple II.16. *Résolvons sur $\mathbb{R}$ l'équation différentielle linéaire $(E) : x^2 y' - y = x^2 - x + 1$.*
En divisant par x^2 l'équation, on se ramène à étudier sur $\mathbb{R}_+^*$ et $\mathbb{R}_-^*$ l'équation : $y' - \frac{1}{x^2} y = \frac{x^2 - x + 1}{x^2}$

— *équation homogène : sur $\mathbb{R}_+^*$ ou sur $\mathbb{R}_-^*$, une primitive de $-\frac{1}{x^2}$ est $\frac{1}{x}$, donc les solutions de l'équation homogène sont de la forme :*

$$x \mapsto \lambda e^{-\frac{1}{x}},\ \lambda \in \mathbb{K}.$$

— *solution particulière : la méthode de variation de la constante conduit à beaucoup de calculs, et doit se faire avec une identification. On va directement raisonner par identification, en cherchant une solution particulière de la forme $f : x \mapsto ax + b$. On a pour une telle fonction f :*

$$f'(x) - \frac{1}{x^2} f(x) = a - \frac{ax + b}{x^2} = \frac{ax^2 - ax - b}{x^2}$$

donc $f : x \mapsto x - 1$ est une solution particulière de (E) (aussi bien sur $\mathbb{R}_+^*$ que sur $\mathbb{R}_-^*$).

— *ensembles solution : les ensembles de solutions sur* $\mathbb{R}_+^*$ *ou* $\mathbb{R}_-^*$ *sont donc données respectivement par les ensembles :*

$$\mathcal{S}_+ = \{x \mapsto x - 1 + \lambda e^{-1/x} \,|\, \lambda \in \mathbb{K}\} \text{ et } \mathcal{S}_- = \{x \mapsto x - 1 + \mu e^{-1/x} \,|\, \mu \in \mathbb{K}\}$$

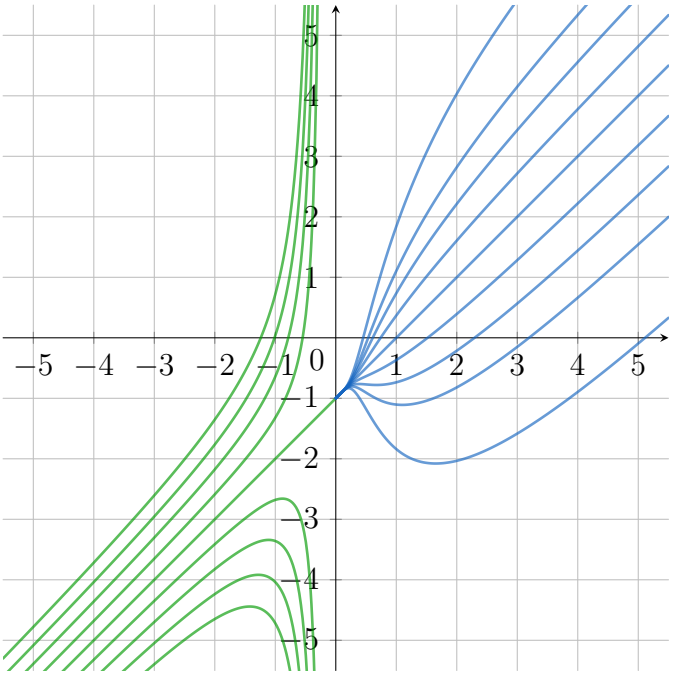
— *recollement continu : comme* $\lim\limits_{x\to 0^-} e^{-1/x} = +\infty$ *et* $\lim\limits_{x\to 0^+} e^{-1/x} = 0$ *(par limite d'une composée), alors le seul moyen d'avoir une solution continue en* 0 *en recollant des éléments de* $\mathcal{S}_+$ *et* $\mathcal{S}_-$ *est de prendre* $\mu = 0$*. Donc les solutions possibles de* (E) *sont les fonctions de la forme :*

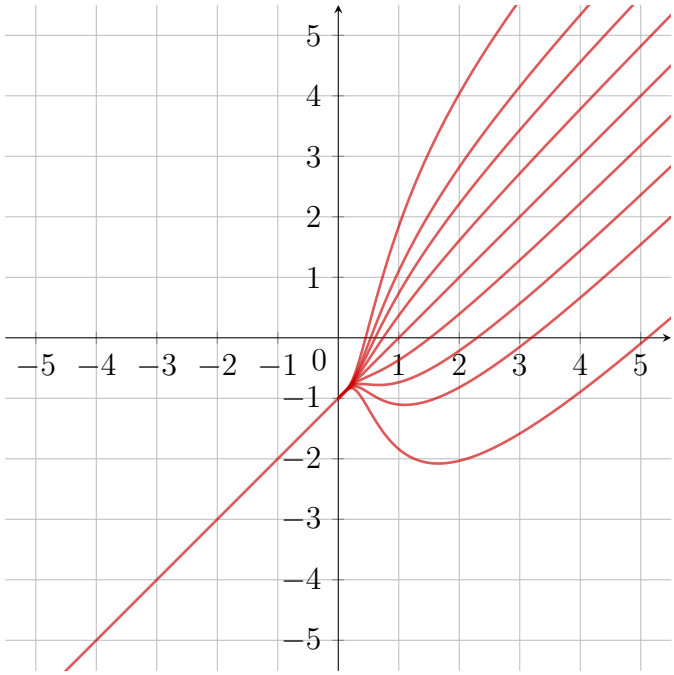
$$x \mapsto \begin{cases} x - 1 + \lambda e^{-1/x} & si\ x > 0 \\ -1 & si\ x = 0 \\ x - 1 & si\ x < 0 \end{cases}, \quad pour\ \lambda \in \mathbb{K}.$$

— *dérivabilité du recollement : soit* f *une solution continue obtenue par recollement. Alors :*
  — *si* $x < 0$ *:* $\dfrac{f(x) - f(0)}{x} = 1 \underset{x\to 0^-}{\longrightarrow} 1$ *;*
  — *si* $x > 0$ *:* $\dfrac{f(x) - f(0)}{x} = 1 + \dfrac{\lambda e^{-1/x}}{x} \underset{x\to 0^+}{\longrightarrow} 1$ *où on utilise que* $\lim\limits_{x\to 0^+} \frac{e^{-1/x}}{x} = \lim\limits_{x\to 0^+} -\left(\frac{-1}{x}\right) e^{-1/x} = \lim\limits_{x\to -\infty} (-x)\cdot e^x = 0$ *par croissances comparées.*
  donc une telle fonction est bien dérivable.

Conclusion : *les solutions de* (E) *sont exactement les fonctions :*

$$x \mapsto \begin{cases} x - 1 + \lambda e^{-1/x} & si\ x > 0 \\ -1 & si\ x = 0 \\ x - 1 & si\ x < 0 \end{cases}, \ \lambda \in \mathbb{K}.$$





Ainsi, le problème de Cauchy associé à (E) *avec condition initiale* $y(x_0) = y_0$ *admet :*
— *une unique solution si* $x_0 > 0$ *et* $y_0 \in \mathbb{K}$ *(quelconque) ;*
— *une infinité de solutions si* $x_0 \leq 0$ *et* $y_0 = x_0 - 1$ *;*
— *aucune solution si* $x_0 \leq 0$ *et* $y_0 \neq x_0 - 1$.

III Équations différentielles linéaires du second ordre à coefficients constants

On considère ici l'équation différentielle : $(E) : y'' + ay' + by = c$, définie sur un intervalle I, où a, b sont des constantes dans $\mathbb{K}$, et c est une fonction continue sur I à valeurs dans $\mathbb{K}$.
On note $(E_0) : y'' + ay' + by = 0$ l'équation homogène associée.

Définition III.1. *Le polynôme $X^2 + aX + b$ est appelé le **polynôme caractéristique** de l'équation (E).*

III.1 Solutions de l'équation homogène

Proposition III.2. *Notons $\Delta = a^2 - 4b$. Alors :*

1. *si $\Delta \neq 0$: notons r_1, r_2 les deux racines distinctes du polynôme caractéristique de (E). Les solutions de (E_0) sont les fonctions de la forme : $x \mapsto \lambda e^{r_1 x} + \mu e^{r_2 x}$, pour $\lambda, \mu \in \mathbb{C}$ (ou leurs parties réelles si on raisonne sur $\mathbb{R}$) ;*
2. *si $\Delta = 0$: notons r l'unique racine du polynôme caractéristique de (E). Les solutions de (E_0) sont les fonctions de la forme : $x \mapsto (\lambda x + \mu)e^{rx}$, pour $\lambda, \mu \in \mathbb{C}$ (ou leurs parties réelles si on raisonne sur $\mathbb{R}$).*

Démonstration. Notons r_1, r_2 les racines du polynôme caractéristique (avec éventuellement $r_1 = r_2 = r$).
Soit f deux fois dérivable sur I. Posons $g = f' - r_2 f$. Alors g est dérivable, avec $g' = f'' - r_2 f'$. Comme $r_1 + r_2 = -a$ et que $r_1 r_2 = b$, on déduit que :

$$\begin{aligned} f \in \mathcal{S}_0 &\Leftrightarrow f'' = -af' - bf \\ &\Leftrightarrow g' = -ag' - bg - r_2 g' \\ &\Leftrightarrow g' = r_1 f' - r_1 r_2 f = r_1 g \end{aligned}$$

donc z est solution de (E_0) si, et seulement si, g est de la forme $x \mapsto \lambda e^{r_1 x}$ pour $\lambda \in \mathbb{K}$.
Ainsi, f est solution de (E_0) si, et seulement si, f est solution de l'équation différentielle linéaire d'ordre 1 :

$$(E') : y' - r_2 y = \lambda e^{r_1 x}$$

dont les solutions de l'équation homogène sont de la forme $x \mapsto \mu e^{r_2 x}$, pour $\mu \in \mathbb{K}$.
Reste à trouver une solution particulière, ce que l'on fait par variation de la constante en cherchant une solution sous la forme $x \mapsto \mu(x) e^{r_2 x}$: c'est une solution si, et seulement si, μ est une primitive de $x \mapsto \lambda e^{(r_1 - r_2)x}$.

1. si $\Delta \neq 0$: alors $r_1 \neq r_2$, donc $\mu : x \mapsto \lambda \dfrac{e^{(r_1 - r_2)x}}{r_1 - r_2}$. Donc :

$$\mathcal{S} = \{x \mapsto \frac{\lambda}{r_1 - r_2} e^{r_1 x} + \mu e^{r_2 x} \mid \lambda, \mu \in \mathbb{K}\} = \{x \mapsto \lambda e^{r_1 x} + \mu e^{r_2 x} \mid \lambda, \mu \in \mathbb{K}\}.$$

2. si $\Delta = 0$: alors $r_1 = r_2 = r$, donc $\mu : x \mapsto \lambda x$. Donc :

$$\mathcal{S} = \{x \mapsto (\lambda x + \mu) e^{rx}\}.$$

□

Exemples III.3.

1. *Les solutions de l'équation $y'' - y' - 2y = 0$ sont les $x \mapsto \lambda e^{-x} + \mu e^{2x}$, $\lambda, \mu \in \mathbb{K}$;*
2. *Les solutions de l'équation $y'' - 4y' + 4y = 0$ sont les $x \mapsto (\lambda x + \mu) e^{2x}$, $\lambda, \mu \in \mathbb{K}$.*

Corollaire III.4. *Si $a, b \in \mathbb{R}$, alors avec les mêmes notations :*

1. *si $\Delta > 0$: alors $r_1, r_2 \in \mathbb{R}$ et les solutions réelles de (E_0) sont les fonctions de la forme : $x \mapsto \lambda e^{r_1 x} + \mu e^{r_2 x}$, pour $\lambda, \mu \in \mathbb{R}$;*
2. *si $\Delta = 0$: alors $r \in \mathbb{R}$ et les solutions réelles de (E_0) sont les fonctions de la forme : $x \mapsto (\lambda x + \mu)e^{rx}$, pour $\lambda, \mu \in \mathbb{R}$;*
3. *si $\Delta < 0$: alors $r_1, r_2 = \alpha \pm i\beta$ avec $\alpha, \beta \in \mathbb{R}$ et les solutions réelles de (E_0) sont les fonctions de la forme : $x \mapsto e^{\alpha x}\left(\lambda \cos(\beta x) + \mu \sin(\beta)\right)$, pour $\lambda, \mu \in \mathbb{R}$.*

Démonstration. Si f est une solution réelle, alors f est une solution complexe telle que $\mathrm{Re}(f) = f$.
Ainsi les cas où $\Delta \geq 0$ se proviennent directement de l'étude de $\mathbb{C}$ (et le fait que $f = \mathrm{Re}(f)$ imposent que $\lambda, \mu \in \mathbb{R}$).
Supposons $\Delta < 0$. Comme $a, b \in \mathbb{R}$, alors $r_1 = \overline{r_2} = \alpha + i\beta$. Si f est une solution réelle, elle est de la forme $f : x \mapsto \lambda_1 e^{(\alpha+i\beta)x} + \mu_1 e^{(\alpha-i\beta)x} = e^{\alpha x}\left((\lambda_1 + \mu_1)\cos(\beta x) + i(\lambda_1 - \mu_1)\sin(\beta x)\right)$.
Et ainsi pour tout $x \in I$:

$$f(x) = \mathrm{Re}(f(x)) = e^{\alpha x}\left(\underbrace{\mathrm{Re}(\lambda_1 + \mu_1)}_{=\lambda}\cos(\beta x) + \underbrace{\mathrm{Re}(i(\lambda_1 - \mu_1))}_{=\mu}\sin(\beta x)\right).$$

Et il est clair que les fonctions de cette forme sont bien des solutions. □

Remarques III.5.

1. *Dans le dernier cas, avec les mêmes notations, les solutions sont aussi les fonctions de la forme : $x \mapsto Ae^{\alpha x}\cos(\beta x + \varphi)$, pour $A \in \mathbb{R}_+$ et $\varphi \in]-\pi; \pi]$, suivant un résultat de trigonométrie. On dit alors que A est l'amplitude, φ le déphasage, α le coefficient d'amortissement, et β la fréquence. Cette notation est fréquente lorsque l'on travaille avec des circuits électriques.*
2. *De manière cachée, la dernière égalité nécessite que $\overline{\lambda_1} = \mu_1$: c'est un résultat que l'on peut retrouver par le théorème de Cauchy–Lipschitz qui assure l'unicité de l'écriture des solutions, et du fait que, pour f réelle, $\overline{f} = f$ fournit une autre écriture qui revient à changer λ_1 en $\overline{\mu_1}$ et μ_1 en $\overline{\lambda_1}$.*

Exemple III.6. *Si $\omega \in \mathbb{R}^*$, les solutions réelles de l'équation différentielle $y'' + \omega^2 y = 0$ sont les fonctions de la forme :*

$$x \mapsto \lambda\cos(\omega x) + \mu\sin(\omega x),\ \lambda, \mu \in \mathbb{R}.$$

III.2 Solutions de l'équation complète

Proposition III.7. *Si $c : x \mapsto Ae^{\lambda x}$, pour $A, \lambda \in \mathbb{K}$, alors il existe une solution particulière de (E) de la forme :*

1. *$x \mapsto \mu e^{\lambda x}$, avec $\mu \in \mathbb{K}$, si λ **n'est pas une racine** du polynôme caractéristique ;*
2. *$x \mapsto \mu x e^{\lambda x}$, avec $\mu \in \mathbb{K}$, si λ est **racine simple** du polynôme caractéristique ;*
3. *$x \mapsto \mu x^2 e^{\lambda x}$, avec $\mu \in \mathbb{K}$, si λ est **racine double** du polynôme caractéristique.*

Démonstration. Soit $k \in \mathbb{N}$ et $\mu \in \mathbb{K}$. On pose $f : x \mapsto \mu x^k e^{\lambda x}$. Alors f est deux fois dérivable sur $\mathbb{R}$, avec :

$$\forall x \in \mathbb{R},\ f'(x) = \mu e^{\lambda x}\left(\lambda x^k + k x^{k-1}\right) \text{ et } f''(x) = \mu e^{\lambda x}\left(\lambda^2 x + 2\lambda k t^{k-1} + k(k-1)x^{k-2}\right).$$

Donc pour tout $x \in \mathbb{R}$:

$$f''(x) + af'(x) + bf(x) = \mu e^{\lambda x}\left((\lambda^2 + a\lambda + b)x^k + (2\lambda + a)kx^{k-1} + k(k-1)x^{k-2}\right)$$

Donc f est une solution si, et seulement si, pour tout $x \in \mathbb{R}$:

$$\mu\left((\lambda^2 + a\lambda + b)x^k + (2\lambda + a)kx^{k-1} + k(k-1)x^{k-2}\right) = A.$$

1. si λ n'est pas racine du polynôme caractéristique : alors $\lambda^2 + a\lambda + b \neq 0$, donc $k = 0$ et $\mu = \dfrac{A}{\lambda^2 + a\lambda + b}$ conviennent ;
2. si λ est racine simple du polynôme caractéristique : alors $\lambda^2 + a\lambda + b = 0$ mais $2\lambda + a \neq 0$, donc $k = 1$ et $\mu = \dfrac{A}{2\lambda + a}$ conviennent ;
3. si λ est racine double du polynôme caractéristique : alors $\lambda^2 + a\lambda + b = 0$ et $2\lambda + a = 0$, donc $k = 2$ et $\mu = \dfrac{A}{2}$ conviennent.

□

Remarque III.8. *Le passage de $\mathbb{C}$ à $\mathbb{R}$ permet de trouver par la même méthodes des solutions réelles lorsque c est de la forme $Be^{\alpha x}\cos(\beta x)$ ou $Be^{\alpha x}\sin(\beta x)$ en raisonnant dans les complexes puis en prenant les parties réelles ou imaginaire.*

Exemple III.9. *Considérons l'équation $(E) : y'' - y' - 2y = e^{-x}$.*
Le polynôme caractéristique est $X^2 - X - 2 = (X - 2)(X + 1)$, donc -1 est racine simple du polynôme caractéristique, et il existe une solution particulière sous la forme $x \mapsto \lambda x e^{-x}$. Posons $f : x \mapsto \lambda x e^{-x}$. Alors :

$$\forall x \in \mathbb{R},\ f'(x) = \lambda(1 - x)e^{-x} \text{ et } f''(x) = \lambda(x - 2)e^{-x}.$$

Donc : $f''(x) - f'(x) - 2f(x) = \lambda e^{-x} \cdot [(x - 2) - (1 - x) - 2x] = -3\lambda e^{-x}$.
Donc : $f : x \mapsto -\frac{1}{3}xe^{-x}$ est une solution de (E).
Donc les solutions de (E) sont les fonctions de la forme :

$$x \mapsto \left(\lambda - \frac{1}{3}x\right)e^{-x} + \mu e^{2x}.$$

Exemple III.10. *Considérons l'équation $(E) : y'' + 2y' + 2y = -2e^{-x}\cos(x)$, dont on cherche les solutions réelles.*
On lui associe l'équation : $(E') : y'' + 2y' + 2y = -2e^{-x}e^{ix} = -2e^{(-1+i)x}$.
Le polynôme caractéristique est $X^2 + 2X + 2 = (X - (-1 + i))(X - (-1 - i))$, donc $(-1 + i)$ est racine simple du polynôme caractéristique, et il existe une solution particulière sous la forme $x \mapsto \lambda x e^{(-1+i)x}$. Posons $f : x \mapsto \lambda x e^{(-1+i)x}$. Alors :

$$\forall x \in \mathbb{R},\ f'(x) = \lambda(1 + (-1 + i)x)e^{(-1+i)x} \text{ et } f''(x) = \lambda(-2 + 2i - 2ix)e^{(-1+i)x}.$$

Donc : $f''(x) + 2f'(x) + 2f(x) = \lambda e^{(-1+i)x} \cdot [(-2 + 2i - 2ix) + 2(1 + (-1 + i)x) + 2x] = 2i\lambda e^{(-1+i)x}$.
Donc : $f : x \mapsto ixe^{(-1+i)x}$ est une solution de (E').
Donc $y : x \mapsto \mathrm{Re}(f(x)) = -xe^{-x}\sin(x)$ est une solution de (E).
Donc les solutions de (E) sont les fonctions de la forme :

$$x \mapsto e^{-x}\left(\lambda e^{ix} + \mu e^{-x} - x\sin(x)\right) = e^{-x}\left[(\lambda + \mu)\cos(x) + (i\lambda - i\mu - x)\sin(x)\right],\ \lambda, \mu \in \mathbb{C}$$

et les solutions à valeurs réelles sont les :

$$x \mapsto e^{-x}\left[\lambda'\cos(x) + (\mu' - x)\sin(x)\right],\ \lambda', \mu' \in \mathbb{R}.$$

Remarque III.11. *Au lieu de passer par les parties réelles, on pouvait aussi utiliser le principe de superposition, en constatant que : $\cos(x) = \frac{e^{ix} + e^{-ix}}{2}$.*

Remarque III.12. *En général, on précisera sous quelle forme chercher une solution particulière. Notons que, plus généralement, si le second membre est de la forme $Q(x)e^{\lambda x}$, on peut trouver une solution de la forme $x^m R(x)e^{\lambda x}$ où m est la multiplicité de λ comme racine du polynôme caractéristique et R est un polynôme de même degré que Q.*

III.3 Problèmes de Cauchy

Théorème III.13 (Théorème de Cauchy–Lipschitz)**.** *Si $x_0 \in I$ et $y_0, y_1 \in \mathbb{K}$, alors il existe une unique solution au problème de Cauchy :*

$$\begin{cases} y'' + ay' + by &= c \\ y(x_0) &= y_0 \\ y'(x_0) &= y_1 \end{cases}.$$

Idée de preuve. On admet que l'équation différentielle (E) possède une solution, que l'on note f. Alors :

1. si $\Delta \neq 0$: les solutions sont de la forme $x \mapsto \lambda e^{r_1 x} + \mu e^{r_2 x} + f(x)$. Donc on souhaite résoudre le système d'inconnues λ, μ suivant :

$$\begin{cases} e^{r_1 x_0}\lambda + e^{r_2 x_0}\mu &= y_0 - f(x_0) \\ r_1 e^{r_1 x_0}\lambda + r_2 e^{r_2 x_0}\mu &= y_1 - f'(x_0) \end{cases}$$

   qui est un système de linéaire à 2 inconnues, et 2 équations. Son déterminant est : $(r_2 - r_1)e^{(r_1+r_2)x_0} \neq 0$, donc ce système admet une unique solution.

2. si $\Delta = 0$: on procède de même, et on est amené à chercher les solutions du système :

$$\begin{cases} x_0 e^{r x_0}\lambda + e^{r x_0}\mu &= y_0 - f(x_0) \\ (1 + r x_0)e^{r x_0}\lambda + r e^{r x_0}\mu &= y_1 - f'(x_0) \end{cases}$$

   qui est de déterminant $-e^{2r x_0} \neq 0$, et admet donc aussi une unique solution.

Dans les deux cas, il n'y a donc qu'une seule solution au problème de Cauchy. □

Remarque III.14. *Comme pour le degré 1, on peut montrer l'existence de solution par une méthode de variation de la constante, mais celle-ci est plus complexe pour le degré 2.*
Si c est de l'une des formes du paragraphe précédent (ou une fonction constante), on sait trouver des solutions donc la démonstration est complète.

Chapitre 11

Arithmétique dans les entiers

I Divisibilité et nombres premiers

I.1 Divisibilité dans $\mathbb{Z}$ et division euclidienne

Définition I.1. *Soient $a, b \in \mathbb{Z}$. On dit que a **divie** b, ce que l'on note $a|b$, s'il existe $x \in \mathbb{Z}$ tel que $b = ac$. On dit alors que a **est un diviseur de** b ou que b **est un multiple de** a.*

Exemples I.2.

1. *les diviseurs de* 15 *sont* $1, 3, 5, 15$ *et leurs opposés ;*
2. 1 *et* -1 *divisent tout entier, tandis que ce sont les seuls diviseurs de* 1 *;*
3. 0 *est multiple de tout entier, tandis que son seul multiple est* 0.

Proposition-Définition I.3. *Si $n \in \mathbb{Z}$, on note $\mathcal{D}(n)$ l'ensemble des diviseurs de n. C'est un ensemble fini si, et seulement si, n est non nul.*
On note de même $n\mathbb{Z} = \{n \times k \,|\, k \in \mathbb{Z}\}$ l'ensemble des multiples de n. C'est un ensemble infini si, et seulement si, n est non nul.

Démonstration. On a déjà $\mathcal{D}(0) = \mathbb{Z}$ qui est infini et $0\mathbb{Z} = \{0\}$ qui est fini.
Si $n \neq 0$: si $a \in \mathcal{D}(n)$, alors il existe $c \in \mathbb{Z}$ tel que $n = ac$. Comme $n \neq 0$, alors $c \neq 0$, donc $|c| \geq 1$. Ainsi : $|a| \leq |n|$, donc $\mathcal{D}(n) \subset [\![-n; n]\!]$ est fini.
Pour un tel n, l'application $\varphi : \left\{ \begin{array}{ccc} \mathbb{Z} & \to & n\mathbb{Z} \\ k & \mapsto & n \times k \end{array} \right.$ est une fonction injective de l'ensemble infini $\mathbb{Z}$ dans $n\mathbb{Z}$, donc $n\mathbb{Z}$ est infini. □

Proposition I.4. *Soient $a, b, n \in \mathbb{Z}$ tels que $n|a$ et $n|b$. Alors :*

$$\forall u, v \in \mathbb{Z},\ n|au + bv.$$

Démonstration. On écrit $a = cn$ et $b = dn$ pour $c, d \in \mathbb{Z}$. Alors :

$$au + bv = cnu + dnv = \underbrace{(cu + dv)}_{\in\mathbb{Z}} n.$$

□

Proposition-Définition I.5. *Si $a, b \in \mathbb{Z}$ vérifient simultanément que $a|b$ et $b|a$, on dira que a et b sont **associés**.*
C'est le cas si, et seulement si, $|a| = |b|$.

Démonstration. Si $a = 0$, alors $b = 0$ donc le résultat est vérifié.
Sinon, on pose $c, d \in \mathbb{Z}$ tels que $a = cb$ et $b = da$. Et donc $a = cda$, donc $cd = 1$ (comme $a \neq 0$), et $c = d = \pm 1$. Si $c = 1$, alors $a = b$. Si $c = -1$, alors $a = -b$. Dans les deux cas : $|a| = |b|$.
Réciproquement, si $|a| = |b|$: alors $a = \pm b$ donc $b|a$; et $b = \pm a$, donc $a|b$. □

Théorème-Définition I.6. *Si $a \in \mathbb{Z}$ avec $b \in \mathbb{N}^*$, il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que :*

$$a = bq + r \text{ et } 0 \leq r < b.$$

*On dit alors que q est le **quotient** et que r est le **reste** de la division euclidienne de a par b.*

Démonstration.
- existence : l'ensemble $A = \{a - bk \,|\, k \in \mathbb{Z}\} \cap \mathbb{N}$ est une partie non vide de $\mathbb{N}$ (prendre $k = -|a|$), donc elle possède un plus petit élément r. En notant q la valeur de k associée à r, on a : $r = a - bq$. Par définition de r, on a $r \geq 0$. Il suffit de montrer que $r < b$: si ce n'était pas le cas, alors $r - b \geq 0$, et $r - b = a - b(q + 1)$, donc $(r - b) \in A$, ce qui contredit la définition de r.
- unicité : si $bq_1 + r_1 = bq_2 + r_2$, alors $b(q_1 - q_2) = r_2 - r_1$ avec $-b < r_2 - r_1 < b$. Donc : $-1 < q_1 - q_2 < 1$, donc $q_1 - q_2 = 0$, c'est-à-dire $q_1 = q_2$, puis $r_1 = r_2$. Ce qui montre l'unicité.

□

Remarque I.7. *Le théorème reste vrai si $b < 0$, en imposant que $0 \leq r < |b|$.*

I.2 Congruences

Définition I.8. *Si $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$, on dit que a et b sont **congrus modulo** n, ce que l'on note $a \equiv b\ [n]$, si $n|(a - b)$.*

Remarque I.9. *L'entier a est un multiple de n si, et seulement si, $a \equiv 0\ [n]$.*

Proposition I.10. *La relation de congruence est une relation d'équivalence sur $\mathbb{Z}$.*

Démonstration. Évident. □

Proposition I.11 (Calculs modulaires)**.** *Si $n \in \mathbb{N}^*$ et $a, b, c, d \in \mathbb{Z}$, alors :*

1. *si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors $a + c \equiv b + d\ [n]$;*
2. *si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors $ac \equiv bd\ [n]$;*
3. *si $a \equiv b\ [n]$ et $k \in \mathbb{N}$, alors : $a^k \equiv b^k\ [n]$;*
4. *si $m \in \mathbb{N}^*$, alors : $a \equiv b\ [n] \Leftrightarrow am \equiv bm\ [nm]$.*

Démonstration.

1. on note $a - b = nk$ et $c - d = nl$. Alors : $(a + c) - (b + d) = n(k + l)$, donc $a + c \equiv b + d\ [n]$.
2. Avec les mêmes notations : $ac = (b + nk)(d + nl) = bd + n(kd + lb + nkl)$ donc $ac \equiv bd\ [n]$.
3. Par récurrence sur k, grâce au résultat précédent.
4. On procède par équivalence :

$$\begin{aligned} a \equiv b\ [n] &\Leftrightarrow \exists k \in Z, a - b = kn \\ &\Leftrightarrow \exists k \in \mathbb{Z}, m(a - b) = mnk \text{ car } m \neq 0 \\ &\Leftrightarrow \exists k \in \mathbb{Z}, am - bm = (mn)k \\ &\Leftrightarrow am \equiv bm\ [mn] \end{aligned}.$$

□

Exemple I.12. *Par exemple, pour $n = 3$ ou 9, on retrouve les critères usuels de divisibilité car :*

— $10 \equiv 1\ [n]$;
— *pour tout* $k \in \mathbb{N}$: $10 \equiv 1^k = 1\ [n]$;
— *si* $m \in \mathbb{N}^*$ *a pour écriture décimale* $\overline{a_r a_{r-1} \dots a_1 a_0}$, *alors* $m = \sum_{k=0}^{r} a_k 10^k$, *et donc :* $a \equiv \sum_{k=0}^{N} a_k\ [n]$.
Et on peut adapter un peu pour trouver un critère de divisibilité par 37.

Proposition I.13. *Soient* $n \in \mathbb{N}^*$ *et* $a, b \in \mathbb{Z}$:

1. *si* $a = nq + r$ *est la division euclidienne de* a *par* n, *alors :* $a \equiv r\ [n]$;
2. a *et* b *sont congrus modulo* n *si, et seulement si, ils ont même reste dans la division euclidienne par* n.

Démonstration.

1. on a directement $a - r = nq$ est un multiple de n, donc $a \equiv r\ [n]$;
2. si $a = nq_1 + r_1$ et $b = nq_2 + r_2$ sont les divisions euclidiennes de a et b par n, alors :
   — si $a \equiv b\ [n]$: alors $r_1 \equiv r_2\ [n]$, donc $r_1 - r_2$ est un multiple de n. Mais $-n < r_1 - r_2 < n$, donc $r_1 = r_2$.
   — si $r_1 = r_2$: alors $r_1 \equiv r_2\ [n]$ donc $a \equiv b\ [n]$.

□

Corollaire I.14. *Si* $n \in \mathbb{N}^*$ *et* $a \in \mathbb{Z}$, *il y a équivalence entre :*

1. a *est divisible par* n ;
2. $a \equiv 0\ [n]$;
3. *le reste de la division euclidienne de* a *par* n *est nul.*

Corollaire I.15. *Il y a exactement* n *classes d'équivalence pour la relation de congruence modulo* n, *à savoir :* $\overline{0}, \overline{1}, \dots, \overline{n-1}$.

I.3 Les nombres premiers

Définition I.16. *Un* ***nombre premier*** *est un entier naturel possédant exactement deux diviseurs positifs (*1 *et lui-même). Un entier naturel qui n'est pas premier est dit* ***composé****.*

Remarque I.17. *Comme tout nombre est divisible par* 1 *et par lui-même, les nombres premiers sont les nombres distincts de* 1 *possédant le moins de diviseurs possibles.*

Proposition I.18. *Un entier* $p \geq 2$ *est premier si, et seulement si :*

$$\forall a, b \in \mathbb{N},\ p = ab \Rightarrow (a = 1 \text{ ou } b = 1).$$

Démonstration. Si p est premier et $p = ab$, alors a, b sont des diviseurs de p, donc égaux à 1 ou p. Donc si $a \neq 1$, alors $a = p$ donc $b = 1$.
Réciproquement, soit a un diviseur de p différent de 1. Alors il existe b tel que $ab = p$. Mais, comme $a \neq 1$, alors $b = 1$ donc $a = p$. □

Exemples I.19. *Les premiers nombres premiers sont* 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 *et* 37.

Proposition I.20. *Si* n *est un entier naturel composé, alors son plus petit diviseur plus grand que* 1 *est un nombre premier inférieur ou égal à* $\sqrt{n}$.

Démonstration. Soit p ce diviseur. On écrit $n = pq$ avec $q \in \mathbb{N}^*$:
— comme n n'est pas premier, alors $p \neq n$, donc $q \neq 1$;
— par définition de p, on a donc $p \leq q$, donc $p^2 \leq n$, donc $p \leq \sqrt{n}$;

— si p n'était pas premier, comme $p > 1$, alors p possède un diviseur d avec $1 < d < p$. Mais d serait un diviseur de n, plus grand que 1 et plus petit que p, ce qui est impossible.

□

Corollaire I.21. *Tout entier admet un diviseur premier.*

Corollaire I.22. *Un entier p est premier si, et seulement si, il n'admet aucun diviseur parmi les nombres premiers inférieurs ou égaux à $\sqrt{p}$.*

Remarque I.23. *Ce résultat permet d'expliquer la méthode du crible pour déterminer les nombres premiers :*
— *on représente dans une grille tous les nombres entiers (par exemple ceux plus petits que 40) ;*
— *on barre 1 ;*
— *on entoure le premier nombre non barré, puis on barre tous ses multiples ;*
— *on répète ce processus jusqu'à ce que tous les nombres soient barrés ou entourés.*
Les nombres entourés sont les nombres premiers.

~~1~~	②	③	~~4~~	⑤	~~6~~	⑦	~~8~~	~~9~~	~~10~~
⑪	~~12~~	⑬	~~14~~	~~15~~	~~16~~	⑰	~~18~~	⑲	~~20~~
~~21~~	~~22~~	㉓	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	㉙	~~30~~
㉛	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	㊲	~~38~~	~~39~~	~~40~~

Théorème I.24. *Il existe une infinité de nombres premiers.*

Démonstration. Raisonnons par l'absurde, en notant $p_1, p_2, \ldots, p_n$ les nombres premiers, où n désigne le nombre de nombres premiers. Alors $N = p_1 \times \cdots \times p_n + 1$ est soit premier, soit il admet un diviseur premier :
— il ne peut pas être premier, comme il est distincts de tous les p_i ;
— s'il était divisible par un nombre premier, ce serait l'un des p_i, mais alors p_i diviserait $n - p_1 \times \cdots \times p_n = 1$, ce qui est impossible.
D'où la contradiction, donc il existe une infinité de nombres premiers. □

II PGCD et PPCM

II.1 PGCD et algorithme d'Euclide

Définition II.1. *Si $a, b \in \mathbb{Z}$, avec a ou b non nul, le **plus grand commun diviseur** (abrégé en pgcd ou PGCD) de a et b est le plus grand diviseur commun à a et b :*

$$a \wedge b = \mathrm{pgcd}(a, b) = \max\left(\mathcal{D}(a) \cap \mathcal{D}(b)\right).$$

Par convention, on pose $0 \wedge 0 = 0$.

Exemples II.2.

1. $90 \wedge 75 = 15$ *car* $\mathcal{D}(90) \cap \mathcal{D}(75) = \{\pm 1, \pm 3, \pm 5, \pm 15\}$;
2. *si $a|b$, alors $a \wedge b = |a|$. Plus généralement, si $b = 0$, alors $a \wedge b = |a|$.*

Proposition II.3. *Si $a, b \in \mathbb{Z}$ et $k \in \mathbb{Z}$, alors : $a \wedge b = (a + kb) \wedge b$.*
En particulier, si r est le reste de la division euclidienne de a par b, alors $a \wedge b = r \wedge b$.

Démonstration. Soit $d \in \mathbb{Z}$:
— si d divise à la fois a et b, alors d divise $a + kb$ et b ;
— si d divise à la fois $a + kb$ et b, alors d divise $a = (a + kb) - kb$ et b.

Et donc : $\mathcal{D}(a) \cap \mathrm{D}(b) = \mathcal{D}(a+kb) \cap \mathcal{D}(b)$. D'où l'égalité cherchée en prenant le maximum dans les deux ensembles.
Si on écrit $a = bq + r$ comme étant la division euclidienne de a par b, alors $r = a - qb$, donc on a bien un cas particulier. □

Théorème II.4 (Algorithme d'Euclide)**.** *Si $a, b \in \mathbb{N}$ avec $a \geq b$, on détermine le pgcd de a et b avec **l'algorithme d'Euclide** :*

1. *on pose r_1 le reste de la division euclidienne de a par b ; donc $a \wedge b = b \wedge r_1$ et $0 \leq r_1 < b$;*
2. *si $r_1 \neq 0$, on pose pose r_2 le reste de la division euclidienne de b par r_1 ;*
3. *on continue en posant r_{k+1} le reste de la division euclidienne de r_{k-1} par r_k, tant que r_k est non nul.*

La suite des r_k ainsi construite est une suite strictement décroissante d'entiers (ce qui assure bien que l'un des r_k est nul et que l'on s'arrête).
Si l'on note r_n le dernier reste non nul, alors :

$$a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = \cdots = r_n \wedge \underbrace{r_{n+1}}_{=0} = r_n.$$

*Donc le pgcd de a et b est le **dernier reste non nul** dans l'algorithme d'Euclide.*

Remarque II.5. *Quitte à changer a et b par $|a|$ et $|b|$, ou à échanger les rôles de a et b, on sera bien dans cette situation.*

Exemple II.6. *Calculons $5742 \wedge 1320$:*

- $5742 = 1320 \times 4 + 462$;
- $1320 = 462 \times 2 + 396$;
- $462 = 396 \times 1 + 66$;
- $396 = 66 \times 6 + 0$.

Donc $5742 \wedge 1320 = 66$.

Corollaire II.7. *Si $a, b \in \mathbb{Z}$, alors : $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a \wedge b)$.*

Démonstration. On avait vu que, si $k \in \mathbb{Z}$: $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a+kb) \cap \mathcal{D}(b)$.
En reprenant l'algorithme d'Euclide, on a donc :

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(r_1) \cap \mathcal{D}(b) = \cdots = \mathcal{D}(r_n) \cap \underbrace{\mathcal{D}(r_{n+1})}_{=\mathbb{Z}} = \mathcal{D}(r_n) = \mathcal{D}(a \wedge b).$$

□

Corollaire II.8. *Si $a, b \in \mathbb{Z}$, le pgcd de a et b est le plus grand élément de $\mathcal{D}(a) \cap \mathcal{D}(b)$ **au sens de la divisibilité**, c'est-à-dire que le pgcd de a et b est l'unique entier naturel d tel que :*

$$\forall n \in \mathbb{Z},\ (n|a \text{ et } n|b) \Leftrightarrow n|d.$$

Démonstration. Il est clair que $a \wedge b$ vérifie bien ces hypothèses comme $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a \wedge b)$.
Réciproquement, si $d \in \mathbb{N}$ les vérifie, alors :

— comme $d|d$, on utilise l'implication précédente avec $n = d$, et alors $d|a$ et $d|b$, donc $d \in \mathcal{D}(a) \cap \mathrm{D}(b) = \mathcal{D}(a \wedge b)$, donc $d|a \wedge b$;
— $a \wedge b$ divise a et b, alors en utilisant l'implication précédente avec $n = a \wedge b$ on trouve que $a \wedge b|d$.

Donc d et $a \wedge b$ sont des entiers naturels associés : ils sont égaux. □

Proposition II.9. *Si $a, b, k \in \mathbb{Z}$, alors :*

$$(ak) \wedge (bk) = |k|(a \wedge b).$$

Démonstration. On utilise la proposition précédente :
- si n divise $|k|(a \wedge b)$, comme $(a \wedge b)$ divise a et b, alors n divise $|k|a$ et $|k|b$ donc ka et kb ;
- si n divise ka et kb : alors n divise $ka - q \times kb = kr_1$; donc en répétant le processus n divise $|k|r_{n-1} = |k|(a \wedge b)$.

D'où l'égalité cherchée. □

Théorème II.10 (Identité de Bézout)**.** *Si $(a, b) \in \mathbb{Z}$, il existe $u, v \in \mathbb{Z}$ tels que : $a \wedge b = au + bv$.*

Démonstration. Montrons par récurrence sur $b \in \mathbb{N}^*$ que :

$$\forall a \in \mathbb{Z},\ \exists u, v \in \mathbb{Z},\ a \wedge b = au + bv.$$

- si $b = 1$: alors $a \wedge b = 1 = a \times 0 + b \times 1$;
- si $b \in \mathbb{N}^*$ tel que la proposition a été vérifiée jusqu'à $b - 1$.
  Soit $a \in \mathbb{Z}$. On écrit $a = bq + r$ avec $0 \leq r \leq b - 1$:
  - si $r = 0$: alors b divise a donc $a \wedge b = b = a \times 0 + b \times 1$;
  - si $r > 0$: alors $a \wedge b = b \wedge r$. Par hypothèse de récurrence, il existe $u, v \in \mathbb{Z}$ tels que $b \wedge r = bu + rv$.
    Et donc : $a \wedge b = b \wedge r = bu + rv = bu + (a - bq)v = av + b(u - qv)$

Ce qui prouve la récurrence.
Le cas où $b = 0$ est immédiat. Et le cas où $b < 0$ se déduit du cas où $b \in \mathbb{N}^*$. □

Remarque II.11. *Suivant la preuve, on peut trouver u et v grâce à l'algorithme d'Euclide à l'envers, en tenant compte des quotients obtenus à chaque étape. Il s'agit de* ***l'algorithme d'Euclide étendu****.*

Exemple II.12. *Reprenons le calcul de* $5742 \wedge 1320 = 66$ *:*

$$\begin{aligned} 66 &= 462 - 396 \\ &= 462 - (1320 - 462 \times 2) = -1320 + 462 \times 3 \\ &= -1320 + (5742 - 1320 \times 4) \times 3 = 5742 \times 3 - 1320 \times 13 \end{aligned}$$

Remarque II.13. *On savait déjà que, pour tous $u, v \in \mathbb{Z}$, $a \wedge b$ divise $au + bv$. Ce résultat dit ainsi que :*

$$a \wedge b = \min\left((a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{N}^*\right).$$

Et on a même l'égalité : $(a \wedge b)\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.

II.2 Entiers premiers entre eux

Définition II.14. *Deux entiers relatifs a et b sont dits* ***premiers entre eux*** *si $a \wedge b = 1$.*

Exemples II.15.

1. *deux nombres premiers sont premiers entre eux si, et seulement si, ils sont distincts ;*
2. 999 *et* 484 *sont premiers entre eux,* 354 *et* 2035 *aussi, et il y en a beaucoup d'autres...*

Théorème II.16 (de Bézout)**.** *Deux entiers a et b sont premiers entre eux si, et seulement si, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.*

Démonstration.
- si $a \wedge b = 1$: on utilise la relation de Bézout ;
- si $au + bv = 1$ pour $u, v \in \mathbb{Z}$: soit d un diviseur de a et b. Alors d divise $au + bv = 1$, donc $d = \pm 1$. Donc $\mathcal{D}(a) \cap \mathcal{D}(b) = \{\pm 1\}$, puis $a \wedge b = 1$.

□

Remarque II.17. *Du fait de la preuve, on peut trouver u, v par l'algorithme d'Euclide étendu.*

Exemple II.18. *On effectue l'algorithme d'Euclide étendu pour* 484 *et* 999*. On a :*

$$\begin{aligned} 999 &= 2\times 484+31\\ 484 &= 15\times 31+19\\ 31 &= 1\times 19+12\\ 19 &= 1\times 12+7\\ 12 &= 1\times 7+5\\ 7 &= 1\times 5+2\\ 5 &= 2\times 2+1 \end{aligned} \quad .$$

puis on remonte pour trouver u *et* v *:*

$$\begin{aligned} 1 &= 5-2\times 2 = 5-2\times(7-1\times 5)\\ &= 3\times 5-2\times 7 = 3\times(12-1\times 7)-2\times 7\\ &= 3\times 12-5\times 7 = 3\times 12-5\times(19-1\times 12)\\ &= 8\times 12-5\times 19 = 8\times(31-1\times 19)-5\times 19\\ &= 8\times 31-13\times 19\\ &= 8\times 31-13\times(484-15\times 31)\\ &= 203\times 31-13\times 484 = 203\times(999-2\times 484)-13\times 484\\ &= 203\times 999-419\times 484 \end{aligned}$$

Pour 354 *et* 2035*, on trouve par l'algorithme d'Euclide étendu :* $1 = 175\times 2035 - 1006\times 354$*.*

Définition II.19 (Inverse modulaire)**.** *Si* $n\in\mathbb{N}^*$ *et* $a\in\mathbb{Z}$*, on dit que* a *est* ***inversible modulo*** n *s'il existe* $b\in\mathbb{Z}$ *tel que* $ab\equiv 1\ [n]$*.*
On dira alors que b *est* ***l'inverse modulaire de*** a *(ou que* $\overline{b}$ *est l'inverse de* $\overline{a}$*).*

Proposition II.20. *Si* $n\in\mathbb{N}^*$*, alors* a *admet un inverse modulaire si, et seulement si,* a *est premier avec* n*.*

Démonstration. L'entier a admet un inverse si, et seulement si, il existe b tel que $ab\equiv 1\ [n]$. C'est-à-dire si, et seulement si, il existe $b,k\in\mathbb{Z}$ tels que $ab-nk=1$, ce qui revient à ce que $a\wedge n=1$ par théorème de Bézout. □

Remarque II.21. *En particulier, l'inverse modulaire est donné par l'identité de Bézout.*

Exemple II.22.

1. 999 *et* 203 *sont inverses l'un de l'autre modulo* 419 *ou* 484 *;*
2. -419 *et* 484 *sont inverses l'un de l'autre modulo* 999 *ou* 203*.*

Proposition II.23. *Soient* a,b,c *trois entiers non nuls.*
Alors a *est premier avec* (bc) *si, et seulement si,* a *est premier à la fois avec* b *et avec* c*.*

Démonstration.

- si $a\wedge bc=1$: on considère $u,v\in\mathbb{Z}$ tels que $au+bcv=1$. Alors :
  - comme $au+b(cv)=1$: $a\wedge b=1$;
  - comme $au+c(bv)=1$: $a\wedge c=1$.
- si $a\wedge b=a\wedge c=1$: alors, par théorème de Bézout, il existe $u_1,v_1,u_2,v_2\in\mathbb{Z}$ tels que : $1=au_1+bv_1=au_2+cv_2$. Donc en les multipliant :

$$1=(au_1+bv_1)(au_2+cv_2)=a\,(au_1u_2+cu_1v_2+bv_1u_2)+bc\,(v_1v_2)$$

  donc $a\wedge(bc)=1$ par théorème de Bézout.

□

Corollaire II.24. *Soient $a, b_1, \dots, b_n \in \mathbb{Z}$.*
Alors a est premier avec le produit $b_1 \dots b_n$ si, et seulement si, il est premier avec chacun des b_i pour $i \in [\![1; n]\!]$.

Proposition II.25 (Lemme de Gauss)**.** *Soient a, b, c trois entiers non nuls.*
Si a divise bc et que a est premier avec b, alors a divise c.

Démonstration. Par théorème de Bézout, on écrit : $au + bv = 1$. Donc $auc + bvc = c$.
Mais a divise auc et bvc, donc leur somme. Donc a divise c. □

Corollaire II.26 (Division modulaire)**.** *Si $n \in \mathbb{N}^*$ et $a, b, c \in \mathbb{Z}$ tels que $c \wedge n = 1$, alors : $ac \equiv bc\ [n] \Leftrightarrow a \equiv b\ [n]$.*

Démonstration. On peut multiplier par l'inverse modulaire de c (qui existe bien comme $c \wedge n = 1$), comme les calculs modulaires se comportent bien avec les produits.
Ou alors on applique le lemme de Gauss : si $ac \equiv bc\ [n]$, alors n divise $(ac - bc) = c(a - b)$, donc n divise $a - b$, donc $a \equiv b\ [n]$ et la réciproque est évidente. □

Corollaire II.27. *Soient a, b, c trois entiers non nuls tels que : a divise c, b divise c et $a \wedge b = 1$.*
Alors ab divise c.

Démonstration. Comme $a|c$, on écrit $ad = c$ pour un $d \in \mathbb{Z}$. Mais b divise $c = ad$ et est premier avec a, donc b divise d.
On écrit donc $d = bd'$ pour $d' \in \mathbb{Z}$. Et finalement : $abd' = c$, donc $ab|c$. □

Proposition II.28. *Si $a, b \in \mathbb{Z}$ sont non nuls, alors $\frac{a}{a \wedge b}$ et $\frac{b}{a \wedge b}$ sont premiers entre eux.*
De plus, si $n \in \mathbb{N}$ et $a', b' \in Z$ vérifient que : $a' \wedge b' = 1$, $a = na'$ et $b = nb'$, alors $n = a \wedge b$.

Démonstration. On note $d = a \wedge b$ pour simplifier.
Par propriété du pgcd, on a déjà :

$$d = a \wedge b = \left(d\frac{a}{d}\right) \wedge \left(d\frac{b}{d}\right) = d \cdot (\frac{a}{d} \wedge \frac{b}{d}).$$

donc $\frac{a}{d} \wedge \frac{b}{d} = 1$.
Pour n, a', b' comme dans l'énoncé, on a :

$$d = a \wedge b = (na') \wedge (nb') = n(a' \wedge b') = n$$

□

Proposition-Définition II.29. *Si $r \in \mathbb{Q}$, alors il existe une unique écriture de la forme $r = \frac{a}{b}$ avec $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$, et a et b premiers entre eux.*
*Cette écriture est appelée **forme irréductible** de r.*
Si $r = \frac{a'}{b'}$ est une autre écriture avec $(a', b') \in \mathbb{Z} \times \mathbb{N}^*$, alors il existe $k \in \mathbb{N}^*$ tel que $a' = ak$ et $b' = bk$.

Démonstration. Soit $r = \frac{A}{B} \in \mathbb{Q}$ avec $A, B \in \mathbb{Z}$ et $B \neq 0$. Quitte à changer (A, B) en $(-A, -B)$, on peut supposer que $B \in \mathbb{N}^*$.
Le cas où $r = 0$ est immédiat (car alors $a = 0$ et $b = 1$ conviennent). Supposons donc $r \neq 0$, c'est-à-dire $A \neq 0$.
Alors $a = \frac{A}{A \wedge B}$ et $b = \frac{B}{A \wedge B}$ conviennent, ce qui assure l'existence.
Donnons-nous $\frac{a'}{b'}$ une autre écriture. Alors $\frac{a'}{b'} = \frac{a}{b}$, donc $a'b = ab'$. Ainsi, b divise ab' et est premier avec a, donc b' divise b. Et de même a' divise a. Ce qui assure que $\frac{a'}{a} = \frac{b'}{b}$ est un entier (par divisibilité) positif (comme $b, b' \in \mathbb{N}^*$). En le notant k, on a donc : $a' = ka$ et $b' = kb$.
Si l'écriture $\frac{a'}{b'}$ est irréductible, alors on trouve de même que b' divise b, et a' divise a. Donc b et b' sont associés et de même signe : ils sont égaux. Donc $k = 1$, et $a = a'$. Ce qui assure l'unicité. □

Corollaire II.30. *Si $a, b \in \mathbb{Z}$ avec $b \neq 0$ et $u_0, v_0 \in \mathbb{Z}$ tels que $au_0 + bv_0 = a \wedge b$, alors :*

$$\{(u, v) \in \mathbb{Z}^2 \,|\, au + bv = a \wedge b\} = \{(u_0 + k\beta, v_0 - k\alpha) \,|\, k \in \mathbb{Z}\}$$

où $\frac{\alpha}{\beta}$ est la fonction irréductible de $\frac{a}{b}$.

Démonstration. En exercice. □

II.3 PPCM

Définition II.31. *Si $a, b \in \mathbb{Z}$, avec a et b non nul, le **plus petit commun multiple** (abrégé en ppcm ou PPCM) de a et b est le plus petit multiple strictement positif commun à a et b :*

$$a \vee b = \text{ppcm}(a, b) = \min\left(a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*\right).$$

Par convention, on pose $a \vee 0 = 0$ pour tout entier a.

Proposition II.32. *Si $a, b \in \mathbb{Z}$, le ppcm de a et b est le plus petit élément de $a\mathbb{Z} \cap b\mathbb{Z}$ **au sens de la divisibilité**, c'est-à-dire que le ppcm de a et b est l'unique entier naturel m tel que :*

$$\forall n \in \mathbb{Z},\ (a|n \text{ et } b|n) \Leftrightarrow m|n.$$

Démonstration. Posons $m = a \vee b$, qui est un multiple de a et b. Considérons n un multiple de a et b, et écrivons $n = mq + r$ la division euclidienne de n par m, avec donc $0 \leq r < m$. Alors $r = n - mq$ est aussi un multiple de a et de b, et par minimalité de m on a donc $r = 0$, donc on a bien que m divise n.
Réciproquement, si $m \in \mathbb{N}$ vérifie ces hypothèse, alors :
- avec $n = a \vee b$: comme $a|a \vee b$ et $b|a \vee b$, alors $m|a \vee b$;
- avec $n = m$: comme $m|m$, alors $a|m$ et $b|m$, donc $a \vee b|m$ (comme $a \vee b$ vérifie aussi l'équivalence précédente).

Donc m et $a \vee b$ sont associés, donc égaux (comme ils appartiennent à $\mathbb{N}$). □

Proposition II.33. *Si $a, b, k \in \mathbb{Z}$, alors :*

$$(ak) \vee (bk) = |k|(a \vee b).$$

Démonstration. On utilise la proposition précédente :
- si n est un multiple de $|k|(a \vee b)$, comme $(a \vee b)$ est un multiple de a et b, alors n est un multiple de $|k|a$ et $|k|b$;
- si n est un multiple de (ka) et de (kb), alors c'est un multiple de k ; si on pose $n = kn'$, alors n' est un multiple de a et de b, donc un multiple de $(a \vee b)$. Donc $n = kn'$ et un multiple de $|k|(a \vee b)$.

D'où l'égalité cherchée. □

Proposition II.34. *Si $a, b \in \mathbb{Z}$, alors : $(a \wedge b) \times (a \vee b) = |a \times b|$.*

Démonstration. Supposons déjà que a et b sont premiers entre eux. On chercher alors à montrer que $a \vee b = |ab|$, et donc :

$$\forall n \in \mathbb{Z},\ (a|n \text{ et } b|n) \Leftrightarrow ab|n.$$

Considérons donc $n \in \mathbb{Z}$:
- si $ab|n$: comme ab est un multiple de a et b, alors n est un multiple de a et de b (par transitivité) ;
- si n est un multiple de a et b : on écrit $m = au = bv$ pour $u, v \in \mathbb{Z}$. Et ainsi : a divise bv et est premier avec b, donc a divise v. On peut donc écrire $v = ak$, pour $k \in \mathbb{Z}$, et donc $m = bv = abk$ est un multiple de ab.

Donc $a \vee b = |ab|$ et l'égalité est vérifiée.
Si a et b ne sont pas premiers entre eux : le résultat est clair si a ou b est nul, car alors :

$$(a \vee b) = 0 = ab$$

Sinon, on applique le résultat précédent à $\frac{a}{a\wedge b}$ et $\frac{b}{a\wedge b}$, qui sont premiers entre eux. On a par la proposition précédente :

$$a \vee b = (a \wedge b)\left(\frac{a}{a \wedge b} \vee \frac{b}{a \wedge b}\right) = (a \wedge b) \times \frac{ab}{(a \wedge b)^2} = \frac{ab}{a \wedge b}$$

donc, en multipliant par $(a \wedge b)$ on trouve bien l'égalité voulue. □

II.4 PGCD d'un nombre fini d'entiers

Définition II.35. *Si $a_1, \ldots, a_n \in \mathbb{Z}$ non tous nuls, on définit le pgcd de $a_1, \ldots, a_n$ comme le plus grand diviseur commun de tous les a_i :*

$$a_1 \wedge \cdots \wedge a_n = \bigwedge_{i=1}^{n} a_i = \operatorname{pgcd}(a_1, \ldots, a_n) = \max\left(\bigcap_{i=1}^{n} \mathcal{D}(a_i)\right)$$

et on pose $0 \wedge \cdots \wedge 0 = 0$.

Proposition II.36. *Si $a_1 \ldots, a_n$ sont des entiers, alors :*

$$\mathcal{D}(\operatorname{pgcd}(a_1, \ldots, a_n)) = \bigcap_{i=1}^{n} \mathcal{D}(a_i).$$

Démonstration. On procède par récurrence sur $n \in \mathbb{N}$ avec $n \geq 2$. Le cas $n = 2$ ayant été montré avant. Pour l'hérédité, on pose $d = \operatorname{pgcd}(a_1, \ldots, a_n)$. On a :

$$\bigcap_{i=1}^{n+1} \mathcal{D}(a_i) = \left(\bigcap_{i=1}^{n} \mathcal{D}(a_i)\right) \cap \mathcal{D}(a_{n+1}) = \mathcal{D}(d) \cap \mathcal{D}(a_{n+1}) = \mathcal{D}(d \wedge a_{n+1})$$

et en prenant le maximum des ensembles précédents, il vient que $d \wedge a_{n+1}$ est le pgcd de $a_1, \ldots, a_{n+1}$, ce qui donne le résultat voulu. □

Remarque II.37. *On peut ainsi calculer récursivement le pgcd d'une famille d'entier.*

Corollaire II.38. *Le pgcd de $a_1, \ldots, a_n$ est le plus grand diviseur commun des a_i* ***pour la divisibilité****.*

Proposition II.39. *Si $a_1, \ldots, a_n$ sont des entiers non nuls, alors il existe $u_1, \ldots, u_n \in \mathbb{Z}$ tels que : $\sum_{i=1}^{n} a_i u_i = \bigwedge_{i=1}^{n} a_i$.*

Démonstration. On procède par récurrence sur $n \in \mathbb{N}$ avec $n \geq 2$. Le cas $n = 2$ ayant été montré avant. Pour l'hérédité, on pose $d = \operatorname{pgcd}(a_1, \ldots, a_n)$:

- par hypothèse de récurrence (pour n) : $d = \sum_{i=1}^{n} a_i u_i$;
- par le point précédent : $\bigwedge_{i=1}^{n+1} a_i = d \wedge a_{n+1}$.

Et ainsi par théorème de Bézout :

$$\bigwedge_{i=1}^{n+1} a_i = du + a_{n+1}v = \sum_{i=1}^{n} a_i(du_i) + a_{n+1}v.$$

□

Corollaire II.40. *Si $a_1, \dots, a_n \in \mathbb{Z}$, alors :*

$$\bigwedge_{i=1}^{n} a_i = \min\left((a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}) \cap \mathbb{N}^*\right).$$

Définition II.41. *On dit que des entiers $a_1, \dots, a_n$ sont* ***premiers entre eux dans leur ensemble*** *si leur pgcd vaut 1.*
On dit qu'ils sont ***premiers entre eux deux-à-deux*** *si a_i et a_j sont premiers entre eux pour tous $i \neq j$*

Proposition II.42. *Si les a_i sont deux-à-deux premiers entre eux, ils le sont dans leur ensemble.*

Démonstration. On a : $\underbrace{a_1 \wedge a_2}_{=1} \wedge \cdots \wedge a_n == 1$. □

Remarque II.43. *La réciproque est fausse : $(a_1, a_2, a_3) = (2, 3, 6)$ donne un contre-exemple.*

Proposition II.44. *Des entiers $a_1, \dots, a_n$ sont premiers entre eux si, et seulement si, il existe des entiers $u_1, \dots, u_n$ tels que $\sum_{i=1}^{n} a_i u_i = 1$.*

Démonstration. Comme pour deux entiers : une implication par théorème de Bézout ; l'autre car un diviseur commun aux a_i divise $\sum_{i=1}^{n} a_i u_i$. □

III Décomposition en produit de nombres premiers

III.1 La décomposition en facteurs premiers

Proposition III.1. *Soient p un nombre premier et $n \in \mathbb{Z}$.*
Alors n est divisible par p si, et seulement si, p et n ne sont pas premiers entre eux.

Démonstration. Les diviseurs positifs de p sont 1 et p, donc :

$$p \wedge n \neq 1 \Leftrightarrow p \wedge n = p \Leftrightarrow p | n.$$

□

Corollaire III.2 (Lemme d'Euclide)**.** *Un nombre premier divise un produit si, et seulement si, il divise l'un des facteurs.*

Démonstration. Soit p un nombre premier :

$$\begin{array}{rcl} p \text{ ne divise pas } a_1 \dots a_n & \Leftrightarrow & p \text{ est premier avec } a_1 \dots a_n \\ & \Leftrightarrow & p \text{ est premier avec chaque } a_i \ . \\ & \Leftrightarrow & p \text{ ne divise aucun } a_i \end{array}$$

□

Théorème III.3 (Théorème fondamental de l'arithmétique)**.** *Tout entier strictement positif s'écrit comme produit (éventuellement vide) de nombres premiers, de manière unique à l'ordre près des facteurs.*

Démonstration. Montrons l'existence par récurrence forte sur $n \in \mathbb{N}^*$:
- si $n = 1$: alors n est le produit de 0 nombres premiers (un produit vide) ;
- supposons le résultat vrai jusqu'à $n \in \mathbb{N}^*$. Alors :
  - si $n+1$ est premier : $n + 1 = n + 1$ (produit à un élément) ;
  - si $n+1$ est composé : alors $n+1$ a un diviseur premier $p \geq 2$ et on peut écrire $n + 1 = pm$ avec $m \in \mathbb{N}^*$ et $m \leq \frac{n+1}{2} \leq n$; et on applique l'hypothèse de récurrence à m.

Ce qui assure l'existence d'une telle décomposition.
Pour l'unicité, supposons par l'absurde $p_1, \dots, p_n$ et $q_1, \dots, q_m$ des nombres premiers tels que $p_1 \dots p_n = q_1 \dots q_m$ soient deux écritures différentes.
Quitte à diviser les deux égalités ou à échanger les rôles des p_i et des q_j, on peut supposer qu'aucun des p_i n'apparaît parmi les q_j. Mais alors p_1 divise le produit des q_j, donc l'un des q_j. Mais comme p_1 et les q_j sont premiers, alors p_1 est égal à l'un des q_j, d'où la contradiction.
D'où l'unicité. □

III.2 La valuation p-adique

Définition III.4. *Soient $n \in \mathbb{N}^*$ et p un nombre premier. La **valuation p-adique** de n est le nombre (éventuellement nul) de fois qu'apparait p dans la décomposition de p comme produit de nombres premiers. On la note $v_p(n)$.*

Remarque III.5. *On a en particulier que p divise n si, et seulement si, $v_p(n) > 0$ (ou $v_p(n) \neq 0$).*

Proposition III.6. *Si n est un entier et p un nombre premier, alors $p^{v_p(n)}$ est la plus grande puissance de p qui divise n.*
En particulier, on a :

$$n = \prod_{p \text{ premier}} p^{v_p(n)}.$$

Démonstration. On regroupe les "p" ensemble dans l'écriture de n en produit de nombres premiers, ce qui donne l'écriture voulue et le fait que $p^{v_p(n)}$ divise n. L'unicité assure que c'est bien la plus grande puissance de p qui divise n. □

Remarque III.7. *Le produit ci-dessus est en fait fini (dans le sens où seulement un nombre fini de facteurs sont différents de 1). Les diviseurs premiers de n sont en nombre fini, donc les nombres premiers p tels que $v_p(n) > 0$ sont en nombre fini. Pour les autres : $v_p(n) = 0$ donc $p^{v_p(n)} = 1$.*

Proposition III.8. *Soient $a, b \in \mathbb{N}^*$ et p un nombre premier :*

1. *$v_p(ab) = v_p(a) + v_p(b)$;*
2. *si a divise b : $v_p\left(\frac{b}{a}\right) = v_p(b) - v_p(a)$.*

Démonstration. On exprime ab comme produit de puissances de nombres premiers distincts :

$$\begin{aligned} ab &= \left(\prod_{p \text{ premier}} p^{v_p(a)}\right) \cdot \left(\prod_{p \text{ premier}} p^{v_p(b)}\right) \\ &= \left(\prod_{p \text{ premier}} p^{v_p(a)+v_p(b)}\right) \end{aligned}$$

ce qui donne bien que pour tout p premier : $v_p(ab) = v_p(a) + v_p(b)$ par unicité de l'écriture précédente.
Le deuxième point s'en déduit en utilisant que $a \times \frac{b}{a} = b$. □

III.3 Application aux diviseurs

Proposition III.9. *Soient $a, b \in \mathbb{N}^*$. Alors a divise b si, et seulement si, pour tout nombre premier p : $v_p(a) \leq v_p(b)$.*

Démonstration.
— si a divise b : soit p un nombre premier. On a alors $v_p(a) = v_p(b) - v_p\left(\frac{b}{a}\right) \leq v_p(b)$.

— réciproquement : on pose $c = \prod_{p \text{ premier}} p^{v_p(b)-v_p(a)}$ qui est un entier naturel (comme tous les $v_p(b) - v_p(a)$ sont des entiers naturels) et qui vérifie :

$$a \times c = \prod_{p \text{ premier}} p^{v_p(a)} \times \prod_{p \text{ premier}} p^{v_p(b)-v_p(a)} = \prod_{p \text{ premier}} p^{v_p(b)} = b$$

donc a divise b.

□

Théorème III.10. *Soient $a, b \in \mathbb{N}^*$. Alors :*

1. $a \wedge b = \prod_{p \text{ premier}} p^{\min(v_p(a),v_p(b))}$;
2. $a \vee b = \prod_{p \text{ premier}} p^{\max(v_p(a),v_p(b))}$.

Autrement dit : pour tout p premier, on a :

$$v_p(a \wedge b) = \min(v_p(a), v_p(b)) \text{ et } v_p(a \vee b) = \max(v_p(a), v_p(b)).$$

Démonstration.

1. le lien entre valuation et diviseurs donne que, pour tout entier d :

$$\begin{array}{rcl} \left\{ \begin{array}{c} c \text{ divise } a \\ \text{et } c \text{ divise } b \end{array} \right. & \Leftrightarrow & \forall p \text{ premier}, \left\{ \begin{array}{c} v_p(c) \leq v_p(a) \\ v_p(c) \leq v_p(b) \end{array} \right. \\ & \Leftrightarrow & \forall p \text{ premier}, \ v_p(c) \leq \min(v_p(a), v_p(b)) \\ & \Leftrightarrow & c \text{ divise } \prod_{p \text{ premier}} p^{\min(v_p(a),v_p(b))} \end{array}$$

   et comme le pgcd de a et b est le plus grand diviseur commun **pour la divisibilité**, on trouve le résultat voulu.

2. On utilise que $a \vee b = \dfrac{ab}{a \wedge b}$ et que pour tous $m, n \in \mathbb{N}$: $m + n = \max(m, n) + \min(m, n)$.

□

Corollaire III.11. *Soient $a, b \in \mathbb{N}^*$. Alors a et b sont premiers entre eux si, et seulement si : pour tout p premier, $v_p(a) \cdot v_p(b) = 0$.*

Démonstration. On a les équivalences suivantes :

$$\begin{array}{rcl} a \wedge b = 1 & \Leftrightarrow & \forall p \text{ premier}, \ v_p(a \wedge b) = 0 \\ & \Leftrightarrow & \forall p \text{ premier}, \ \min(v_p(a), v_p(b)) = 0 \\ & \Leftrightarrow & \forall p \text{ premier}, \ v_p(a) = 0 \text{ ou } v_p(b) = 0 \\ & \Leftrightarrow & \forall p \text{ premier}, \ v_p(a) \cdot v_p(b) = 0 \end{array}$$

ce qui est bien le résultat voulu. □

III.4 Le (petit) théorème de Fermat

Théorème III.12. *Soit p un nombre premier et a un entier. Alors : $a^p \equiv a \ [p]$.*
Si de plus a n'est pas divisible par p, alors : $a^{p-1} \equiv 1 \ [p]$.

Démonstration. La démonstration s'appuie sur le lemme suivant :

Lemme III.13. *Si p est un nombre premier, alors pour tout $k \in [\![1; p-1]\!]$ on a : $\binom{p}{k} \equiv 0 \ [p]$.*

Preuve du lemme : Par définition, on a : $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ et donc : $p! = \binom{p}{k} \cdot k! \cdot (p-k)!$.
Donc p divise le membre de droite, donc un de ses facteurs. Mais il ne divise pas $k! = 1 \cdot \cdots \cdot k$ comme $k < p$, et pas non plus $(p-k)! = 1 \cdot \cdots \cdot (p-k)$ comme $k > 1$. Donc p divise $\binom{p}{k}$. □

Montrons alors par récurrence que le résultat est vrai si $a \in \mathbb{N}$:
— si $a = 0$: $a^p = 0^p \equiv 0 = a\ [p]$;
— si $a^p \equiv a\ [p]$: alors par formule du binôme :

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k \equiv a^p + 1 \equiv a + 1\ [p]$$

ce qui prouve la récurrence.
Le cas général se déduit car, si $a \in \mathbb{Z}$, il est congru modulo p à un entier naturel (par exemple le reste de sa division euclidienne par p). Et alors on a :

$$a^p \equiv r^p \equiv r \equiv a\ [p]$$

ce qui conclut la preuve du cas général.
Si a n'est pas divisible par p, alors il est premier avec p et on peut donc diviser par a dans les congruences modulo p. □

Remarque III.14. *La réciproque du théorème de Fermat est fausse : les nombres non premiers qui la vérifient sont les* ***nombres de Carmichael*** *(par exemple* 561*).*
En revanche la réciproque du lemme est vraie.

Exemple III.15. *Donnons la liste des congruences de puissances modulo* 7*. On donne ci-dessous, pour* $a, n \in \{0, \dots 6\}$*, la quantité* a^n *modulo* 7 *:*

a \ n	0	1	2	3	4	5	6
0	1	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	1	2	4	1	2	4	1
3	1	3	2	6	4	5	1
4	1	4	2	1	4	2	1
5	1	5	4	6	2	3	1
6	1	6	1	6	1	6	1

Remarque III.16. *On déduit ainsi que les puissances positives de* a *modulo* p *sont* $(p-1)$ *périodiques ce qui permet facilement de calculer des puissances modulaires.*

Exemple III.17. *Calculons :* $48^{2021}\ [37]$ *:*
— 37 *est premier et* 48 *n'est pas divisible par* 37*, donc* 48 *et* 37 *sont premiers entre eux ;*
— *la division euclidienne de* 2021 *par* 36 *est :* $2021 = 56 \times 36 + 5$ *;*
— *le reste de la division euclidienne de* 48 *par* 37 *est* 11*.*
Et ainsi :

$$\begin{aligned} 48^{2021} &\equiv 48^5\ [37] \\ &\equiv 11^5\ [37] \\ &\equiv 121 \times 121 \times 11\ [37] \\ &\equiv 10 \times 10 \times 11\ [37] \\ &\equiv 10 \times 110\ [37] \\ &\equiv -10\ [37] \end{aligned}$$

où on a utilise que $111 = 37 \times 3$ *est un multiple de* 37 *pour en déduire que* $121 = 111 + 10 \equiv 10\ [37]$ *et que* $110 \equiv -1\ [37]$*.*

Exemple III.18. *Montrons que, si $n \in \mathbb{Z}$, tous les diviseurs premiers impairs de n^2+1 sont congrus à 1 modulo 4.*
Soit p un nombre premier impair divisant n^2+1. Alors p ne divise pas n^2 (sinon il diviserait 1), donc il ne divise pas non plus n.
Donc par le petit théorème de Fermat : $n^{p-1} \equiv 1\ [p]$.
Mais $n^2 \equiv -1\ [p]$. Et comme p est impair, $\frac{p-1}{2} \in \mathbb{N}$. Et on a :

$$1 \equiv n^{p-1} \equiv (n^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}\ [p]$$

Mais $(-1)^k = \pm 1$, pour $k \in \mathbb{Z}$. Et -1 n'est pas congru à 1 modulo p (comme p est premier impair, donc $p > 2$). Donc finalement : $(-1)^{\frac{p-1}{2}} = 1$, donc $\frac{p-1}{2}$ est pair, c'est-à-dire que p est bien congru à 1 modulo 4.

Chapitre 12

Calculs matriciels

On note $\mathbb{K}$ l'ensemble $\mathbb{R}$ ou $\mathbb{C}$. Les éléments de $\mathbb{K}$ sont appelés scalaires.

I Les ensembles de matrices

I.1 Définitions et notations

Définition I.1. *Si $n, p \in \mathbb{N}^*$, on appelle* ***matrice à n lignes et p colonnes et à coefficients dans $\mathbb{K}$*** *est une application $A : \left\{ \begin{array}{ccc} [\![1;n]\!] \times [\![1;p]\!] & \to & \mathbb{K} \\ (i,j) & \mapsto & a_{i,j} \end{array} \right.$.*
On la représente plutôt sous forme d'un tableau à n lignes et p colonnes :

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,p} \\ a_{2,1} & a_{2,2} & \dots & a_{2,p} \\ \vdots & \vdots & & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,p} \end{pmatrix}.$$

Si $(i,j) \in [\![1;n]\!] \times [\![1;p]\!]$, le scalaire $a_{i,j}$ est appelé le ***coefficient d'indice*** *(i,j) de A.*
On note $\mathcal{M}_{n,p}(\mathbb{K})$ l'ensemble des matrices à n lignes et p colonnes à coefficients dans $\mathbb{K}$.
Si $n = p$, on notera plus simplement $\mathcal{M}_n(\mathbb{K})$ au lieu de $\mathcal{M}_{n,n}(\mathbb{K})$, et on parlera de matrices carrées de taille n.

Remarques I.2.

1. *Pour spécifier une matrice par ses coefficients, en précisant son nombre de lignes et de colonne, on pourra noter $A = (a_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}}$, ou plus simplement $A = (a_{i,j})$ s'il n'y a pas d'ambiguïté.*
2. *Inversement, on notera $[A]_{i,j}$ le coefficient d'indice (i,j) de A, pour éviter d'introduire trop de notations.*
3. *Deux matrices sont égales si elles définissent la même application, c'est-à-dire si elles ont* ***même taille*** *et* ***mêmes coefficients****.*

Exemples I.3. *On a :*

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 4 \end{pmatrix} \in \mathcal{M}_{2,3}(\mathbb{R}) \text{ et } \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \in \mathcal{M}_2(\mathbb{C})$$

.
On a de même :

$$\left(i^j\right)_{\substack{1 \leq i \leq 3 \\ 1 \leq j \leq 2}} = \begin{pmatrix} 1 & 1 \\ 2 & 4 \\ 3 & 9 \end{pmatrix} \in \mathcal{M}_{3,2}(\mathbb{C}).$$

I.2 Matrices remarquables

Définition I.4. *Si $n \in \mathbb{N}^*$, les éléments de $\mathcal{M}_{1,n}(\mathbb{K})$ sont appelés **matrices lignes** (de taille n), tandis que ceux de $\mathcal{M}_{n,1}(\mathbb{K})$ sont appelés **matrices colonnes** (de taille n).*
*Plus généralement, si $A = (a_{i,j}) \in \mathcal{M}_{n,p}$, on dira que les matrices $\begin{pmatrix} a_{i,1} & \dots & a_{i,p} \end{pmatrix}$ sont les **lignes** de A, tandis que les matrices $\begin{pmatrix} a_{1,j} \\ \vdots \\ a_{n,j} \end{pmatrix}$ pour $j \in [\![1;p]\!]$ sont les **colonnes** de A.*

Remarque I.5. *Un élément de $\mathbb{K}^n$ pourra être vu comme une matrice ligne ou colonne, par les bijections suivantes :*

$$\begin{cases} \mathbb{K}^n & \to & \mathcal{M}_{1,n}(\mathbb{K}) \\ (x_1, \dots, x_n) & \mapsto & \begin{pmatrix} x_1 & \dots & x_n \end{pmatrix} \end{cases} \quad \text{et} \quad \begin{cases} \mathbb{K}^n & \to & \mathcal{M}_{n,1}(\mathbb{K}) \\ (x_1, \dots, x_n) & \mapsto & \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \end{cases}.$$

Définition I.6. *On appelle **matrice nulle** l'unique matrice de $\mathcal{M}_{n,p}(\mathbb{K})$ dont tous les coefficients sont nuls. On la note parfois $0_{n,p}$.*
Quand $n = p$, on la note plus simplement 0_n.
Quand il n'y aura pas d'ambiguïté, on la notera plus simplement 0.

Définition I.7. *Soient $n \in \mathbb{N}^*$ et $A = (a_{i,j}) \in \mathcal{M}_n(\mathbb{K})$. On dira que la matrice A est :*

1. ***triangulaire supérieure** si : $\forall i, j \in [\![1;n]\!],\ i > j \Rightarrow a_{i,j} = 0$, c'est-à-dire que A est de la forme :*

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \dots & \dots & a_{1,n} \\ 0 & a_{2,2} & \dots & \dots & a_{2,n} \\ 0 & 0 & a_{3,3} & \dots & a_{3,n} \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & \dots & a_{n,n} \end{pmatrix}$$

2. ***triangulaire inférieure** si : $\forall i, j \in [\![1;n]\!],\ i < j \Rightarrow a_{i,j} = 0$, c'est-à-dire que A est de la forme :*

$$\begin{pmatrix} a_{1,1} & 0 & 0 & \dots & 0 \\ a_{2,1} & a_{2,2} & 0 & \dots & 0 \\ a_{3,1} & a_{3,2} & a_{3,3} & \dots & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \dots & \dots & a_{n,n} \end{pmatrix}$$

3. ***diagonale** si $\forall i, j \in [\![1;n]\!],\ i \neq j \Rightarrow a_{i,j} = 0$, c'est-à-dire que A est de la forme :*

$$\begin{pmatrix} a_{1,1} & 0 & \dots & 0 \\ 0 & a_{2,2} & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & a_{n,n} \end{pmatrix}$$

4. ***scalaire** si elle est diagonale et que tous ses coefficients diagonaux sont égaux, c'est-à-dire qu'il existe $\lambda \in \mathbb{K}$ tel que A est de la forme :*

$$\begin{pmatrix} \lambda & 0 & \dots & 0 \\ 0 & \lambda & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & \lambda \end{pmatrix}$$

*Dans le cas particulier où $\lambda = 1$, on parlera de la **matrice identité (d'ordre n)**, notée aussi I_n.*

Remarques I.8.

1. *Les matrices diagonales correspondent aux matrices à la fois triangulaire supérieure et triangulaire supérieure.*
2. *Si* $\lambda_1, \dots, \lambda_n \in \mathbb{K}$, *on note* $\mathrm{Diag}(\lambda_1, \dots, \lambda_n)$ *la matrice diagonale dont les coefficients sont les* $\lambda_1, \dots, \lambda_n$ *dans cet ordre, c'est-à-dire que :*

$$\mathrm{Diag}(\lambda_1, \dots, \lambda_n) = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & \lambda_n \end{pmatrix}$$

II Combinaisons linéaires de matrices

II.1 Addition et multiplication par un scalaire

Définition II.1 (Multiplication d'une matrice par un scalaire)**.** *Soit* $A = (a_{i,j}) \in \mathcal{M}_{n,p}(\mathbb{K})$ *et* $\lambda \in \mathbb{K}$. *On note alors* $\lambda \cdot A$, *ou plus simplement* λA, *la matrice :* $(\lambda a_{i,j}) \in \mathcal{M}_{n,p}(\mathbb{K})$

Remarque II.2. *Pour tout* $A \in \mathcal{M}_{n,p}(\mathbb{K})$ *:* $1 \cdot A = A$ *et* $0 \cdot A = 0_{n,p}$ *;*

Proposition II.3. *Si* $A \in \mathcal{M}_{n,p}(\mathbb{K})$ *et* $\lambda, \mu \in \mathbb{K}$, *alors :*

$$(\lambda\mu) \cdot A = \lambda \cdot (\mu \cdot A).$$

Démonstration. Si $(i,j) \in [\![1;n]\!] \times [\![1;p]\!]$, alors par associativité du produit sur $\mathbb{K}$:

$$[(\lambda\mu) \cdot A]_{i,j} = (\lambda \cdot \mu) \cdot a_{i,j} = \lambda \cdot \mu \cdot a_{i,j} = \lambda \cdot (\mu \cdot a_{i,j}) = [\lambda \cdot (\mu \cdot A)]_{i,j}$$

donc les matrices considérées ont même taille et mêmes coefficients : elles sont égales. □

Définition II.4 (Somme de matrices)**.** *Si* $A = (a_{i,j})$ *et* $B = (b_{i,j})$ *sont deux matrices de* $\mathcal{M}_{n,p}(\mathbb{K})$, *on définit la* ***somme*** *de* A *et* B, *notée* $A + B$, *comme la matrice :* $A + B = (a_{i,j} + b_{i,j}) \in \mathcal{M}_{n,p}(\mathbb{K})$.

Proposition II.5. *Si* $A, B, C \in \mathcal{M}_{n,p}(\mathbb{K})$ *et* $\lambda, \mu \in \mathbb{K}$, *alors :*

1. $A + B = B + A$ *(commutativité de la somme) ;*
2. $A + (B + C) = (A + B) + C$ *(associativité de la somme) ;*
3. $0_{n,p} + A = A = A + 0_{n,p}$ *(*$0_{n,p}$ *est un élément neutre pour la somme) ;*
4. *la matrice* $(-1) \cdot A$, *qu'on notera plus simplement* $-A$, *est l'unique matrice* $D \in \mathcal{M}_{n,p}(\mathbb{K})$ *telle que :* $A + D = 0_{n,p} = D + A$ *;*
5. $(\lambda + \mu)A = \lambda A + \mu A$ *;*
6. $\lambda \cdot (A + B) = \lambda \cdot A + \lambda \cdot B$.

Démonstration. Dans toutes les égalités à montrer, les matrices ont même taille (à savoir (n,p)). Donc pour vérifier les égalités, il suffit de vérifier les égalités des coefficients. Soit $(i,j) \in [\![1;n]\!] \times [\![1;p]\!]$:

1. Par commutativité de l'addition sur $\mathbb{K}$, on a :

$$[A + B]_{i,j} = [A]_{i,j} + [B]_{i,j} = [B]_{i,j} + [A]_{i,j} = [B + A]_{i,j} \ ;$$

2. Par associativité de l'addition sur $\mathbb{K}$, on a :

$$\begin{aligned} [A + (B + C)]_{i,j} &= [A]_{i,j} + [B + C]_{i,j} = [A]_{i,j} + \Big([B]_{i,j} + [C]_{i,j}\Big) \\ = \ \Big([A]_{i,j} + [B]_{i,j}\Big) + [C]_{i,j} &= [A + B]_{i,j} + [C]_{i,j} = [(A + B) + C]_{i,j} \end{aligned}$$

3. Comme additionner 0 ne changer rien sur $\mathbb{K}$:

$$[0_{n,p} + A]_{i,j} = [0_{n,p}]_{i,j} + [A]_{i,j} = 0 + [A]_{i,j} = [A]_{i,j}$$

et la seconde égalité se déduit par commutativité de la somme matricielle ;

4. on procède directement par équivalences. Si $D \in \mathcal{M}_{n,p}(\mathbb{K})$, alors :

$$\begin{array}{rcl} A + D = 0_{n,p} & \Leftrightarrow & \forall (i,j) \in [\![1;n]\!] \times [\![1;p]\!],\ [A+D]_{i,j} = 0 \\ & \Leftrightarrow & \forall (i,j) \in [\![1;n]\!] \times [\![1;p]\!],\ [A]_{i,j} + [D]_{i,j} = 0 \\ & \Leftrightarrow & \forall (i,j) \in [\![1;n]\!] \times [\![1;p]\!],\ [D]_{i,j} = -[A]_{i,j} = [-A]_{i,j} \\ & \Leftrightarrow & D = -A \end{array}$$

5. même méthode que pour *1,2,3*
6. idem

□

Remarque II.6. *L'idée est que l'on peut manipuler les additions de matrices et les multiplications par des scalaires exactement comme les opérations usuelles $+$ et $\times$ sur $\mathbb{K}$.*

II.2 Matrices élémentaires

Définition II.7 (Matrices élémentaires)**.** *Soient $n, p \in \mathbb{N}^*$ et $(i,j) \in [\![1;n]\!] \times [\![1;p]\!]$. On note $E_{i,j}$ la matrice de $\mathcal{M}_{n,p}(\mathbb{K})$ dont le coefficient d'indice (i,j) vaut 1 et tous les autres valent 0, c'est-à-dire que $E_{i,j}$ s'écrit :*

$$\begin{array}{c} \\ i^{\text{-ème}}\ \textit{ligne} \rightarrow \end{array} \begin{array}{c} \begin{array}{ccccc} & & j^{ème}\ \textit{colonne} & & \\ & & \downarrow & & \end{array} \\ \begin{pmatrix} 0 & \dots & 0 & \dots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \dots & 1 & \dots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & \dots & 0 \end{pmatrix} \end{array}$$

*Les matrices $E_{i,j}$ ainsi définies sont appelées **matrices élémentaires** (de taille (n,p)).*

Remarque II.8. *On prendra garde au fait que la taille d'une matrice élémentaire n'apparaît pas dans sa notation.*

Exemples II.9. *L'ensemble $\mathcal{M}_{n,p}(\mathbb{K})$ contient $n \times p$ matrices élémentaires.*
Par exemple pour $\mathcal{M}_{2,3}$, on trouve les 6 matrices suivantes :

$$E_{1,1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, E_{1,2} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, E_{1,3} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

$$E_{2,1} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, E_{2,2} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, E_{2,3} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Définition II.10 (Symbole de Kronecker)**.** *Si $i, j \in \mathbb{Z}$ (et plus souvent $i, j \in \mathbb{N}$), on appelle **symbole de Kronecker** la quantité notée $\delta_{i,j}$ et définie par : $\delta_{i,j} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$.*

Proposition II.11. *Si $n, p \in \mathbb{N}^*$, les matrices élémentaires de $\mathcal{M}_{n,p}$ sont données par :*

$$\forall (k,l) \in [\![1;n]\!] \times [\![1;p]\!],\ E_{k,l} = (\delta_{i,k} \cdot \delta_{j,l})\,.$$

Démonstration. Il suffit de regarder les coefficients. On a :

$$\delta_{i,k} \cdot \delta_{j,l} \neq 0 \Leftrightarrow \delta_{i,k} \neq 0 \text{ et } \delta_{j,l} \neq 0 \Leftrightarrow i = k \text{ et } j = l$$

donc seuls le coefficient d'indice (k, l) est non nul, et vaut alors 1. Il s'agit donc bien de $E_{k,l}$. □

Proposition II.12. *Si $A \in \mathcal{M}_{n,p}(\mathbb{K})$, alors A est une **combinaison linéaire** de matrices élémentaires : il existe des scalaires $\lambda_{i,j}$ tels que :*

$$A = \sum_{i=1}^{n} \sum_{j=1}^{p} \lambda_{i,j} E_{i,j}.$$

De plus, cette écriture est unique. Plus précisément, si $A = (a_{i,j})$, alors :

$$A = \sum_{i=1}^{n} \sum_{j=1}^{p} a_{i,j} E_{i,j}.$$

est la seule écriture possible de A comme combinaison linéaire des matrices élémentaires.

Démonstration. Considérons $\lambda_{i,j}$ une famille de scalaire indexée par $(i, j) \in [\![1; n]\!] \times [\![1; p]\!]$. Posons $B = \sum_{i=1}^{n} \sum_{j=1}^{p} \lambda_{i,j} E_{i,j}$.
Par définition des opérations matricielles, le coefficient d'indice (k, l) de B est $\lambda_{k,l}$: puisque c'est le coefficient de $\lambda_{k,l} E_{k,l}$, et toutes les autres matrices de la double somme ont comme coefficient 0 en indice (k, l).
Et ainsi, comme les matrices A et B ont même taille :

$$\begin{aligned} A = B &\Leftrightarrow \forall (k, l) \in [\![1; n]\!] \times [\![1; p]\!],\ [A]_{k,l} = [B]_{k,l} \\ &\Leftrightarrow \forall (k, l) \in [\![1; n]\!] \times [\![1; p]\!],\ a_{k,l} = \lambda_{k,l} \end{aligned}$$

ce qui est bien le résultat voulu. □

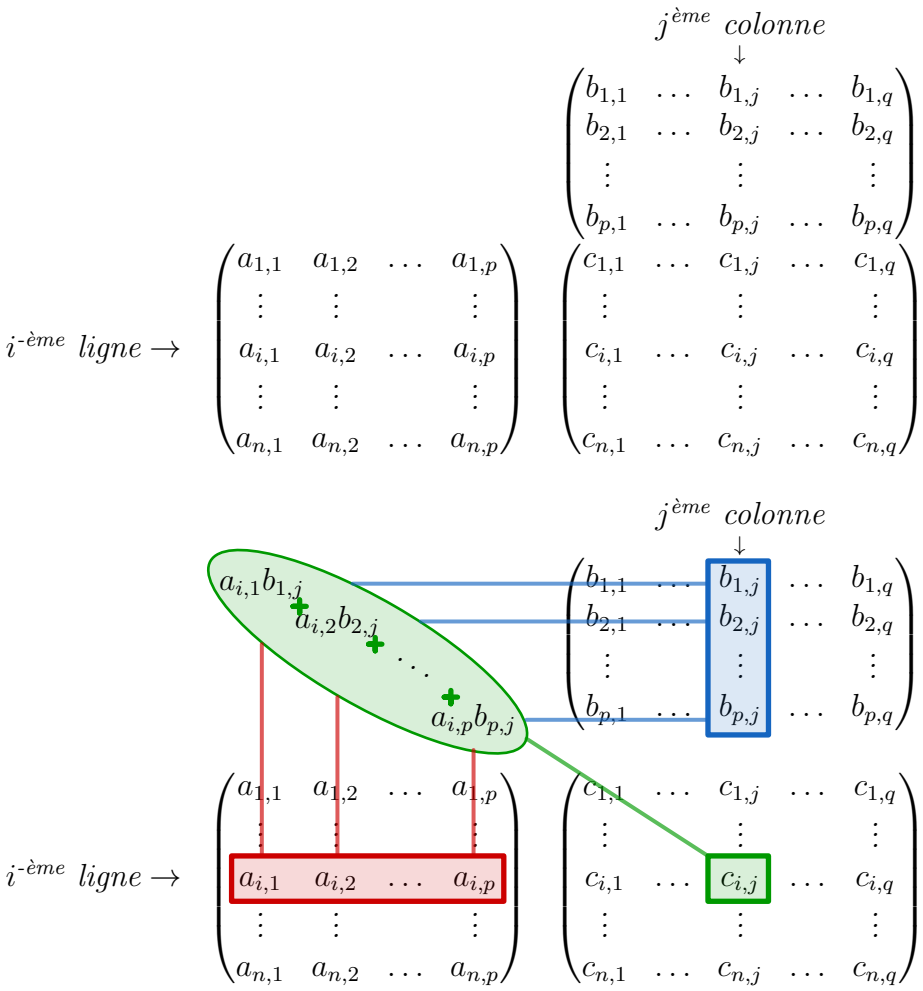
III Produit matriciel

III.1 Définition et premières propriétés

Définition III.1. *Soient $n, p, q \in \mathbb{N}^*$, $A = (a_{i,j}) \in \mathcal{M}_{n,p}(\mathbb{K})$ et $B \in \mathcal{M}_{p,q}(\mathbb{K})$.*
*On définit le **produit matriciel** de A et B, noté $A \times B$ ou AB, comme la matrice $C = (c_{i,j}) \in \mathcal{M}_{n,q}(\mathbb{K})$ définie par :*

$$\forall (i, j) \in [\![1; n]\!] \times [\![1; q]\!],\ c_{i,j} = \sum_{k=1}^{p} a_{i,k} b_{k,j}.$$

Remarque III.2. *Cette formule se visualise assez bien : pour calculer le coefficient d'indice (i, j) de la matrice AB, on multiplie dans l'ordre les éléments de la i-ème ligne de A avec ceux de la j-ème colonne de B, et on ajoute les produits obtenus.*
Pour multiplier deux matrices, il faut donc que la première matrice ait autant de colonnes que la seconde a de lignes ; par exemple, on peut toujours multiplier ensemble des matrices carrées de même taille.



Exemples III.3.

1. $\begin{pmatrix} 2 & 3 \\ 1 & -2 \\ 2 & -3 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ -1 & -2 \end{pmatrix} = \begin{pmatrix} 1 & -4 \\ 4 & 5 \\ 7 & 8 \end{pmatrix}$;
2. $\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 6 & 10 \\ 2 & 3 \end{pmatrix}$
3. $\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 2 & 9 \end{pmatrix}$;
4. $\begin{pmatrix} 1 & -1 \\ -2 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Remarque III.4.
Si A, B sont deux matrices non carrées, les produits AB et BA n'ont pas la même taille (il se peut même qu'un seul ait un sens).
Mais même si A et B sont carrées de même taille, on n'a pas toujours $AB = BA$ (c'est même rare).
Pire : on peut avoir $AB = 0$ sans que ni A ni B ne soit nulles.

Proposition III.5. *Le produit matriciel vérifie les propriétés suivantes : si $A, A' \in \mathcal{M}_{n,p}(\mathbb{K})$, $B, B' \in \mathcal{M}_{p,q}(\mathbb{K})$, $C \in \mathcal{M}_{q,r}(\mathbb{K})$, $\lambda, \mu \in \mathbb{K}$, alors :*

1. *$(AB)C = A(BC)$ (associativité du produit matriciel) ;*
2. *$(\lambda A + \mu A')B = \lambda AB + \mu A'B$ et $A(\lambda B + \mu B') = \lambda AB + \mu AB'$ (bilinéarité du produit matriciel);*

3. $I_nA = A = AI_p$ *(élément neutre pour la multiplication matricielle)*

4. $(\lambda A)(\mu B) = (\lambda\mu)(AB)$.

Démonstration.
Dans toutes les égalités à montrer, les matrices considérées ont même taille. Il reste donc à montrer l'égalité entre leurs coefficients de même indice.

1. soit $(i,j) \in [\![1;n]\!] \times [\![1;r]\!]$:

$$\begin{array}{rcl}[(AB)C]_{i,j} & = & \sum_{k=1}^{q}[AB]_{i,k}[C]_{k,j} = \sum_{k=1}^{q}\sum_{l=1}^{p}[A]_{i,l}[B]_{l,k}[C]_{k,j} \\ & = & \sum_{l=1}^{p}\sum_{k=1}^{q}[A]_{i,l}[B]_{l,k}[C]_{k,j} = \sum_{l=1}^{p}[A]_{i,l}[BC]_{l,j} \\ & = & [A(BC)]_{i,j}\end{array}$$

   ce qui donne bien l'égalité cherchée.

2. Montrons la première égalité. Soit $(i,j) \in [\![1;n]\!] \times [\![1;q]\!]$:

$$\begin{array}{rcl}[(\lambda A+\mu A')B]_{i,j} & = & \sum_{k=1}^{p}[\lambda A+\mu A']_{i,k}[B]_{k,j} = \sum_{k=1}^{p}\left(\lambda[A]_{i,k}+\mu[A']_{i,k}\right)[B]_{k,j} \\ & = & \lambda\sum_{k=1}^{p}[A]_{i,k}[B]_{k,j} + \mu\sum_{k=1}^{p}[A']_{i,k}[B]_{k,j} = \lambda[AB]_{i,j}+\mu[A'B]_{i,j}\end{array}.$$

3. Montrons la première égalité. Soit $(i,j) \in [\![1;n]\!] \times [\![1;p]\!]$:

$$[I_nA]_{i,j} = \sum_{k=1}^{n}[I_n]_{i,k}[A]_{k,j} = [A]_{i,j}$$

   en notant que, à i fixé, la seule valeur de k pour laquelle $[I_n]_{i,k} \neq 0$ est $k = i$, et alors $[I_n]_{i,i} = 1$.

4. soit $(i,j) \in [\![1;n]\!] \times [\![1;q]\!]$:

$$[(\lambda A)(\mu B)]_{i,j} = \sum_{k=1}^{n}[\lambda A]_{i,k}[\mu B]_{k,j} = \lambda\mu\sum_{k=1}^{p}[A]_{i,k}[B]_{k,j} = \lambda\mu[AB]_{i,j} = [(\lambda\mu)(AB)]_{i,j}.$$

□

Corollaire III.6. *Si* $\lambda \in \mathbb{K}$*, la multiplication par la matrice scalaire de coefficient* λ *(à gauche ou à droite) coïncide avec la multiplication scalaire par* λ*.*

Démonstration. On applique les points *3* et *4* :

$$(\lambda I_n)A = \lambda(I_nA) = \lambda A = \lambda(AI_p) = A(\lambda I_p).$$

□

III.2 Utilisation des matrices lignes ou colonnes

Exemple III.7. *Le produit (dans cet ordre) d'une matrice ligne par une matrice colonne de même taille est une matrice de taille* $(1,1)$ *:*

$$\begin{pmatrix}a_1 & a_2 & \dots & a_n\end{pmatrix}\cdot\begin{pmatrix}b_1\\b_2\\\vdots\\b_n\end{pmatrix} = (a_1b_1+a_2b_2+\cdots+a_nb_n) = \left(\sum_{k=1}^{n}a_kb_k\right) \in \mathcal{M}_{1,1}(\mathbb{K})$$

et en particulier le produit d'une matrice ligne par une matrice colonne n'a de sens que si elles ont autant de coefficients.

À l'inverse, le produit (dans cet ordre) d'une matrice colonne par une matrice ligne a toujours un sens, et la matrice obtenue a autant de lignes que la matrice colonne, et de colonnes que la matrice ligne. Ses coefficients donnent tous les produits possibles de coefficients des deux matrices :

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \cdot \begin{pmatrix} b_1 & b_2 & \dots & b_p \end{pmatrix} = \begin{pmatrix} a_1b_1 & a_1b_2 & \dots & a_1b_p \\ a_2b_1 & a_2b_2 & \dots & a_2b_p \\ \vdots & \vdots & & \vdots \\ a_nb_1 & a_nb_2 & \dots & a_nb_p \end{pmatrix} = (a_ib_j)_{i,j} \in \mathcal{M}_{n,p}(\mathbb{K})$$

Proposition III.8. *Si A, B sont deux matrice, alors AB est la matrice des produits des lignes de A par les colonnes de B (en identifiant $\mathcal{M}_{1,1}(\mathbb{K})$ à $\mathbb{K}$).*

Démonstration. Soient $A = (a_{i,j}) \in \mathcal{M}_{n,p}(\mathbb{K})$ et $B = (b_{i,j}) \in \mathcal{M}_{p,q}(\mathbb{K})$. Notons $A_1, \dots, A_n$ les lignes de A, et $B_1, \dots, B_q$ les colonnes de B. Alors pour tout $(i,j) \in [\![1;n]\!] \times [\![1;q]\!]$:

$$[AB]_{i,j} = \sum_{k=1}^{p} a_{i,k}b_{k,q} = \sum_{k=1}^{p} [A_i]_{1,k}[B_j]_{k,1} = [A_iB_j]_{1,1}.$$

□

Proposition III.9. *Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$:*

1. *si on note $C_1, \dots, C_p \in \mathcal{M}_{n,1}$ les colonnes de A, et si $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \in \mathcal{M}_{p,1}(\mathbb{K})$, alors :*

$$AX = x_1C_1 + \dots + x_pC_p = \sum_{k=1}^{p} x_kC_k$$

   c'est-à-dire que AX est une combinaison linéaire des colonnes de A ;
2. *si on note $L_1, \dots, L_n \in \mathcal{M}_{1,p}$ les lignes de A, et si $Y = \begin{pmatrix} y_1 & \dots & y_n \end{pmatrix} \in \mathcal{M}_{1,n}(\mathbb{K})$, alors :*

$$YA = y_1L_1 + \dots + y_nL_n = \sum_{k=1}^{n} y_kL_k$$

   c'est-à-dire que YA est une combinaison linéaire des lignes de A.

Démonstration. Notons déjà que, du fait de la définition du produit matriciel, AX est un vecteur colonne de taille n et YA est un vecteur ligne de taille p.
Soit $i \in [\![1;n]\!]$:

$$[AX]_{i,1} = \sum_{k=1}^{p} [A]_{i,k}[X]_k = \sum_{k=1}^{p} x_k[C_k]_{i,1} = \left[\sum_{k=1}^{p} x_kC_k\right]_{i,1}.$$

Soit $j \in [\![1;p]\!]$:

$$[YA]_{1,j} = \sum_{k=1}^{n} [Y]_{1,k}[A]_{k,j} = \sum_{k=1}^{n} y_k[L_k]_{1,j} = \left[\sum_{k=1}^{n} y_kL_k\right]_{1,j}.$$

□

Remarque III.10. *Si $(i,j) \in [\![1;n]\!] \times [\![1;p]\!]$, en prenant $X = E_j = \begin{pmatrix} \vdots \\ 1 \\ \vdots \end{pmatrix} \in \mathcal{M}_{p,1}(\mathbb{K})$ avec un 1 en j-ème position et des 0 sinon, et $Y = F_j = \begin{pmatrix} \dots & 1 & \dots \end{pmatrix} \in \mathcal{M}_{1,n}(\mathbb{K})$ avec un 1 en i-ème position et des 0 sinon, on trouve : $F_iA = L_i$ et $AE_j = C_j$.*

III.3 Puissances de matrices

Définition III.11 (Puissance d'une matrice carrée)**.** *Si $A \in \mathcal{M}_n(\mathbb{K})$ et $k \in \mathbb{N}$, on définit la* ***puissance k-ème de*** *A comme :*

$$A^k = \begin{cases} I_n & \text{si } k = 0 \\ \underbrace{A \times \cdots \times A}_{k \text{ fois}} & \text{si } k > 0 \end{cases}.$$

Remarque III.12. *On peut aussi définir récursivement, en notant que $A^k = A \times A^{k-1}$ si $k > 0$.*

Remarque III.13. *Si on ne considère qu'une seule matrice A, les puissances se comportent bien avec les produits : $\forall k, l \in \mathbb{N},\ A^k A^l = A^{k+l}$.*
En revanche, on n'a pas en général que $(AB)^k = A^k B^k$.

Définition III.14 (Matrices nilpotentes)**.** *Soit $A \in \mathcal{M}_n(\mathbb{K})$. On dit que A est* ***nilpotente*** *s'il existe $p \in \mathbb{N}$ tel que $A^p = 0_n$.*
On appelle alors ***l'indice de nilpotence*** *de A le plus petit entier k tel que $A^k = 0_n$, c'est-à-dire que : $A^k = 0_n$ et que $A^{k-1} \neq 0_n$.*

Exemples III.15.

1. *la matrice nulle est la seule matrice nilpotente d'indice 1 ;*
2. *considérons $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$. Alors :*

$$A^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \neq 0_3 \text{ et } A^3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = 0_3$$

donc A est nilpotente d'indice 3.

Définition III.16. *Soient A, B deux matrices. On dit que A et B* ***commutent*** *si les produits AB et BA sont bien définis et sont égaux.*

Remarque III.17. *Les matrices scalaires commutent avec toute matrice carrée de même taille. On verra en exercice que ce sont les seules matrices vérifiant cette propriété.*

Proposition III.18. *Si A, B sont deux matrices qui commutent, alors :*

1. *A et B sont des matrices carrées de même taille ;*
2. *pour tout $k \in \mathbb{N}$: $(AB)^k = A^k B^k = (BA)^k$.*

Démonstration.

1. si $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et $\mathcal{M}_{q,r}(\mathbb{K})$, alors :
   — comme AB est défini, alors : $p = q$;
   — comme BA est défini, alors : $r = n$;
   — on a donc $AB \in \mathcal{M}_n(\mathbb{K})$ et $BA \in \mathcal{M}_p(\mathbb{K})$;
   — comme $AB = AB$, alors AB et BA ont même taille donc $n = p$.
   Et ainsi : $n = p = q = r$ ce qui donne le résultat.
2. si $k = 0$, le résultat est toujours vrai (même si A et B ne commutent pas). Supposons $k > 0$:

$$(AB)^k = \underbrace{(AB) \times (AB) \times \cdots \times (AB)}_{k \text{ fois}} = \underbrace{A \times A \times \cdots \times A}_{k \text{ fois}} \underbrace{B \times B \times \cdots \times B}_{k \text{ fois}} = A^k B^k$$

où on a changé l'ordre des facteurs grâce à la commutativité et l'associativité.

□

Remarque III.19. *En fait, le précédent est un peu plus fort : on peut changer l'ordre des facteurs comme on veut dans une succession de puissances de A et B, et le regrouper comme cela nous arrange.*

Théorème III.20 (Formule du binôme)**.** *Soient A, B deux matrices **qui commutent** et $n \in \mathbb{N}$. Alors :*

$$(A+B)^n = \sum_{k=0}^{n} \binom{n}{k} A^k B^{n-k}.$$

Démonstration. On procède comme pour $\mathbb{R}$ ou $\mathbb{C}$ à l'aide d'une récurrence et du triangle de Pascal. □

Proposition III.21. *Soient A, B deux matrices **qui commutent** et $n \in \mathbb{N}$. Alors :*

$$A^n - B^n = (A-B) \cdot \left(\sum_{k=0}^{n-1} A^k B^{n-1-k} \right).$$

Exemple III.22. *Calculons les puissances de la matrice $A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$.*

On a : $A = \underbrace{\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}}_{=2\cdot I_2} + \underbrace{\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}}_{=B}$.

Comme $2I_2$ est scalaire, alors elle commute avec B et on peut appliquer la formule du binôme, qui donne pour tout $n \in \mathbb{N}$:

$$A^n = (2I_2 + B)^n = \sum_{k=0}^{n} \binom{n}{k} (2I_2)^{n-k} B^k = \sum_{k=0}^{n} \binom{n}{k} 2^{n-k} B^k$$

Calculons les puissances de B. On a :

$$B^2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_2$$

et ainsi (par associativité) toutes les puissances de B plus grande que 2 sont nulles.
La somme donnée par le binôme se simplifie donc pour $n \neq 0$:

$$A^n = \sum_{k=0}^{1} \binom{n}{k} 2^{n-k} B^k = \underbrace{2^n I_2}_{k=0} + \underbrace{n \cdot 2^{n-1} B}_{k=1} = \begin{pmatrix} 2^n & n \cdot 2^{n-1} \\ 0 & 2^n \end{pmatrix}.$$

Pour $n = 0$, on a $A^0 = I_2$ et la formule précédente reste donc valable.
Et ainsi pour tout $n \in \mathbb{N}$: $A^n = \begin{pmatrix} 2^n & n \cdot 2^{n-1} \\ 0 & 2^n \end{pmatrix}$.

Exemple III.23. *Calculons les puissances de la matrice $A = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}$.*

On a : $A = \underbrace{\begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}}_{=3\cdot I_2} + \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{=B}$.

Comme $3I_2$ est scalaire, alors elle commute avec B et on peut appliquer la formule du binôme, qui donne pour tout $n \in \mathbb{N}$:

$$A^n = (3I_2 + B)^n = \sum_{k=0}^{n} \binom{n}{k} (2I_2)^{n-k} B^k = \sum_{k=0}^{n} \binom{n}{k} 2^{n-k} B^k$$

Calculons les puissances de B. On a :

$$B^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

et ainsi on déduit (par récurrence on de manière directe) que pour $k \in \mathbb{N}$:

$$B^k = \begin{cases} I_2 & \text{si } k \text{ est pair} \\ B & \text{si } k \text{ est impair} \end{cases}.$$

On peut alors regrouper les termes dans la somme précédente :

$$\begin{aligned} A^n &= \sum_{\substack{k=0 \\ k \text{ pair}}}^{n} \binom{n}{k} 3^{n-k} I_2 + \sum_{\substack{k=0 \\ k \text{ impair}}}^{n} \binom{n}{k} 3^{n-k} B \\ &= S_1 I_2 + S_2 B \end{aligned}.$$

où $S_1 = \sum_{\substack{k=0 \\ k \text{ pair}}}^{n} \binom{n}{k} 3^{n-k}$ et $S_2 = \sum_{\substack{k=0 \\ k \text{ impair}}}^{n} \binom{n}{k} 3^{n-k}$ que l'on va calculer. On a :

$$S_1 + S_2 = \sum_{k=0}^{n} \binom{n}{k} 3^{n-k} 1^k = 4^n \text{ et } S_1 - S_2 = \sum_{k=0}^{n} \binom{n}{k} 3^{n-k} (-1)^k = 2^n$$

et ainsi : $S_1 = \dfrac{4^n + 2^n}{2}$ et $S_2 = \dfrac{4^n - 2^n}{2}$.
Et en réinjectant ces valeurs on trouve que pour tout $n \in \mathbb{N}$:

$$A^n = \frac{4^n + 2^n}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{4^n - 2^n}{2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 4^n + 2^n & 4^n - 2^n \\ 4^n - 2^n & 4^n + 2^n \end{pmatrix}.$$

On pourrait aussi calculer les puissances de A par la formule du binôme en décomposant A comme :

$$A = 2 \cdot I_2 + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \text{ ou } A = 4 \cdot I_2 + \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}$$

où le point important est que les matrices que l'on somme pour obtenir A commutent, et leurs puissances se calculent facilement.

Remarque III.24. *Il est fondamental que les matrices commutent. Par exemple, la même méthode ne fonctionnerait pas pour calculer les puissances de $\begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$ car :*

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 4 \\ 0 & 0 \end{pmatrix}.$$

Dans ce cas il faudrait plutôt utiliser la somme :

$$\begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} = I_2 + \begin{pmatrix} 0 & 2 \\ 0 & 1 \end{pmatrix}.$$

III.4 Produits de matrices particulières

Proposition III.25. *Soient $E_{i,j} \in \mathcal{M}_{n,p}(\mathbb{K})$ et $E_{k,l} \in \mathcal{M}_{p,q}(\mathbb{K})$ deux matrices élémentaires. Alors :*

$$E_{i,j}E_{k,l} = \delta_{j,k}E_{i,l} \in \mathcal{M}_{n,q}(\mathbb{K})$$

c'est-à-dire que : $E_{i,j}E_{k,l} = 0_{n,q}$ si $k \neq j$, et qu'il s'agit sinon de la matrice élémentaire d'indice (i,l) de taille (n,q).

Démonstration. On calcule chaque coefficient. □

Corollaire III.26. *Si A est une matrice et $E_{i,j}$ une matrice élémentaire. Alors si les produits suivants sont bien définis :*

1. *$A \cdot E_{i,j}$ est la matrice dont la j-ème colonne est la i-ème colonne de A, et tous ses autres coefficients sont nuls ;*
2. *$E_{i,j} \cdot A$ est la matrice dont la i-ème ligne est la j-ème ligne de A, et tous ses autres coefficients sont nuls.*

Démonstration. On écrit A comme combinaisons de matrices élémentaires : $A = \sum_{k,l} a_{k,l}E_{k,l}$.
Par bilinéarité du produit matriciel, on trouve que :

$$A \cdot E_{i,j} = \sum_{k,l} a_{k,l}E_{k,l}E_{i,j} = \sum_{k} a_{k,i}E_{k,j}$$

$$E_{i,j} \cdot A = \sum_{k,l} a_{k,l}E_{i,j}E_{k,l} = \sum_{l} a_{j,l}E_{i,l}$$

qui sont bien les égalités voulues. □

Proposition III.27. *Le produit de deux matrices triangulaires supérieures (resp. triangulaires inférieures, diagonales) est une matrice triangulaire supérieure (resp. triangulaire inférieure, diagonale).*
De plus, les coefficients diagonaux de la matrice produit sont égaux (dans l'ordre) aux produits deux-à-deux des coefficients diagonaux des matrices de départ.

Démonstration. Montrons le cas de matrices triangulaires supérieures. Soient $A, B \in \mathcal{M}_n(\mathbb{K})$ triangulaires supérieures. On écrit $A = (a_{i,j})$ et $B = (b_{i,j}$, et ainsi : $i > j \Rightarrow a_{i,j} = b_{i,j} = 0$.
Soient $i, j \in [\![1; n]\!]$ avec $i \geq j$. Alors :

$$[AB]_{i,j} = \sum_{k=1}^{n} a_{i,k}b_{k,j} = \sum_{k=1}^{i-1} \underbrace{a_{i,k}}_{=0} b_{k,j} + a_{i,i}b_{i,j} + \sum_{k=i+1}^{n} a_{i,k} \underbrace{b_{k,j}}_{=0} = a_{i,i}b_{i,j}$$

Et ainsi on trouve bien que :
— si $i > j$: $[AB]_{i,j} = 0$;
— si $i = j$: $[AB]_{i,i} = a_{i,i}b_{i,i}$.
Le cas des matrices triangulaires inférieures se montre de même.
Le cas des matrices diagonales en découle : un matrice diagonale étant à la fois triangulaire supérieure et inférieure. □

Remarque III.28. *On retrouve que le produit de matrices scalaires est une matrice scalaire. Qu'on savait déjà car :*

$$(\lambda I_n)(\mu I_n) = (\lambda\mu)I_n.$$

Définition III.29 (Matrices par blocs)**.** *Si $n_1, n_2, p_1, p_2 \in \mathbb{N}^*$ et $A_{1,1} \in \mathcal{M}_{n_1,p_1}(\mathbb{K}), A_{1,2} \in \mathcal{M}_{n_1,p_2}(\mathbb{K}), A_{2,1} \in \mathcal{M}_{n_2,p_1}(\mathbb{K}), A_{2,2} \in \mathcal{M}_{n_2,p_2}(\mathbb{K})$, on leur associe la **matrice en blocs** notée $\begin{pmatrix} A_{1,1} & A_{1,2} \\ A_{2,1} & A_{2,2} \end{pmatrix}$, qui est l'élément $A \in \mathcal{M}_{n_1+n_2,p_1+p_2}(\mathbb{K})$ défini par :*

$$[A]_{i,j} = \begin{cases} [A_{1,1}]_{i,j} & si\ 1 \leq i \leq n_1\ et\ 1 \leq j \leq p_1 \\ [A_{1,2}]_{i,(j-p_1)} & si\ 1 \leq i \leq n_1\ et\ p_1+1 \leq j \leq p_1+p_2 \\ [A_{2,1}]_{(i-n_1),j} & si\ n_1+1 \leq i \leq n_1+n_2\ et\ 1 \leq j \leq p_1 \\ [A_{2,2}]_{(i-n_1),(j-p_1)} & si\ n_1+1 \leq i \leq n_1+n_2\ et\ p_1+1 \leq j \leq p_1+p_2 \end{cases}$$

Proposition III.30. *Le produit d'une matrice est compatible avec les matrices en blocs, dans le sens où, sous réserve que tous les produits matriciels ci-dessous aient un sens :*

$$\begin{pmatrix} A_{1,1} & A_{1,2} \\ A_{2,1} & A_{2,2} \end{pmatrix} \cdot \begin{pmatrix} B_{1,1} & B_{1,2} \\ B_{2,1} & B_{2,2} \end{pmatrix} = \begin{pmatrix} A_{1,1}B_{1,1} + A_{1,2}B_{2,1} & A_{1,1}B_{1,2} + A_{1,2}B_{2,2} \\ A_{2,1}B_{1,1} + A_{2,2}B_{2,1} & A_{2,1}B_{1,2} + A_{2,2}B_{2,2} \end{pmatrix}.$$

Démonstration. En regardant chaque coefficient. □

IV Transposition

Définition IV.1. *Si $A = (a_{i,j}) \in \mathcal{M}_{n,p}(\mathbb{K})$, on appelle **transposée de** A, notée A^T (ou parfois ${}^tA$) la matrice $A^T = (b_{i,j}) \in \mathcal{M}_{p,n}(\mathbb{K})$ telle que :*

$$\forall (i,j) \in [\![1;n]\!] \times [\![1;p]\!],\ a_{i,j} = b_{j,i}.$$

Remarque IV.2. *Prendre la transposée revient à échanger les lignes et les colonnes (les lignes de A sont les colonnes de A^T et inversement). Visuellement, prendre la transposée revient à effectuer une symétrie par rapport à la diagonale. En particulier, les coefficients diagonaux ne changent pas.*

Exemple IV.3. *Si $A = \begin{pmatrix} \mathbf{1} & 3 & 2 & -1 \\ 0 & \mathbf{-2} & 1 & 2 \end{pmatrix}$, alors $A^T = \begin{pmatrix} \mathbf{1} & 0 \\ 3 & \mathbf{-2} \\ 2 & 1 \\ -1 & 2 \end{pmatrix}$.*

Proposition IV.4. *La transposition est **involutive**, c'est-à-dire que, si $A \in \mathcal{M}_{n,p}(\mathbb{K})$, alors :*

$$\left(A^T\right)^T = A$$

Démonstration. Si $(i,j) \in [\![1;n]\!] \times [\![1;p]\!]$:

$$\left[\left(A^T\right)^T\right]_{i,j} = \left[A^T\right]_{j,i} = [A]_{i,j}.$$

□

Remarque IV.5. *La transposition est une application de $\mathcal{M}_{n,p}(\mathbb{K})$ sur $\mathcal{M}_{p,n}(\mathbb{K})$: comme ces ensembles sont a priori distincts (sauf si $n = p$), alors il ne s'agit pas d'une involution comme on l'entendait pour les applications.*
Mais on peut pallier ce problème en posant $E = \bigcup_{n,p \in \mathbb{N}^*} \mathcal{M}_{n,p}(\mathbb{K})$: et dans ce cas on peut bien voir la transposition comme une application bijective de E sur lui-même qui est sa propre réciproque.

Proposition IV.6 (Linéarité de la transposition)**.** *Si $A, B \in \mathcal{M}_{n,p}$ et $\lambda, \mu \in \mathbb{K}$, alors :*

$$(\lambda A + \mu B)^T = \lambda A^T + \mu B^T$$

Démonstration. Comme les matrices ont même taille, on regarde chaque coefficient. Si $(i,j) \in [\![1;p]\!] \times [\![1;n]\!]$:

$$\left[(\lambda A + \mu B)^T\right]_{i,j} = [\lambda A + \mu B]_{j,i} = \lambda [A]_{j,i} + \mu [B]_{j,i} = \lambda \left[A^T\right]_{i,j} + \mu \left[B\right]_{i,j}.$$

□

Proposition IV.7. *Si $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et $B \in \mathcal{M}_{p,q}(\mathbb{K})$, alors :*

$$(AB)^T = B^T A^T.$$

Démonstration. Soit $(i,j) \in [\![1;q]\!] \times [\![1;n]\!]$:

$$\begin{aligned} \left[(AB)^T\right]_{i,j} &= [AB]_{j,i} = \sum_{k=1}^{p} [A]_{j,k}[B]_{k,i} \\ &= \sum_{k=1}^{p} [B^T]_{i,k}[A^T]_{k,j} = [B^T A^T]_{i,j} \end{aligned}.$$

□

Définition IV.8. *Une matrice carrée A est dite :*

1. ***symétrique*** *si $A^T = A$;*
2. ***antisymétrique*** *si $A^T = -A$.*

On notera $\mathcal{S}_n(\mathbb{K})$ l'ensemble des matrices symétriques de taille n, et $\mathcal{A}_n(\mathbb{K})$ celui des matrices antisymétriques.

Proposition IV.9.

1. *Les coefficients diagonaux d'une matrice antisymétrique sont nuls.*
2. *La matrice nulle est la seule matrice symétrique et antisymétrique.*
3. *Toute matrice se décompose de manière unique comme somme d'une matrice symétrique et d'une matrice antisymétrique.*

Démonstration.

1. Si $A \in \mathcal{M}_n(\mathbb{K})$ est antisymétrique, et $i \in [\![1;n]\!]$, alors :
$$[A]_{i,i} = [-A^T]_{i,i} = -[A^T]_{i,i} = -[A]_{i,i}$$
donc $[A]_{i,i} = 0$.
2. Pour une telle matrice A, on a : $-A = A^T = A$, donc $A = 0_n$.
3. Les matrices $S = \dfrac{A + A^T}{2}$ et $T = \dfrac{A - A^T}{2}$ sont respectivement symétrique et antisymétrique, et vérifient $A = S + T$, ce qui assure l'existence. L'unicité vient du point précédent.

□

Remarque IV.10. *Le dernier point ressemble beaucoup à l'écriture d'une fonction comme somme d'une fonction paire et d'une fonction impaire. L'idée derrière est que l'on cherche à décomposer en somme d'un élément stable (c'est-à-dire dont l'image est lui-même) par une involution et d'un élément "anti"-stable (c'est-à-dire un élément dont l'image est son opposé) par cette même involution.*
Pour les fonction, il s'agissait de l'involution :

$$\varphi : \left\{ \begin{array}{rcl} \mathcal{F}(\mathbb{R},\mathbb{R}) & \to & \mathcal{F}(\mathbb{R},\mathbb{R}) \\ f & \mapsto & (x \mapsto f(-x)) \end{array} \right.$$

Et on retrouve même un autre résultat analogue : la valeur "$x = 0$" correspond sensiblement aux coefficients de la diagonale dans une matrice (ce sont les éléments stables par la symétrie derrière l'involution). Et une fonction impaire s'annule en 0, comme les coefficients diagonaux d'une matrice antisymétrique.

V Matrices inversibles et systèmes linéaires

V.1 Inversibilité matricielle

Définition V.1. *Soit $A \in \mathcal{M}_n(\mathbb{K})$. S'il existe $B \in \mathcal{M}_n(\mathbb{K})$ telle que $AB = BA = I_n$, on dit que la matrice A est **inversible**.*
*La matrice B est appelée l'**inverse** de A, et est notée A^{-1}.*
*L'ensemble des matrices inversibles de taille n est noté $\mathrm{GL}_n(\mathbb{K})$, et est appelé le **groupe linéaire**.*

Proposition V.2. *L'inverse d'une matrice inversible est unique.*

Démonstration. Soient B, C deux inverses de A. Alors :

$$B = B \cdot I_n = B \cdot (AC) = (BA) \cdot C = I_n \cdot C = C.$$

□

Exemples V.3.

1. *la matrice I_n est inversible, d'inverse elle-même.*
2. *plus généralement, une matrice diagonale dont les coefficients valent tous ± 1 est inversible d'inverse elle-même.*
3. *dès lors qu'une matrice possède une ligne ou une colonne nulle, elle ne peut pas être inversible. Par exemple la matrice nulle n'est pas inversible.*
4. *Une matrice nilpotente n'est pas inversible.*

Proposition V.4. *Soient $A, B \in \mathrm{GL}_n(\mathbb{K})$. Alors :*

1. *A^{-1} est inversible, avec : $(A^{-1})^{-1} = A$;*
2. *si $\lambda \in \mathbb{K}$ avec $\lambda \neq 0$, alors λA est inversible d'inverse $\frac{1}{\lambda}A^{-1}$;*
3. *la matrice AB est inversible, d'inverse : $(AB)^{-1} = B^{-1}A^{-1}$;*
4. *si $k \in \mathbb{N}$, alors A^k est inversible d'inverse $(A^k)^{-1} = (A^{-1})^k$;*
5. *A^T est inversible, d'inverse $\left(A^T\right)^{-1} = (A^{-1})^T$.*

Démonstration.

1. $A \cdot A^{-1} = I_n = A^{-1}A$;
2. $(\lambda A)\left(\frac{1}{\lambda}A^{-1}\right) = \left(\lambda\frac{1}{\lambda}\right)AA^{-1} = I_n$, et de même $\left(\frac{1}{\lambda}A^{-1}\right)(\lambda A) = I_n$;
3. $(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n$ et de même $(B^{-1}A^{-1})(AB) = I_n$;
4. on procède par récurrence sur k en utilisant le point précédent ;
5. par transposée d'un produit : $A^T(A^{-1})^T = (A^{-1}A)^T = I_n^T = I_n$ et de même $(A^{-1})^T A^T$.

□

Définition V.5 (Puissances négatives d'une matrice inversible)**.** *Si $A \in \mathrm{GL}_n(\mathbb{K})$ et $k \in \mathbb{Z}$. On pose :*

$$A^k = \begin{cases} A^k & \text{si } k \geq 0 \\ (A^{-1})^{-k} & \text{si } k < 0 \end{cases}.$$

Proposition V.6. *Une matrice triangulaire supérieure (resp. triangulaire inférieure) est inversible si, et seulement si, ses coefficients diagonaux sont non nuls.*
Dans ce cas, son inverse est également triangulaire supérieure (resp. triangulaire inférieure) et se coefficients diagonaux sont les inverses de ceux de la matrice de départ.

Démonstration. Montrons le pour une matrice triangulaire supérieure. Le cas des matrices triangulaires inférieures découlera par transposition.
Montrons par récurrence sur $n \in \mathbb{N}^*$ que : tout matrice triangulaire supérieure de taille n est inversible si, et seulement si, ses coefficients diagonaux sont non nuls.

- si $n = 1$: alors $A = (a)$. Et donc : si $a = 0$, $A = 0_1$ n'est pas inversible ; si $a \neq 0$, A est inversible d'inverse $\left(\frac{1}{a}\right)$.
- supposons le résultat vérifié pour toutes les matrices triangulaires supérieure de taille n, et donnons-nous $A \in \mathcal{M}_{n+1}(\mathbb{K})$ triangulaire supérieure. Écrivons A sous forme de la matrice par blocs : $A = \begin{pmatrix} A_1 & A_2 \\ 0_{1,n} & a \end{pmatrix}$ où $A_1 \in \mathcal{M}_n(\mathbb{K})$, $A_2 \in \mathcal{M}_{n,1}(\mathbb{K})$ et $a \in \mathbb{K}$. Notons que A_1 est triangulaire supérieure, et que les coefficients diagonaux de A sont ceux de A_1 et a.
  - si A est inversible : notons, suivant les mêmes tailles de blocs que A, écrivons : $A^{-1} = \begin{pmatrix} B_1 & B_2 \\ B_3 & b \end{pmatrix}$.

    Par produit en blocs, on a :

    $$AA^{-1} = \begin{pmatrix} A_1B_1 + A_2B_3 & A_1B_2 + A_2b \\ aB_3 & ab \end{pmatrix} = \underbrace{\begin{pmatrix} I_n & 0_{n,1} \\ 0_{1,n} & 1 \end{pmatrix}}_{I_{n+1}} = A^{-1}A = \begin{pmatrix} B_1A_1 & B_1A_2 + B_2a \\ B_3A_1 & B_3A_2 + ab \end{pmatrix}$$

    dont on regarde les égalités bloc par bloc.
    On a déjà que $B_AA_1 = I_n$ avec l'égalité de droite.
    Avec celle de gauche, on trouve $ab = 1$, donc $a \neq 0$ et $b = \frac{1}{a}$. Comme $aB_3 = 0_{1,n}$, et $a \neq 0$, alors $B_3 = 0_{1,n}$. Et donc on trouve $A_1B_1 = I_n$.
    Ainsi A_1 est inversible, d'inverse B_1. Par hypothèse de récurrence appliquée à A_1, on trouve que B_1 est triangulaire supérieur, et ses coefficients diagonaux sont les inverses de ceux de A_1, donc des n premiers de A.
    Et finalement, comme $A^{-1} = \begin{pmatrix} A_1^{-1} & B_2 \\ 0_{1,n} & \frac{1}{a} \end{pmatrix}$, qui est bien de la forme voulue.
  - si A a tous ses coefficients diagonaux non nuls : alors A_1 aussi, donc on peut lui appliquer l'hypothèse de récurrence et A_1 est inversible. On a alors :

    $$\begin{pmatrix} A_1 & A_2 \\ 0_{1,n} & a \end{pmatrix} \cdot \begin{pmatrix} A_1^{-1} & -\frac{1}{a}A_1^{-1}A_2 \\ 0_{1,n} & \frac{1}{a} \end{pmatrix} = \begin{pmatrix} A_1A_1^{-1} & -\frac{1}{a}A_1A_1^{-1}A_2 + \frac{1}{a}A_2 \\ 0_{1,n} & 1 \end{pmatrix} = I_{n+1}$$

    et de même on trouve que $\begin{pmatrix} A_1^{-1} & -\frac{1}{a}A_1^{-1}A_2 \\ 0_{1,n} & \frac{1}{a} \end{pmatrix} \cdot \begin{pmatrix} A_1 & A_2 \\ 0_{1,n} & a \end{pmatrix} = I_{n+1}$.
    Donc A est inversible et son inverse est $\begin{pmatrix} A_1^{-1} & -\frac{1}{a}A_1^{-1}A_2 \\ 0_{1,n} & \frac{1}{a} \end{pmatrix}$, qui est bien de la forme voulue.

  ce qui conclut l'hérédité.

D'où la récurrence. □

Corollaire V.7. *Si $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$, la matrice $\mathrm{Diag}(\lambda_1, \ldots, \lambda_n)$ est inversible si, et seulement si : $\lambda_1 \times \cdots \times \lambda_n \neq 0$.*
Et dans ce cas on a :

$$(\mathrm{Diag}(\lambda_1, \ldots, \lambda_n))^{-1} = \mathrm{Diag}\left(\frac{1}{\lambda_1}, \ldots, \frac{1}{\lambda_n}\right).$$

Démonstration. Une matrice diagonale est à la fois triangulaire inférieure et supérieure, donc son inverse aussi. □

Corollaire V.8. *Si $\lambda_1, \ldots, \lambda_n \in \mathbb{K}^*$ et $k \in \mathbb{Z}$, alors :*

$$(\mathrm{Diag}(\lambda_1, \ldots, \lambda_n))^k = \mathrm{Diag}(\lambda_1^k, \ldots, \lambda_n^k).$$

V.2 Lien avec les systèmes linéaires

Proposition V.9. *Considérons le système linéaire à n inconnues et p équations :*

$$(\mathcal{S}) : \begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \ldots + a_{1,p}x_p = b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \ldots + a_{n,p}x_p = b_2 \\ \vdots \quad\quad \vdots \quad\quad \vdots \quad\quad \vdots \quad \vdots \quad \vdots \\ a_{n,1}x_1 + a_{n,2}x_2 + \ldots + a_{n,p}x_p = b_n \end{cases}$$

Alors la résolution de $(\mathcal{S})$ revient à résoudre l'équation :

$$(\mathcal{E}) : AX = B$$

où $A = (a_{i,j}) \in \mathcal{M}_{n,p}(\mathbb{K})$ et $B = (b_i) \in \mathcal{M}_{n,1}$ sont donnés, et $X = (x_i) \in \mathcal{M}_{p,1}(\mathbb{K})$ est l'inconnue.

Démonstration. Clair. □

Proposition V.10. *Avec les mêmes notations, le système précédent est compatible si, et seulement si, B est combinaison linéaire des colonnes de A.*

Démonstration. Découle de la multiplication d'une matrice par une matrice colonne. □

Proposition V.11. *On suppose le système $(\mathcal{S})$ compatible, et on pose X_0 une de ses solutions.*
Alors les solutions de $(\mathcal{S})$ sont les $X_0 + Y$, où Y est une solution du système homogène associé.

Démonstration. Soit $X \in \mathcal{M}_{p,1}$. Alors on a :

$$AX = B \Leftrightarrow AX = AX_0 \Leftrightarrow A(X - X_0) = 0$$

par bilinéarité du produit. Ce qui donne bien le résultat voulu. □

Corollaire V.12. *Avec les mêmes notations, si $p > n$, alors l'équation $AX = B$ admet soit une infinité de solutions, soit aucune.*

Démonstration. Découle de l'ensemble solution d'un système homogène possédant plus d'inconnues que d'équations. □

Proposition V.13. *Soit $A \in \mathcal{M}_n(\mathbb{K})$. Alors A est inversible si, et seulement si, l'équation $AX = B$ d'inconnue $X \in \mathcal{M}_{n,1}(\mathbb{K})$ possède une solution pour tout $B \in \mathcal{M}_{n,1}(\mathbb{K})$.*
Dans ce cas, pour tout B, le système $AX = B$ admet une unique solution.

Démonstration. On traite séparément les deux implications.
Si A est inversible. Soient $X, B \in \mathcal{M}_{n,1}(\mathbb{K})$. Alors :

$$AX = B \Leftrightarrow AA^{-1}X = A^{-1}B \Leftrightarrow X = A^{-1}B$$

donc le système $AX = B$ admet une (unique) solution, qui est $X = A^{-1}B$.
Réciproquement, si le système $AX = B$ admet toujours une solution. Pour tout $i \in [\![1; n]\!]$, posons X_i une solution de l'équation $AX = E_i$ (où E_i est la matrice élémentaire d'indice i de taille $(n, 1)$). Posons $\widetilde{X} = \left([X_i]_j\right) \in \mathcal{M}_n(\mathbb{K})$ la matrice carrée dont les colonnes sont les X_i. Alors :

— par définition des X_i, on a : $A\widetilde{X} = \left([E_i]_j\right) = I_n$;

— considérons l'équation $YA = yI_n$, d'inconnues $Y \in \mathcal{M}_n(\mathbb{K})$ et $y \in \mathbb{K}$: cette équation est un système linéaire à $n^2 + 1$ inconnues (n^2 qui proviennent de Y et 1 pour y) et à n^2 équations (une par coefficient dans l'égalité matricielle), et admet donc une solution non-nulle. Si on la note (Y_0, y_0), alors on a $Y_0 \neq 0$ ou $y_0 \neq 0$.
Mais on a aussi :

$$y_0 = 0 \Rightarrow Y_0 A = 0 \Rightarrow Y_0 A\widetilde{X} = 0 \Rightarrow Y_0 = 0$$

donc nécessairement $y_0 \neq 0$.
En posant $\widetilde{Y} = \frac{1}{y_0} Y_0$, on a ainsi : $\widetilde{Y}A = I_n$.

Ainsi A est inversible à gauche (d'inverse $\widetilde{X}$) et à droite (d'inverse $\widetilde{Y}$). Et on a aussi que :

$$\widetilde{Y} = \widetilde{Y} \cdot I_n = \widetilde{Y}(A\widetilde{X}) = (\widetilde{Y}A)\widetilde{X} = I_n\widetilde{X} = \widetilde{X}$$

et donc $\widetilde{Y} = \widetilde{X}$: donc A est inversible d'inverse $\widetilde{X}$.
L'unicité dans les solutions des systèmes $AX = B$ découle de la première implication. □

Théorème V.14. *Soit $A \in \mathcal{M}_n(\mathbb{K})$. Alors A est inversible si, et seulement si, l'une des conditions suivantes est vérifiée :*

1. *pour tout $B \in \mathcal{M}_{n,1}(\mathbb{K})$ le système $AX = B$ a une solution ;*
2. *pour tout $B \in \mathcal{M}_{n,1}(\mathbb{K})$ le système $AX = B$ a une unique solution ;*
3. *il existe $B \in \mathcal{M}_{n,1}(\mathbb{K})$ le système $AX = B$ a une unique solution ;*
4. *l'équation $AX = 0$ a pour seule solution $X = 0$;*
5. *il existe une matrice $C \in \mathcal{M}_n(\mathbb{K})$ telle que $AC = I_n$;*
6. *il existe une matrice $C \in \mathcal{M}_n(\mathbb{K})$ telle que $CA = I_n$.*

Démonstration. Les deux premiers points ont déjà été vus.
Les points *3* et *4* seront vus au paragraphe suivant.
Pour *5* : si $AC = I_n$ et $B \in \mathcal{M}_{n,1}(\mathbb{K})$, alors : CB est une solution du système $AX = B$, donc par le résultat précédent A est inversible. La réciproque est claire.
Pour *6* : si $CA = I_n$, alors $A^T C^T = I_n$, donc par le point précédent A^T est inversible, donc A aussi. La réciproque est claire. □

Remarque V.15. *Un matrice est donc inversible à droite si, et seulement si, elle est inversible à gauche. Ceci est tout à fait remarquable compte tenu du fait que la multiplication matricielle n'est pas commutative sur $\mathcal{M}_n(\mathbb{K})$. En particulier, dans 5 et 6, la matrice C est unique et est égale à A^{-1}.*

Corollaire V.16. *Si $A, B \in \mathcal{M}_n(\mathbb{K})$, alors :*

$$A, B \in \mathrm{GL}_n(\mathbb{K}) \Leftrightarrow AB \in \mathrm{GL}_n(\mathbb{R}).$$

Démonstration. Le sens direct a déjà été montré.
Pour la réciproque, notons $C = (AB)^{-1}$. Alors :
— comme $(AB)C = I_n$, alors $A(BC) = I_n$ (par associativité), donc A est inversible d'inverse BC ;
— comme $C(AB) = I_n$, alors $(CA)B = I_n$ (par associativité), donc B est inversible d'inverse CA.
□

Remarque V.17. *On retrouve au passage que : $B^{-1}A^{-1} = CABC = C = (AB)^{-1}$.*

V.3 Opérations élémentaires sur les lignes et les colonnes

Proposition V.18 (Écriture matricielle des opérations élémentaires)**.** *Faire une opération élémentaires sur les* ***lignes*** *(resp. les colonnes) d'une matrice revient à la multiplier* ***à gauche*** *(resp. à droite) par la transformée de la matrice identité.*

Démonstration. Soit $A \in \mathcal{M}_n(\mathbb{K})$. On considère $E_{i,j}$ la matrice élémentaire d'indice (i,j) de taille n. On rappelle que :
- la matrice $E_{i,j}A$ est la matrice dont la i-ème ligne est la j-ème ligne de A ;
- la matrice $AE_{i,j}$ est la matrice dont la j-ème colonne est la i-ème colonne de A.

On peut alors exprimer les opérations élémentaires sur les lignes en terme de multiplication à gauche :
- la permutation $L_i \leftrightarrow L_j$: par $I_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$;
- la dilatation $L_i \leftarrow \lambda L_i$: par $\mathrm{Diag}(1,\dots,1,\lambda,1,\dots,1) = I_n + (\lambda-1)E_{i,i}$;
- la transvection $L_i \leftarrow L_i + \lambda L_j$: par $I_n + \lambda E_{i,j}$.

Donc on trouve bien le résultat voulu.
Les opérations élémentaires sur les colonnes s'obtiennent de même par multiplication à droite :
- la permutation $C_i \leftrightarrow C_j$: par $I_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$ (comme pour les lignes) ;
- la dilatation $C_i \leftarrow \lambda C_i$: par $\mathrm{Diag}(1,\dots,1,\lambda,1,\dots,1) = I_n + (\lambda-1)E_{i,i}$ (comme pour les lignes) ;
- la transvection $C_i \leftarrow C_i + \lambda C_j$: par $I_n + \lambda E_{j,i}$ (la transposée de la matrice pour les lignes).

□

Proposition V.19. *Réaliser des opérations élémentaires sur les lignes ou les colonnes d'une matrice ne change pas son inversibilité.*

Démonstration. Notons que, si B est une matrice inversible, alors une matrice A est inversible si, et seulement si, AB est inversible (par inversibilité d'un produit).
Le résultat découle alors du fait que les matrices associées aux opérations élémentaires sont inversibles : pour les dilatations ou transvection, il s'agit de matrices triangulaires de coefficients diagonaux non nuls ; pour les permutations on peut voir que la matrice est son propre inverse. □

Corollaire V.20. *Une matrice possédant deux lignes identiques ou deux colonnes identiques n'est pas inversible.*

Démonstration. Par opérations élémentaires, on se ramène à l'inversibilité d'une matrice qui possède une ligne ou une colonne nulle. □

Corollaire V.21. *Si $A \in \mathcal{M}_n(\mathbb{K})$, alors A est inversible si, et seulement si, le système $AX = 0$ a pour seule solution* 0*.*

Démonstration. Si A est inversible, le résultat est clair.
Si A n'est pas inversible, considérons le système $AX = 0$. Par opérations élémentaires sur les lignes, on se ramène au système échelonné équivalent $TX = 0$, où T est une matrice triangulaire supérieure. Comme A n'est pas inversible, T non plus donc T possède un coefficient diagonal nul.
Quitte à échanger les inconnues, on peut supposons que son dernier coefficient diagonal est non nul. Mais alors, pour tout $x_n \in \mathbb{K}$, le système $TX = 0$ admet une solution dont la dernière coordonnée vaut x_n. Donc le système $TX = 0$ admet une infinité de solution, tout comme le système $AX = 0$. □

Corollaire V.22. *La matrice A est inversible si, et seulement si, pour* ***un*** *$B \in \mathcal{M}_{n,1}(\mathbb{K})$ l'équation $AX = B$ admet une unique solution.*

Démonstration. Si A est inversible, on peut prendre $B = 0$ par le résultat précédent.
Réciproquement, si un tel B existe, alors notons X_1 tel que $AX_1 = B$. Comme les solutions de l'équation $AX = B$ sont de la forme $X_1 + X_0$, avec X_0 solution de l'équation homogène, on déduit que l'équation homogène a pour seule solution $X = 0$. Et on utilise à nouveau le point précédent. □

V.4 Calcul d'inverses de matrices

Proposition V.23. *Si $A \in \mathcal{M}_n(\mathbb{K})$ et $X, Y \in \mathcal{M}_{n,1}(\mathbb{K})$.*

Si le système $AX = Y$ (d'inconnue X) est équivalent à un système $A'Y = X$ (d'inconnue Y), alors A est inversible d'inverse A'.

Sinon A n'est pas inversible.

Démonstration. Pour le premier cas, le système admet toujours une solution peu importe la valeur de Y, donc A est inversible.

Réciproquement, si A est inversible, alors $A' = A^{-1}$ convient. □

Remarque V.24. *En pratique on cherchera simplement à résoudre le système $AX = Y$ (par méthode du pivot par exemple).*

Exemple V.25. *Considérons la matrice* $A = \begin{pmatrix} 1 & -1 & 1 \\ -2 & -1 & 0 \\ 3 & -1 & 2 \end{pmatrix}$. *Posons* $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ *et* $Y = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$. *Alors :*

$$
\begin{aligned}
AX = Y \quad &\Leftrightarrow \quad \begin{cases} x - y + z = a \\ -2x - y = b \\ 3x - y + 2z = c \end{cases} \\
&\Leftrightarrow \quad \begin{cases} x - y + z = a \\ -3y + 2z = 2a + b \\ 2y - z = -3a + c \end{cases} \\
&\Leftrightarrow \quad \begin{cases} x - y + z = a \\ -3y + 2z = 2a + b \\ z = -5a + 2b + 3c \end{cases} \\
&\Leftrightarrow \quad \begin{cases} x - y = 6a - 2b - 3c \\ -3y = 12a - 3b - 6c \\ z = -5a + 2b + 3c \end{cases} \\
&\Leftrightarrow \quad \begin{cases} x - y = 6a - 2b - 3c \\ y = -4a + b + 2c \\ z = -5a + 2b + 3c \end{cases} \\
&\Leftrightarrow \quad \begin{cases} x = 2a - b - c \\ y = -4a + b + 2c \\ z = -5a + 2b + 3c \end{cases} \\
&\Leftrightarrow \quad X = \begin{pmatrix} 2 & -1 & -1 \\ -4 & 1 & 2 \\ -5 & 2 & 3 \end{pmatrix} Y
\end{aligned}
$$

Donc $\begin{pmatrix} 1 & -1 & 1 \\ -2 & -1 & 0 \\ 3 & -1 & 2 \end{pmatrix}$ *est inversible d'inverse* $\begin{pmatrix} 2 & -1 & -1 \\ -4 & 1 & 2 \\ -5 & 2 & 3 \end{pmatrix}$.

Exemple V.26. *Faisons la même chose avec* $B = \begin{pmatrix} 1 & -1 & 1 \\ -2 & -1 & 1 \\ 3 & -1 & 1 \end{pmatrix}$ *et reprenons les mêmes* X, Y. *Alors :*

$$AX = Y \Leftrightarrow \begin{cases} x - y + z = a \\ -2x - y + z = b \\ 3x - y + z = c \end{cases} \Leftrightarrow \begin{cases} x - y + z = a \\ -3y + 3z = 2a + b \\ 2y - 2z = -3a + c \end{cases} \Leftrightarrow \begin{cases} x - y + z = a \\ -3y + 2z = 2a + b \\ 0 = -5a + 2b + 3c \end{cases}$$

Donc l'équation $BX = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ *n'a pas de solution, car alors :*$-5a + 2b + 3c = -5 \neq 0$.

Donc B *n'est pas inversible.*

On pouvait aussi directement chercher à résoudre $BX = 0$, *et voir qu'il y a une solution non nulle. Comme les deuxième et troisième colonnes de* B *sont opposées, on a (sans calcul) que* $B \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = 0$, *donc l'équation* $BX = 0$ *admet une solution non nulle, et* B *n'est pas inversible.*

Proposition V.27. *Si* A *est inversible, la suite d'opérations élémentaires sur les lignes qui transforme* A *en* I_n *transformera* I_n *en* A^{-1}.

Démonstration. Notons $P_1, P_2, \ldots, P_r$ les opérations élémentaires que l'on effectue dans cet ordre, c'est-à-dire que :

$$P_r \ldots P_1 P_0 A = I_n.$$

Alors en multipliant par A^{-1}, on trouve : $A^{-1} = P_r \ldots P_1 P_0 = P_r \ldots P_1 P_0 I_n$. □

Remarques V.28.

1. *On pourrait faire avec les opérations sur les colonnes, mais il ne faut pas mélanger les opérations sur les lignes et les colonnes dans un même calcul d'inverse de matrice.*

2. *On a même mieux : si, avec des opérations élémentaires, on transforme* A *en une matrice non inversible, alors* A *n'était pas inversible.*

Exemple V.29. *Étudions l'inversibilité de la matrice* $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 4 & 8 \end{pmatrix}$ *par opérations élémentaires sur les*

lignes :

$$\begin{array}{ll}
\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 4 & 8 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 3 & 7 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \\
\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 2 & -3 & 1 \end{pmatrix} \\
\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} -1 & 3 & -1 \\ -5 & 7 & -2 \\ 2 & -3 & 1 \end{pmatrix} \\
\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 4 & -4 & 1 \\ -5 & 7 & -2 \\ 2 & -3 & 1 \end{pmatrix}
\end{array}$$

donc la matrice A est inversible. Son inverse est : $A^{-1} = \begin{pmatrix} 4 & -4 & 1 \\ -5 & 7 & -2 \\ 2 & -3 & 1 \end{pmatrix}$.

Remarque V.30. *Quand on cherche à inverser la matrice A par opérations élémentaires sur les lignes, au lieu de travailler avec deux matrices simultanément, on peut travailler avec la matrice rectangulaire (AI_n) (de taille $n \times 2n$), que l'on cherche à échelonner, ce qui revient exactement au même.*

Chapitre 13

Les réels

I Théorème de la borne supérieure

Définition I.1. *Soit E un ensemble muni d'une relation d'ordre $\preceq$, et A une partie de E :*

1. *on dit qu'un élément a de E est la* ***borne inférieure*** *de A si : a est le plus grand minorant de A ; on note $a = \inf(A)$;*
2. *on dit qu'un élément b de E est la* ***borne supérieure*** *de A si : b est le plus petit majorant de A ; on note $b = \sup(A)$.*

Proposition I.2. *Si A possède un maximum (resp. un minimum), alors A possède une borne supérieure (resp. inférieure), et alors :* $\max(A) = \sup(A)$ *(resp.* $\min(A) = \inf(A)$*).*

Démonstration. Soit $a = \max(a)$. Donc a est un majorant de A et $a \in A$. Si M est un majorant de A, comme $a \in A$, alors : $a \leq M$. Donc a est bien le plus petit majorant : donc $\sup(A)$ existe, et $\sup(A) = \max(A)$. □

Théorème I.3 (de la borne supérieure)**.**

1. *Toute partie non vide majorée de $\mathbb{R}$ admet une borne supérieure.*
2. *Toute partie non vide minorée de $\mathbb{R}$ admet une borne inférieure.*

Exemples I.4.

1. $A =]0; 1]$ *est non vide (il contient* 1*), majoré (par* 2*) et minoré (par* -41*) ;* $\sup(A) = 1$ *et* $\inf(A) = 0$ *;*
2. $B = \{x \in \mathbb{R} \,|\, x^2 \leq 2\}$ *vérifie* $\sup(B) = \sqrt{2}$ *et* $\inf(B) = -\sqrt{2}$ *;*
3. $C = \{x \in \mathbb{R} \,|\, x^2 < 2\}$ *vérifie aussi* $\sup(C) = \sqrt{2}$ *et* $\inf(C) = -\sqrt{2}$.

Remarque I.5. *L'ensemble $\mathbb{Q}$ ne vérifie pas le théorème de la borne supérieure.*
Posons $A = \{x \in \mathbb{Q} \,|\, x^2 \leq 2\}$: alors A est non vide et majorée, mais n'admet pas de borne supérieure (dans $\mathbb{Q}$).
Le fait que A est non vide et majorée est clair.
Montrons que A n'a pas de borne supérieure. Soit $a \in \mathbb{Q}$ un majorant de A (dans $\mathbb{Q}$) : montrons qu'il ne peut pas être le plus petit. Pour cela, on pose $b = \dfrac{a}{2} + \dfrac{1}{a}$:

- *comme $1 \in A$, alors $a \geq 1$ donc $b \geq 0$;*
- *on a $b^2 = \frac{a^2}{4} + \frac{1}{a^2} + 1 = 2 + \left(\frac{a^2}{4} + \frac{1}{a^2} - 1\right) = 2 + \left(\frac{a}{2} - \frac{1}{a}\right)^2 \geq 2$, donc $b \geq \sqrt{2}$ est un majorant de A ;*
- *$\left(\frac{2}{b}\right)^2 = \frac{4}{b^2} \leq 2$ donc $\frac{2}{b} \in A$; donc $a \geq \frac{2}{b}$, c'est-à-dire $ab \geq 2$.*
- *en remplaçant b par sa valeur, on déduit que $a^2 \geq 2$, donc $a > \sqrt{2}$ (car $\sqrt{2} \notin \mathbb{Q}$) ;*
- *et donc $b - a = \frac{1}{a} - \frac{a}{2} = \frac{2-a^2}{2a} < 0$, donc $b < a$.*

Donc, peu importe le majorant choisi, on peut toujours trouver un majorant strictement plus petit : A n'a pas de borne supérieure.

Proposition I.6. *Soit A une partie non vide de $\mathbb{R}$. Alors :*

1. $M = \sup A \Leftrightarrow \left\{ \begin{array}{l} M \text{ est un majorant de } A \\ \forall \varepsilon > 0, \exists a \in A, M - \varepsilon < a \leq M \end{array} \right.$;
2. $m = \inf A \Leftrightarrow \left\{ \begin{array}{l} m \text{ est un minorant de } A \\ \forall \varepsilon > 0, \exists a \in A, m \leq a < m + \varepsilon \end{array} \right.$;

Démonstration. Montrons le premier résultat :
- si $M = \sup A$:
  - M est un majorant de A (par définition) ;
  - si $\varepsilon > 0$, alors $M - \varepsilon < M$ donc $M - \varepsilon$ n'est plus un majorant de A. Donc il existe $a \in A$ tel que $M - \varepsilon < a$. Donc $M - \varepsilon < a \leq M$.
- réciproquement : soit $M' < M$. Posons $\varepsilon = M' - M > 0$. Alors il existe $a \in A$ tel que $M' < a$, donc M' n'est pas un majorant de A. Donc M est le plus petit majorant de A et $M = \sup A$.

□

Remarque I.7. *L'idée derrière étant que la borne supérieure est le plus petit majorant : tout nombre strictement plus petit n'est plus un majorant.*

Définition I.8. *Étant donné I un intervalle non-vide de $\mathbb{R}$, notons ∂I l'ensemble (éventuellement vide) de ses bornes inférieure et supérieure (selon que I est minoré, majoré ou borné). On définit alors l'adhérence de I, notée $\overline{I}$, comme $\overline{I} = I \cup \partial I$.*
L'ensemble ∂I est appelé l'ensemble des ***extrémités*** *de I.*

Remarques I.9.

1. *L'adhérence se voit bien sur la notation avec les crochets : cela consiste à tourner les crochets qui définissent I vers l'intérieur.*
2. *Un segment est égal à son adhérence.*

Exemples I.10.

1. $\overline{[0;1[} = [0;1]$;
2. $\overline{\mathbb{R}_+^*} = \mathbb{R}_+$;
3. *si $I = \mathbb{R}$, alors $\overline{I} = \mathbb{R}$ (et donc on prendra garde à ne pas confondre avec $\overline{\mathbb{R}}$).*

Théorème I.11. *L'ensemble $\mathbb{R}$ est* ***archimédien****, c'est-à-dire que :*

$$\forall a \in \mathbb{R}_+^*, \forall b \in \mathbb{R},\ \exists n \in \mathbb{N},\ na \geq b.$$

Démonstration. Soient $a \in \mathbb{R}_+^*$ et $b \in \mathbb{R}$. Par l'absurde, supposons que : $\forall n \in \mathbb{N},\ na < b$.
Alors l'ensemble $A = \{na,\ n \in \mathbb{N}\}$ est une partie non vide majorée de $\mathbb{R}$, donc possède une borne supérieure M.
Soit $n \in \mathbb{N}$. Alors $(n+1) \in \mathbb{N}$, donc $(n+1)a \in A$, donc : $(n+1)a \leq M$. Et finalement : $na \leq M - a$, donc $M - a$ est un autre majorant de A.
Ceci contredit le fait que M est la borne supérieure de A. □

Théorème-Définition I.12. *Soit $x \in \mathbb{R}$. On appelle* ***partie entière*** *de x, notée $\lfloor x \rfloor$, l'unique entier relatif n tel que : $n \leq x < n + 1$.*

Démonstration. 1. unicité : supposons que $n, n' \in \mathbb{Z}$ conviennent, c'est-à-dire tels que :

$$\left\{ \begin{array}{rcl} n & \leq x < & n+1 \\ n' & \leq x < & n'+1 \end{array} \right. .$$

Alors : $\left\{ \begin{array}{rcl} n & < & n'+1 \\ n' & < & n+1 \end{array} \right.$ et donc $-1 < n - n' < 1$.
Mais $n - n'$ est un entier, donc $n - n' = 0$, donc $n = n'$.

2. existence : posons $A = \{k \in \mathbb{Z} \,|k \leq x\}$, qui est une partie de $\mathbb{Z}$ majorée (par x) et non vide car :
   — si $x \geq 0$: alors $0 \in A$;
   — si $x < 0$: comme $\mathbb{R}$ est archimédien, il existe $n \in \mathbb{N}$ tel que $n \times 1 \geq -x$, et alors $-n \in A$.
   Ainsi, A possède un plus grand élément, que l'on note n, et qui vérifie :
   — comme $n \in A$: $n \leq x$;
   — comme $n+1 \notin A$: $x < n+1$.
   Et donc n convient.

□

Théorème-Définition I.13 (Division euclidienne)**.** *Soit $y \in \mathbb{R}_+^*$:*

$$\forall x \in \mathbb{R},\ \exists!(q,r) \in \mathbb{Z} \times [0; y[,\ x = qy + r.$$

*Cette écriture est appelée **division euclidienne** de x par y. On appelle r le **reste** et q le **quotient**.*

Démonstration. Découle des propriétés de la partie entière appliquées à $\dfrac{x}{y}$. □

Remarque I.14. *La partie entière n'est autre que le quotient de la division euclidienne par 1.*

II Approximation d'un réel

Proposition-Définition II.1. *Si $x \in \mathbb{R}$ et $n \in \mathbb{N}$, on appelle **approximation décimale** de x à 10^{-n} le décimal : $x_n = \dfrac{\lfloor 10^n x \rfloor}{10^n}$.*
On a : $x_n \leq x < x_n + \dfrac{1}{10^n}$.

Démonstration. Découle des propriétés de la partie entière. □

Remarque II.2. *Plus précisément, x_n est l'approximation de x **par défaut**. Et $x_n + \dfrac{1}{10^n}$ est appelée approximation **par excès**.*

Proposition-Définition II.3. *Une partie A de $\mathbb{R}$ est dite **dense** dans $\mathbb{R}$ si elle vérifie l'une des propriétés équivalentes suivantes :*

1. *entre deux réels, il existe un élément de A ;*
2. *tout intervalle ouvert non vide de $\mathbb{R}$ contient un élément de A.*

Démonstration.
— $1 \Rightarrow 2$: si I est un intervalle ouvert non-vide, et $x, y \in I$ avec $x < y$. Alors il existe $a \in A$ tel que : $x \leq a \leq y$, et donc $a \in [x, y] \subset I$, donc $a \in I$;
— $2 \Rightarrow 1$: soient $x, y \in \mathbb{R}$, avec $x < y$. Alors l'intervalle $]x, y[$ contient un élément $a \in A$, et $x < a < y$ pour un tel A.

□

Théorème II.4. *L'ensemble $\mathbb{Q}$ des rationnels est dense dans $\mathbb{R}$.*

Démonstration. Soient $x, y \in \mathbb{R}$ avec $x < y$. On veut montrer qu'il existe $r \in \mathbb{Q}$ tel que : $x < r < y$.

1. comme $\mathbb{R}$ est archimédien, il existe $q \in \mathbb{N}^*$ tel que : $q(y-x) > 1$;
2. en notant $p = \lfloor xq \rfloor$ et $r = \dfrac{p+1}{q}$, on a que $p \in \mathbb{Z}$ et $r \in \mathbb{Q}$ vérifient : $p \leq xq < p+1$, donc $x < r$;
3. de plus : $\begin{cases} \dfrac{1}{q} & < & y - x \\ \dfrac{p}{q} & \leq & x \end{cases}$, donc $r < y$.

□

Remarque II.5. *En fait, on a même que $\mathbb{D}$ est dense dans $\mathbb{R}$ grâce à l'approximation décimale.*

Théorème II.6. *L'ensemble $\mathbb{R} \setminus \mathbb{Q}$ des irrationnels est dense dans $\mathbb{R}$.*

Démonstration. Soient $x, y \in \mathbb{R}$ avec $x < y$. Alors $x' = x - \sqrt{2}$ et $y' = y - \sqrt{2}$ vérifient ces mêmes propriétés.
Par densité de $\mathbb{Q}$ dans $\mathbb{R}$, il existe $r' \in \mathbb{Q}$ tel que : $x' < r' < y'$.
Et donc, en posant $r = r' + \sqrt{2}$, on a : $x < r < y$.
Reste à montrer que $r \in \mathbb{R} \setminus \mathbb{Q}$: par l'absurde, si on avait $r \in \mathbb{Q}$, alors on aurait que : $\sqrt{2} = r - r'$ serait la différence de deux rationnels, donc serait un rationnel. D'où la contradiction. □

III La droite achevée

Définition III.1. *On appelle **droite achevée**, notée $\overline{\mathbb{R}}$, l'ensemble : $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty; +\infty\} = [-\infty; +\infty]$.*
On prolonge l'ordre sur $\mathbb{R}$ à $\overline{\mathbb{R}}$ en posant : $\forall x \in \overline{\mathbb{R}},\ -\infty \leq x \leq +\infty$.
On prolonge les opérations usuelles de $\mathbb{R}$ à $\overline{\mathbb{R}}$ en posant :

1. $\forall x \in \mathbb{R}$: $x + (-\infty) = -\infty$ *et* $x + (+\infty) = +\infty$;
2. $-\infty + (-\infty) = -\infty$ *et* $+\infty + (+\infty) = +\infty$;
3. $\forall x \in \mathbb{R}_+^*$: $x \times (+\infty) = +\infty$ *et* $x \times (-\infty) = -\infty$;
4. $\forall x \in \mathbb{R}_-^*$: $x \times (+\infty) = -\infty$ *et* $x \times (-\infty) = +\infty$;
5. $+\infty \times (+\infty) = -\infty \times (-\infty) = +\infty$ *et* $+\infty \times (-\infty) = -\infty \times (+\infty) = -\infty$;
6. $\forall x \in \mathbb{R}$: $\dfrac{x}{+\infty} = \dfrac{x}{-\infty} = 0$;
7. $\forall x \in \overline{R},\ x \neq 0$: $\left|\dfrac{x}{0}\right| = \infty$.

Remarque III.2. *Les autres opérations, comme $+\infty + (-\infty)$ ou $0 \times \pm\infty$ sont des **formes indéterminées** : elles ne sont pas bien définies.*

Proposition III.3. *Tout intervalle I de $\mathbb{R}$ est de la forme $]a; b[$, $]a; b]$, $[a; b[$ ou $[a; b]$ pour $a, b \in \overline{R}$.*
Et dans ce cas, si ces quantités sont définies, on a : $\sup(I) = b$ *et* $\inf(I) = a$.

Démonstration. Par disjonction de cas, selon les différentes formes d'intervalle. □

Chapitre 14

Suites numériques

I Généralités

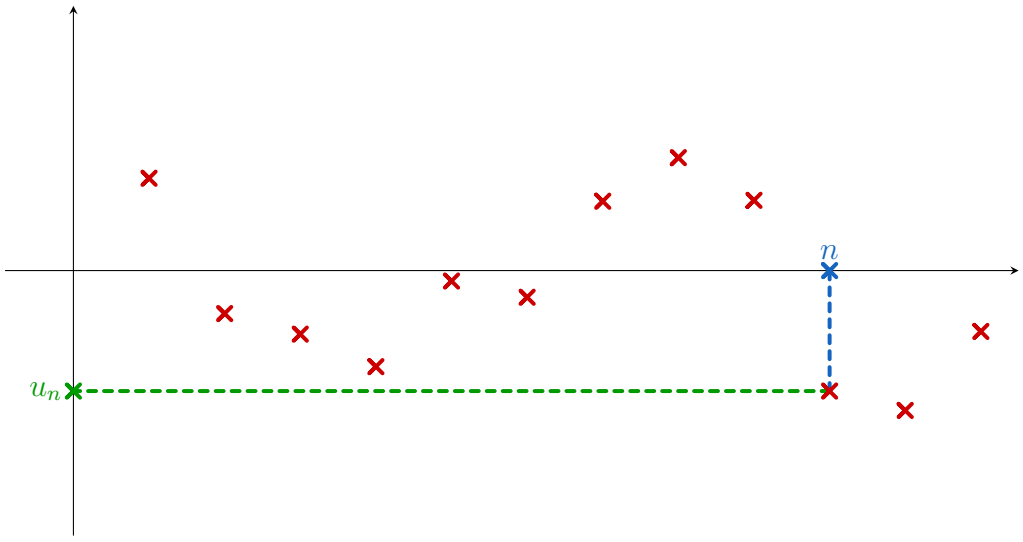
Dans cette partie $\mathbb{K}$ désignera $\mathbb{R}$ ou $\mathbb{C}$.

Définition I.1. *On appelle* ***suite numérique*** *une famille $(u_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ indexée par $\mathbb{N}$.*
On notera plus simplement u ou (u_n) la suite, et u_n est le ***terme général*** *de u.*

Remarque I.2. *On pourra indexer une suite par $\mathbb{N}$ privé de ses premiers éléments. Par exemple, une suite indexée par $\mathbb{N}\setminus[\![0;n_0[\![$ sera notée : $(u_n)_{n\geq n_0}$.*

Exemples I.3. *Une suite peut être définie de différentes manières :*
- ***explicite****, avec une formule : $\forall n\in\mathbb{N},\ u_n = n^2+3n+1$;*
- ***implicite*** *: $\forall n\in\mathbb{N}$, u_n est l'unique solution positive de l'équation $x^n+nx-1=0$;*
- ***par récurrence*** *: $u_0 = 10$ et $\forall n\in\mathbb{N},\ u_{n+1} = \sin(u_n)$.*

Remarque I.4. *On peut voir une suite comme une fonction $u:\mathbb{N}\to\mathbb{R}$, et la représenter comme telle :*



Définition I.5. *Si u, v sont deux suites numériques et $\lambda\in\mathbb{K}$, on définit les suites $u+v$, λu et $u\times v$ par :*

$$\forall n\in\mathbb{N},\ \begin{cases} (u+v)_n &= u_n+v_n \\ (\lambda u)_n &= \lambda u_n \\ (u\times v)_n &= u_n\times v_n \end{cases}.$$

Définition I.6. *Les indices $n\in\mathbb{N}$ sont appelés les* ***rangs*** *de la suite.*
On dira qu'une suite $(u_n)_{n\in\mathbb{N}}$ vérifie une propriété ***à partir d'un certain rang*** *s'il existe $n_0\in\mathbb{N}$ tel que la suite $(u_n)_{n\geq n_0}$ vérifie cette propriété.*

Exemple I.7. *La suite $(u_n) = (n!)$ est paire à partir du rang 2.*

Définition I.8. *On dira qu'une suite u est **constante** si elle ne prend qu'une seule valeur.*
*On dira qu'une suite est **stationnaire** si elle est constante à partir d'un certain rang.*

Définition I.9. *On dira qu'une suite réelle u est :*
- ***majorée** s'il existe un réel M tel que : $\forall n \in \mathbb{N},\ u_n \leq M$;*
- ***minorée** s'il existe un réel m tel que : $\forall n \in \mathbb{N},\ u_n \geq m$;*
- ***bornée** si elle est majorée et minorée.*

Remarque I.10. *Il faut bien faire attention à ce que les majorants ou minorants **ne dépendent pas** de n.*

Proposition I.11. *La suite (u_n) est bornée si, et seulement si,la suite $(|u_n|)$ est majorée.*

Démonstration. Comme pour les fonctions. □

Définition I.12. *On dira qu'une suite réelle u est :*

1. ***croissante** si : $\forall n \in \mathbb{N},\ u_{n+1} \geq u_n$;*
2. ***décroissante** si : $\forall n \in \mathbb{N},\ u_{n+1} \leq u_n$;*
3. ***strictement croissante** si : $\forall n \in \mathbb{N},\ u_{n+1} > u_n$;*
4. ***strictement décroissante** si : $\forall n \in \mathbb{N},\ u_{n+1} < u_n$.*

*Dans les deux premiers cas, u sera dite **monotone**, et **strictement monotone dans les autres cas**.*

Remarque I.13. *En pratique, pour étudier la monotonie d'une suite, on étudie le signe de la suite $(u_{n+1} - u_n)$. Si la suite (u_n) est de signe constant, on peut aussi étudier la suite $\left(\frac{u_{n+1}}{u_n}\right)$ (en faisant attention au signe de u_n).*

Exemple I.14. *Étudions la monotonie de la suite : $(u_n) = \left(\dfrac{n+1}{n+2}\right)$.*
La suite u_n a tous ses termes strictement positifs. Et pour tout $n \in \mathbb{N}$ on a :

$$\frac{u_{n+1}}{u_n} = \frac{\frac{n+2}{n+3}}{\frac{n+1}{n+2}} = \frac{(n+2)^2}{(n+1)(n+3)} = \frac{n^2+4n+4}{n^2+4n+3} > 1$$

et ainsi : $u_{n+1} > u_n$, donc la suite (u_n) est strictement croissante.

Définition I.15. *Un suite (u_n) est dite périodique s'il existe $N \in \mathbb{N}^*$ tel que :*

$$\forall n \in \mathbb{N},\ u_{n+N} = u_n.$$

Proposition I.16. *Une suite périodique (ou périodique à partir d'un certain) ne prend qu'un nombre fini de valeurs.*

Démonstration. Si $n \in \mathbb{N}$, on écrit $n = Nq + r$ la division euclidienne de n par N. Alors $u_n = u_r \in \{u_0, \ldots, u_{N-1}\}$.
Le cas général en découle en rajoutant les premières valeurs de la suite. □

Remarque I.17. *De fait, les suites périodiques ne présentent pas un grand intérêt...*

II Limite d'une suite réelle

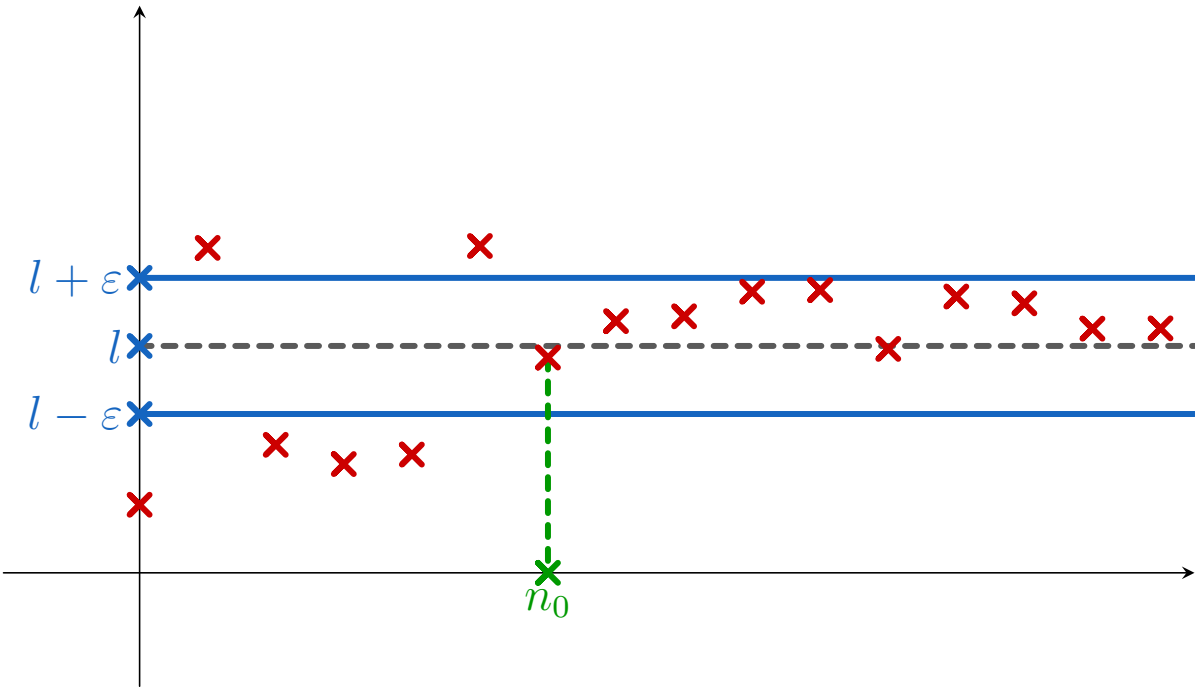
II.1 Limites finies ou infinies

Définition II.1. *Si (u_n) est une suite réelle, et $l \in \mathbb{R}$, on dit que la suite (u_n)* ***converge vers*** *l si :*

$$\forall \varepsilon > 0,\ \exists n_0 \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geq n_0 \Rightarrow |u_n - l| \leq \varepsilon.$$

On écrira alors : $\lim\limits_{n\to+\infty} u_n = l$ *(ou plus simplement* $\lim u_n = l$*) ou* $u_n \underset{n\to+\infty}{\to} l$.
Plus généralement, on dira que la suite (u_n) est ***convergente*** *si elle converge vers un réel l, et* ***divergente*** *sinon.*

Remarque II.2. *Cela revient à dire que : pour tout $\varepsilon > 0$, l'intervalle $[l-\varepsilon; l+\varepsilon]$ contient tous les termes de la suites à partir d'un certain rang.*



Remarques II.3.

1. *En pratique, on montre que la suite $(|u_n - l|)$ converge vers 0.*
2. *Toute la subtilité sera de trouver les bons ε, en étant sûr que $\varepsilon > 0$, ou de trouver un n_0 convenable.*

Exemple II.4. *Montrons que la suite $(\frac{1}{n})_{n\geq 1}$ converge vers 0 :*
Soit $\varepsilon > 0$. Alors $n_0 = \lfloor \frac{1}{\varepsilon} \rfloor + 1$ convient car $n_0 > \frac{1}{\varepsilon}$ et :

$$n \geq n_0 \Rightarrow n \geq \frac{1}{\varepsilon} \Rightarrow 0 \leq \frac{1}{n} \leq \varepsilon \Rightarrow |\frac{1}{n} - 0| \leq \varepsilon.$$

Proposition II.5 (unicité de la limite)**.** *Si une suite converge, alors sa limite est unique.*

Démonstration. Par l'absurde, supposons que la suite (u_n) converge simultanément vers $l_1, l_2 \in \mathbb{R}$ avec $l_1 \neq l_2$.
Posons $\varepsilon = \dfrac{|l_1 - l_2|}{3}$ et utilisons la définition de la limite :

- il existe n_1 tel que : $n \geq n_1 \Rightarrow |u_n - l_1| \leq \varepsilon$;
- il existe n_2 tel que : $n \geq n_2 \Rightarrow |u_n - l_2| \leq \varepsilon$.

Posons $N = n_1 + n_2$. Alors $N \geq n1$ et $N \geq n_2$. Mais par inégalité triangulaire :

$$3\varepsilon = |l_1 - l_2| = |l_1 - u_N + u_N - l_2| \leq |l_1 - u_N| + |l_2 - u_N| \leq 2\varepsilon$$

d'où la contradiction.
Donc $l_1 = l_2$. □

Proposition II.6. *Toute suite convergente est bornée.*

Démonstration. Soit (u_n) une suite convergente de limite l. Avec $\varepsilon = 1$, il existe $n_0 \in \mathbb{N}$ tel que : $n \geq n_0 \Rightarrow |u_n - l| \leq 1$. Et donc :

$$\forall n \geq n_0,\ |u_n| = |u_n - l + l| \leq |u_n - l| + |l| \leq |l| + 1.$$

Donc $M = \max\{1 + |l|, |u_0|, |u_1|, \ldots, |u_{n_0-1}|\}$ est un majorant de $(|u_n|)$: la suite (u_n) est donc bornée.
Le point important dans la preuve est que M existe bien car tout ensemble fini de réels admet un maximum. □

Remarques II.7.

1. *La réciproque est évidemment fausse : la suite $(u_n) = (-1)^n$ est bornée mais ne converge pas.*
2. *L'idée de la preuve est qu'une suite est bornée si elle l'est à partir d'un certain rang ; et c'est clairement le cas pour une suite convergente.*

Proposition II.8. *Si (u_n) converge vers $l \neq 0$, alors tous les termes sont du signe de l (et ne s'annulent pas) à partir d'un certain rang.*

Démonstration. On utilise $\varepsilon = \dfrac{|l|}{2}$. À partir d'un certain rang, les termes sont dans $\left[\dfrac{l}{2}; \dfrac{3l}{2}\right]$ ou $\left[\dfrac{3l}{2}; \dfrac{l}{2}\right]$ selon le signe de l. □

Remarques II.9.

1. *On utilisera plutôt que, si u converge vers $l > 0$, alors u est strictement positive à partir d'un certain rang.*
2. *Le résultat montré est plus fort en fait : si $l > 0$, alors il existe $m > 0$ tel que u est minorée par m à partir d'un certain rang ; si $l < 0$, il existe $M < 0$ tel que u est majorée par M à partir d'un certain rang. Ce résultat est plus fort dans le sens où la suite $\left(\frac{1}{u_n}\right)$ est ainsi bornée.*

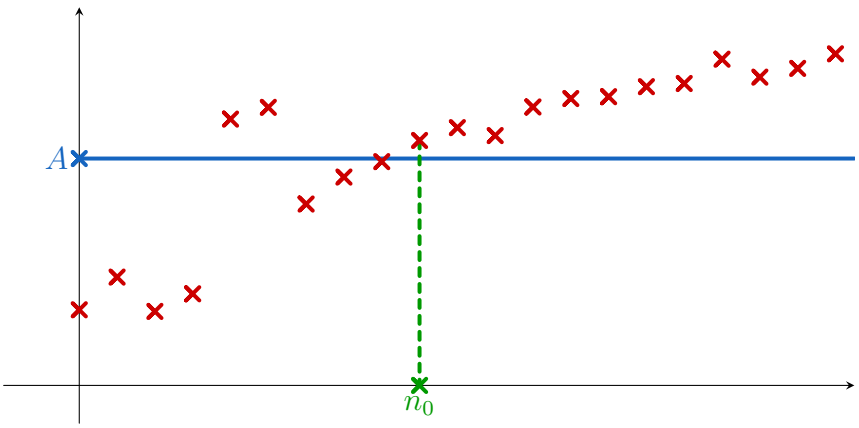
Définition II.10. *On dit qu'une suite réelle (u_n)* ***tend vers*** *$+\infty$ si :*

$$\forall A \in \mathbb{R},\ \exists n_0 \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geq n_0 \Rightarrow u_n \geq A.$$

On écrira alors : $\lim\limits_{n\to+\infty} u_n = +\infty$ (ou plus simplement $\lim u_n = +\infty$) ou $u_n \underset{n\to+\infty}{\to} +\infty$.
De même, on dit qu'une suite (u_n) ***tend vers*** *$-\infty$ si :*

$$\forall A \in \mathbb{R},\ \exists n_0 \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geq n_0 \Rightarrow u_n \leq A.$$

et on utilisera les notations idoines.



Exemple II.11. *Montrons que la suite $(\sqrt{n})$ tend vers $+\infty$:*
Soit $A \in \mathbb{R}$. Alors $n_0 = \lfloor A^2 \rfloor + 1$ convient car $n_0 > A^2$ et ainsi :

$$n \geq n_0 \Rightarrow n \geq A^2 \Rightarrow \sqrt{n} \geq \sqrt{A^2} = |A| \geq A.$$

Proposition II.12. *Soit (u_n) une suite réelle :*

1. *si (u_n) tend vers $+\infty$: alors elle est minorée, et elle n'est pas majorée ;*
2. *si (u_n) tend vers $-\infty$: alors elle est majorée, et elle n'est pas minorée.*

Démonstration. Le fait de ne pas être majorée ou minorée découle de la définition.
Montrons qu'une suite qui tend vers $+\infty$ est minorée. Prenons la définition avec $A = 0$. Il existe n_0 tel que : $n \geq n_0 \Rightarrow u_n \geq 0$. Donc (u_n) est minorée par : $m = \min\{u_0, u_1, \ldots, u_{n_0-1}, 0\}$. □

Corollaire II.13. *Une suite ayant une limite est majorée ou minorée.*

Démonstration. Par disjonction de cas suivant que la limite est finie ou non. □

II.2 Opérations sur les limites

Théorème II.14. *Si u, v sont deux suites réelles avec $\lim u = l$ et $\lim v = l'$ (pour $l, l' \in \overline{R}$), et $\lambda \in \mathbb{R}$ alors, sous réserve que les quantités ci-dessous soient bien définies :*

1. *la suite $(u + v)$ a pour limite $l + l'$;*
2. *la suite (λu) a pour limite λl ;*
3. *la suite (uv) a pour limite $l \times l'$;*
4. *si $l' \neq 0$, la suite $\dfrac{u}{v}$ est bien définie à partir d'un certain rang, et a pour limite $\dfrac{l}{l'}$.*

Remarque II.15. *Il faudra bien prendre garde aux* ***formes indéterminées*** *(les opérations interdites dans $\overline{\mathbb{R}}$). Par exemple, si $l = +\infty$ et $l' = -\infty$, la suite $w = u + v$ peut avoir tout type de comportement :*
— *si $(u_n) = n$ et $(v_n) = -n$: w est stationnaire ;*
— *si $(u_n) = 2n$ et $(v_n) = -n$: w tend vers $+\infty$;*
— *si $(u_n) = n$ et $(v_n) = -2n$: w tend vers $-\infty$;*
— *si $(u_n) = n$ et $(v_n) = (-1)^n - n$: w n'a même pas de limite.*

Démonstration (de quelques cas) :

1. notons que $l + l'$ est bien défini à moins que $l = \pm\infty$ et $l' = -l$:
   — si $l, l' \in \mathbb{R}$: on veut montrer que $(u + v)$ converge vers $l + l' \in \mathbb{R}$. Soit $\varepsilon > 0$. Si $n \in \mathbb{N}$:

$$|(u_n + v_n) - (l + l')| = |(u_n - l) + (v_n - l')| \leq |u_n - l| + |v_n - l'|.$$

   On applique les définitions des limites pour u et v avec $\dfrac{\varepsilon}{2} > 0$:

$$\begin{cases} \exists n_1 \in \mathbb{N},\ \forall n \geq n_1,\ |u_n - l| \leq \frac{\varepsilon}{2} \\ \exists n_2 \in \mathbb{N},\ \forall n \geq n_2,\ |v_n - l'| \leq \frac{\varepsilon}{2} \end{cases}$$

   et ainsi, en posant $n_0 = \max(n_1, n_2)$, pour tout $n \geq n_0$ on a :

$$|(u_n + v_n) - (l + l')| \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

   donc $(u + v)$ tend bien vers $(l + l')$.

— si $l = +\infty$ et $l' \neq -\infty$: alors u tend vers $+\infty$, et v est nécessairement minorée (elle est soit convergente, soit elle tend vers $+\infty$). Donc $u+v$ tend bien vers $l+l' = +\infty$ d'après la proposition suivante.
— si $l = -\infty$ et $l' \neq +\infty$: même constat.

2. la seule forme indéterminée est serait $\lambda = 0$ et $l = \pm\infty$, mais en fait λu serait la suite stationnaire (de valeur 0), qui converge vers 0. On considère donc $\lambda \neq 0$:
— si $l \in \mathbb{R}$: on veut montrer que (λu) converge vers $\lambda l \in \mathbb{R}$. Soit $\varepsilon > 0$. Si $n \in \mathbb{N}$:

$$|\lambda u_n - \lambda l| = |\lambda| \times |u_n - l|.$$

On applique la définition de la limite de u à $\frac{\varepsilon}{|\lambda|} > 0$, donc il existe n_0 tel que : $n \geq n_0 \Rightarrow |u_n - l| \leq \frac{\varepsilon}{|\lambda|}$.
Et donc : $n \geq n_0 \Rightarrow |\lambda u_n - \lambda l| < \varepsilon$. Donc (λu) tend bien vers λl.
— si $l = +\infty$: on veut montrer que (λu) converge vers $\lambda l = \text{signe}(\lambda)\infty$. Soit $A \in \mathbb{R}$. On applique la définition de la limite de u à $\frac{A}{\lambda}$, donc il existe n_0 tel que : $n \geq n_0 \Rightarrow u_n \geq \frac{A}{\lambda}$. Et donc :

$$n \geq n_0 \Rightarrow \begin{cases} \lambda u_n \geq A & \text{si} \quad \lambda > 0 \\ \lambda u_n \leq A & \text{si} \quad \lambda < 0 \end{cases}.$$

donc λu tend bien vers $\lambda l = \begin{cases} +\infty & \text{si} \quad \lambda > 0 \\ -\infty & \text{si} \quad \lambda < 0 \end{cases}$.

3. les formes indéterminées sont si $l = \pm\infty$ et $l' = 0$ (ou l'inverse) :
— si $l, l' \in \mathbb{R}$: on veut montrer que (uv) converge vers $ll' \in \mathbb{R}$. Soit $\varepsilon > 0$. Si $n \in \mathbb{N}$:

$$|(u_n v_n) - (ll')| = |u_n v_n - l v_n + l v_n - ll'| = |(u_n - l)v_n + l(v_n - l')| \leq |v_n||u_n - l| + |l||v_n - l'|.$$

Comme v est convergente, alors elle est bornée, et il existe donc $M \in \mathbb{R}$ tel que : $\forall n \in \mathbb{N},\ |v_n| \leq M$. Posons $a = \max(M, |l|, 1) > 0$.
On applique la définition des limites de u et v à $\frac{\varepsilon}{2a} > 0$:

$$\begin{cases} \exists n_1 \in \mathbb{N},\ \forall n \geq n_1,\ |u_n - l| \leq \frac{\varepsilon}{2a} \\ \exists n_2 \in \mathbb{N},\ \forall n \geq n_2,\ |v_n - l'| \leq \frac{\varepsilon}{2a} \end{cases}$$

En prenant $n_0 = \max(n_1, n_2)$, pour tout $n \geq n_0$, on a :

$$|u_n v_n - ll'| \leq a\frac{\varepsilon}{2a} + a\frac{\varepsilon}{2a} = \varepsilon.$$

Donc (uv) converge bien vers ll'.
— pour les autres cas : on aura toujours une des suites qui tend vers $\pm\infty$ et l'autre qui est minorée par un nombre strictement positif ou majorée par un nombre strictement négatif à partir d'un certain rang. Donc le résultat découle d'une proposition suivante.

4. grâce à la limite d'un produit, il suffit de montrer que $\frac{1}{u}$ tend vers $\frac{1}{l}$:
— si $l \in \mathbb{R}^*$: on veut montrer que $\frac{1}{u}$ converge vers $\frac{1}{l} \in \mathbb{R}$. Soit $\varepsilon > 0$. Comme $l \neq 0$, il existe un rang n_1 tel que : $n \geq n_1 \Rightarrow |u_n| \geq \frac{|l|}{2} > 0$, ce qui assure déjà que u est bien définie à partir d'un certain rang.
Si $n \geq n_1$, on a :

$$\left|\frac{1}{u_n} - \frac{1}{l}\right| = \left|\frac{l - u_n}{l u_n}\right| \leq 2\frac{|u_n - l|}{l^2}.$$

On applique la définition de la limite de u à $\varepsilon\frac{l^2}{2}$ donc il existe n_2 tel que : $n \geq n_2 \Rightarrow |u_n - l| \leq \varepsilon\frac{l^2}{2}$.
D'où, avec $n_0 = \max(n_1, n_2)$:

$$\forall n \geq n_0,\ \left|\frac{1}{u_n} - \frac{1}{l}\right| \leq \varepsilon.$$

Donc $\frac{1}{u}$ converge vers $\frac{1}{l}$.

— si $l = +\infty$: on veut montrer que $\frac{1}{u}$ converge vers 0. Soit $\varepsilon > 0$.
On applique la définition de la limite de u à $A = \frac{1}{\varepsilon} > 0$. Il existe un rang n_0 tel que : $n \geq n_0 \Rightarrow u_n \geq \frac{1}{\varepsilon} > 0$. Ce qui assure que u est bien définie à partir d'un certain rang.
Et donc :

$$n \geq n_0 \Rightarrow \left|\frac{1}{u_n}\right| = \frac{1}{u_n} \leq \varepsilon.$$

Donc $\frac{1}{u}$ tend bien vers 0.

□

Remarque II.16. *Une autre manière de dire est que les limites se comportent bien avec les opérations dans $\overline{R}$: la limite d'une somme est la somme des limites, la limite d'un produit est le produit des limites, etc.*

Proposition II.17 (Limites d'autres sommes)**.** *Si u, v sont deux suites réelles :*

1. *si u est minorée et que v tend vers $+\infty$, alors $u + v$ tend vers $+\infty$;*
2. *si u est majorée et que v tend vers $-\infty$, alors $u + v$ tend vers $-\infty$.*

Démonstration. Montrons le premier cas. Soit m un minorant de u, donc : $\forall n \in \mathbb{N},\ u_n \geq m$.
Soit $A \in \mathbb{R}$. On applique la définition de la limite de v avec $A - m$, donc il existe n_0 tel que : $n \geq n_0 \Rightarrow v_n \geq A - m$.
Et donc : $\forall n \geq n_0,\ (u_n + v_n) \geq m + (A - m) = A$.
Donc $(u + v)$ tend vers $+\infty$. □

Proposition II.18 (Limites d'autres produits)**.** *Si u, v sont deux suites réelles :*

1. *si u est bornée et que v converge vers 0, alors uv converge vers 0 ;*
2. *si u est minorée par $m > 0$ à partir d'un certain rang et que v tend vers $\pm\infty$, alors uv a même limite que v ;*
3. *si u est majorée par $M < 0$ à partir d'un certain rang et que v tend vers $\pm\infty$, alors uv a une limite opposée à celle de v.*

Démonstration. 1. notons $M > 0$ un majorant de $|u|$, donc : $\forall n \in \mathbb{N},\ |u_n| \leq M$.
Soit $\varepsilon > 0$. On applique la définition de la limite de v avec $\frac{\varepsilon}{M} > 0$, donc il existe n_0 tel que : $n \geq n_0 \Rightarrow |v_n| \leq \frac{\varepsilon}{M}$.
Et donc : $\forall n \geq n_0,\ |u_n v_n| = |u_n| \cdot |v_n| \leq \varepsilon$.
Donc (uv) converge bien vers 0.

2. si $\lim v = +\infty$: soit $A > 0$. Notons $n_1, n_2 \in \mathbb{N}$ tels que :

$$\begin{cases} \forall n \geq n_1,\ u_n \geq m > 0 \\ \forall n \geq n_2,\ v_n \geq \frac{|A|}{m} > 0 \end{cases}$$

Et donc, avec $n = \max(n_1, n_2)$, on a :

$$n \geq n_0 \Rightarrow u_n v_n \geq m v_n \geq m\frac{|A|}{m} = |A| \geq A$$

donc uv tend bien vers $+\infty$.

3. idem.

□

Proposition II.19 (Limite de valeurs absolues)**.** *Si u a pour limite $l \in \overline{\mathbb{R}}$, alors $|u|$ a pour limite $|l|$.*

Démonstration. — si $l \in \mathbb{R}$: alors pour tout $n \in \mathbb{N}$: $||u_n| - |l|| \leq |u_n - l|$ (par inégalité triangulaire).
Si $\varepsilon > 0$, il existe $n_0 \in \mathbb{N}$ tel que : $n \geq n_0 \Rightarrow |u_n - l| \leq \varepsilon$.
Et donc : $n \geq n_0 \Rightarrow ||u_n| - |l|| \leq \varepsilon$, donc $|u|$ converge vers $|l|$.
— si $l = +\infty$: soit $A \in \mathbb{R}$. Par définition de la limite de u avec $|A|$, il existe n_0 tel que : $n \geq n_0 \Rightarrow u_n \geq |A| \geq 0$.
Et donc : $n \geq n_0 \Rightarrow |u_n| = u_n \geq |A| \geq A$.

□

Remarque II.20. *La réciproque est fausse en générale (reprendre la suite $(u_n) = ((-1)^n)$). Elle est vraie si $l = 0$:* $\lim u = 0 \Leftrightarrow \lim |u| = 0$.

Proposition II.21 (Limites d'autres quotients)**.** *Si u est une suite réelle :*

1. *si u a tous ses termes strictement positifs à partir d'un certain rang et converge vers 0, alors $\frac{1}{u}$ tend vers $+\infty$;*
2. *si u a tous ses termes strictement négatifs à partir d'un certain rang et converge vers 0, alors $\frac{1}{u}$ tend vers $-\infty$.*

Démonstration. Montrons le premier cas.
Soit $A \in \mathbb{R}$.
Notons n_1 tel que : $n \geq n_1 \Rightarrow u_n > 0$.
Il existe n_2 tel que : $n \geq n_2 \Rightarrow |u_n| \leq \dfrac{1}{|A|+1}$.
Et donc, avec $n_0 = \max(n_1, n_2)$: $n \geq n_0 \Rightarrow 0 < u_n \leq |u_n| \leq \dfrac{1}{|A|+1} \Rightarrow \dfrac{1}{u_n} \geq |A| + 1 \geq A$.
Donc $\frac{1}{u}$ tend vers $+\infty$. □

Corollaire II.22. *Soit u une suite réelle qui ne s'annule plus à partir d'un certain rang.*
Alors $|u|$ tend vers $+\infty$ si, et seulement si, $\frac{1}{u}$ converge vers 0.

Corollaire II.23. *Si u converge vers $l \neq 0$ et si v tend vers 0, alors la suite $\left|\frac{u}{v}\right|$ tend vers $+\infty$.*

Démonstration. Il suffit de voir que $\frac{v}{u}$ tend vers 0. Mais, comme u tend vers $l \neq 0$, alors $\frac{1}{u}$ converge, donc est bornée. Donc $\frac{v}{u} = v \times \frac{1}{u}$ tend vers 0. □

III Limites et inégalités

III.1 Liens entre inégalités et limites

Proposition III.1. *Si u et v sont deux suites réelles convergentes telles que : $\forall n \in \mathbb{N},\ u_n \leq v_n$, alors* $\lim u \leq \lim v$.
Si de plus : $\forall n \in \mathbb{N},\ u_n < v_n$, alors $\lim u \leq \lim v$.

Démonstration. Notons $l = \lim u$ et $l' = \lim v$. Par opérations sur les limites :
— la suite $v - u$ converge vers $l' - l$;
— la suite $|v - u|$ converge vers $|l' - l|$.
Mais ces deux suites sont égales par l'inégalité. Par unicité de la limite, on déduit que : $|l' - l| = l' - l$. Et ainsi : $l' \geq l$. □

Remarques III.2.

1. *on ne peut pas avoir d'inégalité stricte en passant à la limite : par exemple prendre $u = 0$ (la suite nulle) et $(v_n) = (\frac{1}{n})$;*
2. *il suffit en fait d'avoir $u_n \leq v_n$ à partir d'un certain rang ;*
3. *en pratique, on l'utilisera avec u ou v qui est une suite constante.*

Théorème III.3 (Théorème d'encadrement, ou des gendarmes)**.** *Si u, v, w sont des suites réelles telles que :*

$$\forall n \in \mathbb{N},\ u_n \leq v_n \leq w_n.$$

Si les suites u et w convergent vers une même limite l, alors v converge aussi vers l.

Démonstration. Soit $\varepsilon > 0$. Par définition des limites de u et w :

$$\begin{cases} \exists n_1 \in \mathbb{N},\ n \geq n_1 \Rightarrow |u_n - l| \leq \varepsilon & \text{donc } l - \varepsilon \leq u_n \\ \exists n_2 \in \mathbb{N},\ n \geq n_2 \Rightarrow |w_n - l| \leq \varepsilon & \text{donc } w_n \leq l + \varepsilon \end{cases}.$$

En posant $n_0 = \max(n_1, n_2)$, on a :

$$n \geq n_0 \Rightarrow l - \varepsilon \leq u_n \leq v_n \leq w_n \leq l + \varepsilon \text{ donc } |v_n - l| \leq \varepsilon$$

donc v_n converge vers l. □

Remarque III.4. *Il suffit en fait d'avoir l'inégalité à partir d'un certain rang.*

Exemples III.5.

1. *montrons que la suite $(u_n) = \left(\frac{\sin(n)}{n}\right)$ tend vers 0.*
   Pour tout $n \in \mathbb{N}^*$, on a : $\frac{-1}{n} \leq u_n \leq \frac{1}{n}$.
   Les suites de terme général $\frac{-1}{n}$ et $\frac{1}{n}$ convergent vers 0, donc u converge vers 0 par encadrement.
2. *étudions la limite de la suite u de terme général : $u_n = \frac{n}{n^2+1} + \frac{n}{n^2+2} + \cdots + \frac{n}{n^2+n} = \sum_{k=1}^{n} \frac{n}{n^2+k}$.*
   Pour tout $k \in [\![1; n]\!]$: $\frac{n}{n^2+n} \leq \frac{n}{n^2+k} \leq \frac{n}{n^2+1}$.
   Donc en sommant pour k allant de 1 à n : $\frac{n^2}{n^2+n} \leq u_n \leq \frac{n^2}{n^2+1}$.
   Mais $\frac{n^2}{n^2+n} = \frac{1}{1+\frac{1}{n}} \to \frac{1}{1+0} = 1$ et $\frac{n^2}{n^2+1} = \frac{1}{1+\frac{1}{n^2}} \to 1$: donc par encadrement u tend vers 1.

Proposition III.6 (Divergence par minoration ou majoration)**.** *Soient u, v deux suites réelles telles que : $\forall n \in \mathbb{N},\ u_n \leq v_n$. Alors :*

1. *si u tend vers $+\infty$, alors v aussi ;*
2. *si v tend vers $-\infty$, alors u aussi.*

Démonstration. Montrons le premier cas. Soit $A \in \mathbb{R}$. Il existe $n_0 \in \mathbb{N}$ tel que ; $n \geq n_0 \Rightarrow u_n \geq A$. Et donc : $n \geq n_0 \Rightarrow v_n \geq A$. □

III.2 Suites monotones et suites adjacentes

Théorème III.7 (de la limite monotone)**.**

1. *Soit u une suite croissante :*
   — *si u est majorée : elle converge vers $\sup\{u_n \,|\, n \in \mathbb{N}\}$;*
   — *si u n'est pas majorée : alors u tend vers $+\infty$.*
2. *Soit u une suite décroissante :*
   — *si u est minorée : elle converge vers $\inf\{u_n \,|\, n \in \mathbb{N}\}$;*
   — *si u n'est pas minorée : alors u tend vers $-\infty$.*

Démonstration. Montrons pour une suite croissante.
- si u est majorée : notons $l = \sup\{u_n \,|\, n \in \mathbb{N}\}$, et prenons $\varepsilon > 0$.
  Par caractérisation de la borne supérieure, on déduit que : il existe $n_0 \in \mathbb{N}$ tel que $l - \varepsilon \leq u_{n_0} \leq l$.
  Mais u est croissante et majorée par l, donc pour tout $n \geq n_0$: $u_{n_0} \leq u_n \leq l$.
  Et donc pour tout $n \geq n_0$: $l - \varepsilon \leq u_n \leq l$, donc $|u_n - l| \leq \varepsilon$.
- si u n'est pas majorée : soit $A \in \mathbb{R}$. Alors il existe $n_0 \in \mathbb{N}$ tel que $u_{n_0} \geq A$ (sinon A serait un majorant de u).
  Par croissance, on a donc : $n \geq n_0 \Rightarrow u_n \geq u_{n_0} \geq A$, donc u tend vers $+\infty$.

□

Exemple III.8. *Étudions la suite de terme général :* $u_n = 1 + \frac{1}{2^2} + \cdots + \frac{1}{n^2} = \sum_{k=1}^{n} \frac{1}{k^2}$.
- *u est croissante : si* $n \in \mathbb{N}$, $u_{n+1} - u_n = \frac{1}{(n+1)^2} > 0$;
- *u est majorée par 2 : si* $k \in \mathbb{N}^* \setminus \{1\}$, $\frac{1}{k^2} \leq \frac{1}{k(k-1)} = \frac{1}{k-1} - \frac{1}{k}$. *Et ainsi :*

$$\begin{array}{rcl} u_n & = & \sum_{k=1}^{n} \frac{1}{k^2} = 1 + \sum_{k=2}^{n} \frac{1}{k^2} \\ & \leq & 1 + \sum_{k=2}^{n} \left(\frac{1}{k-1} - \frac{1}{k}\right) \\ & \leq & 1 + \left(1 - \frac{1}{n}\right) = 2 - \frac{1}{n} \leq 2 \end{array}$$

Donc u converge, et sa limite l vérifie : $l \leq 2$. (en fait sa limite vaut $\frac{\pi^2}{6} \simeq 1.65$.

Remarque III.9. *Le majorant utilisé n'est pas toujours la limite de la suite.*

Corollaire III.10. *Toute suite réelle monotone a une limite (finie ou non).*

Théorème-Définition III.11. *Soient u, v deux suites réelles telles que :*

1. *u est croissante ;*
2. *v est décroissante ;*
3. $\lim (u_n - v_n) = 0$.

Alors on dit que u et v sont ***adjacentes****.*
Sous ces conditions, u et v convergent vers une même limite l, qui est l'unique réel vérifiant :

$$\forall n, m \in \mathbb{N},\ u_n \leq l \leq v_m.$$

Démonstration. Comme u est croissante et v est décroissante, alors la suite $u - v$ est croissante. Comme elle converge vers 0, on déduit que : 0 est un majorant de $u - v$, donc $u - v$ est toujours négative ou nulle. Ainsi : $\forall n \in \mathbb{N},\ u_n \leq v_n$.
En utilisant à nouveau les monotonies, on a :

$$\forall n \in \mathbb{N},\ u_0 \leq u_n \leq v_n \leq v_0$$

donc :
- la suite u est croissante, majorée par v_0, donc converge vers un réel l ;
- la suite v est décroissante, minorée par u_0, donc converge vers un réel l' ;
- $\lim (u_n - v_n) = l' - l = 0$.

Donc u et v convergent toutes les deux vers l.
Par monotonies de u et v, on a :

$$\sup\{u_n \,|\, n \in \mathbb{N}\} = l = \inf\{v_n \,|\, n \in \mathbb{N}\}$$

ce qui justifie déjà que : $\forall n, m \in \mathbb{N},\ u_n \leq l \leq v_m$.
Si l' vérifie les mêmes inégalités, alors :
- l' est un majorant de u, donc : $l \leq l'$;

— l' est un minorant de v, donc : $l' \leq l$.
Donc $l = l'$, ce qui assure l'unicité. □

Remarque III.12. *Si les suites u, v sont strictement monotones, on peut mettre des inégalités strictes à la fin.*

Exemple III.13. *Démonstration de l'irrationalité de e.*

1. *On considère les suites u, v définies par :*

$$u_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} \text{ et } v_n = u_n + \frac{1}{n \cdot n!}.$$

Alors :
— $u_{n+1} - u_n = \frac{1}{(n+1)!} > 0$, *donc u est strictement croissante ;*
— $v_{n+1} - v_n = (u_{n+1} - u_n) + \frac{1}{(n+1)((n+1)!)} - \frac{1}{n \cdot n!} = \frac{1}{(n+1)!} + \frac{1}{(n+1)((n+1)!)} - \frac{1}{n \cdot n!} = \frac{n(n+1)+n-(n+1)^2}{n(n+1)((n+1)!)} = \frac{-1}{n(n+1)((n+1)!)} < 0$ *donc v est strictement décroissante ;*
— $\lim (u_n - v_n) = \lim \frac{1}{n \cdot n!} = 0$.
Donc u et v sont adjacentes : elles convergent vers une même limite l. On admet (voir chapitre plus tard) que $l = e$.

2. *Par l'absurde, supposons que e est rationnel : on écrit $e = \frac{p}{q}$, avec $p, q \in \mathbb{N}^*$ (comme $l \geq u_0 > 0$).*
Par stricte monotonie, on a : $u_q < \frac{p}{q} < v_q = u_q + \frac{1}{q \cdot q!}$. Donc :

$$q \cdot q! \cdot u_q < p \cdot q! < q \cdot q! \cdot u_q + 1.$$

Mais $q! \cdot u_q \in \mathbb{N}$ (en regardant la formule). Donc $p \cdot q!$ serait un entier strictement compris entre deux entiers consécutifs, ce qui est impossible.
Donc e est irrationnel.

Théorème III.14 (des segments emboîtés)**.** *On considère (I_n) une suite décroissante (pour l'inclusion) de segments, dont la longueur tend vers 0.*
Alors : $\bigcap_{n=0}^{+\infty} I_n$ est un singleton.

Démonstration. Pour tout $n \in \mathbb{N}$, notons : $I_n = [u_n, v_n]$.
— par décroissance de (I_n), on a : $\forall n \in \mathbb{N},\ [u_{n+1}, v_{n+1}] \subset [u_n, v_n]$. Donc u est croissante et v est décroissante ;
— comme la longueur des I_n tend vers 0, alors : $\lim (v_n - u_n) = 0$.
Donc u et v sont adjacentes. On note l leur limite.
Alors : $\forall n \in \mathbb{N},\ u_n \leq l \leq v_n$, donc $l \in I_n$. Donc $\{l\} \subset \cap_{n \in \mathbb{N}} I_n$.
Inversement, soit $x \in \cap_{n \in \mathbb{N}} I_n$. Alors : $\forall n \in \mathbb{N},\ u_n \leq x \leq v_n$. Et en passant à la limite : $l \leq x \leq l$, donc $x = l$. Donc $\cap_{n \in \mathbb{N}} I_n \subset \{l\}$.
D'où l'égalité. □

IV Suites extraites

Définition IV.1. *Soient u une suite et $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante. La suite $\left(u_{\varphi(n)}\right)$, notée aussi u_φ, est appelée **suite extraite de** u. La fonction φ est appelée **fonction extractrice**.*

Exemples IV.2.

1. *les suites (u_{2n}) et (u_{2n+1}) sont les suites extraites de u correspondant aux indices pairs et impairs ;*
2. *la suite (u_{n+n_0}) correspond à la suite u privée de ses n_0 premiers termes.*

Proposition IV.3. *Si u est (strictement) croissante (ou (strictement) décroissante, constante, stationnaire, majorée, minorée, bornée), alors toute suite extraite de u aussi.*

Démonstration. Évident. □

Proposition IV.4. *Si u a pour limite $l \in \overline{R}$, alors toute suite extraite de u a aussi pour limite l.*

Démonstration. Montrons le résultat lorsque u converge vers $l \in \mathbb{R}$.
Soit $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante. Alors on a le lemme suivant :

Lemme IV.5. $\forall n \in \mathbb{N},\ \varphi(n) \geq n$.

preuve du lemme. On procède par récurrence :
- $\varphi(0) \in \mathbb{N}$, donc $\varphi(0) \geq 0$;
- supposons $\varphi(n) \geq n$. Alors, par monotonie : $\varphi(n+1) > \varphi(n) \geq n$, donc $\varphi(n+1) > n$, et finalement : $\varphi(n+1) \geq n+1$.

□

Soit $\varepsilon > 0$. Par convergence de u, il existe n_0 tel que : $n \geq n_0 \Rightarrow |u_n - l| \leq \varepsilon$.
Et donc par le lemme : $n \geq n_0 \Rightarrow \varphi(n) \geq \varphi(n_0) \geq n_0 \Rightarrow |u_{\varphi(n)} - l| \leq \varepsilon$. □

Remarque IV.6. *En pratique, on utilise plutôt la contraposée pour montrer qu'une suite n'a pas de limite :*
- *soit en exhibant une suite extraite qui n'a pas de limite ;*
- *soit en exhibant deux suites extraites qui ont des limites différentes.*

Exemple IV.7. *La suite $(u_n) = ((-1)^n)$ diverge car :*
- *la suite extraite (u_{2n}) est constante égale à 1, donc converge vers 1 ;*
- *la suite extraite (u_{2n+1}) est constante égale à -1, donc converge vers -1.*

Proposition IV.8. *Si u converge, alors la suite $(u_{n+1} - u_n)$ tend vers 0.*

Démonstration. Notons l la limite de u. Alors (u_{n+1}) converge vers l. Donc $(u_{n+1} - u_n)$ converge vers $l - l = 0$. □

Remarque IV.9. *La réciproque est fausse.*
On considère la suite définie par : $u_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n} = \sum_{k=1}^{n} \frac{1}{k}$.
On a pour $n \in \mathbb{N}$: $u_{n+1} - u_n = \frac{1}{n+1}$ qui tend vers 0. Mais u ne converge pas.
Par l'absurde, supposons qu'elle converge vers une limite l. Alors la suite extraite $(v_n) = (u_{2n})$ convergerait aussi vers l. Donc la suite $v - u$ convergerait vers 0.
Mais pour tout $n \in \mathbb{N}^*$:

$$v_n - u_n = \sum_{k=1}^{2n} \frac{1}{k} - \sum_{k=1}^{n} \frac{1}{k} = \sum_{k=n+1}^{2n} \frac{1}{k} \geq \frac{n}{2n} = \frac{1}{2}$$

et donc en passant à la limite : $0 \geq \frac{1}{2}$, d'où la contradiction.
Donc u ne converge pas. Au passage, comme elle est croissante, cela montre aussi qu'elle tend vers $+\infty$.

Proposition IV.10. *La suite u a pour limite $l \in \overline{R}$ si, et seulement si, les deux suites (u_{2n}) et (u_{2n+1}) aussi.*

Démonstration. La première implication découle du fait que l'on a des suites extraites.
Réciproquement, supposons que (u_{2n}) et (u_{2n+1}) convergent vers $l \in \mathbb{R}$ (les cas $l = \pm\infty$ se traitent pareil).
Soit $\varepsilon > 0$. Alors :

$$\begin{cases} \exists n_1 \in \mathbb{N},\ \forall n \geq n_1,\ |u_{2n} - l| \leq \varepsilon \\ \exists n_2 \in \mathbb{N},\ \forall n \geq n_2,\ |u_{2n+1} - l| \leq \varepsilon \end{cases}$$

Posons $n_0 = \max(2n_1, 2n_2 + 1)$. Alors si $n \geq n_0$:
- si n est pair : $n = 2m$ avec $m \geq n_1$, donc : $|u_n - l| = |u_{2m} - l| \leq \varepsilon$;

— si n est impair : $n = 2m + 1$ avec $m \geq n_2$, donc : $|u_n - l| = |u_{2m+1} - l| \leq \varepsilon$.

Donc u converge vers l. □

Théorème IV.11 (de Bolzano–Weierstrass)**.** *De toute suite bornée on peut extraire une suite convergente.*

Démonstration. Considérons une suite bornée u. On veut construire une fonction extractrice φ telle que u_φ converge, ce que l'on va faire récursivement.

On fixe $I_0 = [a_0; b_0]$ qui contient tous les termes de la suite u, c'est-à-dire : $\forall n \in \mathbb{N},\ a_0 \leq u_n \leq b_0$.Et on pose $\varphi(0) = 0$.

On partage I_0 en son milieu en deux segments : nécessairement l'un de ces segments contient une infinité de termes de u. Notons le $I_1 = [a_1; b_1]$. Et on choisit $N_1 \in \mathbb{N}$ tel que : $u_{N_1} \in I_1$.

On répète ce processus : pour tout $n \in \mathbb{N}$, on construit une suite décroissante de segments $(I_n) = ([a_n; b_n])$ et une suite **strictement croissante** d'entiers (N_n) tels que pour tout $n \in \mathbb{N}^*$:

— I_n est une des moitiés de I_{n-1} ;

— I_n contient une infinité de termes de u ;

— $u_{N_n} \in I_n$.

Comme la longueur de I_n est $(b_n - a_n) = \dfrac{b_0 - a_0}{2^n} \to 0$, alors on peut appliquer le théorème des fermés emboîtés, et les suites $(a_n), (b_n)$ convergent vers l'unique élément l de $\cap_{n\in\mathbb{N}} I_n$.

Considérons la fonction $\varphi : n \mapsto N_n$. Elle est bien strictement croissante par construction. Et comme $u_{N_n} = u_{\varphi(n)} \in I_n$, on déduit que :

$$\forall n \in N,\ a_n \leq u_{\varphi(n)} \leq b_n.$$

Donc par encadrement u_φ converge vers l : on a bien une suite extraite convergente. □

V Traduction séquentielle de propriétés de $\mathbb{R}$

Proposition V.1 (Caractérisation séquentielle de la borne supérieure)**.** *Soit A une partie non vide de $\mathbb{R}$, et $M \in \mathbb{R}$. Alors :*

1. *M est la borne supérieure de A si, et seulement si, M est un majorant de A et qu'il existe une suite à valeurs dans A qui converge vers M ;*
2. *A n'est pas majorée si, et seulement si, il existe une suite à valeurs dans A qui tend vers $+\infty$.*

Démonstration.

1. Supposons que $M = \sup(A)$: alors M est un majorant de A. On construit une suite u d'élément de A avec : u_0 quelconque, et pour tout $n \in \mathbb{N}^*$, $M - \frac{1}{n} \leq u_n \leq M$ (par définition de la borne supérieure, comme $\frac{1}{n} > 0$).

   Par encadrement, on a : $\lim u = M$.

   Réciproquement, si M est un majorant de A et que u converge vers M : soit $\varepsilon > 0$, alors :

   $$\exists n_0,\ n \geq n_0 \Rightarrow |u_n - M| < \varepsilon \Rightarrow M - \varepsilon < u_n \leq M.$$

   Et donc $M = \sup A$.

2. Si A n'est pas majoré. Alors, pour tout $n \in \mathbb{N}$, n n'est pas un majorant de A. On construit ainsi une suite u d'éléments de A avec : $\forall n \in \mathbb{N}, u_n \geq n$.

   Par minoration, on a $\lim u = +\infty$.

   Inversement, si u tend vers $+\infty$, on a vu que u n'est pas majorée, donc A non plus.

□

Proposition V.2 (Caractérisation séquentielle de la borne inférieure)**.** *Soit A une partie non vide de $\mathbb{R}$, et $m \in \mathbb{R}$. Alors :*

1. *m est la borne inférieure de A si, et seulement si, m est un minorant de A et qu'il existe une suite à valeurs dans A qui converge vers m ;*
2. *A n'est pas minorée si, et seulement si, il existe une suite à valeurs dans A qui tend vers $-\infty$.*

Exemple V.3. *L'ensemble $A = \{\frac{1}{n}, \mid n \in \mathbb{N}^*\}$ admet 1 comme maximum (donc comme borne supérieure), et 0 comme borne inférieure.*
Il est clair que 0 est un minorant de A, et la suite de terme général $\frac{1}{n}$ tend vers 0.

Proposition V.4 (Caractérisation séquentielle de la densité)**.** *Soit A une partie de $\mathbb{R}$. Alors A est dense dans $\mathbb{R}$ si, et seulement si, pour tout $x \in \mathbb{R}$ il existe une suite à valeurs dans A qui converge vers x.*

Démonstration. Si A est dense dans $\mathbb{R}$: tout intervalle non vide de $\mathbb{R}$ contient un élément de A. En particulier, si $x \in \mathbb{R}$, pour $n \in \mathbb{N}^*$ il existe $u_n \in A \cap \left]x - \frac{1}{n}; x + \frac{1}{n}\right[$. La suite u ainsi construite converge vers x par théorème d'encadrement.
Réciproquement, supposons que pour tout $x \in \mathbb{R}$ il existe une suite d'éléments de A qui converge vers x. Soit I intervalle ouvert non vide. Soient $a < b$ deux éléments distincts de I (qui existent bien par description des intervalles ouverts). Posons $x = \frac{a+b}{2}$ et $\varepsilon = \frac{b-a}{2} > 0$. Si u est une suite d'éléments de A qui converge vers x :

$$\exists n_0 \in \mathbb{N},\ n \geq n_0 \Rightarrow |u_n - x| \leq \varepsilon.$$

Ainsi : $u_{n_0} \in A$ vérifie : $x - \varepsilon \leq u_{n_0} \leq x + \varepsilon$. C'est-à-dire : $u_{n_0} \in [a; b] \subset I$. Donc I contient bien un élément de A. □

Proposition V.5. *Les ensembles $\mathbb{D}$, $\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$ sont denses dans $\mathbb{R}$.*

Démonstration. Soit $x \in \mathbb{R}$. Montrons qu'on peut écrire x comme limite d'une suite de décimaux, de rationnels, ou d'irrationnels :
- décimaux : on utilise la suite u, où u_n est l'approximation décimale à 10^{-n} près de x, qui converge vers x par encadrement ;
- rationnels : on utilise l'inclusion des décimaux parmi les rationnels ;
- irrationnels : si $x \notin \mathbb{Q}$ on prend la suite constante de valeur x ; sinon on considère la suite de terme général $x + \frac{\sqrt{2}}{n}$ qui tend vers x par opérations sur les limites.

□

VI Suites complexes

Proposition-Définition VI.1. *Une suite complexe u est dite **bornée** si la suite réelle $|u|$ est bornée.*
C'est le cas si, et seulement si, les suites réelles $(\mathrm{Re}(u))$ et $(\mathrm{Im}(u))$ sont bornées.

Démonstration. Provient des inégalités :
- $|\mathrm{Re}(u_n)| \leq |u_n|$ et $|\mathrm{Im}(u_n)| \leq |u_n|$;
- $|u_n| \leq |\mathrm{Re}(u_n)| + |\mathrm{Im}(u_n)|$.

□

Définition VI.2. *On dit qu'une suite complexe u **converge vers** $l \in \mathbb{C}$ si :*

$$\forall \varepsilon > 0,\ \exists n_0 \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geq n_0 \Rightarrow |u_n - l| < \varepsilon.$$

Remarque VI.3. *Cela revient à dire que la suite réelle $|u - l|$ tend vers 0.*

Proposition VI.4. *Si u est une suite complexe, alors u converge vers l si, et seulement si, les suites $\mathrm{Re}(u)$ et $\mathrm{Im}(u)$ convergent.*
Et dans ce cas, si u converge vers $l \in \mathbb{C}$, alors $\mathrm{Re}(u)$ et $\mathrm{Im}(u)$ convergent respectivement vers $\mathrm{Re}(l)$ et $\mathrm{Im}(l)$.

Démonstration. On utilise le théorème d'encadrement, grâce aux inégalités précédentes. □

Théorème VI.5 (de Bolzano–Weierstrass)**.** *De toute suite complexe bornée on peut extraire une sous-suite convergente.*

Démonstration. On s'appuie sur le théorème pour les suites réelles. Soit u une suite complexe bornée. On pose $a = \mathrm{Re}(u)$ et $b = \mathrm{Im}(u)$.
- comme u est bornée, alors a aussi. Il existe une fonction extractrice φ telle que a_φ converge ;
- mais b aussi est bornée. Et la suite b_φ est extraite de b, donc bornée aussi. On peut donc appliquer à nouveau le théorème réel : il existe une fonction extractrice ψ telle que $b_{\varphi\circ\psi}$ converge ;
- alors $a_{\varphi\circ\psi}$ est une suite extraite de a_φ, donc elle converge.

Et finalement $u_{\varphi\circ\psi}$ converge, comme ses parties réelles et imaginaires convergent. □

VII Suites classiques

VII.1 Suites arithmético-géométriques

Proposition-Définition VII.1 (suites arithmétiques)**.** *Soient u une suite numérique et $r \in \mathbb{K}$. On dit que u est une* ***suite arithmétique de raison*** *r si :*

$$\forall n \in \mathbb{N},\ u_{n+1} = u_n + r.$$

On a alors : $\forall n \in \mathbb{N},\ u_n = u_0 + nr$, et plus généralement :

$$\forall n, m \in \mathbb{N},\ u_n = u_m + (n-m)r.$$

Proposition VII.2. *Une suite arithmétique de raison r converge si, et seulement si, $r = 0$ (elle est alors constante).*
Une suite arithmétique de raison $r > 0$ (resp. $r < 0$) tend vers $+\infty$ (resp. $-\infty$).

Proposition-Définition VII.3 (suites géométriques)**.** *Soient u une suite numérique et $q \in \mathbb{K}$. On dit que u est une* ***suite géométrique de raison*** *q si :*

$$\forall n \in \mathbb{N},\ u_{n+1} = u_n \times q.$$

On a alors : $\forall n \in \mathbb{N},\ u_n = u_0 \times q^n$, et plus généralement :

$$\forall n \geq m \in \mathbb{N},\ u_n = u_m \times q^{n-m}.$$

Proposition VII.4. *Une suite géométrique (non nulle) de raison q converge si, et seulement si, $|q| < 1$ (elle tend alors vers 0) ou si $q = 1$ (elle est alors constante).*

Démonstration. Les cas où $|q| \neq 1$ découlent du lemme qui suit.
Le cas où $|q| = 1$ est plus subtile, et découle de la divergence des suites $(\cos(n\theta))$ et $\sin(n\theta))$ pour $\theta \in]0; 2\pi[$. □

Lemme VII.5. *Soit $q \in \mathbb{R}$:*

1. *si $q > 1$, alors $\lim q^n = +\infty$;*
2. *si $q \in]-1; 1[$, alors $\lim q^n = 0$;*
3. *si $q = 1$, alors $\lim q^n = 1$;*
4. *si $q \leq -1$, la suite (q^n) n'a pas de limite.*

Démonstration.

1. si $q > 1$: posons $a = q - 1 > 0$. Pour tout $n \in \mathbb{N}$, on a :

$$q^n = (1+a)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \geq 1 + na$$

et comme $\lim na = +\infty$ (car $a > 0$), alors par encadrement : $\lim q^n = +\infty$;

2. si $q \in]-1;1[$: si $q = 0$, la suite q^n est constante (de valeur 0). Sinon, posons $a = |\frac{1}{q}| > 1$. Alors $\lim a^n = +\infty$, donc $\lim q^n = 0$ (par opérations sur les limites) ;
3. si $q = 1$: la suite est constante ;
4. si $q = -1$: alors (q^{2n}) est stationnaire à 1, et (q^{2n+1}) est stationnaire à -1, donc la suite ne converge pas (mais est bornée) ;
5. si $q < -1$: la suite extraite (q^{2n}) tend vers $+\infty$, tandis que la suite extraite $(q^{2n+1}) = q \times (q^{2n})$ tend vers $q \times (+\infty) = -\infty$. Donc la suite (q^n) n'a pas de limite (et n'est d'ailleurs ni majorée ni minorée).

□

Définition VII.6 (suites arithmético-géométriques)**.** *On dit qu'une suite u est **arithmético-géométrique** s'il existe $a, b \in \mathbb{K}$ tels que :*

$$\forall n \in \mathbb{N},\ u_{n+1} = au_n + b.$$

Remarque VII.7. *Si $a = 1$, la suite est arithmétique. Si $b = 0$, la suite est géométrique.*

Méthode VII.8. *Si u est arithmético-géométrique avec $a \neq 1$:*

1. *on cherche l l'unique solution de l'équation $l = al + b$;*
2. *la suite $(u_n - l)$ est une suite géométrique de raison a.*

Démonstration. Si $n \in \mathbb{N}$:

$$u_{n+1} - l = au_n + b - (al + b) = a(u_n - l).$$

□

Remarque VII.9. *On a donc la formule : $u_n = a^n \left(u_0 - \dfrac{b}{1-a}\right) + \dfrac{b}{1-a}$, mais qu'il ne faut pas retenir par cœur.*

Exemple VII.10. *Si u est définie par $u_0 = 0$ et $\forall n \in \mathbb{N},\ u_{n+1} = \frac{1}{3}u_n - 2$.*
On commence par trouver l. On a :

$$l = \frac{1}{3}l - 2 \Leftrightarrow \frac{2}{3}l = -2 \Leftrightarrow l = -3.$$

Donc la suite $(v_n) = (u_n + 3)$ est géométrique de raison $\frac{1}{3}$, et de premier terme $v_0 = u_0 + 3 = 3$.
Donc pour tout $n \in \mathbb{N}$: $v_n = 3 \times \left(\frac{1}{3}\right)^n$, donc $u_n = v_n - 3 = \frac{1}{3^{n-1}} - 3$.
Et u converge vers -3.

Remarque VII.11. *D'autres suites se ramènent à des suites arithmético-géométriques. Par exemple, si $a, b, k \in \mathbb{K}$ ($k \neq 0$), considérons la suite u telle que : $\forall n \in \mathbb{N},\ u_{n+1} = au_n + b \cdot k^n$.*
Alors la suite $(v_n) = \left(\frac{u_n}{k^n}\right)$ vérifie : $\forall n \in \mathbb{N},\ v_{n+1} = \frac{a}{k}v_n + \frac{b}{k}$.

VII.2 Suites linéaires récurrentes d'ordre 2

Définition VII.12. *Une **suite linéaire récurrente d'ordre** 2 est une suite u définie par une relation du type :*

$$\forall n \in \mathbb{N},\ u_{n+2} = au_{n+1} + bu_n$$

où $a, b \in \mathbb{K}$.
*On lui associe l'équation $x^2 = ax + b$, appelée **équation caractéristique**.*

Lemme VII.13. *Une suite linéaire récurrente d'ordre 2 est entièrement déterminée par ses deux premiers termes.*

Démonstration. Soient u, v deux suite linéaires récurrentes d'ordre 2 telles que :

$$\forall n \in \mathbb{N},\ \begin{cases} u_{n+2} = au_{n+1} + bu_n \\ v_{n+2} = av_{n+1} + bv_n \end{cases}$$

et telles que $(u_0, u1) = (v_0, v_1)$.
Montrons par récurrence (d'ordre 2) sur $n \in \mathbb{N}$ que $u_n = v_n$ (ce qui conclura que $u = v$) :
— c'est vrai pour $n = 0$ ou 1 ;
— supposons le résultat vrai au rangs n et $n + 1$ (pour $n \in \mathbb{N}$). Alors on a :

$$v_{n+2} = av_{n+1} + bv_n = au_{n+1} + bu_n = u_{n+2}.$$

D'où la récurrence. □

Théorème VII.14. *On considère u une suite linéaire récurrente d'ordre 2, et on note Δ le discriminant de son équation caractéristique :*

1. *si $\Delta \neq 0$: l'équation caractéristique possède deux racines distinctes, que l'on note r_1, r_2. Et il existe $\lambda, \mu \in \mathbb{C}$ tels que :*
$$\forall n \in \mathbb{N},\ u_n = \lambda r_1^n + \mu r_2^n.$$
2. *si $\Delta = 0$: l'équation caractéristique possède une unique solution, que l'on note r. Et il existe $\lambda, \mu \in \mathbb{C}$ tels que :*
$$\forall n \in \mathbb{N},\ u_n = \lambda r^n + \mu n r^n.$$

Dans les deux cas, le choix de λ, μ est unique et peut être fixé en utilisant les valeurs de u_0 et u_1.

Démonstration. Prouvons le premier cas :
— si $\lambda, \mu \in \mathbb{C}$, posons $(v_n) = (\lambda r_1^n + \mu r_2^n)$. Pour tout $n \in \mathbb{N}$, on a :

$$\begin{aligned} v_{n+2} &= \lambda r_1^{n+2} + \mu r_2^{n+2} = \lambda r_1^n \cdot r_1^2 + \mu r_2^n \cdot r_2^2 \\ &= \lambda r_1^n (ar_1 + b) + \mu r_2^n (ar_2 + b) \\ &= a \underbrace{(\lambda r_1^{n+1} + \mu r_2^{n+1})}_{v_{n+1}} + b \underbrace{(\lambda r_1^n + \mu r_2^n)}_{v_n} \end{aligned}$$

donc v vérifie la même relation de récurrence que u, peu importe le choix de λ et μ.
— reste à choisir λ, μ tels que u et v aient leurs deux premiers termes identiques, c'est-à-dire :

$$\begin{cases} \lambda + \mu = u_0 \\ r_1\lambda + r_2\mu = u_1 \end{cases}$$

mais on reconnaît un système linéaire à deux équations et deux inconnues : son déterminant est $r_1 - r_2 \neq 0$ donc un tel choix de λ, μ est possible (et est même unique).
Pour le deuxième cas tout se passe pareil. On utilise que, si r est l'unique solution de $x^2 = ax + b$, alors $r = \frac{a}{2}$ et $b = -\frac{a^2}{4}$. □

Corollaire VII.15. *Avec les mêmes notations, si a, b, u_0, u_1 sont réels, alors la suite u est à valeurs réelles. Si l'équation caractéristique admet deux solutions distinctes, celles-ci sont complexes conjuguées, donc de la forme $\rho e^{\pm i\theta}$ (pour $\rho > 0$ et $\theta \in \mathbb{R}$). Il existe alors $\lambda, \mu \in \mathbb{R}$ tels que :*

$$\forall n \in \mathbb{N},\ u_n = \rho^n \left[\lambda \cos(n\theta) + \mu \sin(n\theta)\right].$$

Démonstration. Une récurrence immédiate montre déjà bien que tous les u_n sont réels.
Par le théorème, il existe λ_1, μ_1 tels que : $\forall n \in \mathbb{N}, u_n = \lambda_1 r_1^n + \mu_1 r_2^n$.
Et donc pour tout $n \in \mathbb{N}$:

$$u_n = \rho^n \left[(\lambda_1 + \mu_1)\cos(n\theta) + i(\lambda_1 - \mu_1)\sin(n\theta)\right].$$

Mais u est réelle, donc :

$$u_n = \mathrm{Re}(u_n) = \rho^n \left[\lambda \cos(n\theta) + \mu \sin(n\theta)\right] \text{ avec } \left\{ \begin{array}{rcl} \lambda & = & \mathrm{Re}(\lambda_1 + \mu_1) \\ \mu & = & \mathrm{Re}(i(\lambda_1 - \mu_1)) \end{array} \right. .$$

□

Remarque VII.16. *Dans la preuve, comme u est réelle, on peut voir que l'unicité du choix de λ_1, μ_1 impose que $\lambda_1 = \overline{\mu_1}$. Et ainsi : $\lambda = 2\mathrm{Re}(\lambda_1)$ et $\mu = -2\mathrm{Im}(\lambda_1)$.*

Exemple VII.17. *On considère la suite de Fibonacci, définie par : $u_0 = 0$, $u_1 = 1$ et pour tout $n \in \mathbb{N}$, $u_{n+2} = u_{n+1} + u_n$.*
*L'équation caractéristique est $x^2 = x + 1$, qui possède comme solutions : $r_1 = \frac{1-\sqrt{5}}{2}$ et $r_2 = \frac{1+\sqrt{5}}{2}$ (le **nombre d'or**). Donc il existe $\lambda, \mu \in \mathbb{C}$ tels que :*

$$\forall n \in \mathbb{N},\ u_n = \lambda \left(\frac{1+\sqrt{5}}{2}\right)^n + \mu \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Comme $u_0 = 0$ et $u_1 = 1$, alors :

$$\left\{ \begin{array}{rcrcl} \lambda & + & \mu & = & 0 \\ \frac{1+\sqrt{5}}{2}\lambda & + & \frac{1-\sqrt{5}}{2}\mu & = & 1 \end{array} \right.$$

ce qui donne : $\lambda = \frac{1}{\sqrt{5}} = \frac{\sqrt{5}}{5}$ et $\mu = -\lambda = -\frac{\sqrt{5}}{5}$.
Et finalement :

$$\forall n \in \mathbb{N},\ u_n = \frac{\sqrt{5}}{5}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

Au passage, montrons que la formule précédente définit bien des rationnels : suivant la définition de la suite de Fibonacci, on peut voir par une récurrence immédiate qu'il doit s'agir d'entiers, ce qui n'est clair quand on regarde la formule précédente.
Par la formule du binôme, pour $n \in \mathbb{N}$, on a :

$$\left(1+\sqrt{5}\right)^n = \sum_{k=0}^{n} \binom{n}{k} \sqrt{5}^k \text{ et } \left(1-\sqrt{5}\right)^n = \sum_{k=0}^{n} \binom{n}{k} (-\sqrt{5})^k$$

et ainsi :

$$\begin{array}{rcl} \left(1+\sqrt{5}\right)^n - \left(1-\sqrt{5}\right)^n & = & \displaystyle\sum_{k=0}^{n} \binom{n}{k} \left(\sqrt{5}^k - (-\sqrt{5})^k\right) \\ & = & \displaystyle\sum_{k=0, k \text{ impair}}^{n} \left(\sqrt{5}^k - (-\sqrt{5})^k\right) \text{ car les termes de rangs pairs sont nuls} \\ & = & \displaystyle\sum_{l=0}^{\lfloor n-1/2 \rfloor} \binom{n}{2l+1} \sqrt{5} \cdot 2 \cdot 5^l \text{ en simplifiant l'expression précédente} \\ & = & \sqrt{5} \cdot 2 \cdot N \text{ pour } N = \displaystyle\sum_{l=0}^{\lfloor n-1/2 \rfloor} \binom{n}{2l+1} \cdot 5^l \in \mathbb{N} \end{array}$$

et ainsi on trouve avec la notation précédente que :

$$\frac{\sqrt{5}}{5}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right)=\frac{2N}{2^n}=2^{1-n}\cdot N\in\mathbb{Q}.$$

Les suites définies par une relation du type $u_{n+1}=f(u_n)$, pour f une fonction continue, seront vues plus tard.

Chapitre 15

Structures algébriques

I Loi de composition interne

I.1 Généralités

Définition I.1. *Si E est un ensemble non vide, une* ***loi de composition interne*** *(abrégée en lci) est une application de $E \times E$ dans E.*

Remarque I.2. *On les note souvent par des symboles ($*$, $\star$, $\times$, $+$, etc.) et on utilise la notation $x \star y$ pour désigner $\star(x, y)$.*

Définition I.3. *Une lci $*$ sur E est dite :*

1. ***associative*** *si :*
$$\forall x, y, z \in E,\ (x * y) * z = x * (y * z);$$
2. ***commutative*** *si :*
$$\forall x, y \in E,\ x * y = y * x.$$

Exemples I.4.

1. *la somme $(x, y) \mapsto x + y$ et le produit $(x, y) \mapsto x \times y$ sont des lci commutatives et associatives sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{R}$;*
2. *la différence $(x, y) \mapsto x - y$ est une lci sur $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{R}$, mais pas sur $\mathbb{N}$ ($0 - 1 = -1 \notin \mathbb{N}$) ; elle n'est ni commutative ni associative ;*
3. *le quotient $(x, y) \mapsto \frac{x}{y}$ est une lci sur $\mathbb{Q}^*$ ou $\mathbb{R}^*$, mais pas sur $\mathbb{D}^*$, $\mathbb{Z}^*$ ou $\mathbb{N}^*$; il n'est ni associatif ni commutatif ;*
4. *l'union, l'intersection et la différence symétriques sont des lci associatives et commutatives sur $\mathcal{P}(E)$;*
5. *la composition est une lci sur $\mathcal{F}(\mathbb{R}, \mathbb{R})$ qui est associative, mais non commutative ;*
6. *l'addition matricielle sur $\mathcal{M}_{n,p}(\mathbb{K})$ est une lci associative et commutative ; la multiplication matricielle sur $\mathcal{M}_n(\mathbb{K})$ est une lci associative, mais non commutative.*

Définition I.5. *Si E est muni de deux lci $*$ et $\top$, on dit que $*$ est* ***distributive par rapport à*** *$\top$ si :*
$$\forall x, y, z \in E,\ \begin{cases} x * (y \top z) &= (x * y) \top (x * z) \\ (y \top z) * x &= (y * x) \top (z * x) \end{cases}.$$

Exemples I.6.

1. *Dans $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ ou $\mathbb{N}$, la multiplication est distributive par rapport à l'addition, mais pas l'inverse.*
2. *Dans $\mathcal{P}(E)$, l'union est distributive par rapport à l'intersection, et l'intersection par rapport à l'union.*
3. *Dans $\mathcal{M}_n(\mathbb{K})$, la multiplication matricielle est distributive par rapport à l'addition matricielle.*

I.2 Inversibilité et élément neutre

Proposition-Définition I.7. *Si $*$ est une lci sur E, et $e \in E$. On dit que e est **un élément neutre** pour $*$ si :*

$$\forall x \in E,\ x * e = x = e * x.$$

*S'il existe, un élément neutre est unique. Et on le désignera comme **l'élément neutre**.*

Démonstration. Si e_1, e_2 sont des éléments neutres, alors : $e_1 = e_1 * e_2 = e_2$. □

Exemples I.8.

1. *sur $\mathbb{C}$ ou un de ses sous-ensembles usuels, 0 est l'élément neutre pour la somme, et 1 pour le produit ;*
2. *id_E est l'élément neutre de la composition sur $\mathcal{F}(E, E)$;*
3. *E est l'élément neutre de l'intersection sur $\mathcal{P}(E)$, et $\emptyset$ celui de l'union ;*
4. *$0_{n,p}$ est l'élément neutre pour la somme matricielle sur $\mathcal{M}_{n,p}(\mathbb{K})$, tandis que I_n est l'élément neutre pour la multiplication matricielle sur $\mathcal{M}_n(K)$.*

Proposition-Définition I.9. *Soit E est muni d'une lci $*$ associative, possédant un élément neutre e.*
*Un élément $x \in E$ est dit **inversible** s'il existe $y \in E$ tel que : $x * y = e = y * x$.*
*Un tel élément y est nécessairement unique, et on l'appelle **l'inverse** de x. On le note x^{-1}.*

Démonstration. Montrons l'unicité. Si y_1, y_2 sont deux inverses de x, alors :

$$y_1 = y_1 * e = y_1 * (x * y_2) = (y_1 * x) * y_2 = e * y_2 = y_2.$$

□

Remarques I.10.

1. *Si x est inversible, alors x^{-1} aussi, avec : $(x^{-1})^{-1} = x$.*
2. *L'élément neutre est son propre inverse, mais d'autres éléments peuvent vérifier cette propriété :*
   - *-1 pour le produit sur $\mathbb{C}$;*
   - *les matrices diagonales avec juste des ± 1 pour la multiplication matricielle sur $\mathcal{M}_n(\mathbb{C})$;*
   - *les applications involutives pour la composition sur $\mathcal{F}(E, E)$.*
3. *Il faut bien avoir $x * y = e$ et $y * x = e$. Il y a juste pour les matrices carrées qu'on avait vu qu'une seule des égalités suffisait mais c'est un cas très particulier (et à connaître !).*

Proposition I.11. *Si x, y sont deux éléments inversibles, alors $x*y$ est inversible, avec : $(x*y)^{-1} = y^{-1}*x^{-1}$.*

Démonstration. Il suffit de vérifier que $y^{-1} * x^{-1}$ est bien l'inverse de $x * y$:

$$\begin{cases} (y^{-1} * x^{-1}) * (x * y) = y^{-1} * \underbrace{(x^{-1} * x)}_{=e} * y = y^{-1} * y = e \\ (y * x) * (x^{-1} * y^{-1}) = y * \underbrace{(x * x^{-1})}_{=e} * y^{-1} = y * y^{-1} = e \end{cases}.$$

□

Remarque I.12. *Il y a deux notations fréquentes pour les lci :*

1. *notation additive : la lci est notée $+$, son élément neutre 0 ou 0_E, l'inverse de x sera $-x$ et pour $n \in \mathbb{N}$ on notera : $\underbrace{x + \cdots + x}_{n\ fois} = nx$;*
2. *notation multiplicative : la lci est notée $\times$, son élément neutre 1 ou 1_E, l'inverse de x sera x^{-1} et pour $n \in \mathbb{N}$ on notera : $\underbrace{x \times \cdots \times x}_{n\ fois} = x^n$.*

Proposition-Définition I.13. *Si x est inversible, alors x est **régulier**, c'est-à-dire que :*

$$\forall y,z\in E,\ \begin{cases} x*y=x*z\Rightarrow y=z\\ y*x=z*x\Rightarrow y=z\end{cases}.$$

Démonstration. Si $x*y=x*z$, alors en multipliant par x^{-1} on a : $y=z$. Et pareil pour l'autre implication. □

Remarque I.14. *Cela signifie qu'on peut "simplifier par x" des égalités. Et on peut utiliser la contraposée pour montrer qu'un élément n'est pas inversible.*

Exemple I.15. *Sur $\mathcal{P}(E)$ on a par analyse-synthèse que :*
- *E est l'unique élément inversible pour l'intersection car : si $A\in\mathcal{P}(E)$, alors $A\cap E=A\cap A$, donc si A est inversible on a $A=E$; et E est inversible (car l'élément neutre) ;*
- *$\emptyset$ est l'unique élément inversible pour l'union car : si $A\in\mathcal{P}(E)$, alors $A\cup\emptyset=A\cup A$, donc si A est inversible on a $A=\emptyset$; et $\emptyset$ est inversible (car l'élément neutre).*

tandis que tout élément est inversible pour la différence symétrique !

I.3 Parties stables

Définition I.16. *Soit E est muni d'une lci $*$ et $A\subset E$. On dit que A est **stable par** $*$ si : $\forall x,y\in A,\ x*y\in A$.*
Dans ce cas, la restriction de $*$ à $A\times A$ définit une lci sur A.

Remarque I.17. *Si $*$ est associative (resp. commutative), alors sa restriction l'est aussi. La réciproque est fausse, comme le montre la restriction de la différence sur $\mathbb{C}$ à $\{0\}$.*

Définition I.18. *Si E est muni d'une lci associative $*$, d'élément neutre e, et $x\in E$, on définit pour tout $n\in\mathbb{N}$:*

$$x^n=\begin{cases} e & si\quad n=0\\ x*x^{n-1} & si\quad n>0\end{cases}.$$

Si de plus x est inversible, on définit pour $n\in\mathbb{Z}$ avec $n<0$ par :

$$x^n=\left(x^{-1}\right)^{-n}.$$

Proposition I.19. *Si $x\in E$, alors : $\forall n,m\in\mathbb{N},\ x^n*x^m=x^{n+m}$.*
Si de plus x est inversible, alors : $\forall n,m\in\mathbb{Z},\ x^n*x^m=x^{n+m}$.

Démonstration. Notons déjà que :
- la formule avec $n,m\in\mathbb{N}$ est immédiate par récurrence ;
- si x est inversible, alors pour tout $n\in\mathbb{N}$, x^n est inversible d'inverse x^{-n} (par formule de l'inverse d'un produit).

Supposons x inversible et montrons le cas où $n,m\in\mathbb{Z}$ par disjonction de cas :
- si $n,m\geq 0$: c'est le cas précédent ;
- si $n,m\leq 0$:
$$x^n*x^m=\left(x^{-1}\right)^{-n}*\left(x^{-1}\right)^{-m}=\left(x^{-1}\right)^{-n-m}=x^{n+m}.$$
- si $n\leq 0$ et $m\geq 0$:
  - si $n+m\geq 0$:
$$x^n*x^m=x^n*\left(x^{-n}*x^{n+m}\right)=\underbrace{x^n*x^{-n}}_{=e}*x^{m+n}=x^{m+n}.$$
  - si $n+m\leq 0$:
$$x^n*x^m=\left(x^{-1}\right)^{-n}*x^m=\left(\left(x^{-1}\right)^{-n-m}*\left(x^{-1}\right)^{m}\right)*x^m=\left(x^{-1}\right)^{-n-m}=x^{n+m}.$$

□

Corollaire I.20. *Si E est muni l'une lci associative, alors :*

1. *$\{x^n \mid n \in \mathbb{N}^*\}$ est la plus petite partie de E stable par $*$ contenant x ;*
2. *si de plus x est inversible, $\{x^n \mid n \in \mathbb{Z}\}$ est la plus petite partie de E stable par $*$, contenant x, et dans laquelle x (et en fait chaque élément) est inversible.*

Démonstration. La stabilité découle de la proposition précédente.
Pour la minimalité :

1. si A est stable et $x \in A$, une récurrence immédiate montre que : $\forall n \in \mathbb{N}^*,\ x^n \in A$;
2. si x est de plus inversible dans A, alors $x^{-1} \in A$, donc $\forall n \in \mathbb{Z}_-^*,\ x^n \in A$; et $x * x^{-1} \in A$ donc : $\forall n \in \mathbb{Z},\ x^n \in A$.

□

II Groupes

II.1 Généralités

Définition II.1 (Groupe)**.** *Si G est un ensemble muni d'une lci $*$, on dit que $(G, *)$ est un **groupe** si :*

1. *$*$ est associative ;*
2. *$*$ possède un élément neutre **dans** G ;*
3. *tout élément x de G possède un inverse **dans** G.*

*Si la loi $*$ est commutative, on dira que G est un **groupe commutatif** ou un **groupe abélien**.*

Exemples II.2.

1. *$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, munis de l'addition, sont des groupes abéliens ;*
2. *$\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{R}_+^*$ ou $\mathbb{C}^*$, munis de la multiplication, sont des groupes abéliens ;*
3. *$(\mathbb{N}, +)$ ou $(\mathbb{R}, \times)$ ne sont pas des groupes : dans le premier cas, 0 est l'unique élément possédant un inverse, tandis que dans le second 0 est le seul n'en possédant pas ;*
4. *si $n \in \mathbb{N}^*$, l'ensemble des classes modulo n des entiers, muni de l'addition modulaire, est un groupe commutatif.*
5. *l'ensemble $\mathcal{M}_{n,p}(\mathbb{K})$ est un groupe pour l'addition ; $\mathcal{M}_n(\mathbb{K})$ n'est pas un groupe pour la multiplication, mais $\mathrm{GL}_n(\mathbb{K})$ en est un.*

Remarque II.3. *Si $(G, *)$ est un groupe, tout élément est régulier. Et il suffit d'avoir $x * y = e_G$ pour avoir $y = x^{-1}$ (même si G n'est pas commutatif).*

Proposition-Définition II.4. *Si E est un ensemble non vide, on note $\mathcal{S}_E$ ou $\mathfrak{S}(E)$ l'ensemble des bijections de E sur lui-même.*
*Alors $(\mathcal{S}_E, \circ)$ est un groupe, qu'on appelle le **groupe symétrique sur** E. Ses éléments sont appelés les **permutations sur** E.*
Si $n \in \mathbb{N}^*$, on notera plus simplement $\mathfrak{S}_n$ ou S_n le groupe symétrique sur $[\![1; n]\!]$.

Démonstration. Il est clair que $\circ$ est une lci sur $\mathcal{S}_E$ (la composée de deux bijections est une bijection).
La composition est associative, et id_E est l'élément neutre.
Et si $\sigma \in \mathcal{S}_E$, son inverse est la bijection réciproque σ^{-1} qui est bien dans $\mathcal{S}_E$.
Donc $(\mathcal{S}_E, \circ)$ est bien un groupe. □

Remarque II.5. *Le groupe $\mathfrak{S}(E)$ est non commutatif si, et seulement si, E possède au moins trois éléments.*

Proposition-Définition II.6 (Groupe produit)**.** *Si $(G_1, *_1)$ et $(G_2, *_2)$ sont deux groupes, on définit la lci $*$ sur $G_1 \times G_2$ par :*

$$\forall (g_1, g_2), (g_1', g_2') \in G_1 \times G_2,\ (g_1, g_2) * (g_1', g_2') = (g_1 *_1 g_1', g_2 *_2 g_2').$$

Muni de cette loi, $G_1 \times G_2$ est un groupe, appelé ***groupe produit*** *ou* ***produit direct*** *de G_1 et G_2.*
De plus, $(G_1 \times G_2, *)$ est abélien si, et seulement si, $(G_1, *_1)$ et $(G_2, *_2)$ le sont.

Démonstration. Il est clair que $*$ est une lci sur $G_1 \times G_2$.
Pour l'associativité, si $x_1, y_1, z_1 \in G_1$ et $x_2, y_2, z_2 \in G_2$, alors :

$$\begin{array}{rcl} ((x_1, x_2) * (y_1, y_2)) * (z_1, z_2) & = & (x_1 *_1 y_1, x_2 *_2 y_2) * (z_1, z_2) = (x_1 *_1 y_1 *_1 z_1, x_2 *_2 y_2 *_2 z_2) \\ & = & (x_1, x_2) * (y_1 *_1 z_1, y_2 *_2 z_2) = (x_1, x_2) * ((y_1, y_2) * (z_1, z_2)) \end{array}$$

L'élément neutre est (e_1, e_2).
Et il est clair que $(x_1, x_2)^{-1} = (x_1^{-1}, x_2^{-1})$. □

II.2 Sous-groupes

Définition II.7. *Si $(G, *)$ est un groupe et H est une partie de G, on dit que H est un* ***sous-groupe*** *de G si H est stable par $*$ et que $(H, *)$ est un groupe.*

Remarque II.8. *Les parties G et $\{e_G\}$ sont toujours des sous-groupes, qu'on appelle* ***sous-groupes triviaux****.*

Proposition II.9. *Si $(G, *)$ est un groupe et H une partie de G, on a équivalence entre :*

1. *H est un sous-groupe de G ;*
2. $\left\{ \begin{array}{ccc} (i) & H \neq \emptyset & \\ (ii) & \forall x, y \in H & x * y \in H \\ (iii) & \forall x \in H & x^{-1} \in H \end{array} \right.$;
3. $\left\{ \begin{array}{ccc} (i) & H \neq \emptyset & \\ (ii) & \forall x, y \in H & x * y^{-1} \in H \end{array} \right.$.

Démonstration. Les implications *1.*⇒*2.*⇒*3.* sont claires.
Montrons que *3.*⇒*1.* :

— comme $H \neq \emptyset$, on peut considérer $a \in H$. Mais alors : $a * a^{-1} = e \in H$.
Donc si $y \in H$: $e * y^{-1} = y^{-1} \in H$.
Et donc si $x, y \in H$: $x * (y^{-1})^{-1} = x * y \in H$.
Donc H est stable par $*$.

— L'associativité de $*$ est conservée par restriction.
Comme $e \in H$, alors $*$ a bien un élément neutre.
Si $x \in H$, alors $x^{-1} \in H$ et $x * x^{-1} = e = x^{-1} * x$.
Donc $(H, *)$ est bien un groupe.

Ce qui conclut la preuve. □

Remarque II.10. *Un sous-groupe de G contient toujours e_G, donc en pratique pour montrer que H est non vide on pourra chercher à montrer que $e_G \in H$.*

Exemples II.11.

1. *$\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{R}$ sont des sous-groupes de $(\mathbb{C}, +)$;*
2. *$\mathbb{Q}_+^*$, $\mathbb{Q}^*$, $\mathbb{R}_+^*$, $\mathbb{R}^*$, $\mathbb{U}$ sont des sous-groupes de $(\mathbb{C}^*, \times)$;*

3. *si $n \in \mathbb{N}$, l'ensemble $n\mathbb{Z} = \{na \,|\, a \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}, +)$ (et on verra que tous les sous-groupes de $\mathbb{Z}$ sont de cette forme).*

Proposition II.12. *Si $(H_i)_{i\in I}$ est une famille de sous-groupes de $(G, *)$, alors $H = \cap_{i\in I} H_i$ est un sous-groupe de G.*

Démonstration. Puisque e_G est toujours un élément d'un sous-groupe, alors : pour tout $i \in I$, $e_G \in H_i$. Donc $e_G \in H$ et $H \neq \emptyset$.
Si $x, y \in H$ et $i \in I$: alors $x, y \in H_i$, donc $x * y^{-1} \in H_i$. Comme c'est vrai pour tout i, alors : $x * y^{-1} \in H$, donc H est un sous-groupe de G. □

Corollaire II.13. *Si $X \subset G$, alors :* $\bigcap_{\substack{H \text{ sous-groupe de } G \\ X \subset H}}$ *H est le plus petit sous-groupe de G contenant X.*

Proposition-Définition II.14. *Soit G un groupe et $g \in G$. on définit $\langle g \rangle = \{g^n \,|\, n \in \mathbb{Z}\}$, qu'on appelle le* ***sous-groupe engendré par*** *g.*
C'est le plus petit sous-groupe de G contenant g.

Démonstration. On montre facilement que $\langle g \rangle$ est un sous-groupe de G : il est non vide et : $\forall n, m \in \mathbb{Z},\ g^n * (g^m)^{-1} = g^n * g^{-m} = g^{n-m}$.
Il est minimal par les propriétés des parties stables. □

II.3 Morphismes de groupe

Définition II.15. *Soient $(G, *)$ et $(H, \cdot)$ deux groupes. Une application $f : G \to H$ est un* ***morphisme de groupes*** *si elle vérifie :*

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

Exemples II.16.

1. *la fonction* ln *est un morphisme de groupe de $(\mathbb{R}_+^*, \times)$ sur $(\mathbb{R}, +)$;*
2. *la fonction* exp *est un morphisme de groupe de $(\mathbb{R}, +)$ sur $(\mathbb{R}_+^*, \times)$;*
3. *si $a \in \mathbb{R}^*$, l'application : $f : \left\{ \begin{array}{ccc} (\mathbb{Z}, +) & \to & (\mathbb{R}^*, \times) \\ n & \mapsto & a^n \end{array} \right.$ est un morphisme de groupe.*

Proposition II.17. *Si f est un morphisme de groupe de G vers H :*

1. *$f(e_G) = e_H$;*
2. *si $x \in G$: $f(x^{-1}) = [f(x)]^{-1}$.*

Démonstration. 1. $f(e_G) = f(e_G * e_G) = f(e_G) \cdot f(e_G)$, donc en simplifiant par $f(e_G)$: $f(e_G) = e_H$;
2. $f(x) \cdot f(x^{-1}) = f(x * x^{-1}) = f(e_G) = e_H$ donc $f(x^{-1}) = (f(x))^{-1}$.

□

Définition II.18. *Si $f : G \to H$ est un morphisme de groupe, on définit son* ***noyau*** *comme :*

$$\mathrm{Ker} f = f^{-1}(\{e_H\}) = \{x \in G \,|\, f(x) = e_H\}$$

et son ***image*** *comme :*

$$\mathrm{Im} f = f(G) = \{f(x) \,|\, x \in G\}.$$

Proposition II.19. *Si $f : G \to H$ est un morphisme de groupe, alors :*

1. *$\mathrm{Ker} f$ est un sous-groupe de G ;*

2. $\mathrm{Im}f$ *est un sous-groupe de* H.

Plus généralement :

1. *l'image réciproque par* f *d'un sous-groupe de* H *est un sous-groupe de* G *;*
2. *l'image directe par* f *d'un sous-groupe de* G *est un sous-groupe de* H.

Démonstration. On montre directement le cas général. Soit G' un sous-groupe de G, et H' un sous-groupe de H :

1. comme $e_H \in H'$ et $f(e_G) = e_H$, alors $e_G \in f^{-1}(H')$, donc $f^{-1}(H') \neq \emptyset$. Si $x_1, x_2 \in f^{-1}(H')$, (donc $f(x_1), f(x_2) \in H'$) alors :

$$f(x_1 * x_2^{-1}) = f(x_1) \cdot f(x_2^{-1}) = f(x_1) \cdot [f(x_2)]^{-1} \in H'$$

   donc $x_1 * x_2^{-1} \in f^{-1}(H')$, qui est donc un sous-groupe de G.

2. comme $e_G \in G'$ et $f(e_G) = e_H$, alors $e_H \in f(G')$, donc $f(G') \neq \emptyset$. Si $y_1, y_2 \in f(G')$. Notons $x_1, x_2 \in G'$ tels que : $f(x_1) = y_1$ et $f(x_2) = y_2$. Alors $y_1 \cdot y_2^{-1} = f(x_1 * x_2^{-1}) \in f(G')$, donc $f(G')$ est un sous-groupe de H.

□

Proposition II.20. *Si* $f : G \to H$ *est un morphisme de groupe, alors* f *est injectif si, et seulement si,* $\mathrm{Ker}f = \{e_G\}$.

Démonstration.
- si f est injective : on a déjà $f(e_G) = e_H$. Mais par injectivité, e_H possède au plus un antécédent par f, donc $\mathrm{Ker}f = \{e_G\}$;
- si $\mathrm{Ker}f = \{e_G\}$: soient $x, y \in G$. Alors :

$$f(x) = f(y) \Leftrightarrow f(x) \cdot [f(y)]^{-1} = e_H \Leftrightarrow f(x * y^{-1}) = e_H \Leftrightarrow x * y^{-1} \in \mathrm{Ker}f \Leftrightarrow x * y^{-1} = e_G \Leftrightarrow x = y$$

  d'où l'injectivité de f.

□

Proposition II.21. *Si* $f : G \to H$ *et* $g : H \to K$ *sont deux morphismes de groupes, alors* $g \circ f$ *est un morphisme de groupe de* G *dans* K.

Démonstration. Évident. □

Proposition-Définition II.22. *Un morphisme de groupe* $f : G \to H$ *bijectif est appelé un* ***isomorphisme de groupes****. Sous ces conditions,* f^{-1} *est aussi un isomorphisme de groupe de* H *sur* G.
Quand $G = H$*, on parlera d'****automorphisme du groupe*** G.

Démonstration. Soient $y_1, y_2 \in H$. On pose $x_1 = f^{-1}(y_1)$ et $x_2 = f^{-1}(y_2)$. Alors :

$$\begin{array}{rcl} f^{-1}(y_1) * f^{-1}(y_2) & = & x_1 * x_2 = f^{-1}\left[f(x_1 * x_2)\right] \\ & = & f^{-1}\left[f(x_1) \cdot f(x_2)\right] = f^{-1}\left(y_1 \cdot y_2\right) \end{array}$$

et ainsi : $f^{-1}\left(y_1 \cdot y_2\right) = f^{-1}(y_1) * f^{-1}(y_2)$, donc f^{-1} est bien un morphisme de groupe. □

III Anneaux

III.1 Généralités

Définition III.1 (Anneau)**.** *Si A est un ensemble muni de deux lci $+$ et $\times$, on dit que $(A,+,\times)$ est un* ***anneau (unitaire)*** *si :*

1. *$(A,+)$ est un groupe abélien ;*
2. *$\times$ est associative et possède un élément neutre ;*
3. *$\times$ est distributive par rapport à $+$.*

Si $\times$ est commutative, on dira que A est un ***anneau commutatif***

Remarque III.2. *Pour correspondre aux lois usuelles, on notera 0_A le neutre de $+$ et 1_A celui de $\times$. On adopte la notation additive pour la loi $+$ et multiplicative pour $\times$.*

Exemples III.3.

1. *$(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des anneaux commutatifs ;*
2. *si E est un ensemble non vide, l'ensemble $A=\mathcal{F}(E,\mathbb{R})$ muni des lois : $f+g : x\mapsto f(x)+g(x)$ et $f\times g : x\mapsto f(x)\times g(x)$ est un anneau commutatif ; 0_A est la fonction nulle $x\mapsto 0$ et 1_A est la fonction indicatrice de E : $x\mapsto 1$;*
3. *si $n\in\mathbb{N}^*$, l'ensemble des classes modulo n des entiers, muni de l'addition et de la multiplication modulaires, est un anneau commutatif avec $0_A=\overline{0}$ et $1_A=\overline{1}$. On note cet anneau $\mathbb{Z}/n\mathbb{Z}$;*
4. *$\mathcal{M}_n(\mathbb{K})$ muni de l'addition et de la multiplication matricielles est un anneau ; il est non commutatif dès que $n\geq 2$.*

Proposition III.4 (Règles de calcul dans un anneau)**.** *Si $(A,+,\times)$ est un anneau et $x,y,z\in A$, alors :*

1. *$x\times 0_A=0_A=0_A\times x$;*
2. *$x\times(-y)=-(x\times y)=(-x)\times y$;*
3. *$x\times(y-z)=x\times y-x\times z$ et $(y-z)\times x=y\times x-z\times x$;*
4. *pour tout $n\in\mathbb{Z}$: $x\times(ny)=n(x\times y)=(nx)\times y$.*

Démonstration.

1. $x\times 0_A+x\times 0_A=x\times(0_A+0_A)=x\times 0_A$. Et en simplifiant par $x\times 0_A$ (dans le groupe $(A,+)$), on a :$x\times 0_A=0_A$;
2. $x\times y+x\times(-y)=x\times(y+(-y))=x\times 0_A=0_A$ donc $x\times(-y)=-(x\times y)$;

et le reste en exercice. □

Proposition III.5. *Si $a,b\in A$ commutent (soit $a\times b=b\times a$) et $n\in\mathbb{N}^*$, alors :*

1. $(a+b)^n=\displaystyle\sum_{k=0}^{n}\binom{n}{k}a^kb^{n-k}$;
2. $a^n-b^n=(a-b)\displaystyle\sum_{k=0}^{n-1}a^kb^{n-1-k}$.

Démonstration. Comme dans $\mathbb{R}$ ou $\mathbb{C}$, ou dans les matrices. □

Remarque III.6. *Si a et b ne commutent pas, les formules deviennent vite compliquées. Par exemple :*

$$(a+b)^2=a^2+a\times b+b\times a+b^2.$$

III.2 Division dans les anneaux

Définition III.7. *Si $(A,+,\times)$ est un anneau :*

1. *un élément $a \in A \setminus \{0\}$ est appelé **diviseur de zéro** s'il existe $b \in A \setminus \{0\}$ tel que $a \times b = 0_A$ ou $b \times a = 0_A$;*
2. *un élément $a \in A \setminus \{0\}$ est dit **nilpotent** s'il existe $n \in \mathbb{N}^*$ tel que : $a^n = 0_A$;*
3. *A est dit **intègre** si A est commutatif et que : $\forall a, b \in A,\ a \times b = 0_A \Rightarrow a = 0_A$ ou $b = 0_A$.*

Remarques III.8.

1. *On peut diviser une égalité par un nombre qui n'est pas un diviseur de zéro.*
2. *Un anneau intègre ne possède pas de diviseurs de zéro. Et donc dans un anneau intègre, si $a \neq 0$: $ab = ac \Rightarrow b = c$.*

Exemples III.9.

1. *les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ sont intègres ;*
2. *si E possède plus d'un élément, l'anneau $(\mathcal{F}(E,\mathbb{R}),+,\times)$ est un anneau commutatif mais n'est pas intègre : si $a \neq b \in E$, alors $\mathbb{1}_{\{a\}} \times \mathbb{1}_{\{b\}} = 0$;*
3. *si $n \in \mathbb{N}^*$ et $m \in \mathbb{Z}$, alors $\overline{m}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, il est premier avec n ; et $\mathbb{Z}/n\mathbb{Z}$ est intègre si, et seulement si, n est premier ;*
4. *si $n \geq 2$, alors $\mathcal{M}_n(\mathbb{K})$ n'est pas intègre ; les matrices triangulaires de diagonales nulles (triangulaires strictes) sont nilpotentes ;*

Proposition-Définition III.10. *Un élément de l'anneau $(A,+,\times)$ est dit **inversible** s'il possède un inverse pour la loi $\times$.*
*L'ensemble des éléments inversibles de A est noté $A^\times$: c'est un groupe pour la loi $\times$ appelé **groupe des inversibles** ou **groupe des unités** de A.*

Démonstration. On montre toutes les propriétés d'un groupe :
— si $a, b \in A^\times$, alors :
$$(a \times b) \times (b^{-1} \times a^{-1}) = 1_A = (b^{-1} \times a^{-1}) \times (a \times b)$$
par associativité, donc $a \times b \in A^\times$: $\times$ est bien une lci sur $A^\times$.
— l'associativité est acquise par restriction, et 1_A est clairement le neutre ;
— si $a \in A^\times$, alors : $a \times a^{-1} = 1_A = a^{-1} \times a$, donc $a^{-1} \in A^\times$.
Donc $(A^\times,\times)$ est un groupe. □

Proposition III.11. *Si a est inversible, alors a n'est pas un diviseur de 0.*

Démonstration. Si $b \in A$: $a \times b = 0 \Rightarrow b = a^{-1} \times 0 = 0$ (et pareil si $b \times a = 0$). □

Exemples III.12.
1. *On a $\mathbb{Q}^* = \mathbb{Q}^\times$, $\mathbb{R}^* = \mathbb{R}^\times$ et $\mathbb{C}^* = \mathbb{C}^\times$.*
En revanche : $\mathbb{Z}^\times = \{-1;1\} \neq \mathbb{Z}^*$.
Et $\mathbb{D}$ n'est pas non plus un corps (par exemple : $\frac{1}{3} \notin \mathbb{D}$, donc 3 n'est pas inversible dans $\mathbb{D}$).
2. *Les éléments de $(\mathcal{F}(E,\mathbb{R}),+,\times)$ inversibles sont exactement les fonctions ne s'annulant jamais.*
3. *Pour les matrices, on a : $\mathcal{M}_n(\mathbb{K})^\times = \mathrm{GL}_n(\mathbb{K})$.*

Définition III.13. *Un anneau commutatif dont tous les éléments non-nuls sont inversible est appelé un **corps***

Remarque III.14. *Cela revient à dire qu'un anneau commutatif A est un corps si : $A^\times = A \setminus \{0\}$.*

Exemples III.15.

1. *$\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps, mais pas $\mathbb{D}$;*
2. *l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est un nombre premier.*

III.3 Sous-anneaux

Définition III.16. *Si $(A,+,\times)$ est un anneau, et B est une partie de A, on dit que B est un* ***sous-anneau*** *de A si :*

1. *B est stable par $+$ et par $\times$;*
2. *B contient 1_A ;*
3. *$(B,+,\times)$ est un anneau.*

Proposition III.17. *Si B est une partie d'un anneau $(A,+,\times)$, alors B est un sous-anneau de A si, et seulement si :*

1. $1_A \in B$;
2. $\forall x,y \in B,\ x-y \in B$;
3. $\forall x,y \in B,\ x\times y \in B$.

Démonstration. La nécessité est évidente.
Pour la suffisance :

— par *1* et *2*, on déduit que V est un sous-groupe de $(A,+)$, donc est un groupe abélien (donc est stable par $+$) ;
— par *3* : B est stable par $\times$;
— l'associativité et la distributivité de $\times$ découlent de celle sur A ;
— B possède 1_A donc a un neutre pour $\times$.

Donc B est bien un sous-anneau. □

Exemples III.18.

1. *les ensembles Z, $\mathbb{Q}$,$\mathbb{R}$ sont des sous-anneaux de $(\mathbb{C},+,\times)$.*
2. *Si $n \in \mathbb{N}$, l'ensemble $n\mathbb{Z} = \{na \,|\, a \in \mathbb{Z}\}$ est un sous-anneau de $(\mathbb{Z},+)$ (et tous les sous-anneaux de $\mathbb{Z}$ sont de cette forme).*
3. *Les ensembles des matrices triangulaires supérieures, des matrices triangulaires supérieures, ou des matrices diagonales sont des sous-anneaux de $\mathcal{M}_n(\mathbb{K})$ (comme on a vu qu'ils sont stables par produit).*

Remarque III.19. *On a aussi ne notion de sous-corps : c'est un sous-anneau qui est un corps.*

Exemple III.20. *Montrons que $\mathbb{Z}[i] = \{a+ib \,|\, a,b \in \mathbb{Z}\}$ est un anneau (muni de $+,\times$).*
Il suffit de montrer que c'est un sous-anneau de $(\mathbb{C},+,\times)$;

1. $1 = 1 + 0\cdot i \in \mathbb{Z}[i]$;
2. *si $x = a+ib, y = \alpha+i\beta \in \mathbb{Z}[i]$, alors :* $x-y = \underbrace{(a-\alpha)}_{\in\mathbb{Z}} + i\,\underbrace{(b-\beta)}_{\in\mathbb{Z}} \in \mathbb{Z}[i]$;
3. *de même :* $x\times y = \underbrace{(a\alpha - b\beta)}_{\in\mathbb{Z}} + i\,\underbrace{(a\beta+b\alpha)}_{\in\mathbb{Z}} \in \mathbb{Z}[i]$.

Donc $(\mathbb{Z}[i],+,\times)$ est un anneau.
On peut voir en revanche que ce n'est pas un corps, et plus précisément que : $\mathbb{Z}[i]^\times = \{\pm 1; \pm i\}$.

III.4 Morphismes d'anneaux

Définition III.21. *Si $(A,+_A,\times_A)$ et $(B,+_B,\times_B)$ sont deux anneaux, un* ***morphisme d'anneaux*** *est une application $f : A \to B$ telle que :*

1. $\forall x,y \in A,\ f(x+_A y) = f(x) +_B f(y)$;
2. $\forall x,y \in A,\ f(x\times_A y) = f(x) \times_B f(y)$;

3. $f(1_A) = 1_B$.

Exemples III.22.

1. *La conjugaison complexe est un morphisme d'anneaux de $\mathbb{C}$ dans lui-même. Sa restriction à $\mathbb{Z}[i]$ est aussi un morphisme d'anneau.*
2. *L'identité est le seul morphisme d'anneaux de $(\mathbb{R}, +, \times)$ dans lui-même.*
3. *Pour $n \in \mathbb{N}^*$, l'application $\begin{cases} \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ k & \mapsto & \overline{k} \end{cases}$ qui à un entier associe sa classe de congruence modulo n est un morphisme d'anneaux surjectif de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$. Plus généralement, si n divise m, l'application $\begin{cases} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \\ \overline{k}_n & \mapsto & \overline{k}_m \end{cases}$ qui à une classe modulo n associe la classe correspondant modulo m est également un morphisme d'anneaux.*

Proposition III.23. *Si $f : A \to B$ est un morphisme d'anneaux, et que A' (resp. B') est un sous-anneau de A (resp. de B), alors $f(A')$ (resp. $f^{-1}(B')$) est un sous-anneau de B (resp. de A).*

Démonstration. Comme pour les morphismes de groupes, en vérifiant les propriétés des sous-anneaux. □

Proposition III.24. *Le composée de morphismes d'anneaux est encore un morphisme d'anneaux.*
Un morphisme d'anneau bijectif est appelé un ***isomorphisme d'anneaux****, et son application réciproque est aussi un isomorphisme d'anneaux.*
Un isomorphisme d'anneau sur lui-même est appelé ***automorphisme d'anneau****.*

Chapitre 16

Continuité et limites

I Limites de fonctions

I.1 Voisinage et points adhérents

Définition I.1. *Si $I \subset \mathbb{R}$ et $a \in \mathbb{R}$, on dit que I est un* ***voisinage*** *de a s'il existe $\varepsilon > 0$ tel que $]a-\varepsilon; a+\varepsilon[\subset I$. Si $a = +\infty$ (resp. -∞) on dira de même que I est un voisinage de a s'il existe $A \in \mathbb{R}$ tel que $]A; +\infty[\subset I$ (resp. $]-\infty; A[\subset I$).*

Remarques I.2.

1. *Si $a \in \mathbb{R}$ et que I est un voisinage de a, alors $a \in I$ (c'est une condition nécessaire, mais non suffisante).*
2. *Pour le cas où $a \in \mathbb{R}$, cela revient à dire que I contient un intervalle ouvert contenant a.*

Exemple I.3. *Considérons l'ensemble $I = [0; 1[$. Alors :*
- *I est un voisinage de $\frac{1}{2}$, car : $]\frac{1}{4}; \frac{3}{4}[=]\frac{1}{2} - \frac{1}{4}; \frac{1}{2} + \frac{1}{4}[\subset I$ (qui correspond bien à la définition avec $\varepsilon = \frac{1}{4} > 0$) ;*
- *plus généralement, I est un voisinage de tout élément de $]0; 1[$: si $a \in]0; 1[$, alors en posant $\varepsilon = \min(a, 1-a)$ on a bien $\varepsilon > 0$ et $a - \varepsilon \geq 0$, $a + \varepsilon \leq 1$ donc $]a-\varepsilon; a+\varepsilon[\subset I$;*
- *à l'inverse, I n'est le voisinage d'aucun élément n'appartenant pas à I ;*
- *reste donc le cas de 0, dont I n'est pas un voisinage : par l'absurde, si on avait $\varepsilon > 0$ avec $]-\varepsilon; \varepsilon[\subset I$, alors on aurait $-\frac{\varepsilon}{2} \in I$, ce qui est impossible car $-\frac{\varepsilon}{2} < 0$.*

Définition I.4. *Si $I \subset \mathbb{R}$ et $a \in \overline{\mathbb{R}}$, on dit que a est* ***adhérent*** *à I si tout voisinage de a intersecte I.*

Remarques I.5.

1. *Si $a \in I$ alors a est adhérent à I (c'est une condition suffisante, mais non nécessaire)*
2. *Si $a = +\infty$ (resp. $-\infty$), du fait de la forme des voisinages de a, cela revient à dire que I n'est pas majoré (resp. pas minoré).*

Exemple I.6. *Reprenons l'ensemble $I = [0; 1[$. Alors :*
- *tout élément de I lui est adhérent ;*
- *si $a > 1$ (resp. $a < 0$), alors a n'est pas adhérent à I : on considère le voisinage $]1; a+1[$ (resp. $]a-1; 0[$) qui est d'intersection vide avec I ;*
- *reste le cas de 1, qui est adhérent à I : si J est un voisinage de 1, alors il existe $\varepsilon > 0$ tel que $]1-\varepsilon; 1+\varepsilon[\subset J$; et donc $1 - \frac{\varepsilon}{2} \in J \cap I$, donc $J \cap I \neq \emptyset$.*

Proposition I.7. *Si $a \in \mathbb{R}$ et I est un intervalle de $\mathbb{R}$, alors :*

1. *I est un voisinage de a si, et seulement si : $a \in \overset{\circ}{I}$;*

2. *a est adhérent à I si, et seulement si : $a \in \overline{I}$.*

Démonstration. Par disjonction de cas suivants la forme de I. □

Remarque I.8. *Les voisinages et les points adhérents se comprennent bien en terme de réels que l'on peut approcher. Plus précisément, si $a \in \mathbb{R}$ et $I \subset \mathbb{R}$, alors :*

1. *I est un voisinage de a si tout réel suffisamment proche de a est dans I :*

$$\exists \varepsilon > 0, \forall x \in \mathbb{R}, |x - a| \leq \varepsilon \Rightarrow x \in I;$$

2. *a est adhérent à I si on peut trouver des réel aussi proche de a que l'on veut dans I :*

$$\forall \varepsilon > 0, \exists x \in \mathbb{R}, |x - a| \leq \varepsilon \text{ et } x \in I.$$

Définition I.9. *Si f est une fonction définie sur un ensemble I, et $a \in \overline{R}$, on dira que f vérifie une propriété* ***au voisinage de*** *a s'il existe un voisinage J de a tel que $f|_{I \cap J}$ vérifie cette propriété.*

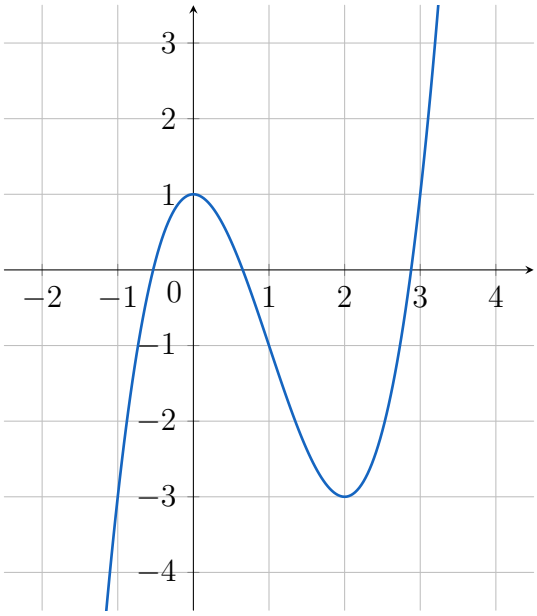
Exemples I.10.

1. *du fait des formes des voisinages de $+\infty$, une propriété vraie au voisinage de $+\infty$ est vérifiée pour x suffisamment grand. Par exemple :* ln *est positive au voisinage de $+\infty$, de même que tout polynôme de coefficient dominant positif.*
2. *au voisinage de 0, on peut dire que :*
   — *la fonction* sin *est strictement croissante : en la regardant sur $[-\frac{\pi}{2}; \frac{\pi}{2}$ par exemple ,*
   — *la fonction* cos *ne s'annule pas : en la regardant sur le même intervalle.*
   En revanche, la fonction cos *n'est pas monotone au voisinage de 0.*

Définition I.11. *On dit qu'une fonction f définie sur I admet un* ***maximum local*** *(resp. minimum local, extremum local) en $a \in I$ si elle admet au voisinage de a un maximum (resp. minimum, extremum) en a.*

Remarque I.12. *Pour différencier un extremum d'un extremum local, on parlera d'extremum global.*

Exemple I.13. *La fonction $f : x \mapsto x^3 - 3x^2 + 1$ admet un maximum local en 0 (avec $f(0) = 1$) et un minimum local en 2 (avec $f(2) = -3$). Ils ne sont pas globaux comme f n'est ni majorée ni minorée sur $\mathbb{R}$ (en tant que polynôme de degré impair).*



I.2 Limite d'une fonction

Définition I.14. *Soient $f : I \to \mathbb{R}$, $a \in \overline{\mathbb{R}}$ adhérent à I et $l \in \overline{\mathbb{R}}$. Alors on définit le fait que f tende vers l en a de l'une des 9 manières suivantes :*

1. *si $a \in \mathbb{R}$:*
   (a) *on dit que f tend vers $l \in \mathbb{R}$ lorsque x tend vers a, ce que l'on note $\lim\limits_{x\to a} f(x) = l$, si :*
   $$\forall \varepsilon > 0, \exists \eta > 0,\ \forall x \in I,\ |x - a| \leq \eta \Rightarrow |f(x) - l| \leq \varepsilon;$$
   (b) *on dit que f tend vers $+\infty$ en a, ce que l'on note $\lim\limits_{x\to a} f(x) = +\infty$, si :*
   $$\forall A \in \mathbb{R}, \exists \eta > 0,\ \forall x \in I,\ |x - a| \leq \eta \Rightarrow f(x) \geq A;$$
   (c) *on dit que f tend vers $-\infty$ en a, ce que l'on note $\lim\limits_{x\to a} f(x) = -\infty$, si :*
   $$\forall A \in \mathbb{R}, \exists \eta > 0,\ \forall x \in I,\ |x - a| \leq \eta \Rightarrow f(x) \leq A;$$
2. *si $a = +\infty$:*
   (a) *on dit que f tend vers $l \in \mathbb{R}$ lorsque x tend vers $+\infty$, ce que l'on note $\lim\limits_{x\to+\infty} f(x) = l$, si :*
   $$\forall \varepsilon > 0, \exists B \in \mathbb{R},\ \forall x \in I,\ x \geq B \Rightarrow |f(x) - l| \leq \varepsilon;$$
   (b) *on dit que f tend vers $+\infty$ en $+\infty$, ce que l'on note $\lim\limits_{x\to+\infty} f(x) = +\infty$, si :*
   $$\forall A \in \mathbb{R}, \exists B \in \mathbb{R},\ \forall x \in I,\ x \geq B \Rightarrow f(x) \geq A;$$
   (c) *on dit que f tend vers $-\infty$ en $+\infty$, ce que l'on note $\lim\limits_{x\to+\infty} f(x) = -\infty$, si :*
   $$\forall A \in \mathbb{R}, \exists B \in \mathbb{R},\ \forall x \in I,\ x \geq B \Rightarrow f(x) \leq A;$$
3. *si $a = -\infty$:*
   (a) *on dit que f tend vers $l \in \mathbb{R}$ lorsque x tend vers $-\infty$, ce que l'on note $\lim\limits_{x\to-\infty} f(x) = l$, si :*
   $$\forall \varepsilon > 0, \exists B \in \mathbb{R},\ \forall x \in I,\ x \leq B \Rightarrow |f(x) - l| \leq \varepsilon;$$
   (b) *on dit que f tend vers $+\infty$ en $-\infty$, ce que l'on note $\lim\limits_{x\to-\infty} f(x) = +\infty$, si :*
   $$\forall A \in \mathbb{R}, \exists B \in \mathbb{R},\ \forall x \in I,\ x \leq B \Rightarrow f(x) \geq A;$$
   (c) *on dit que f tend vers $-\infty$ en $-\infty$, ce que l'on note $\lim\limits_{x\to-\infty} f(x) = -\infty$, si :*
   $$\forall A \in \mathbb{R}, \exists B \in \mathbb{R},\ \forall x \in I,\ x \leq B \Rightarrow f(x) \leq A;$$

Remarques I.15.

1. *Vue comme une fonction sur $\mathbb{N}$, on retrouve bien la définition de la limite d'une suite, qui correspond à la limite en $+\infty$ de la fonction qui lui est associée (où le B joue le rôle de n_0).*
2. *Comme pour les suites, on pourra aussi noter $f(x) \underset{x\to a}{\to} l$ au lieu de $\lim\limits_{x\to a} f(x) = l$.*

Remarques I.16.

1. *Le fait de prendre a adhérent à I permet de travailler avec des objets bien définis, et qui existent bien. Si ce n'était pas le cas, toutes les limites seraient possibles car alors l'ensemble des $x \in I$ tels que $|x-a| \leq \eta,\ x \leq B,\ x \geq B$ (selon les cas) serait vide pour des valeurs suffisamment mal choisies de η ou de B.*
2. *On peut synthétiser ces résultats en disant que f tend vers l en a si, et seulement si, pour tout voisinage V_l de l, il existe un voisinage V_a de a tel que : $f(V_a) \subset V_l$. Cela permet surtout de n'avoir qu'une seule définition, et donc de n'avoir qu'un seul cas à traiter pour toutes les démonstrations (ce que l'on ne fera pas pour autant dans la suite).*

Proposition I.17 (Unicité de la limite)**.** *Si une fonction tend vers une limite en a, alors cette limite est unique.*

Démonstration. Montrons le par exemple dans le cas où $a \in \mathbb{R}$ avec des limites finies.
Par l'absurde, supposons que la fonction f définie sur I tend simultanément en a vers $l_1, l_2 \in \mathbb{R}$, avec $l_1 \neq l_2$.
Posons $\varepsilon = \dfrac{|l_1 - l_2|}{3}$. Par définition de la limite de f en a :
— il existe $\eta_1 > 0$ tel que, pour tout $x \in I$: $|x-a| \leq \eta_1 \Rightarrow |f(x) - l_1| \leq \varepsilon$;
— il existe $\eta_2 > 0$ tel que, pour tout $x \in I$: $|x-a| \leq \eta_2 \Rightarrow |f(x) - l_2| \leq \varepsilon$.
En posant $\eta = \min(\eta_1, \eta_2)$, considérons $x \in I$ tel que $|x-a| \leq \eta$ (qui existe bien, comme a est adhérent à I). On a alors, pour un tel x :

$$3\varepsilon = |l_1 - l_2| = |f(x) - l_1 + l_2 - f(x)| \leq |f(x) - l_1| + |f(x) - l_2| \leq 2\varepsilon$$

d'où la contradiction avec le fait que $\varepsilon > 0$. □

Proposition I.18. *Supposons que la fonction f tende vers $l \in \overline{\mathbb{R}}$ en $a \in \overline{\mathbb{R}}$. Alors :*

1. *si $l \in \mathbb{R}$, alors f est bornée au voisinage de a ;*
2. *si $l = +\infty$ (resp. $-\infty$), alors f est minorée (resp. majorée) au voisinage de a.*

Démonstration. Montrons le par exemple lorsque $a \in \mathbb{R}$, et appliquons la définition de la limite :

1. si $l \in \mathbb{R}$: avec $\varepsilon = 1$, il existe $\eta > 0$ tel que :

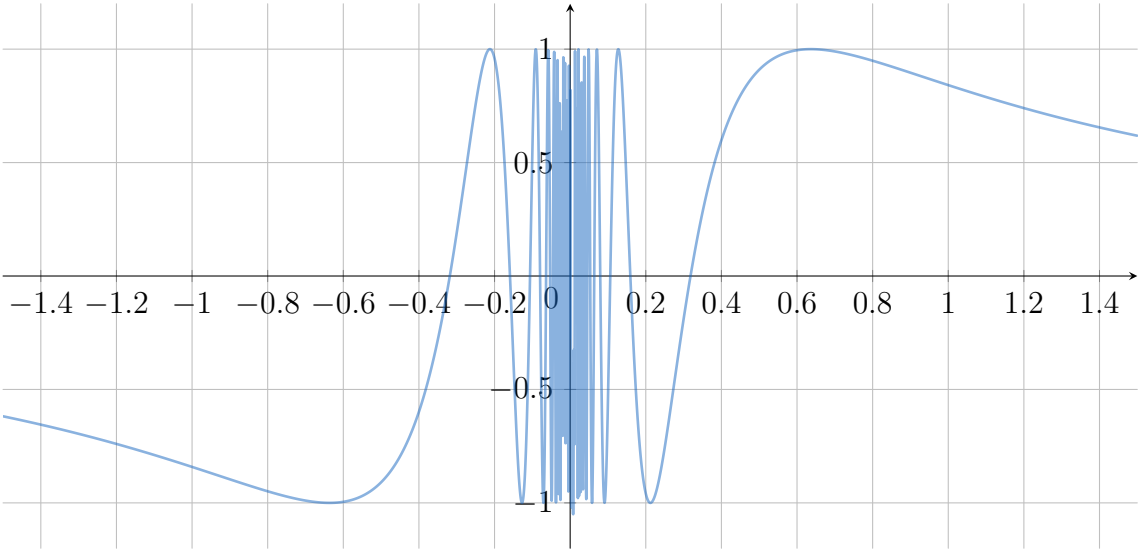
$$\forall x \in I,\ |x-a| \leq \eta \Rightarrow |f(x) - l| \leq 1$$

   et donc, en notant $J =]a-\eta; a+\eta[$, J est un voisinage de a sur lequel f est bornée par $l-1$ et $l+1$, ce qui montre le résultat.
2. si $l = +\infty$ (resp. $-\infty$) : avec $A = 0$, en prenant $\eta > 0$ donné par la définition de la limite, alors $J =]a-\eta; a+\eta[$ est un voisinage de a sur lequel f est minorée (resp. majorée) par 0.

□

Remarques I.19.

1. *Il faut bien prendre garde que le résultat n'est vrai que **au voisinage** de a.*
2. *Les réciproques sont fausses, comme on peut le voir en 0 avec la fonction $x \mapsto \sin(\frac{1}{x})$, qui est bornée mais n'a pas de limite.*



Proposition I.20. *Si f tend vers l en a, avec $l \neq 0$, alors f est non nulle au voisinage de a.*

Démonstration. On distingue suivant la forme de l, et ce peu importe la forme de a :
- si $l \in \mathbb{R}^*$: prendre la définition avec $\varepsilon = \frac{|l|}{2}$ (comme pour le suites) ;
- si $l = +\infty$: prendre la définition avec $A = 1$;
- si $l = -\infty$: prendre la définition avec $A = -1$.

□

Définition I.21. *Si f est définie sur I et $a \in I$, on dit que f est **continue en** a si :* $\lim\limits_{x \to a} f(x) = f(a)$.

Proposition I.22. *Si f est définie en a, et que f a une limite en a, alors :* $\lim\limits_{x \to a} f(x) = f(a)$.

Démonstration. Si $\eta > 0$, alors : $a \in I \cap]a - \eta; a + \eta[$. Ainsi, en notant l la limite de f en a, on a :
- si $l = +\infty$:
$$\forall A \in \mathbb{R},\ f(a) \geq A$$
ce qui est faux, car $A = f(a) + 1$ fournit un contre-exemple ;
- si $l = -\infty$:
$$\forall A \in \mathbb{R},\ f(a) \leq A$$
ce qui est faux, car $A = f(a) - 1$ fournit un contre-exemple ;
- si $l \in \mathbb{R}$:
$$\forall \varepsilon > 0, |f(a) - l| \leq \varepsilon$$
et donc $l = f(a)$, sinon $\varepsilon = \frac{|f(a)-l|}{2}$ fournirait un contre-exemple.

□

Corollaire I.23. *Si f est définie sur I et $a \in I$, alors f est continue en a si, et seulement si, f a une limite en a.*

I.3 Limites à gauche et à droite

Définition I.24. *Si f est définie sur I, et $a \in \mathbb{R}$, on dit que f est définie **à gauche au voisinage de** a (resp. à droite au voisinage de a) si a est adhérent à $I \cap]-\infty; a[$ (resp. à $I \cap]a; +\infty[$).*

Exemple I.25. *Si f est définie sur $[0; 1[$, alors f est définie :*
- *à gauche au voisinage de tout réel de $]0; 1]$;*
- *à droite au voisinage de tout réel de $[0; 1[$.*

Définition I.26. *Si $a \in \mathbb{R}$, $l \in \overline{\mathbb{R}}$ et f définie à gauche (resp. à droite) au voisinage de a, on dit que f a pour limite à gauche (resp. à droite) l en a, ce que l'on note $\lim\limits_{\substack{x\to a\\ x<a}} f(x) = l$ ou $\lim\limits_{x\to a^-} f(x) = l$ (resp. $\lim\limits_{\substack{x\to a\\ x>a}} f(x) = l$ ou $\lim\limits_{x\to a^+} f(x) = l$) si $f|_{I\cap]-\infty;a[}$ (resp. $f|_{I\cap]a;+\infty[}$) tend vers l en a.*

Remarque I.27. *On peut aussi définir les limites à gauche et à droite avec des ε. Par exemple, dire que f a pour limite à gauche l en a se traduit par :*

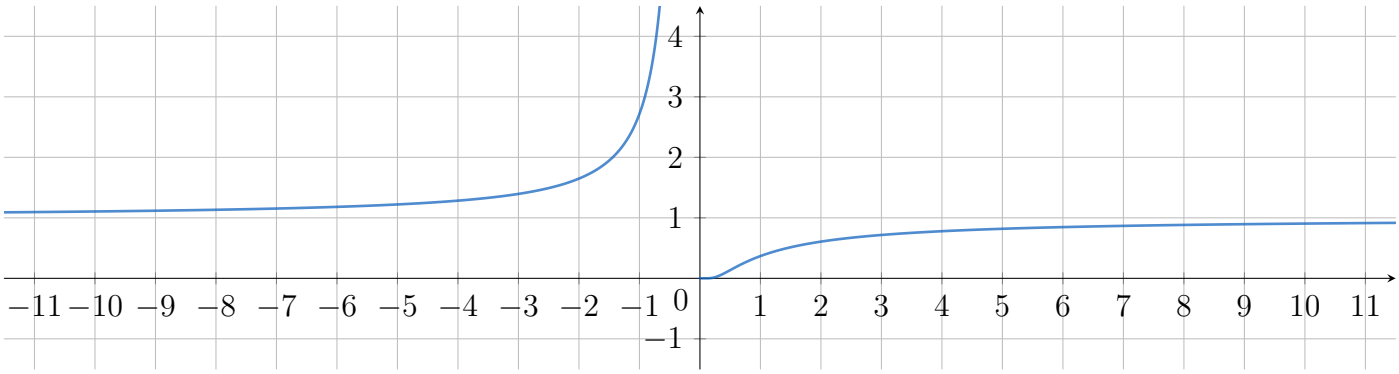
— *si $l \in \mathbb{R}$:*
$$\forall \varepsilon > 0,\ \exists \eta > 0,\ \forall x \in I,\ a - \eta \leq x < a \Rightarrow |f(x) - l| \leq \varepsilon;$$

— *si $l = +\infty$:*
$$\forall A \in \mathbb{R},\ \exists \eta > 0,\ \forall x \in I,\ a - \eta \leq x < a \Rightarrow f(x) \geq A;$$

— *si $l = -\infty$:*
$$\forall A \in \mathbb{R},\ \exists \eta > 0,\ \forall x \in I,\ a - \eta \leq x < a \Rightarrow f(x) \leq A.$$

*Il faut bien faire attention que a n'est **jamais** considéré pour les limites à gauche ou à droite.*

Exemple I.28. *La fonction $f : x \mapsto e^{-\frac{1}{x}}$, définie sur $\mathbb{R}^*$ vérifie :*
$$\lim_{x\to 0^-} f(x) = +\infty \text{ et } \lim_{x\to 0^+} f(x) = 0.$$



Proposition I.29. *Si $a \in \mathbb{R}$, $l \in \overline{\mathbb{R}}$, et f définie sur I, et définie à gauche et à droite au voisinage de a. Alors :*

1. *si $a \in I$: $\lim\limits_{x\to a} f(x) = l$ si, et seulement si, $\lim\limits_{x\to a^+} f(x) = \lim\limits_{x\to a^-} f(x) = f(a) = l$;*
2. *si $a \notin I$: $\lim\limits_{x\to a} f(x) = l$ si, et seulement si, $\lim\limits_{x\to a^+} f(x) = \lim\limits_{x\to a^-} f(x) = l$.*

Remarque I.30. *Dans le premier cas, le fait que $f(a) = l$ exclut le cas où $l = \pm\infty$.*

Démonstration.

1. Montrons les deux implications :
   — Supposons que $\lim\limits_{x\to a} f(x) = l$: on a déjà montré que $f(a) = l$. De plus, pour $\varepsilon > 0$, il existe η tel que :
   $$\forall x \in I,\ |x - a| \leq \eta \Rightarrow |f(x) - l| \leq \varepsilon$$
   et les limites à gauche et à droite découlent alors des implications : $a - \eta \leq x < a \Rightarrow |x - a| \leq \eta$ et $a < x \leq a + \eta \Rightarrow |x - a| \leq \eta$.
   — Réciproquement : supposons que $\lim\limits_{x\to a^+} f(x) = \lim\limits_{x\to a^-} f(x) = f(a) = l$. Soit $\varepsilon > 0$:
   — par définition de la limite à gauche, il existe $\eta_1 > 0$ tel que :
   $$\forall x \in I,\ a - \eta_1 \leq x < a \Rightarrow |f(x) - l| \leq \varepsilon;$$

— par définition de la limite à droite, il existe $\eta_2 > 0$ tel que :

$$\forall x \in I,\ a < x \leq a + \eta_2 \Rightarrow |f(x) - l| \leq \varepsilon.$$

En posant $\eta = \min(\eta_1, \eta_2)$, alors pour tout $x \in I$ tel que $|x - a| \leq \eta$, on a :
— soit $a - \eta \leq x < a$: et donc par la limite à gauche $|f(x) - l| \leq \varepsilon$;
— soit $x = a$: et donc $f(x) = f(a) = l$, donc $|f(x) - l| = 0 \leq \varepsilon$;
— soit $a < x < a + \eta$: et donc par la limite à droite $|f(x) - l| \leq \varepsilon$.
c'est-à-dire que, dans tous les cas : $|x - a| \leq \eta \Rightarrow |f(x) - l| = 0 \leq \varepsilon$.
Comme ceci est pour tout $\varepsilon > 0$, alors on a bien : $\lim\limits_{x \to a} f(x) = l$.

2. Le cas où $a \notin I$ se traite de manière très proche. Il n'y a pas à se soucier de ce qui se passe en a, mais il y a davantage de cas à traiter car on pourrait avoir $l = \pm\infty$.

□

Exemples I.31.

1. *on peut voir ainsi que la fonction inverse n'a pas de limite en* 0*, puisque :*

$$\lim_{x \to 0^+} \frac{1}{x} = +\infty \neq \lim_{x \to 0^-} \frac{1}{x} = -\infty.$$

2. *En revanche, la fonction* $x \mapsto \frac{1}{x^2}$ *a bien une limite en* 0 *puisque :*

$$\lim_{x \to 0^+} \frac{1}{x} = +\infty = \lim_{x \to 0^-} \frac{1}{x}.$$

3. *Plus généralement, un fonction paire définie sur* $\mathbb{R}^*$ *a une limite en* 0 *si, et seulement si, elle a une limite à gauche ou à droite. Tandis qu'une fonction impaire (définie en* 0 *ou non) a une limite en* 0 *si, et seulement si, elle a une limite à gauche ou à droite et que cette limite est nulle.*

I.4 Lien avec les suites

Une première chose à dire est qu'une suite peut être vue comme une fonction définie sur $\mathbb{N}$, et on peut donc s'intéresser à ses limites en tant que fonction. Tout se passe alors comme pour les fonctions, puisque $\mathbb{N}$ étant non majoré, cela a bien un sens de regarder la limite en $+\infty$. Les autres limites n'ont pas beaucoup d'intérêt, car il s'agirait de regarder les limites en les entiers, en lesquels la suite est bien définie donc sa limite est donné en chaque entier par son image.

Théorème I.32 (Caractérisation séquentielle de la limite)**.** *Soit* f *définie sur* I*,* $a \in \overline{\mathbb{R}}$ *adhérent à* I *et* $l \in \overline{\mathbb{R}}$*. Il y a équivalence entre :*

1. $\lim\limits_{x \to a} f(x) = l$ *;*
2. *pour toute suite* (u_n) *à valeurs dans* I *et tendant vers* a*, la suite* $(f(u_n))$ *tend vers* l*.*

Démonstration. Par exemple, montrons le résultat lorsque $a, l \in \mathbb{R}$. On montre séparément les deux implications.

— si $\lim\limits_{x \to a} f(x) = l$: soit (u_n) une suite à valeurs dans I tendant vers a.
Soit $\varepsilon > 0$:
— f tend vers l en a, il existe $\eta > 0$ tel que :

$$\forall x \in I,\ |x - a| \leq \eta \Rightarrow |f(x) - l| \leq \varepsilon;$$

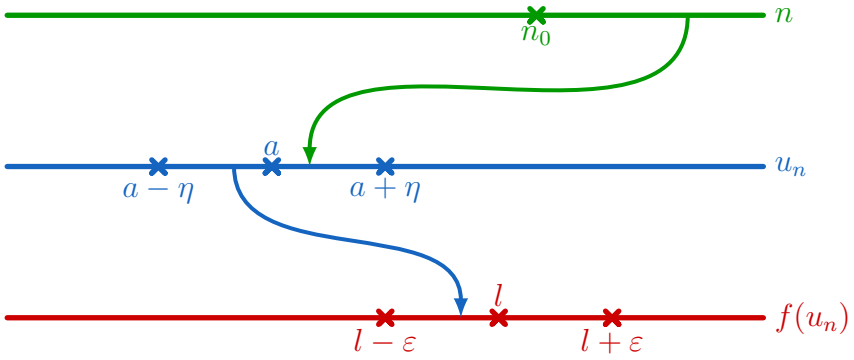
— (u_n) tend vers a, donc il existe n_0 tel que :

$$\forall n \in \mathbb{N},\ n \geq n_0 \Rightarrow |u_n - a| \leq \eta.$$

Et ainsi, pour tout $n \in \mathbb{N}$:

$$n \geq n_0 \Rightarrow |u_n - a| \leq \eta \Rightarrow |f(u_n) - l| \leq \varepsilon$$

donc la suite $(f(u_n))$ tend bien vers l.



— procédons par contraposée pour la réciproque : supposons que f ne tende pas vers l en a, c'est-à-dire que :

$$\exists \varepsilon > 0,\ \forall \eta > 0,\ \exists x \in I,\ |x - a| \leq \eta \text{ et } |f(x) - l| > \varepsilon \quad (\star)$$

et donnons-nous un tel ε.
Appliquons $(\star)$ avec $\eta = \frac{1}{n+1}$ pour $n \in \mathbb{N}$, et notons u_n l'élément de I donné par $(\star)$. On a ainsi pour tout $n \in \mathbb{N}$:

$$|u_n - a| \leq \frac{1}{n+1} \text{ et } |f(u_n) - l| > \varepsilon.$$

La première inégalité montre que la suite (u_n) tend vers a (par encadrement). Tandis que la seconde assure que la suite $(f(u_n))$ ne tend pas vers l.
D'où la contraposée.

D'où l'équivalence. □

Remarques I.33.

1. *En pratique, on utilisera surtout l'implication* 1. ⇒ 2. *: soit pour chercher la limite d'une suite, soit pour montrer qu'une fonction n'a pas de limite en un point.*
2. *Il faut que la suite soit bien à valeurs dans I, sinon le résultat devient faux.*

Corollaire I.34. *Si f est définie sur I, et $a \in I$ tel que f a une limite en a, alors pour tout suite (u_n) à valeurs dans I tendant vers a, la suite $(f(u_n))$ tend vers $f(a)$.*

Exemples I.35. 1. *La fonction $f : x \mapsto \sin(\frac{1}{x})$ définie sur $\mathbb{R}^*$ n'a pas de limite en 0 :*
   — *la suite $(u_n) = \left(\frac{1}{n\pi}\right)$ tend vers 0, et la suite $(f(u_n)) = (\sin(n\pi))$ est constante de valeur nulle, donc tend vers 0 ;*
   — *la suite $(v_n) = \left(\frac{1}{2n\pi+\pi/2}\right)$ tend vers 0 aussi, mais la suite $(f(v_n)) = (\sin(2n\pi + \frac{\pi}{2}))$ est constante de valeur 1, donc tend vers 1.*

   Comme $1 \neq 0$, alors f n'a pas de limite en 0.

   On pouvait aussi directement utiliser la suite $(w_n) = \left(\frac{1}{n\pi+\pi/2}\right)$, puisque la suite $(f(v_n)) = ((-1)^n)$ n'a pas de limite.

2. *Si f est une fonction périodique non constante, alors f n'a pas de limite en $+\infty$.*
   Considérons $T > 0$ une période de f. Comme f est non constante, il existe $a, b \in \mathbb{R}$ tels que $f(a) \neq f(b)$. Et alors :
   — *la suite $(u_n) = (a + nT)$ tend vers $+\infty$, tandis que la suite $(f(u_n))$ est constante de valeur $f(a)$, donc tend vers $f(a)$;*
   — *la suite $(v_n) = (b + nT)$ tend vers $+\infty$ aussi, mais la suite $(f(v_n))$ est constante de valeur $f(b)$, donc tend vers $f(b)$.*

   Comme $f(a) \neq f(b)$, alors f n'a pas de limite en $+\infty$.

I.5 Manipulations de limites

Théorème I.36 (Opérations sur les limites)**.** *Si f, g sont deux fonctions définies sur I et $a \in \overline{\mathbb{R}}$ adhérent à I avec $\lim\limits_{x\to a} f(x) = l$ et $\lim\limits_{x\to a} g(x) = l'$ (pour $l, l' \in \overline{\mathbb{R}}$) et $\lambda \in \mathbb{R}$. Alors, sous réserve que les quantités ci-dessous soient bien définies :*

1. *la fonction $(f+g)$ tend vers $l + l'$ en a ;*
2. *la fonction λf tend vers λl en a ;*
3. *la fonction fg tend vers ll' en a ;*
4. *si $l' \neq 0$, la fonction $\dfrac{f}{g}$ est bien définie au voisinage de a, et tend vers $\dfrac{l}{l'}$ en a.*

Démonstration. On peut refaire les mêmes manipulations que pour les suites (avec des ε, selon les différentes limites). Ou directement invoquer le théorème analogue sur les suites, qui se transpose par définition séquentielle de la limite. □

Proposition I.37. *Si f, g sont définies sur I et $a \in \overline{\mathbb{R}}$ adhérent à I, alors :*

1. *si f est minorée (resp. majorée) au voisinage de a, et g tend vers $+\infty$ (resp. $-\infty$) en a, alors $f+g$ tend vers $+\infty$ (resp. $-\infty$) en a ;*
2. *si f est bornée au voisinage de a et que g tend vers 0 en a, alors fg tend vers 0 en a ;*
3. *si f est minorée par $m > 0$ (resp. majorée par $M < 0$) au voisinage de a, et si g tend vers $\pm\infty$ en a, alors fg tend vers $\pm\infty$ (resp. $\mp\infty$) en a.*

Démonstration. Comme pour les suites, ou alors par caractérisation séquentielle. □

Proposition I.38. *Si $f : I \to J$ et $g : J \to \mathbb{R}$, a adhérent à I, b adhérent à J et $l \in \overline{\mathbb{R}}$ tels que : $\lim\limits_{x\to a} f(x) = b$ et $\lim\limits_{y\to b} g(y) = l$.*
Alors : $\lim\limits_{x\to a} g \circ f(x) = l$.

Démonstration. Montrons le par exemple dans le cas où $a, b, l \in \mathbb{R}$.
Soit $\varepsilon > 0$. Alors :

— comme $\lim\limits_{y\to b} g(y) = l$, alors il existe $\alpha > 0$ tel que :

$$\forall y \in J,\ |y - b| \leq \alpha \Rightarrow |g(y) - l| \leq \varepsilon;$$

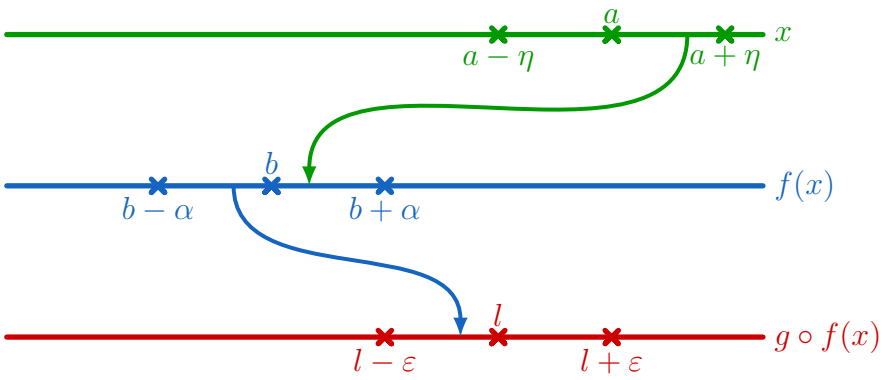
— comme $\lim\limits_{x\to a} f(x) = b$, alors il existe $\eta > 0$ tel que :

$$\forall x \in I,\ |x - a| \leq \eta \Rightarrow |f(x) - b| \leq \alpha.$$

Et ainsi, on trouve que, pour tout $x \in I$:

$$|x - a| \leq \eta \Rightarrow |f(x) - b| \leq \alpha \Rightarrow |g(f(x)) - l| = |g \circ f(x) - l| \leq \varepsilon$$

ce qui prouve bien le résultat voulu.



□

Remarque I.39. *On peut aussi le faire par caractérisation séquentielle pour prouver tous les cas. En fait la caractérisation séquentielle est un cas particulier où $a = +\infty$ et f est une suite à valeurs dans J tendant vers b, ce qui explique que la démonstration non séquentielle ressemble beaucoup à la preuve de la caractérisation séquentielle de la limite.*

I.6 Limites et inégalités

Proposition I.40. *Soit f définie sur I et a adhérent à I tel que $\lim\limits_{x\to a} f(x) = l \in \overline{\mathbb{R}}$. Alors pour $m, M \in \mathbb{R}$:*

1. *si $l < M$ (resp. $m < l$) alors $f < M$ (resp. $m < f$) au voisinage de a ;*
2. *si $f \leq M$ (resp. $m \leq f$) au voisinage de a, alors $l \leq M$ (resp. $m \leq l$).*

Remarque I.41.

1. *Pour le 1., on **ne peut pas** mettre des inégalités larges au départ.*
2. *Pour le 2., on peut mettre des inégalités strictes au départ, mais le passage à la limite ne donnera que des inégalités larges.*

Démonstration. On se contente de traiter le cas où $a \in \mathbb{R}$ (les autres cas se traitent de même).
Supposons que $l \in \mathbb{R}$, et montrons le *1.*

— si $l < M$: posons $\varepsilon = \frac{M-l}{2} > 0$. Par définition de la limite, il existe $\eta > 0$ tel que :

$$\forall x \in I,\ |x-a| \leq \eta \Rightarrow |f(x) - l| \leq \varepsilon \Rightarrow f(x) \leq l + \varepsilon$$

et donc, en remplaçant ε par sa valeur :

$$\forall x \in I,\ |x-a| \leq \eta \Rightarrow f(x) \leq \frac{l+M}{2} < M.$$

— si $m < l$: posons $\varepsilon = \frac{m-l}{2} > 0$. Par définition de la limite, il existe $\eta > 0$ tel que :

$$\forall x \in I,\ |x-a| \leq \eta \Rightarrow |f(x) - l| \leq \varepsilon \Rightarrow f(x) \geq l - \varepsilon$$

et donc, en remplaçant ε par sa valeur :

$$\forall x \in I,\ |x-a| \leq \eta \Rightarrow f(x) \geq \frac{l+m}{2} > m.$$

Le *2.* se déduit alors par contraposée.
Si $l = \pm\infty$ on procède de même, en prenant $A = m+1$ ou m, ou $A = M+1$ ou M dans la définition de la limite. □

Corollaire I.42. *Si f, g sont deux fonctions définies sur I, et a adhérent à I. Supposons que f, g ont des limites en a et que, au voisinage de a, on ait : $f(x) \leq g(x)$. Alors :*

$$\lim_{x\to a} f(x) \leq \lim_{x\to a} g(x).$$

Démonstration. Notons $l = \lim\limits_{x\to a} f(x)$ et $l' = \lim\limits_{x\to a} g(x)$.
Si $l - l'$ n'est pas une forme indéterminée, alors il suffit d'appliquer le résultat précédent à la fonction $f - g$, qui a une limite en a (par opération sur les limites).
Mais si $l - l'$ est une forme indéterminée, cela veut dire que : $l = l' = \pm\infty$, et on a alors bien $\lim\limits_{x\to a} f(x) \leq \lim\limits_{x\to a} g(x)$ puisque l'on a même une égalité. □

Théorème I.43 (Théorème d'encadrement, ou des gendarmes)**.** *Si f, g, h sont trois fonctions définies sur I, a adhérent à I, tels qu'au voisinage de a : $f(x) \leq g(x) \leq h(x)$. Si $\lim\limits_{x\to a} f(x) = \lim\limits_{x\to a} h(x) = l \in \mathbb{R}$, alors $\lim\limits_{x\to a} g(x) = l$.*

Démonstration. Montrons le résultat lorsque $a \in \mathbb{R}$.
Soit $\varepsilon > 0$:

— par l'inégalité vérifiée au voisinage de a, il existe $\eta_1 > 0$ tel que :

$$\forall x \in I,\ |x-a| \leq \eta_1 \Rightarrow f(x) \leq g(x) \leq h(x);$$

— par définition de la limite de f en a, il existe $\eta_2 > 0$ tel que :

$$\forall x \in I,\ |x-a| \leq \eta_2 \Rightarrow |f(x)-l| \leq \varepsilon \Rightarrow l-\varepsilon \leq f(x);$$

— par définition de la limite de h en a, il existe $\eta_3 > 0$ tel que :

$$\forall x \in I,\ |x-a| \leq \eta_3 \Rightarrow |h(x)-l| \leq \varepsilon \Rightarrow h(x) \leq l+\varepsilon.$$

Ainsi, en posant $\eta = \min(\eta_1, \eta_2, \eta_3)$, on trouve pour tout $x \in I$:

$$|x-a| \leq \eta \Rightarrow \left\{ \begin{array}{c} f(x) \leq g(x) \leq h(x) \\ l-\varepsilon \leq f(x) \\ h(x) \leq l+\varepsilon \end{array} \right. \Rightarrow l-\varepsilon \leq g(x) \leq l+\varepsilon \Rightarrow |g(x)-l| \leq \varepsilon$$

ce qui donne bien que $\lim\limits_{x\to a} g(x) = l$. □

Remarques I.44.

1. *Si $l = \pm\infty$ le résultat reste vrai, mais on n'a besoin que d'une seule inégalités.*
2. *On peut aussi le démontrer en passant par des suites et en utilisant le théorème d'encadrement pour les suites.*

Proposition I.45. *Si f, g sont définies sur I, et a adhérent à I tels que au voisinage de a : $f(x) \leq g(x)$. Alors :*

1. *si $\lim\limits_{x\to a} f(x) = +\infty$, alors $\lim\limits_{x\to a} g(x) = +\infty$;*
2. *si $\lim\limits_{x\to a} g(x) = -\infty$, alors $\lim\limits_{x\to a} f(x) = -\infty$.*

Démonstration.

1. la fonction $g-f$ est minorée par 0 au voisinage de a, et f tend vers $+\infty$ en a, donc $g = (g-f)+f$ tend vers $+\infty$ en a ;
2. la fonction $f-g$ est majorée par 0 au voisinage de a, et g tend vers $-\infty$ en a, donc $f = (f-g)+g$ tend vers $-\infty$ en a.

□

Théorème I.46 (Théorème de la limite monotone)**.** *Soient $a, b \in \overline{\mathbb{R}}$ avec $a < b$, et $f :]a;b[\to \mathbb{R}$ une fonction* ***croissante****. Alors :*

1. *$\lim\limits_{x\to b} f(x)$ existe, et vaut $\sup\limits_{x\in]a;b[} f(x)$ si f est majorée, et $+\infty$ sinon ;*
2. *$\lim\limits_{x\to a} f(x)$ existe, et vaut $\inf\limits_{x\in]a;b[} f(x)$ si f est minorée, et $-\infty$ sinon.*

Démonstration. Montrons par exemple le *1.* lorsque b est réel. Posons $E = \{f(x) \,|\, x \in]a;b[\}$, qui est un ensemble non vide (car $a < b$). Alors :

— si E est majoré : notons M sa borne supérieure. Et considérons $\varepsilon > 0$. Par définition de M, il existe $y_0 \in E$ tel que : $M - \varepsilon \leq y_0 \leq M$. Par définition de E, il existe $x_0 \in]a;b[$ tel que $y_0 = f(x_0)$. Posons $\eta = b - x_0$, alors pour tout $x \in]a;b[$:

$$\begin{array}{rcll} |x-b| \leq \eta & \Rightarrow & b - \eta \leq x < b & \\ & \Rightarrow & x_0 \leq x < b & \\ & \Rightarrow & \left\{ \begin{array}{cc} y_0 = f(x_0) \leq f(x) & \text{par croissance de } f \\ f(x) \leq M & \text{par définition de } E \end{array} \right. & \\ & \Rightarrow & M - \varepsilon \leq f(x) \leq M & \\ & \Rightarrow & |f(x) - M| \leq \varepsilon & \end{array}$$

ce qui donne bien : $\lim\limits_{x \to b} f(x) = M$.

— si E n'est pas majoré : soit $A \in \mathbb{R}$. Comme E n'est pas majoré, alors A n'est pas un majorant de E donc il existe $y_0 \in E$ tel que $y_0 \geq A$.
Par définition de E, il existe $x_0 \in]a;b[$ tel que $f(x_0) = y_0$. En posant de nouveau $\eta = b - x_0$, on trouve pour tout $x \in]a;b[$:

$$\begin{array}{rcl} |x-b| \leq \eta & \Rightarrow & b - \eta \leq x \\ & \Rightarrow & x_0 \leq x \\ & \Rightarrow & A \leq y_0 \leq f(x) \text{ par croissance de } f \end{array}$$

□

Théorème I.47. *Avec les mêmes notations, si f est supposée décroissante sur $]a;b[$, alors :*

1. $\lim\limits_{x \to b} f(x)$ *existe, et vaut* $\inf\limits_{x \in]a;b[} f(x)$ *si f est minorée, et $-\infty$ sinon ;*
2. $\lim\limits_{x \to a} f(x)$ *existe, et vaut* $\sup\limits_{x \in]a;b[} f(x)$ *si f est majorée, et $+\infty$ sinon.*

Remarque I.48. *Les limites considérées dans les deux théorèmes sont en fait des limites à gauche et à droite. Le théorème peut être mis en défaut si f est défini en a ou b, ou renforcé par le résultat suivant.*

Corollaire I.49. *Soient $a, b \in \mathbb{R}$ avec $a < b$:*

1. *si f est croissante sur $]a;b]$, alors f a une limite à gauche finie en b avec :* $\lim\limits_{x \to b^-} f(x) \leq f(b)$;
2. *si f est décroissante sur $]a;b]$, alors f a une limite à gauche finie en b avec :* $\lim\limits_{x \to b^-} f(x) \geq f(b)$;
3. *si f est croissante sur $[a;b[$, alors f a une limite à droite finie en a avec :* $\lim\limits_{x \to a^+} f(x) \geq f(a)$;
4. *si f est décroissante sur $[a;b[$, alors f a une limite à droite finie en a avec :* $\lim\limits_{x \to a^+} f(x) \leq f(a)$.

Démonstration. Il suffit de voir que f est majorée ou minorée par $f(a)$ ou $f(b)$ suivant les cas considérés. □

Corollaire I.50. *Si f est une fonction monotone définie sur un intervalle I, alors f admet des limites à gauche et à droite finies en tout point de $\overset{\circ}{I}$.*

Corollaire I.51. *Si f est monotone sur I, et $a \in I$, alors f a une limite en a si, et seulement si, elle a des limites à gauche et à droite de a égales.*

II Fonctions continues

II.1 Continuité en un point

Définition II.1. *Si f est définie sur $I \subset \mathbb{R}$, et $a \in I$, on dit que f est* ***continue en*** *a si elle a une limite en a.*
On dit que f est continue sur I si elle est continue en a pour tout $a \in I$.
On note $\mathcal{C}(I, \mathbb{R})$ (ou parfois $\mathcal{C}^0(I, \mathbb{R})$) l'ensemble des fonctions continues sur I.

Proposition II.2. *La somme, le produit, la multiplication par un scalaire, le quotient (s'il est bien défini) et la composition (si elle est bien définie) de fonctions continues est continue.*

Démonstration. Il suffit de regarder les limites en des points donnés. Les opérations sur les limites donnent le résultat. □

Remarque II.3. *On voit apparaître ici que la continuité est une notion locale : il suffit de la regarder au voisinage d'un point pour la constater. Et la continuité sur un ensemble (par exemple un intervalle) pourrait en ce sens être qualifiée de "multi-locale", dans le sens où on ne fait que faire du local en chaque point, mais à aucun moment on ne regarde les points simultanément (ce qui correspondrait à une approche globale de la continuité).*

Corollaire II.4. *Pour $I \subset \mathbb{R}$, l'ensemble $\mathcal{C}(I, \mathbb{R})$ est un sous-anneau de $\mathbb{R}^I$.*

Démonstration.
- La fonction constante de valeur 1 est continue, et est l'élément neutre pour $\times$.
- si f, g sont continues, alors $f - g$ est continue.
- si f, g sont continues, alors fg est continue.

□

Corollaire II.5. *Les fonctions polynomiales sont continues sur $\mathbb{R}$*

Démonstration. Comme la continuité est préservée par somme, produit et multiplication par un scalaire, il suffit de voir que la fonction $x \mapsto x$ est continue sur $\mathbb{R}$.
Soit $a \in \mathbb{R}$ et $\varepsilon > 0$. Alors :

$$|x - a| \leq \varepsilon \Rightarrow |x - a|\varepsilon$$

où on interprète la première inégalité comme $|x - a| \leq \eta$, et la seconde comme $|f(x) - f(a)| \leq \varepsilon$.
Ceci montre bien la continuité en a. Et donc la continuité sur $\mathbb{R}$.
D'où le résultat. □

Définition II.6. *Si f est définie sur I et $a \in I$, on dit que f est :*

1. ***continue à gauche*** *en a si : $\lim\limits_{x \to a^-} f(x) = f(a)$;*
2. ***continue à droite*** *en a si : $\lim\limits_{x \to a^+} f(x) = f(a)$.*

Remarque II.7. *Cela revient à dire que $f|_{I \cap]-\infty;a]}$ ou $f|_{I \cap [a;+\infty[}$ est continue en a.*

Exemple II.8. *La fonction partie entière $x \mapsto \lfloor x \rfloor$ est continue à droite en tout $a \in \mathbb{R}$. Elle est continue à gauche en tout les éléments de $\mathbb{R} \setminus \mathbb{Z}$.*

Proposition II.9. *Si f est définie sur I et $a \in I$, alors f est continue en a si, et seulement si, f est continue à gauche et à droite en a.*

Démonstration. Découle des propriétés des limites à droite et à gauche. □

Proposition II.10 (Caractérisation séquentielle de la continuité)**.** *Soit f définie sur $I \subset \mathbb{R}$ et $a \in I$, alors il y a équivalence entre :*

1. *f est continue en a ;*
2. *pour toute suite (u_n) à valeurs dans I tendant vers a, la suite $(f(u_n))$ tend vers $f(a)$.*

Démonstration. Découle de la caractérisation séquentielle de la limite. □

Proposition-Définition II.11. *Si f est définie sur I, $a \in \mathbb{R} \setminus I$ adhérent à I, et $l \in \mathbb{R}$. Supposons que $\lim\limits_{x\to a} f(x) = l$, alors on appelle* ***prolongement par continuité de*** *f la fonction $\tilde{f}$ définie sur $I \cup \{a\}$ par :*

$$\tilde{f} : \left\{ \begin{array}{ccc} I \cup \{a\} & \to & \mathbb{R} \\ x & \mapsto & \left\{ \begin{array}{ll} f(x) & si\ x \in I \\ l & si\ x = a \end{array} \right. \end{array} \right.$$

qui est continue en a.

Démonstration. Soit $\varepsilon > 0$. Par définition de l, il existe $\eta > 0$ tel que :

$$\forall x \in I,\ |x - a| \leq \eta \Rightarrow |f(x) - l| \leq \varepsilon$$

et donc pour tout $x \in I \cup \{a\}$:

$$|x - a| \leq \eta \Rightarrow \left\{ \begin{array}{l} x \in I \text{ et } |x - a| \leq \eta \\ \text{ou } x = a \end{array} \right. \Rightarrow \left\{ \begin{array}{l} |f(x) - l| \leq \varepsilon \\ \text{ou } \tilde{f}(x) = l \end{array} \right. \Rightarrow |\tilde{f}(x) - l| \leq \varepsilon$$

ce qui donne bien la continuité de $\tilde{f}$. □

Exemples II.12.

1. *Considérons la fonction f définie sur $\mathbb{R}^*$ par : $f(x) = \dfrac{e^x - 1}{x}$. Alors, par limite classique : $\lim\limits_{x\to 0} f(x) = 1$, et donc f se prolonge par continuité en la fonction continue sur $\mathbb{R}$:*

$$\tilde{f} : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \left\{ \begin{array}{ll} \dfrac{e^x - 1}{x} & si\ x \neq 0 \\ 1 & si\ x = 0 \end{array} \right. \end{array} \right.$$

2. *Considérons la fonction g définie sur $\mathbb{R}^*$ par : $g(x) = \dfrac{\sin(x)}{x}$. Alors pour $x \neq 0$ on a :*

$$\frac{\sin(x)}{x} = \frac{\sin(x) - \sin(0)}{x - 0} \underset{x\to 0}{\to} \sin'(0) = \cos(0) = 1$$

donc g se prolonge par continuité en la fonction continue sur $\mathbb{R}$:

$$\tilde{g} : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \left\{ \begin{array}{ll} \dfrac{\sin(x)}{x} & si\ x \neq 0 \\ 1 & si\ x = 0 \end{array} \right. \end{array} \right.$$

II.2 Continuité sur un intervalle

Théorème II.13 (Théorème des valeurs intermédiaires)**.** *L'image d'un intervalle par une fonction continue est un intervalle.*

Remarque II.14. *Cela revient à dire que, si $[a,b] \subset I$, alors tout élément entre $f(a)$ et $f(b)$ a un antécédente par f dans $[a;b]$.*

Démonstration. Considérons $[a;b] \subset I$. Supposons par exemple que $f(a) \leq f(b)$, et considérons y avec : $f(a) \leq y \leq f(b)$. Cherchons un antécédent c de y par f dans $[a;b]$
Si $y = f(a)$ ou $y = f(b)$, alors donc $c = a$ ou $c = b$, convient. Supposons dans la suite que $y \in]f(a); f(b)[$.
On propose deux démonstrations de ce résultats :

- avec des suites adjacentes : on définit les suites (a_n) et (b_n) par $a_0 = a$, $b_0 = b$ et pour tout $n \in \mathbb{N}$:
  — si $f(\frac{a_n+b_n}{2}) < y$: $a_{n+1} = \frac{a_n+b_n}{2}$ et $b_{n+1} = b_n$;
  — si $f(\frac{a_n+b_n}{2}) > y$: $a_{n+1} = a_n$ et $b_{n+1} = \frac{a_n+b_n}{2}$;
  — si $f(\frac{a_n+b_n}{2}) = y$: $a_{n+1} = b_{n+1} = \frac{a_n+b_n}{2}$.
  Alors les suites suites (a_n) et (b_n) sont adjacentes.
  — par récurrence, on montre que pour tout $n \in \mathbb{N}$: $a_n \leq b_n$. En effet, si on pose $(u_n) = (b_n - a_n)$, on a $u_0 = b - a > 0$ et pour tout $n \in \mathbb{N}$: $u_{n+1} = \frac{1}{2}u_n$ ou 0 (selon les cas).
  — on déduit donc que les suites (a_n) et (b_n) sont respectivement croissante et décroissante, puisque pour tout $n \in \mathbb{N}$: $a_{n+1} - a_n = \frac{b_n-a_n}{2}$ ou 0 selon les cas, et $b_{n+1} - b_n = \frac{a_n-b_n}{2}$ ou 0 selon les cas.
  — la suite (u_n) tend vers 0 : soit elle est stationnaire à 0, soit géométrique de raison $\frac{1}{2} \in]-1;1[$.
  Et donc les suites (a_n) et (b_n) convergent vers une même limite $c \in [a;b]$.
  Par construction des suites (a_n) et (b_n), on a pour tout $n \in \mathbb{N}$: $f(a_n) \leq y \leq f(b_n)$.
  En passant à la limite, comme f **est continue** : $f(c) \leq y \leq f(c)$, et donc $f(c) = y$.
- avec le théorème de la borne supérieure : on considère l'ensemble $A = \{x \in [a,b] \mid f(x) \leq y\}$. C'est une partie non vide (car $a \in A$) et majorée (par b) de $\mathbb{R}$, donc A admet une borne supérieure c.
  Par caractérisation séquentielle de la borne supérieure, il existe une suite (a_n) d'éléments de A qui tend vers c.
  Par définition de c, pour tout $n \in \mathbb{N}$: $c + \frac{1}{1+n} \notin A$. Posons $(b_n) = (c + \frac{1}{n+1})$, qui est une suite d'éléments n'appartenant pas à A qui tend vers c.
  Par définition de A, on a pour tout $n \in \mathbb{N}$: $f(a_n) \leq y < f(b_n)$.
  Et donc en passant à la limite, comme f **est continue** : $f(c) \leq y \leq f(c)$, donc $f(c) = y$.

□

Exemples II.15.

1. *Un polynôme P de degré impair possède toujours une racine réelle. Quitte à changer P en $-P$, on peut supposer que le coefficient dominant de P est strictement positif. Ainsi : $\lim\limits_{x\to+\infty} P(x) = +\infty$ et $\lim\limits_{x\to-\infty} P(x) = -\infty$. Par définition des limites, avec $A = \pm 1$, il existe $a, b \in \mathbb{R}$ tels que $P(a) < -1$ et $P(b) > 1$, et donc par théorème des valeurs intermédiaire il existe $c \in \mathbb{R}$ tel que $P(c) = 0$.*
2. *Si f est continue sur $]a;b[$ avec $\lim\limits_{x\to a^+} f(x) = l$ et $\lim\limits_{x\to b^-} f(x) = l'$, alors tout élément **strictement** entre l et l' a un antécédent par f. Supposons par exemple que $l < l'$ et posons $y \in]l, l'[$. Par définition des limites en a et b, il existe $x_1, x_2 \in]a, b[$ tels que $f(x_1) \leq y$ (avec $\varepsilon = y - l$) et $f(x_2) \geq y$ (avec $\varepsilon = l' - y$). Et par théorème des valeurs intermédiaires on a bien le résultat.*

Théorème II.16 (Théorème des bornes atteintes)**.** *L'image d'un segment par une fonction continue est un segment.*

Remarque II.17. *Cela revient à dire qu'une fonction f continue sur $[a,b]$ y est bornée et atteint ses bornes.*

Démonstration. Soit f une fonction continue sur le segment $[a,b]$.

Considérons l'ensemble $A = \{f(x) \,|\, x \in [a;b]\}$, qui est une partie non vide.
Nécessairement, A est majorée : supposons par l'absurde que ce ne soit pas le cas. Alors il existe une suite (y_n) d'éléments de A tendant vers $+\infty$. Donc par définition de A, il existe une suite (x_n) d'éléments de $[a,b]$ telle que la suite $(f(x_n)) = (y_n)$ tend vers $+\infty$.
La suite (x_n) est bornée, donc par théorème de Bolzano–Weierstrass il existe une sous-suite $(x_{\varphi(n)})$ qui converge vers $x \in [a;b]$, et par continuité de f la suite $(f(x_{\varphi(n)})) = (y_{\varphi(n)})$ converge vers $f(x)$, ce qui contredit le fait que (y_n) tend vers $+\infty$.
Comme A est bornée, alors elle a une borne supérieure M. Il faut montrer qu'elle est atteinte. Pour cela, on utilise la caractérisation séquentielle : il existe une suite (y_n) d'éléments de A tendent vers M, et donc une suite (x_n) d'éléments de $[a,b]$ telle que la suite $(f(x_n)) = (y_n)$ tend vers M.
À nouveau par théorème de Bolzano–Weierstrass, il existe une sous-suite $(x_{\varphi(n)})$ qui converge vers $x \in [a;b]$, et par continuité de f la suite $(f(x_{\varphi(n)})) = (y_{\varphi(n)})$ converge vers $f(x)$. Mais $(y_{\varphi(n)})$ est une suite extraite de (y_n), donc a même limite.
Et donc $f(x) = M$.
Le cas de la borne inférieure m de A se traite de même : elle existe et est atteinte.
Et finalement : $f([a,b]) = [m,M]$. □

Remarques II.18.

1. *Les autres types d'intervalles se comportent assez mal. Par exemple, avec $f = \sin$, on a : $f(]-1,10[) = [-1,1]$ et $f([0;\frac{3\pi}{2}[) =]-1;1]$.*

Exemples II.19.

1. *Si f est continue sur $[a,b]$ et ne s'y annule pas, alors la fonction $\frac{1}{f}$ est bien définie sur $[a,b]$ et est bornée.*

   Par théorème des valeurs intermédiaires, f est de signe constant. On peut supposer par exemple f strictement positive. Mais par théorème des bornes atteintes on a $f([a,b]) = [m,M]$, avec $m = f(x_1)$ pour $x_1 \in [a,b]$. En particulier, $m > 0$. Et donc :

$$\forall x \in [a,b],\ f(x) \geq m > 0$$

   puis en passant à l'inverse :

$$\forall x \in [a,b],\ \frac{1}{m} \geq \frac{1}{f(x)} > 0$$

   ce qui donne bien le résultat.

2. *Si f est une fonction continue périodique, alors f est bornée sur $\mathbb{R}$ et atteint ses bornes. En effet, si on note T une période de f, on a : $f([0,T]) = f(\mathbb{R})$ par T-périodicité.*

   Mais par continuité de f, le théorème des bornes atteintes donne que $f([0,T]) = [m,M]$ (avec m, M le minimum et le maximum de f). Et finalement : $f(\mathbb{R}) = [m,M]$.

II.3 Continuité et monotonie

Théorème II.20. *Soit f une fonction continue sur un intervalle I. Posons $J = f(I)$. Alors on a l'équivalence entre :*

1. *f est strictement monotone ;*
2. *f réalise une bijection de I sur J.*

Sous ces conditions, J est un intervalle de "même nature" que I.

Remarque II.21. *Par "même nature" on veut dire que si f est croissante (resp. décroissante) alors les crochets de I sont les mêmes que ceux de J (resp. $-J$) ;*

Démonstration. La première implication a déjà été démontrée au chapitre 3.
Montrons la réciproque : supposons f continue et bijective, donc injective. Supposons par l'absurde qu'elle n'est pas monotone. Alors :

— f n'est pas croissante : il existe $x_1, y_1 \in I$ avec $x_1 < y_1$ et $f(x_1) > f(y_1)$;
— f n'est pas décroissante : il existe $x_2, y_2 \in I$ avec $x_2 < y_2$ et $f(x_2) > f(y_2)$.

On construit alors les deux fonctions affines définies sur $[0;1]$ par :

$$a(t) = (1-t)x_1 + tx_2 \text{ et } b(t) = (1-t)y_1 + ty_2$$

qui sont continues, à valeurs dans I, avec $a(0) = x_1$, $a(1) = x_2$, $b(0) = y_1$ et $b(1) = y_2$.
La fonction $g : t \mapsto f(a(t)) - f(b(t))$ est continue (en tant que combinaison linéaire de composée de fonctions continues), et vérifie : $g(0) = f(x_1) - f(y_1) > 0$ et $g(1) = f(x_2) - f(y_2) < 0$. Par théorème des valeurs intermédiaires, il existe dont $t_0 \in]0;1[$ tel que $g(t_0) = 0$, c'est-à-dire $f(a(t_0)) = f(b(t_0))$.
Par injectivité de f, on a :

$$f(a(t_0)) = f(b(t_0)) \Rightarrow a(t_0) = b(t_0) \Rightarrow (1-t_0)x_1 + t_0x_2 = (1-t_0)y_1 + t_0y_2 \Rightarrow \underbrace{(1-t_0)(x_1-y_1)}_{<0} = \underbrace{t_0(y_2-x_2)}_{>0}$$

d'où la contradiction.
Donc f est monotone. Donc f est strictement monotone par injectivité.
Le fait que J est un intervalle découle du théorème des valeurs intermédiaires. Tandis que la nature de ses bornes (comprises ou non) découle du théorème de la limite monotone. □

Théorème II.22. *Si f est continue sur un intervalle I et réalise une bijection de I sur $J = f(I)$, alors f est strictement monotone, et sa réciproque f^{-1} est continue sur J, de même monotonie que f.*

Démonstration. La stricte monotonie de f découle du résultat précédent.
L'existence et la monotonie de f^{-1} ont été montrées au chapitre 3.
Reste à montrer la continuité de f^{-1} sur J. Supposons par exemple que f (donc f^{-1}) est strictement croissante, et considérons $b \in J$.
Montrons que f^{-1} est continue en b en montrant qu'elle est continue à gauche et à droite en b sous réserve que cela ait un sens : c'est-à-dire une limite à gauche si $b \neq \inf J$ et à droite si $b \neq \sup J$.
Supposons par exemple que $b \neq \inf J$ et montrons à gauche en b : par théorème de la limite monotone, on a déjà que $\lim\limits_{y \to b^-} f^{-1}(y)$ existe, et si on note l sa valeur, alors $l \leq f^{-1}(b)$.
Par continuité de f en l, on a :

$$f(l) = \lim_{x \to l} f(x) = \lim_{y \to b^-} f\left(f^{-1}(y)\right) = b$$

et donc : $l = f^{-1}(b)$.
Ce qui prouve bien la continuité à gauche. □

Exemple II.23. *Si $n \in \mathbb{N}^*$, la fonction $x \mapsto x^{\frac{1}{n}}$ est continue sur $\mathbb{R}_+$, en tant que réciproque de la fonction continue (car polynomiale) $x \mapsto x^n$ sur $\mathbb{R}_+$.*

II.4 Fonctions réelles à valeurs complexes

Définition II.24. *Si $f : I \to \mathbb{C}$, pour $I \subset \mathbb{R}$, $a \in \overline{\mathbb{R}}$ adhérent à I, et $l \in \mathbb{C}$, on dit que f tend vers l en a si :*

$$\forall \varepsilon > 0,\ \exists \eta > 0,\ \forall x \in I,\ |x-a| \leq \eta \Rightarrow |f(x) - l| \leq \varepsilon.$$

Remarques II.25.

1. *Cela revient à dire que la fonction $x \mapsto |f(x) - l|$ tend vers 0 en a.*

2. *La notion de limite infinie sur $\mathbb{C}$ est moins naturelle, notamment par le fait qu'on n'a pas cette relation d'ordre total comme sur $\overline{\mathbb{R}}$.*

Proposition II.26. *Avec les notations précédentes, on a :*

$$\lim_{x\to a} f(x) = l \Leftrightarrow \begin{cases} \lim\limits_{x\to a} \mathrm{Re}(f(x)) &= \mathrm{Re}(l) \\ \lim\limits_{x\to a} \mathrm{Im}(f(x)) &= \mathrm{Im}(l) \end{cases}.$$

Démonstration. Comme pour les suites. □

Définition II.27. *Si $I \subset \mathbb{R}$, on dit que $f : I \to \mathbb{C}$ est **continue** si elle admet une limite en tout réel $a \in I$. On note $\mathcal{C}(I, \mathbb{C})$ l'ensemble des fonctions continues sur I à valeurs complexes.*

Proposition II.28. *Pour $f : I \to \mathbb{C}$, on a l'équivalence :*

$$f \in \mathcal{C}(I, \mathbb{C}) \Leftrightarrow \mathrm{Re}(f), \mathrm{Im}(f) \in \mathcal{C}(I, \mathbb{R}).$$

Démonstration. Découle de la proposition sur les limites de fonctions complexes. □

Remarque II.29. *Les résultats reposant sur la relation d'ordre sur $\mathbb{R}$ (comme la limite monotone, le théorème des valeurs intermédiaires, la bijection monotone, etc.) ne sont **plus valables** sur $\mathbb{C}$. Par exemple, la fonction $t \mapsto e^{it}$ ne vérifie pas le théorème des valeurs intermédiaires : elle prend les valeurs 1 (en 0) et -1 (en π) mais ne s'annule jamais.*

Proposition II.30. *Si $f \in \mathcal{C}(I, \mathbb{C})$, alors $|f| \in \mathcal{C}(I, \mathbb{R})$.*

Démonstration. Comme f est continue sur $\mathbb{C}$, alors $\mathrm{Re}(f)$ et $\mathrm{Im}(f)$ sont continues. Comme la fonction $x \mapsto \sqrt{x}$ est continue sur $\mathbb{R}_+$, tout comme la fonction $x \mapsto x^2$, donc par composée et combinaison linéaire de fonction continue, la fonction $x \mapsto |f(x)| = \sqrt{\mathrm{Re}(f(x))^2 + \mathrm{Im}(f(x))^2}$ est continue. □

Remarque II.31. *La réciproque est fausse : on peut par exemple considérer $f : x \mapsto (-1)^{\lfloor x \rfloor}$, qui vaut alternativement 1 et -1 selon la parité de $\lfloor x \rfloor$, tandis que $|f|$ est constante de valeur 1.*

Définition II.32. *On dit qu'une fonction $f : I \to \mathbb{C}$ est **bornée** si la fonction réelle $x \mapsto |f(x)|$ est majorée sur I.*

Corollaire II.33. *Si $f \in \mathcal{C}([a, b], \mathbb{C})$, alors f est bornée.*

Démonstration. La fonction $|f|$ est continue sur le segment $[a, b]$, donc son image est un segment donc est bornée. □

Remarque II.34. *On a même mieux : la fonction f "atteint sa borne", dans le sens où il existe $c \in [a, b]$ tel que $|f(c)| = \max\limits_{x\in[a,b]} |f(x)|$.*

III Étude des suites du type $u_{n+1} = f(u_n)$

III.1 Généralités

Proposition III.1. *Soit f une fonction définie sur un ensemble D, telle que $f(D) \subset D$. Alors la suite (u_n) définie par :*

$$\begin{cases} u_0 \in D \\ u_{n+1} = f(u_n) \end{cases}$$

est bien définie, et est unique.

Démonstration. Par une récurrence immédiate, on montre que pour tout $n \in \mathbb{N}$: $u_n \in D$, et $u_n = \underbrace{f \circ \cdots \circ f}_{n \text{ fois}}(u_0)$. Ce qui donne bien le résultat. □

Remarque III.2. *En pratique, on pourra travailler avec des fonctions définies sur $\mathbb{R}$. Mais le fait de restreindre f à un sous ensemble stable par f sur lequel f est monotone pourra être intéressant.*

Théorème III.3. *Soient f est définie sur D, et (u_n) une suite d'éléments de D définie par : $\forall n \in \mathbb{N}$, $u_{n+1} = f(u_n)$. On suppose que (u_n) converge vers $l \in D$ et que f est continue en l : alors $f(l) = l$.*

Démonstration. Par continuité de f en l, on a :

$$f(l) = \lim f(u_n) = \lim u_{n+1} = l.$$

□

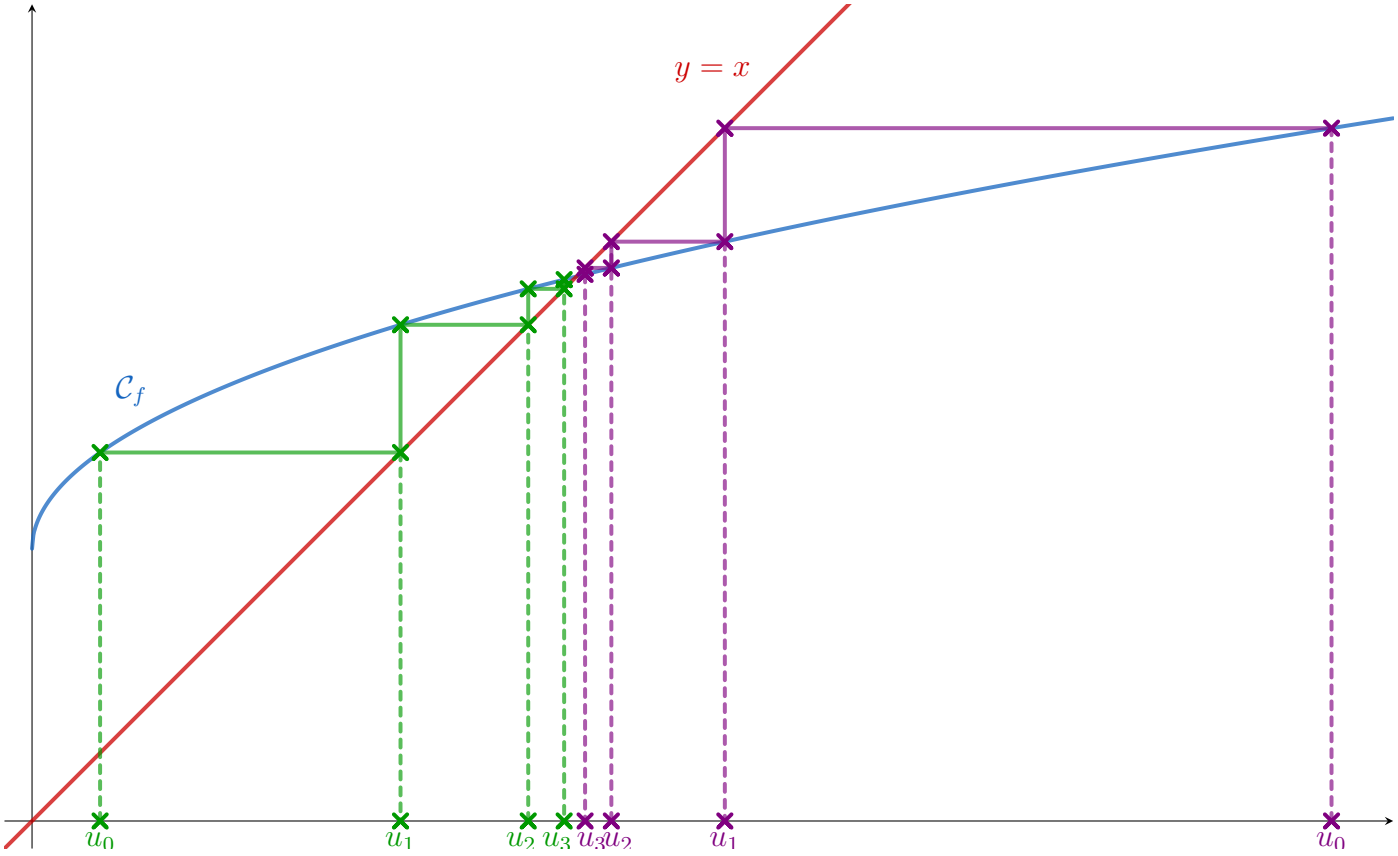
Remarque III.4. *Ce théorème ne donne pas l'existence d'une limite pour (u_n), mais il donne les limites possibles. Et il peut ainsi permettre de montrer que la suite (u_n) ne converge pas.*

III.2 Cas où f est croissante

Théorème III.5. *Soient f est définie sur D, et (u_n) une suite d'éléments de D définie par : $\forall n \in \mathbb{N}$, $u_{n+1} = f(u_n)$. On suppose que f est **croissante**, alors la suite (u_n) est **monotone**.*

Démonstration. Supposons par exemple que $u_1 \geq u_0$.
Alors par croissance de f on a : $f(u_1) = u_2 \geq u_1 = f(u_0)$.
Et une récurrence montre alors que (u_n) est croissante.
Le cas où $u_1 \leq u_0$ se traite de même, et montre que (u_n) est décroissante. □

Remarque III.6. *La croissance de f ne donne pas le sens de variation de (u_n) : pour l'avoir, on utilise le signe de $f(x) - x$. Graphiquement, cela correspond à la position de la courbe de f par rapport à la droite d'équation $y = x$, ce qui donne les graphiques suivants :*



Exemple III.7. *Étudions la suite (u_n) définie par :*

$$\begin{cases} u_0 = 0 \\ u_{n+1} = \sqrt{\frac{3}{4} + u_n} \end{cases}.$$

On pose pour cela la fonction f :

$$f : \begin{cases} \mathbb{R}_+ & \to & \mathbb{R}_+ \\ x & \mapsto & \sqrt{\frac{3}{4} + x} \end{cases}$$

qui est une fonction continue strictement croissante sur $\mathbb{R}_+$.
Résolvons sur $\mathbb{R}_+$ l'équation $f(x) = x$. Pour $x \in \mathbb{R}_+$, on a :

$$f(x) = x \Leftrightarrow \sqrt{\frac{3}{4} + x} = x \Leftrightarrow \frac{3}{4} + x = x^2 \Leftrightarrow x = \frac{3}{2}$$

où l'autre racine est $-\frac{1}{2} \notin \mathbb{R}_+$.
Montrons par récurrence que : $\forall n \in \mathbb{N},\ 0 \leq u_n \leq u_{n+1} \leq \frac{3}{2}$.

— $0 \leq \underbrace{u_0}_{=0} \leq \underbrace{u_1}_{=\sqrt{\frac{3}{4}}} \leq \frac{3}{2}$;

— *par croissance de f :*

$$0 \leq u_n \leq u_{n+1} \leq \frac{3}{2} \Rightarrow f(0) \leq f(u_n) \leq f(u_{n+1}) \leq f(\frac{3}{2}) \Rightarrow 0 \leq u_{n+1} \leq u_{n+2} \leq \frac{3}{2}$$

ce qui conclut la récurrence.
Ainsi, la suite (u_n) est croissante majorée (par $\frac{3}{2}$) donc elle converge vers un réel $l \in [0, \frac{3}{2}]$. Comme f est continue sur $\mathbb{R}_+$, elle est continue en l, donc $f(l) = l$. Donc $l = \frac{3}{2}$.

Exemple III.8. *Étudions la suite (u_n) définie par :*

$$\begin{cases} u_0 = 1 \\ u_{n+1} = \sqrt{1 + u_n^2} \end{cases}.$$

On pose pour cela la fonction f :

$$f : \begin{cases} \mathbb{R}_+ & \to & \mathbb{R}_+ \\ x & \mapsto & \sqrt{1 + x^2} \end{cases}$$

qui est une fonction continue strictement croissante sur $\mathbb{R}_+$.
Comme $u_1 = \sqrt{2} > u_0$, alors la suite (u_n) est croissante, et a donc une limite (finie ou non). Montrons qu'elle tend vers $+\infty$.
Par l'absurde, supposons que (u_n) converge vers $l \in \mathbb{R}_+$. Alors, par continuité de f sur $\mathbb{R}_+$ on aurait $f(l) = l$, et donc $1 + l^2 = l^2$, ce qui est impossible.

III.3 Cas où f est décroissante

Théorème III.9. *Soient f est définie sur D, et (u_n) une suite d'éléments de D définie par : $\forall n \in \mathbb{N},\ u_{n+1} = f(u_n)$. On suppose que f est **décroissante**, alors les sous-suites $(v_n) = (u_{2n})$ et $(w_n) = (u_{2n+1})$ vérifient pour tout $n \in \mathbb{N}$:*

$$v_{n+1} = g(v_n) \text{ et } w_{n+1} = g(w_n).$$

Ces deux suites sont monotones, de sens de variation opposés.

Démonstration. On pose $g = f \circ f$, qui est croissante (en tant que composée de deux fonctions décroissantes). Alors les suites (v_n) et (w_n) vérifient pour tout $n \in \mathbb{N}$:

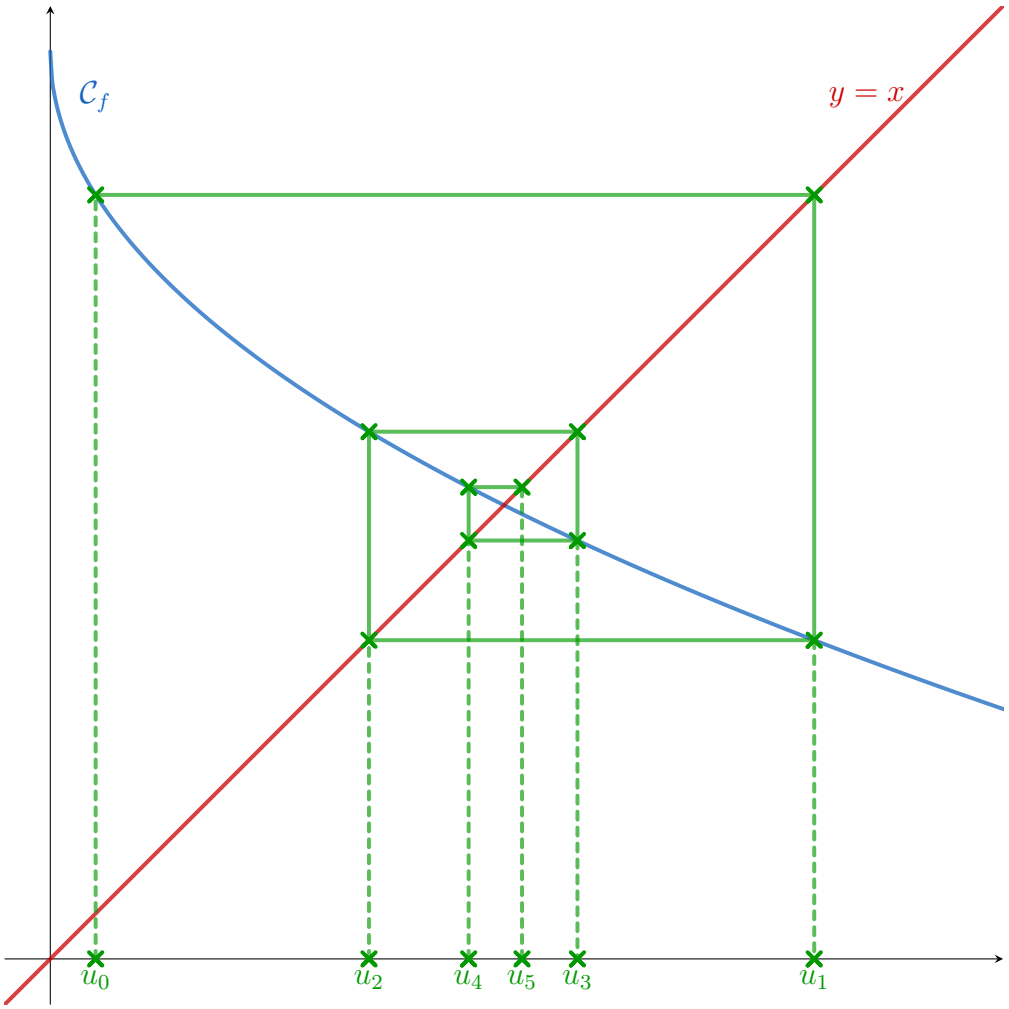
$$v_{n+1} = g(v_n) \text{ et } w_{n+1} = g(w_n)$$

ce qui assure déjà leurs monotonie.
Supposons par exemple que (v_n) soit croissante. Alors $v_0 \leq v_1$, c'est-à-dire que $u_0 \leq u_2$. Et donc :

— par décroissance de f : $f(u_0) \geq f(u_2)$;
— donc $u_1 \geq u_3$, c'est-à-dire $w_0 \geq w_1$;
— donc (w_n) est croissante.

□

Remarque III.10. *On peut ainsi déduire une convergence éventuelle de (u_n) de l'étude de (v_n) et (w_n) : la suite (u_n) a une limite si, et seulement si, les suites (v_n) et (w_n) tendent vers une même limite. Cette limite est alors nécessairement finie du fait des monotonies de (v_n) et (w_n). Graphiquement, la situation de convergence correspond à "l'escargot" suivant :*



Exemple III.11. *Étudions la suite (u_n) définie par :*

$$\begin{cases} u_0 = 1 \\ u_{n+1} = \cos(u_n) \end{cases}.$$

On pose pour cela la fonction f :

$$f : \begin{cases} [0,1] & \to & [0;1] \\ x & \mapsto & \cos(x) \end{cases}$$

qui est bien définie car $[0,1] \subset [0, \frac{\pi}{2}]$ *donc* $f([0,1]) \subset [0,1]$. *Et* f *est décroissante sur* $[0;1]$.
On pose $g = f^2$ *qui est croissante, et les suites* $(v_n) = (u_{2n})$ *et* $(w_n) = (u_{2n+1})$, *qui sont monotones.*
La suite (u_n) *est bornée, donc* (v_n) *et* (w_n) *aussi. Comme elles sont monotones, elles convergent. Notons* l_1, l_2 *leurs limites respectives, qui sont dans* $[0;1]$.
On considère la fonction h *suivante :*

$$h : \left\{ \begin{array}{ccc} [0,1] & \to & [0;1] \\ x & \mapsto & g(x) - x = \cos(\cos(x)) - x \end{array} \right. .$$

La fonction h *est dérivable sur* $[0,1]$, *avec pour tout* $x \in [0,1]$ *:*

$$h'(x) = -\sin(x) \cdot (-\sin(\cos(x))) - 1 = \sin(x)\sin(\cos(x)) - 1 < 0.$$

Ainsi :

— h *est strictement décroissante et continue sur* $[0,1]$ *;*
— $h(0) = \cos(1) - 0 > 0$ *et* $h(1) = \cos(\cos(1)) - 1 < 0$ *;*

donc il existe un unique $l \in [0;1]$ *tel que* $g(l) = l$.
Et finalement, pour un tel l *:* $l_1 = l = l_2$. *Donc* (u_n) *converge vers* l.
On peut même aller plus loin et étudier f *pour voir qu'elle admet elle aussi un unique point fixe, qui est* l.

Remarque III.12. *L'unicité du point fixe de* f *ne doit venir qu'à la fin. Par exemple, si l'on considère la suite définie par :*

$$\left\{ \begin{array}{l} u_0 = 1 \\ u_{n+1} = 1 - u_n \end{array} \right.$$

alors on peut voir que les suites (v_n) *et* (w_n) *convergent (elles sont même constantes), mais* (u_n) *ne converge pas. Alors que la fonction* $f : x \mapsto 1 - x$ *possède un unique point fixe.*
Et on peut généraliser ce contre-exemple avec d'autres fonctions involutives qui possèdent un unique point fixe (comme $f : x \mapsto \frac{1}{x}$ *sur* $\mathbb{R}_+^*$*).*

Chapitre 17

Polynômes

Dans tout ce chapitre, on considère $\mathbb{K}$ le corps $\mathbb{R}$ ou $\mathbb{C}$.

I Polynômes et fonctions polynomiales

I.1 L'ensemble $\mathbb{K}[X]$

Définition I.1. *On note $\mathbb{K}[X]$ l'ensemble des **polynômes à une indéterminée à coefficients dans** $\mathbb{K}$, c'est-à-dire l'ensemble des expressions de la forme :*

$$P(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + a_nX^n$$

où $n \in \mathbb{N}$ et $a_0, \ldots, a_n \in \mathbb{K}$.
*On dit alors que X est l'**indéterminée** et $a_0, \ldots, a_n$ sont les **coefficients**.*
*Les expressions a_iX^i (pour $i \in [\![0; n]\!]$) sont appelées les **monômes** de $P(X)$.*
Plus précisément, pour $i \in [\![0; n]\!]$, on dira que a_iX^i est le monôme de degré i, et a_i le coefficient de degré i.

Remarque I.2. *On notera $0_{\mathbb{K}[X]}$ le polynôme ayant tous ses coefficients nuls. On l'appelle **polynôme nul**, et on le notera plus simplement 0 lorsqu'il n'y aura pas d'ambiguïté.*
Par définition, deux polynômes sont égaux si, et seulement si, ils ont mêmes coefficients.

Exemples I.3.

1. $X^2 + 1 \in \mathbb{R}[X]$;
2. $X^2 + i \in \mathbb{C}[X]$;
3. $0 \in \mathbb{K}[X]$.

Remarques I.4.

1. *Comme $\mathbb{R} \subset \mathbb{C}$, alors $\mathbb{R}[X] \subset \mathbb{C}[X]$.*
2. *S'il n'y a pas d'ambiguïté, on pourra omettre X et noter P au lieu de $P(X)$.*
3. *Un polynôme est la somme de ses monômes.*

Définition I.5. *Si $a_0, \ldots a_n \in \mathbb{K}$, avec $a_n \neq 0$, on dira que le polynôme $P = a_0 + a_1X + \cdots + a_nX^n$ est de **degré** n, ce que l'on notera :* $\deg(P) = n$.
Par convention, on dira que le polynôme nul est de degré $-\infty$.
Pour $n \in \mathbb{N}$, on notera $\mathbb{K}_n[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$ de degré inférieur ou égal à n.
*Les polynômes de degré 0 sont appelés **polynômes constants** (selon les conventions, le polynôme nul pourra être traité à part).*

Exemples I.6. *1.* $\mathbb{K}_0[X] = \{a_0 \,|\, a_0 \in \mathbb{K}\} = \mathbb{K}$ *: c'est l'ensemble des* ***polynômes constants****.*

2. $\mathbb{K}_1[X] = \{aX + b \,|\, a, b \in \mathbb{K}\} \simeq \mathbb{K}^2$ *;*

3. $\mathbb{K}_2[X] = \{aX^2 + bX + c \,|\, a, b, c \in \mathbb{K}\}$*.*

Remarque I.7. *Pour simplifier les expressions, on pourra noter* $P = \sum a_k X^k$ *au lieu de* $P = \sum_{k=0}^{\deg(P)} a_k X^k$ *(et donc omettre les bornes de sommation), ce qui revient à poser* $a_k = 0$ *pour* $k > \deg(P)$*, ce qui donne bien une somme finie dans l'expression précédente.*
À l'inverse, un polynôme constant sera confondu avec son coeffiient constant.

Proposition I.8. *On a les inclusions :*

$$\mathbb{K}_0[X] \subset \mathbb{K}_1[X] \subset \mathbb{K}_2[X] \subset \cdots \subset \mathbb{K}_n[X] \subset \cdots \subset \mathbb{K}[X]$$

et toutes ces inclusions sont strictes.

Démonstration. Les inclusions sont évidentes.
Pour $n \in \mathbb{N}$, on a : $X^{n+1} \in \mathbb{K}_{n+1}[X] \setminus \mathbb{K}_n[X]$ ce qui prouve qu'elles sont strictes. □

Définition I.9. *Si* $P \in K[X]$ *est non nul, son coefficient de degré* $\deg(P)$ *est appelé* ***coefficient dominant****. On dira qu'un polynôme est* ***unitaire*** *si son coefficient dominant vaut* 1*.*

Exemples I.10.

1. *le polynôme* $X^4 + 2X^2 + 1$ *est unitaire ;*
2. *le polynôme* $2X^2 + 1$ *n'est pas unitaire.*

Remarque I.11. *Plus généralement, on dira que le monôme (non nul) de plus haut degré de* P *est son* ***monôme dominant****. Son coefficient de degré* 0 *sera lui appelé son* ***coefficient constant****.*

I.2 Opérations de $\mathbb{K}[X]$

Proposition-Définition I.12. *Si* $P = \sum a_k X^k, Q = \sum b_k X^k \in \mathbb{K}[X]$ *et* $\lambda \in \mathbb{K}$*, on définit :*

1. *la* ***multiplication scalaire*** *de* P *par* λ *comme le polynôme :* $\lambda \cdot P = \sum(\lambda a_k)X^k$ *;*
2. *la* ***somme*** *de* P *et* Q *comme le polynôme :* $P + Q = \sum(a_k + b_k)X^k$ *;*
3. *le* ***produit*** *de* P *et* Q *comme le polynôme :* $PQ = \sum c_k X^k$*, où pour tout* $k \in \mathbb{N}$ *on pose :* $c_k = \sum_{l=0}^{k} a_l b_{k-l} = \sum_{i+j=k} a_i b_j$*.*

Démonstration. La seule chose à vérifier est que les expressions définies précédemment sont bien des polynômes. Comme il s'agit clairement de sommes de monômes, il suffit de vérifier que ces sommes sont finies, c'est-à-dire que leurs coefficients sont nuls à partir d'un certain degré :

1. pour $k > \deg(P)$, on a $a_k = 0$ et donc $\lambda a_k = 0$;
2. pour $k > \max(\deg(P), \deg(Q))$, on a $a_k = b_k = 0$ et donc $a_k + b_k = 0$;
3. pour $k > \deg(P) + \deg(Q)$ et $l \in [\![0; k]\!]$, on a :

$$a_l \neq 0 \Rightarrow l \leq \deg(P) \Rightarrow k - l \geq k - \deg(P) \Rightarrow k - l > \deg(Q) \Rightarrow b_{k-l} = 0$$

et donc : $a_l b_{k-l} = 0$, ce qui donne en sommant : $c_k = 0$.

□

Remarque I.13. *Ces formules correspondent au fait de multiplier par un scalaire, d'additionner ou de multiplier entre elles les expressions suivant les règles usuelles de calcul sur $\mathbb{R}$ ou $\mathbb{C}$, en manipulant X comme on le ferait avec une inconnue dans une équation. C'est clair pour les deux premières opérations. Pour la multiplication, on a :*

$$\begin{array}{rl} & (a_0 + a1X + \cdots + a_nX^n)(b_0 + b_1X + \cdots + a_mX^m) \\ = & (a_0b_0) + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + \cdots + (a_{n-1}b_m + a_nb_{m-1})X^{n+m-1} + (a_nb_m)X^{n+m} \end{array}$$

De plus, l'amalgame entre $\mathbb{K}_0[X]$ et $\mathbb{K}$ est légitimé par le fait que, pour $\lambda \in \mathbb{K}$ et $P \in \mathbb{K}[X]$, alors : $\lambda \cdot P = \lambda P$ (que λ soit vu comme un scalaire ou un polynôme constant).

Proposition-Définition I.14. *Si $P, Q \in \mathbb{K}[X]$, avec $P = \sum a_kX^k$, on définit la* ***composée*** *de P et Q, notée $P \circ Q$, comme le polynôme :*

$$P \circ Q = \sum a_kQ^k$$

où on pose $Q^k = \underbrace{Q \cdot Q \cdot \cdots \cdot Q}_{k \text{ fois}}$.

Démonstration. Il faut vérifier que $P \circ Q$ est bien un polynôme. Comme $Q \in \mathbb{K}[X]$, alors pour tout $k \in \mathbb{N}$ on a $Q^k \in \mathbb{K}[X]$, et donc par stabilité par combinaison linéaire on a bien le résultat. □

Exemple I.15. *Avec $P = X^2 + 1$ et $Q = X + 1$, on obtient :*

$$P \circ Q = Q^2 + 1 = (X + 1)^2 + 1 = X^2 + 2X + 2 \text{ et } Q \circ P = P + 1 = X^2 + 2.$$

Remarque I.16. *Le fait de travailler avec $P(X)$ plutôt qu'avec P permet d'éviter certaines confusions. Par exemple, avec $Q = X + 1$, on notera plutôt $P(Q(X))$, et donc dans le cas présent $P(X + 1)$ au lieu de $P \circ Q$. Pour ne pas confondre avec le produit de P par $(X + 1)$, on notera ce produit $(X + 1)P$, ou on explicitera le signe de multiplication en notant $P \times (X + 1)$ ou $P \cdot (X + 1)$.*

Proposition I.17. *Si $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$, alors :*

1. *si $\lambda \neq 0$, alors $\deg(\lambda P) = \deg(P)$;*
2. *$\deg(PQ) = \deg(P) + \deg(Q)$;*
3. *$\deg(P + Q) \leq \max(\deg(P), \deg(Q))$. Si on a $\deg(P) \neq \deg(Q)$, on a même une égalité : $\deg(P + Q) = \max(\deg(P), \deg(Q))$.*

Démonstration. Notons déjà que, suivant la démonstration précédente, on a déjà certaines inégalités sur les degrés, à savoir :

$$\left\{ \begin{array}{rcl} \deg\lambda P & \leq & \deg P \\ \deg(PQ) & \leq & \deg(P) + \deg(Q) \\ \deg(P + Q) & \leq & \max(\deg(P) + \deg(Q)) \end{array} \right.$$

1. Si $P = 0$, alors $\lambda P = 0$ et le résultat est vérifié. Sinon, en notant $a \neq 0$ le coefficient de degré $\deg(P)$ de P, celui de λP est $\lambda a \neq 0$. Donc $\deg(\lambda P) \geq \deg(P)$ et on a bien l'égalité.
2. Si P ou $Q = 0$, alors $PQ = 0$ et on a le résultat. Sinon, en notant $a \neq 0$ et $b \neq 0$ les coefficients dominants de P et Q, le coefficient de degré $\deg(P) + \deg(Q)$ de PQ est donc $ab \neq 0$, donc $\deg(PQ) \geq \deg(P) + \deg(Q)$, ce qui donne bien l'égalité cherchée.
3. Reste la situation d'égalité. Supposons par exemple que $n = \deg(P) > \deg(Q) = m$. En notant a, b les coefficients de degré n de P et Q, on a donc $a \neq 0$ et $b = 0$. Et donc le coefficient de degré n de $P + Q$ est $a + b = a \neq 0$. Ce qui donne bien l'égalité.

□

Remarque I.18. *Pour la somme, avec $P = X^2 + 1$ et $Q = -X^2 + X$, on trouve $P + Q = X + 1$ qui illustre la situation sans égalité. Plus généralement, si $P \neq 0$ et $Q = (-1) \cdot P$, on a : $P + Q = 0$.*
On peut donner la condition plus générale encore : il y a égalité si, et seulement si, les monômes dominants de P et Q ne sont pas opposés.

Corollaire I.19. *Si $P \in \mathbb{K}[X]$ et $k \in \mathbb{N}^*$, alors :*

$$\deg(P^k) = k\deg(P).$$

Démonstration. Par récurrence. □

Corollaire I.20. *Si $n \in \mathbb{N}$, alors $\mathbb{K}_n[X]$ est stable par addition et par multiplication par un scalaire, c'est-à-dire que :*

$$\forall P, Q \in \mathbb{K}_n[X],\ \forall \lambda \in \mathbb{K},\ \lambda P, (P + Q) \in \mathbb{K}_n[X].$$

Corollaire I.21. *Si $P, Q \in \mathbb{K}[X]$ vérifient $\deg(P + Q) < \deg(P)$, alors $\deg(P) = \deg(Q)$.*

Corollaire I.22. *Si $P, Q \in \mathbb{K}[X]$, alors :*

$$PQ = 0 \Rightarrow P = 0 \text{ ou } Q = 0.$$

Plus généralement, si $P, Q, R \in \mathbb{K}[X]$ avec $P \neq 0$, alors :

$$PQ = PR \Rightarrow Q = R.$$

Démonstration. On prouve le premier résultat par contraposée : si $P \neq 0$ et $Q \neq 0$, alors $\deg(P), \deg(Q) \geq 0$. Et donc $\deg(PQ) = \deg(P) + \deg(Q) \geq 0$, donc $PQ \neq 0$.
Pour le cas général, on a pour $P \neq 0$:

$$PQ = PR \Rightarrow P(Q - R) = 0 \Rightarrow Q - R = 0 \Rightarrow Q = R.$$

□

Remarque I.23. *Il y a en fait une petite "arnaque" dans la dernière preuve : le fait de factoriser par P demande d'avoir la distributivité de la multiplication sur l'addition pour les polynômes, mais on la montrera très bientôt.*

Corollaire I.24. *Si $P, Q \in \mathbb{K}[X]$, avec Q non constant, alors :*

$$\deg(P \circ Q) = \deg(P) \times \deg(Q).$$

Démonstration. On note $P = \sum_{k=0}^{n} a_k X^k$, avec $\deg(P) = n$ (c'est-à-dire $a_n \neq 0$), de sorte que $P \circ Q = \sum_{k=0}^{n} a_k Q^k$.
Pour tout $k \in \mathbb{N}$, le polynôme Q^k est de degré $\deg(Q) \times k$ (en itérant le résultat sur le degré d'un produit). Par degré d'une somme, et comme $a_n \neq 0$, on déduit donc que :

$$\deg\left(\sum_{k=0}^{n-1} a_k Q^k\right) \leq (n-1)\deg(Q) \text{ et } \deg(a_n Q^n) = n\deg(Q)$$

et ainsi on est dans le cas d'égalité pour le degré d'une somme, donc :

$$\deg(P \circ Q) = n\deg(Q) = \deg(P)\deg(Q).$$

□

Remarque I.25. *Si Q est constant, alors $P \circ Q$ aussi, mais on ne sait pas a priori s'il est nul ou non :*
- *si $P = X + 1$ et $Q = 0$: alors $P \circ Q = 1$;*
- *si $P = X + 1$ et $Q = -1$: alors $P \circ Q = 0$.*

I.3 L'anneau $\mathbb{K}[X]$

Proposition I.26. *Soient $P = \sum a_k X^k, Q = \sum b_k X^k, R = \sum c_k X^k$. Alors :*

1. *$P + Q = Q + P$ (commutativité de l'addition) ;*
2. *$(P + Q) + R = P + (Q + R)$ (associativité de l'addition) ;*
3. *$P + 0 = P = 0 + P$ (0 est neutre pour l'addition) ;*
4. *$P + ((-1) \cdot P) = ((-1) \cdot P) + P = 0$ (existence d'un inverse pour l'addition).*

C'est-à-dire que $(\mathbb{K}[X], +)$ est un groupe abélien.

Démonstration. Découle directement de la définition de l'addition de polynômes. Les égalités se montrent coefficient par coefficient : les propriétés de commutativité, associativité et de neutre découlent alors des mêmes propriétés pour l'addition sur $\mathbb{K}$. □

Proposition I.27. *Si $n \in \mathbb{N}$, alors $\mathbb{K}_n[X]$ est un sous-groupe de $\mathbb{K}[X]$.*

Démonstration. On a déjà $0 \in \mathbb{K}_n[X]$, et la stabilité a été montrée précédemment. □

Proposition I.28. *Avec les mêmes notations :*

1. *$PQ = QP$ (commutativité du produit) ;*
2. *$(PQ)R = P(QR)$ (associativité du produit) ;*
3. *$P(Q + R) = PQ + PR$ (distributivité du produit par rapport à la somme) ;*
4. *$1 \times P = P = P \times 1$ (1 est neutre pour la multiplication).*

C'est-à-dire que $(\mathbb{K}[X], +, \times)$ est un anneau commutatif. De plus, il est intègre.

Démonstration. On montre les égalités coefficient par coefficient :

1. Soit $n \in \mathbb{N}$. Par le changement d'indice $l = n - k$, le coefficient de degré n de PQ est :

$$\sum_{k=0}^{n} a_k b_{n-k} = \sum_{l=0}^{n} a_{n-l} b_l$$

   qui est donc égal à celui de QP, ce qui montre bien que $PQ = QP$.

2. Soit $n \in \mathbb{N}$. Le coefficient de degré n de $(PQ)R$ est :

$$\begin{aligned} \textstyle\sum_{k=0}^{n} \left(\sum_{l=0}^{k} a_l b_{k-l} \right) c_{n-k} &= \textstyle\sum_{k=0}^{n} \sum_{l=0}^{k} a_l b_{k-l} c_{n-k} \\ &= \textstyle\sum_{l=0}^{n} \sum_{k=l}^{n} a_l b_{k-l} c_{n-k} \\ &= \textstyle\sum_{l=0}^{n} \sum_{k'=0}^{n-l} a_l b_{k'} c_{(n-l)-k'} \\ &= \textstyle\sum_{l=0}^{n} a_l \left(\sum_{k=0}^{n-l} b_k c_{(n-l)-k} \right) \end{aligned}$$

   qui est donc égal à celui de $P(QR)$, ce qui montre bien que $(PQ)R = P(QR)$.

3. Soit $n \in \mathbb{N}$. Le coefficient de degré n de $P(Q + R)$ est :

$$\sum_{k=0}^{n} a_k (b_{n-k} + c_{n-k}) = \left(\sum_{k=0}^{n} a_k b_{n-k} \right) + \left(\sum_{k=0}^{n} a_k c_{n-k} \right)$$

   qui est donc égal à celui de $PQ + PR$, ce qui montre bien que $P(Q + R) = PQ + PR$.

4. Comme le polynôme 1 a un coefficient constant égal à 1, et tous ses autres coefficients nuls, alors le coefficient de degré n de $1 \times P$ est : $\sum_{k=0}^{n} a_k \delta_{n-k,0} = a_n$. Donc $1 \times P = P$, et par commutativité $P \times 1 = P$.

L'intégrité de $\mathbb{K}[X]$ vient de l'implication $PQ = 0 \Rightarrow P = 0$ ou $Q = 0$ montrée précédemment. □

Proposition I.29. *L'anneau $\mathbb{K}[X]$ vérifie que, pour tous $P, Q \in \mathbb{K}[X]$ et tous $\lambda, \mu \in \mathbb{K}$:*

1. $\lambda \cdot (P + Q) = \lambda \cdot P + \lambda \cdot Q$;
2. $(\lambda + \mu) \cdot P = \lambda \cdot P + \mu \cdot P$;
3. $\lambda \cdot (\mu \cdot P) = (\lambda\mu) \cdot P$;
4. $(\lambda \cdot P)Q = \lambda \cdot (PQ) = P(\lambda \cdot Q)$.

Démonstration. Découle des propriétés d'anneau de $\mathbb{K}[X]$, en constatant que la multiplication scalaire par $\lambda \in \mathbb{K}$ se comporte comme la multiplication polynomiale par le polynôme constant de valeur λ. □

Remarque I.30. *Muni de la multiplication scalaire, $\mathbb{K}[X]$ est plus qu'un anneau : c'est une algèbre, c'est-à-dire un anneau sur lequel $\mathbb{K}$ agit par multiplication scalaire de manière compatible avec les opérations usuelles.*

Proposition I.31. *Le groupe des inversibles de $\mathbb{K}[X]$ est : $\mathbb{K}[X]^\times = \mathbb{K}^*$.*

Démonstration. Par double inclusion :
— si $\lambda \in \mathbb{K}^*$, alors $\lambda \cdot \frac{1}{\lambda} = 1$; donc $\mathbb{K}^* \subset \mathbb{K}[X]^\times$;
— si $P \in \mathbb{K}[X]^\times$, notons $Q \in \mathbb{K}[X]$ tel que $PQ = 1$, alors $\deg(P) + \deg(Q) = 0$, donc $\deg(P) = 0$, et $\mathbb{K}[X]^\times \subset \mathbb{K}^*$.

□

I.4 Dérivation des polynômes

Définition I.32. *Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$. On définit le **polynôme dérivé** de P, noté P', comme le polynôme :*

$$P' = \sum_{k=1}^{n} k a_k X^{k-1} = \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k.$$

*On définit plus généralement, pour $m \in \mathbb{N}$, la **dérivée m-ème** de P, notée $P^{(m)}$, par : $P^{(0)} = P$ et $P^{(m)} = \left(P^{(m-1)}\right)'$ si $m > 0$.*

Remarque I.33. *Bien que cette dérivation ressemble beaucoup à la dérivée classique (pour les fonctions polynomiales), elle est à prendre comme une formule toute faite et n'est pas sensée refléter une limite de taux d'accroissement.*

Proposition I.34. *Si $P, Q \in \mathbb{K}[X]$ et $\lambda, \mu \in \mathbb{K}$, alors :*

1. $\deg(P') = \deg(P) - 1$ *si* $\deg(P) \geq 1$, *et* $-\infty$ *sinon ;*
2. $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$ *(linéarité de la dérivation)*
3. $(PQ)' = P'Q + PQ'$;
4. $(P \circ Q)' = Q' \times (P' \circ Q)$.

Démonstration.

1. Si P est constant, alors $P' = 0$ (en tant que valeur d'une somme vide).
   Sinon, en notant $P = \sum_{k=0}^{n} a_k X^k$ avec $a_n \neq 0$, alors $P' = \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k$, donc P' est de degré au plus $n-1$. Et comme $a_n \neq 0$, alors $n a_n \neq 0$ donc le coefficient de degré $n-1$ de P' est non nul : $\deg(P') = n - 1$.
2. En notant $P = \sum a_k X^k$ et $Q = \sum b_k X^k$, on a : $\lambda P + \mu Q = \sum (\lambda a_k + \mu b_k) X^k$. Et donc :

$$(\lambda P + \mu Q)' = \sum (k+1)(\lambda a_{k+1} + \mu b_{k+1}) X^k = \lambda \left(\sum (k+1) a_{k+1} X^k \right) + \mu \left(\sum (k+1) b_{k+1} X^k \right) = \lambda P' + \mu Q'.$$

3. Montrons l'égalité coefficient par coefficient. Notons $P = \sum a_k X^k$, $Q = \sum b_k X^k$ et $PQ = \sum c_k X^k$, avec $c_k = \sum_{l=0}^{k} a_l b_{k-l}$. Par définition de la dérivée, pour $k \in \mathbb{N}^*$, les coefficients de degré $k-1$ des polynômes considérés sont :
   — pour $(PQ)'$: $kc_k = k \cdot \sum_{l=0}^{k} a_l b_{k-l}$;
   — pour $P \cdot Q'$: $\sum_{l=0}^{k-1} a_l b'_{k-1-l} = \sum_{l=0}^{k-1}(k-l)a_l b_{k-l} = \sum_{l=0}^{k}(k-l)a_l b_{k-l}$;
   — pour $P' \cdot Q$: $\sum_{l=0}^{k-1} a'_l b_{k-1-l} = \sum_{l=0}^{k-1}(l+1)a_{l+1} b_{k-1-l} = \sum_{l=1}^{k} l a_l b_{k-l} = \sum_{l=0}^{k} l a_l b_{k-l}$.
   et comme $\sum_{l=0}^{k} k a_l b_{k-l} = \sum_{l=0}^{k} l a_l b_{k-l} + \sum_{l=0}^{k}(k-l)a_l b_{k-l}$, on a bien le résultat voulu.
4. La formule précédente, ainsi qu'une récurrence immédiate, montrent que : $\forall k \in \mathbb{N}, \left(Q^k\right)' = kQ'Q^{k-1}$. On déduit par linéarité de la dérivation que :

$$(P \circ Q)' = \left(\sum a_k Q^k\right)' = \sum a_k (Q^k)' = \sum a_k k Q' Q^{k-1} = Q' \cdot \left(\sum k a_k Q^{k-1}\right) = Q' \times (P' \circ Q).$$

□

Corollaire I.35. *Si $P, Q \in \mathbb{K}[X]$, $\lambda, \mu \in \mathbb{K}$ et $n \in \mathbb{N}$, alors :*

1. $\deg(P^{(n)}) = \deg(P) - n$ *si* $\deg(P) - n$ *si* $\deg(P) \geq n$ *et* $-\infty$ *sinon.*
2. $(\lambda P + \mu Q)^{(n)} = \lambda P^{(n)} + Q^{(n)}$.

Démonstration. Par récurrence avec le résultat précédent. □

Exemple I.36. *Si P est un polynôme de degré n, de coefficient dominant a_n, alors : $P^{(n)} = n! \cdot a_n$.*

Proposition I.37 (Formule de Leibniz)**.** *Si $P, Q \in \mathbb{K}[X]$ et $n \in \mathbb{N}$, alors :*

$$(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

Démonstration. On procède par récurrence sur n.
— si $n = 0$: alors $(PQ)^{(0)} = PQ$ et $\sum_{k=0}^{0} \binom{0}{k} P^{(k)} Q^{(0-k)} = P^{(0)} Q^{(0)} = PQ$ donc le résultat est vérifié.
— Supposons le résultat vérifié au rang $n \in \mathbb{N}$. Alors :

$$\begin{aligned}
(PQ)^{(n+1)} &= \left((PQ)^{(n)}\right)' \\
&= \left(\sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}\right)' \\
&= \sum_{k=0}^{n} \binom{n}{k} \left(P^{(k)} Q^{(n-k)}\right)' \\
&= \sum_{k=0}^{n} \binom{n}{k} (P^{(k+1)} Q^{(n-k)} + P^{(k)} Q^{(n+1-k)}) \\
&= \left(\sum_{l=1}^{n+1} \binom{n}{l-1} P^{(l)} Q^{(n+1-l)}\right) + \left(\sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n+1-k)}\right) \\
&= P^{(n+1)} Q^{(0)} + \left(\sum_{k=1}^{n} \underbrace{\left(\binom{n}{k-1} + \binom{n}{k} \right)}_{= \binom{n+1}{k}} P^{(k)} Q^{(n+1-k)} \right) + P^{(0)} Q^{(n+1)} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} P^{(k)} Q^{(n+1-k)}
\end{aligned}$$

ce qui conclut l'hérédité, donc la récurrence.

□

I.5 Fonctions polynomiales

Définition I.38. *On appelle **fonction polynomiale** une fonction définie sur $\mathbb{K}$ de la forme $f : x \mapsto a_0 + a_1 x + \cdots + a_n x^n$ avec $a_0, \ldots a_n \in \mathbb{K}$ qui sont appelés les **coefficients** de f.*
Avec ces notations, on dit que f est la fonction polynomiale associée au polynôme $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{K}[X]$. Et on notera alors $f = \widetilde{P}$.

Proposition I.39. *Deux fonctions polynomiales sont égales si, et seulement si, elles ont les mêmes coefficients.*

Démonstration. Supposons f, g deux fonctions polynomiales égales, de coefficients respectifs $a_0, \dots, a_n$ et $b_0, \dots, b_n$. Et supposons par l'absurde qu'il existe $k \in [\![0, n]\!]$ tel que $a_k \neq b_k$.
Notons m le plus grand entier tel que $a_m \neq b_m$. Ainsi, pour tout $x \in \mathbb{R}$, on a :

$$0 = P(x) - Q(x) = (a_m - b_m)x^m + (a_{m-1} - b_{m-1})x^{m-1} + \cdots + (a_0 - b_0).$$

Et donc, pour tout $x \neq 0$:

$$0 = \underbrace{a_m - b_m}_{\neq 0} + \frac{a_{m-1} - b_{m-1}}{x} + \cdots + \frac{a_0 - b_0}{x^m}.$$

En passant à la limite pour x tendant vers l'infini, on déduit que $0 = a_m - b_m$, d'où la contradiction. □

Corollaire I.40. *L'application $P \mapsto \widetilde{P}$ est une bijection de $\mathbb{K}[X]$ sur l'ensemble des fonctions polynomiales sur $\mathbb{K}$.*

Démonstration. La surjectivité vient de la définition des fonctions polynomiales.
L'injectivité découle de la proposition précédente. □

Remarque I.41. *En fait, il préserve les opérations $+$ et $\times$ (c'est comme ça qu'on les a construites) : c'est un isomorphisme d'anneaux.*
De plus, il est compatible avec la multiplication scalaire et la dérivation, dans le sens où :

$$\forall P, Q \in \mathbb{K}[X],\ \forall \lambda, \mu \in \mathbb{K},\ \widetilde{\lambda P + \mu Q} = \lambda \widetilde{P} + \mu \widetilde{Q} \text{ et } \widetilde{P'} = \widetilde{P}'.$$

C'est un morphisme d'algèbres à dérivation.

II Arithmétique élémentaire sur $\mathbb{K}[X]$

II.1 Divisibilité sur $\mathbb{K}[X]$

Définition II.1. *Soient $A, B \in \mathbb{K}[X]$. On dit que B **divise** A, ou que A est un **multiple** de B, ce que l'on note $B|A$, s'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$.*

Exemples II.2.

1. *$(X-1)(X+1) = X^2 - 1$, donc : $X - 1$ et $X + 1$ divisent chacun $X^2 - 1$.*
2. *$1 + X + X^2 + X^3$ divise $X^4 - 1$;*
3. *0 est un multiple de tout polynôme ; inversement, 0 est le seul multiple de 0 ;*
4. *si $a \in \mathbb{K}$ avec $a \neq 0$, alors a divise tout polynôme.*

Proposition II.3. *Soient $A, B \in \mathbb{K}[X]$ avec $A \neq 0$ tels que B divise A, alors $\deg(B) \leq \deg(A)$.*

Démonstration. On écrit $A = BQ$ pour $Q \in \mathbb{K}[X]$. On a donc : $\deg(A) = \deg(B) + \deg(Q)$. Comme $A \neq 0$, alors $Q \neq 0$ donc $\deg(Q) \geq 0$, ce qui donne le résultat. □

Proposition II.4. *Si $A, B, C \in \mathbb{K}[X]$ tels que $A|B$ et $A|C$, alors :*

1. *pour tous $U, V \in \mathbb{K}[X]$: $A|BU + CV$;*
2. *pour tout $P \in \mathbb{K}[X]$: $AP|BP$.*

Démonstration. On note $B = AQ_1$ et $C = AQ_2$ pour $Q_1, Q_2 \in \mathbb{K}[X]$. Alors :

1. $BU + CV = AQ_1U + AQ_2V = A(Q_1U + Q_2V)$;
2. $BP = AQ_1P = AP \cdot Q_1$;

ce qui donne les résultats. □

Proposition II.5. *La relation de divisibilité sur $\mathbb{K}[X]$ est réflexive et transitive, mais n'est pas antisymétrique.*
Plus précisément, pour $A, B \in \mathbb{K}[X]$, on a :

$$(A|B \text{ et } B|A) \Leftrightarrow \exists \lambda \in \mathbb{K}^*,\ A = \lambda B.$$

Remarque II.6. *On a donc sensiblement le même résultat que pour la divisibilité que sur $\mathbb{Z}$: les structures d'anneaux de $\mathbb{Z}$ et de $\mathbb{K}[X]$ sont très proches. On parle d'anneaux **euclidiens**.*

Démonstration. Soient $A, B, C \in \mathbb{K}[X]$. Alors :
- $A = 1 \cdot A$, donc $A|A$, ce qui donne la réflexivité ;
- si $A|B$ et $B|C$, notons $Q_1, Q_2 \in \mathbb{K}[X]$ tels que $AQ_1 = B$ et $BQ_2 = C$. Alors : $C = A(Q_1Q_2)$, donc $A|C$, ce qui donne la transitivité ;
- Montrons l'équivalence relative à la non antisymétrie :
  - si $A|B$ et $B|A$: si $A = 0$, alors $B = 0$ et tout $\lambda \in \mathbb{K}^*$ convient.
    Sinon, alors $A \neq 0$ et $B \neq 0$, et donc $\deg(A) \leq \deg(B)$ et $\deg(B) \leq \deg(A)$, donc $\deg(A) = \deg(B)$.
    Comme $B|A$, notons $Q \in \mathbb{K}[X]$ tel que $A = BQ$: alors $\deg(Q) = 0$, donc $Q = \lambda$ pour $\lambda \in \mathbb{K}^*$, ce qui donne le résultat.
  - réciproquement si $A = \lambda B$ pour $\lambda \in \mathbb{K}^*$, alors $B|A$. Mais on a aussi $B = \frac{1}{\lambda}A$, donc $A|B$.

□

Définition II.7. *On dit que deux éléments de $\mathbb{K}[X]$ sont **associés** chacun divise l'autre. Suivant la remarque précédente, cela revient à dire que l'on passe de l'un à l'autre par multiplication par un scalaire non nul.*

Exemples II.8.

1. *Tous les polynômes constants non nuls sont associés.*
2. *Le polynômes $X^2 + \frac{1}{2}$ et $2X^2 + 1$ sont associés. Plus généralement, tout polynôme à coefficients rationnels est associé à un polynôme à coefficients entiers.*
3. *Tout polynôme non nul est associé à un unique polynôme unitaire.*

II.2 Division euclidienne sur $\mathbb{K}[X]$

Théorème II.9 (Division euclidienne)**.** *Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Alors il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tels que :*

$$A = BQ + R \text{ et } \deg(R) < \deg(B).$$

*On dit que Q et R sont respectivement le **quotient** et le **reste** de la division euclidienne de A par B.*

Démonstration. Montrons séparément l'existence et l'unicité :
- Existence : Procédons par récurrence sur le degré de A :
  - si $A = 0$ ou si $\deg(A) < \deg(B)$: alors $(Q, R) = (0, A)$ convient.
  - hérédité : supposons le résultat vrai pour tous les polynômes de degré inférieur à n, pour $n \geq \deg(B)$. Soit $A \in \mathbb{K}[X]$ de degré n, et posons $a, b \neq 0$ les coefficients dominants respectifs de A et B. Posons $\widehat{A} = A - \frac{a}{b}X^{n-\deg(B)} \cdot B \in \mathbb{K}[X]$. Alors :
    - par degré d'un produit, $\frac{a}{b}X^{n-\deg(B)} \cdot B$ est de degré n ;
    - par degré d'une somme, $\widehat{A}$ est de degré au plus n ;
    - son coefficient de degré n est : $a - \frac{a}{b} \cdot b = 0$, donc il n'est pas de degré n.

et finalement $\widehat{A}$ est de degré au plus $(n-1)$, donc par hypothèse de récurrence il existe $(\widehat{Q},\widehat{R})$ tels que $\widehat{A}=B\widehat{Q}+\widehat{R}$ avec $\deg(\widehat{R})<\deg(B)$.
Et donc le couple $(\widehat{Q}+aX^{n-\deg(B)},\widehat{R})$ convient pour A.
D'où l'existence par récurrence.

— Unicité : Supposons que $(Q_1,R_1),(Q_2,R_2)$ conviennent. Alors on a : $B(Q_1-Q_2)=(R_2-R_1)$.
Comme $\deg(R1),\deg(R_2)<\deg(B)$, alors $\deg(R_2-R_1)<\deg(B)$.
Et ainsi : $\deg(B(Q_1-Q_2))=\deg(B)+\deg(Q_1-Q_2)<\deg(B)$, donc $\deg(Q_1-Q_2)<0$, c'est-à-dire $Q_1-Q_2=0$.
Ainsi on trouve $R_2-R_1=0$, et donc : $(Q_1,R_1)=(Q_2,R_2)$, ce qui assure l'unicité.

□

Remarque II.10. *On pouvait aussi faire un preuve comme pour la division euclidienne sur $\mathbb{Z}$, en notant que, pour A,B fixés l'ensemble $E=\{\deg(A-BQ)\,|\,Q\in\mathbb{K}[X]\}$ est une partie non-vide majorée de $\mathbb{N}$.*
L'intérêt de la preuve par récurrence est qu'elle fait apparaître comment on pose des divisions euclidiennes de polynômes.

Corollaire II.11. *Si $A,B\in\mathbb{K}[X]$ avec $B\neq 0$, alors B divise A si, et seulement si, le reste de la division euclidienne de A par B est nul.*

Démonstration. Découle de l'unicité. □

Exemple II.12. *Si $A,B\in\mathbb{K}[X]$ et $P\in\mathbb{K}[X]$ est non constant, alors on a l'équivalence :*

$$B|A\Leftrightarrow B\circ P|A\circ P.$$

En effet, le résultat est clair si $B=0$ (car alors $A=B=A\circ P=B\circ P=0$). Et sinon, en écrivant $A=BQ+R$ la division euclidienne de A par B, alors en composant avec P on a :

$$A\circ P=(B\circ P)\cdot(Q\circ P)+R\circ P$$

et l'écriture ci-dessus est en fait la division euclidienne de $A\circ P$ par $B\circ P$: en effet, par définition de la division euclidienne de A par B on a $\deg(R)<\deg(B)$, et donc par composition (comme P est non constant) alors $\deg(R\circ P)<\deg(B\circ P)$, ce qui donne bien la division euclidienne voulue par unicité.
Et ainsi on a :

$$B|A\Leftrightarrow R=0\Leftrightarrow R\circ P=0\Leftrightarrow B\circ P|A\circ P.$$

Corollaire II.13. *Si $A,B\in\mathbb{R}[X]$, alors B divise A **dans** $\mathbb{C}[X]$ si, et seulement si, B divise A dans $\mathbb{R}[X]$.*

Démonstration. Commençons par la réciproque : si B divise A dans $\mathbb{R}[X]$, il existe $Q\in\mathbb{R}[X]$ tel que $A=BQ$. L'inclusion $\mathbb{R}[X]\subset\mathbb{C}[X]$ donne le résultat.
Réciproquement : si B divise A dans $\mathbb{C}[X]$, alors le reste de la division euclidienne (sur $\mathbb{C}$) de A par B est nul. Si on note $A=BQ+R$ la division euclidienne (sur $\mathbb{R}$) de A par B, alors cela fournit aussi une division euclidienne sur $\mathbb{C}$ (par l'inclusion $\mathbb{R}[X]\subset\mathbb{C}[X]$). Et donc par unicité : $R=0$. Donc B divise A dans $\mathbb{R}[X]$. □

Exemple II.14. *Posons la division euclidienne de X^3+X^2+1 par $X-1$. On a :*

$$\begin{array}{rrrr|l}
X^3 & +X^2 & & -1 & X \quad -1 \\
\cline{5-5}
-X^3 & +X^2 & & & X^2 \quad +2X \quad +2 \\
\cline{1-2}
 & 2X^2 & & & \\
 & -2X^2 & +2X & & \\
\cline{2-3}
 & & 2X & & \\
 & & -2X & +2 & \\
\cline{3-4}
 & & & +1 &
\end{array}$$

donc le quotient est X^2+2X+2 et le reste est 1.

Exemple II.15. *Posons la division euclidienne de X^4-1 par X^2+1 :*

$$\begin{array}{rrr|rr} X^4 & & -1 & X^2 & +1 \\ \cline{4-5} -X^4 & -X^2 & & X^2 & -1 \\ \cline{1-2} & -X^2 & & & \\ & X^2 & +1 & & \\ \cline{2-3} & & 0 & & \end{array}$$

et donc le quotient est X^2-1 et le reste est nul, c'est-à-dire que X^2+1 divise X^4-1.
On pouvait avoir ce résultat plus directement en constatant que : $X^2-1=(X-1)(X+1)$. Et en composant par X^2 on trouve : $X^4-1=(X^2-1)(X^2+1)$.

III Racines de polynômes

III.1 Évaluation

Définition III.1. *Si $P\in\mathbb{K}[X]$ et $a\in\mathbb{K}$, on appelle **évaluation** de P en a, notée $P(a)$, l'expression obtenue en remplaçant X par a dans $P(X)$.*

Remarque III.2. *Cette expression se généralise pour d'autres valeurs de a, qui peut être une matrice carrée, une fonction à valeurs dans $\mathbb{K}$, ou même un polynôme, ce qu'on a en fait déjà effectué avant.*
Les précautions à prendre sont que :

- *a doit être choisi dans un anneau sur lequel $\mathbb{K}$ agit de manière compatible par multiplication (une algèbre en fait) ;*
- *le monôme constant doit être multiplié par l'élément neutre de l'anneau considéré (pour que tout ait bien un sens).*

Méthode III.3 (Méthode de Horner)**.** *Soit $P=\sum_{k=0}^n a_kX^k$ et $a\in\mathbb{K}$. Alors l'expression suivante permet de calculer $P(a)$ en un minimum d'opérations :*

$$P(a)=((\dots((a_n\cdot a+a_{n-1})\cdot a+a_{n-2})\cdot a+\dots)\cdot a+a_1)\cdot a+a_0$$

Remarque III.4. *Une autre manière de formuler ce résultat est que la suite (finie) définie par :*

$$\begin{cases} u_0 &= a_n \\ u_k &= au_{k-1}+a_{n-k} \text{ pour } 0<k\leq n \end{cases}$$

vérifie $P(a)=u_n$.

Exemple III.5. *Prenons $P(X)=X^3+2X^2-X+1$ et calculons $P(1+i)$. Le calcul de la suite (u_n) précédente donne :*

$$\begin{aligned} u_0 &= 1 \\ u_1 &= (1+i)+2=3+i \\ u_2 &= (3+i)(1+i)-1=1+4i \\ u_3 &= (1+4i)(1+i)+1=-2+5i \end{aligned}$$

et donc $P(1+i)=-2+5i$.

Théorème III.6 (Formule de Taylor polynomiale)**.** *Si $P\in\mathbb{K}[X]$ et $a\in\mathbb{K}$ (quelconque), alors :*

$$P=\sum\frac{P^{(k)}(a)}{k!}(X-a)^k.$$

Remarque III.7. *La somme précédente est en fait finie, car pour $k>\deg(P)$ on a : $P^{(k)}=0$. Et elle définit donc bien un polynôme.*

Démonstration. On procède par récurrence sur $n \in \mathbb{N}$ pour montrer qu'elle est vraie sur $\mathbb{K}_n[X]$:
- si $n = 0$: alors $P \in \mathbb{K}_0[X]$ est constant, donc pour tout $a \in \mathbb{K}$ on a : $P = P(a)$;
- supposons la formule vérifiée sur $\mathbb{K}_{n-1}[X]$ pour $n \in \mathbb{N}^*$, et considérons $P \in \mathbb{K}_n[X]$: alors $P' \in \mathbb{K}_{n-1}[X]$, donc on peut écrire :

$$P' = \sum_{k=0}^{n-1} \frac{(P')^{(k)}(a)}{k!}(X-a)^k = \sum_{k=0}^{n-1} \frac{P^{(k+1)}(a)}{k!}(X-a)^k.$$

Considérons le polynôme $Q = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$. Par linéarité de la dérivation, on a :

$$Q' = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}\left((X-a)^k\right)' = \sum_{k=1}^{n} \frac{P^{(k)}(a)}{(k-1)!}\left((X-a)^{k-1}\right) = \sum_{k=0}^{n-1} \frac{P^{(k+1)}(a)}{k!}\left((X-a)^k\right)$$

et ainsi : $P' - Q' = 0$, donc $P - Q$ est constant.
Or, on a : $(P-Q)(a) = P(a) - Q(a) = 0$, donc $P = Q$.
D'où la récurrence.
D'où le résultat. □

Remarque III.8. *Avec $a = 0$, on trouve :*

$$P = \sum \frac{P^{(k)}(a)}{k!}X^k = \sum a_k X^k$$

c'est-à-dire que les coefficient d'un polynôme sont directement données par les dérivées successives en 0 : $\forall k \in \mathbb{N},\ a_k = \frac{P^{(k)}(0)}{k!}$.
Plus généralement, cela veut dire qu'il suffit de connaître la valeur prise par un polynôme et chacune de ses dérivées pour connaître complètement ce polynôme.

III.2 Racines et multiplicité

Définition III.9. *Si $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$, on dira que a est **racine** (ou **zéro**) de P si $P(a) = 0$.*

Remarques III.10.
- *L'existence même de racines dépend du corps sur lequel on se place. Par exemple, le polynôme $X^2 + 1$ n'a pas de racine dans $\mathbb{R}$, mais il a comme racines $\pm i$ dans $\mathbb{C}$.*
- *Si $a \notin \mathbb{K}$, mais que $P(a)$ a bien un sens, avec $P(a) = 0$, on dira que P est un **polynôme annulateur** de a, mais on ne parlera pas de racine.*

Proposition III.11. *Si $A, B \in \mathbb{K}[X]$ avec $B|A$, alors toute racine de B est aussi une racine de A.*

Démonstration. Notons $A = BQ$. Si a est une racine de B, alors : $A(a) = B(a)Q(a) = 0$, donc a est racine de A. □

Proposition III.12. *Si $A, B, C \in \mathbb{K}[X]$ avec $A = BC$, et $a \in \mathbb{K}$, alors a est racine de A si, et seulement si, il est racine de B ou de C.*

Démonstration. On a : $A(a) = B(a)C(a)$, et donc $A(a) = 0 \Leftrightarrow B(a) = 0$ ou $C(a) = 0$. □

Corollaire III.13. *Si $A, B \in \mathbb{K}[X]$, avec $B \neq 0$, et que R est le reste de la division euclidienne de A par B, alors pour tout racine a de B on a : $A(a) = R(a)$.*

Remarque III.14. *Ce corollaire permet de calculer des restes de divisions euclidienne, ou au moins certaines de leurs propriétés, avec très peu de calculs.*

Exemple III.15. *Soit $n \in \mathbb{N}$. Posons $A_n = X^n \in \mathbb{K}[X]$, et déterminons le reste de la division euclidienne de A_n par $B = X^2 - 3X + 2$.*

- *déterminons déjà les racines de B : par calcul des racines d'un polynôme de degré 2, on trouve qu'il s'agit de 1 et 2 ;*
- *notons R_n le reste de la division euclidienne de A_n par B. Alors :*

$$R_n(1) = A_n(1) = 1^n = 1 \text{ et } R_n(2) = A_n(2) = 2^n.$$

Mais on a aussi que $R_n \in \mathbb{K}_1[X]$ (comme $\deg(B) = 2$), donc $R_n = a_n X + b_n$ pour $a_n, b_n \in \mathbb{K}$.
On est donc ramené à résoudre le système :

$$\begin{cases} a_n + b_n &= 1 \\ 2a_n + b_n &= 2^n \end{cases}$$

ce qui donne finalement : $R_n = (2^n - 1)X + (2 - 2^n)$.

Proposition III.16. *Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors a est racine de P si, et seulement si, $(X - a)$ divise P.*

Démonstration. Écrivons la division euclidienne de P par $(X - a)$: $P = (X - a) \cdot Q + R$, avec $Q, R \in \mathbb{K}[x]$ et $\deg(R) < \deg(X - a) = 1$.
Ainsi, R est constant, et comme $P(a) = R(a)$, alors $R = P(a)$.
On a ainsi l'équivalence : $P(a) = 0 \Leftrightarrow R = 0$.
Et donc a est racine de P si, et seulement si, $(X - a)$ divise P. □

Proposition-Définition III.17. *Soit $P \in \mathbb{K}[X]$ **non nul** et $a \in \mathbb{K}$. Alors l'ensemble $\{k \in \mathbb{N} \,|\, (X - a)^k | P\}$ possède un plus grand élément $m \in \mathbb{N}$, qu'on appelle **multiplicité de** a **comme racine de** P.*
L'entier m est non nul si, et seulement si, a est racine de P.
*Si $m = 1$: alors $(X - a) | P$ mais $(X - a)^2 \nmid P$, et on dit que a est **racine simple** de P.*
*Si $m \geq 2$: alors $(X - a)^m | P$ mais $(X - a)^{m+1} \nmid P$, et on dit que a est **racine multiple** de P.*

Démonstration. Il faut juste montrer que $\{k \in \mathbb{N} \,|\, (X - a)^k | P\}$ possède un plus grand élément. Or, cet ensemble est un sous-ensemble de $\mathbb{N}$:

- non vide : car $(X - a)^0 = 1$ divise P, donc il contient 0 ;
- majoré : car, si $(X - a)^k | P$, comme $P \neq 0$, alors $\deg((X - a)^k) \leq \deg(P)$, et donc $k \leq \deg(P)$.

Donc il possède bien un plus grand élément. □

Proposition III.18. *Si $P \in \mathbb{K}[X]$ non nul, $a \in \mathbb{K}$ et $m \in \mathbb{N}$, alors a est racine de multiplicité m de P si, et seulement si, il existe $Q \in \mathbb{K}[X]$ tel que :*

$$P = (X - a)^m Q \text{ et } Q(a) \neq 0.$$

Démonstration. Supposons a racine de P de multiplicité m. Alors on a déjà $P = (X - a)^m Q$ pour $Q \in \mathbb{K}[X]$. Et nécessairement, pour un tel Q, on a $Q(a) \neq 0$. Sinon, on aurait que $(X - a) | Q$, et donc $Q = (X - a) \cdot R$ pour $R \in \mathbb{K}[X]$, et donc $P = (X - a)^{m+1} R$, ce qui contredit la maximalité de m.
Réciproquement, si $P = (X - a)^m Q$ avec $Q(a) \neq 0$, alors $(X - a)^m$ divise P. Si $(X - a)^{m+1}$ divisait P, alors on pourrait écrire $P = (X - a)^{m+1} R$ (pour $R \in \mathbb{K}[X]$) et donc par intégrité $Q = (X - a)R$, donc $Q(a) = 0$. Donc P n'est pas divisible par $(X - a)^{m+1}$ et a est bien racine de multiplicité m de P. □

Corollaire III.19. *Si $A, B \in \mathbb{K}[X]$ avec $B | A$, alors toute racine de B est une racine de A avec une multiplicité supérieure ou égale.*

Proposition III.20. *Si $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}^*$, alors a est racine de multiplicité m de P si, et seulement si :*

$$P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0 \text{ et } P^{(m)}(a) \neq 0.$$

Démonstration. Notons $n = \deg(P)$.
Si $P(a) = \cdots = P^{(m-1)}(a) = 0$ et $P^{(m)}(a) \neq 0$, alors par la formule de Taylor polynomiale on a :

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k = \sum_{k=m} n\frac{P^{(k)}(a)}{k!}(X-a)^m = (X-a)^m \cdot Q$$

où $Q = \sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^{k-m} \in \mathbb{K}[X]$. Or, on a $Q(a) = \frac{P^{(m)}(a)}{m!} \neq 0$, et on a bien que la multiplicité de a est égale à m.
Inversement, supposons que a est racine de multiplicité m de P, de sorte que $P = (X-a)^m Q$ avec $Q(a) \neq 0$, qui correspond aussi à la division euclidienne de P par $(X-a)^m$ (de reste nul). Par la formule de Taylor on a :

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k = (X-a)^m \left(\sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^{k-m}\right) + \left(\sum_{k=0}^{m-1} \frac{P^{(k)}(a)}{k!}(X-a)^k\right)$$

ce qui donne par unicité de la division euclidienne :

$$Q = \sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^{k-m} \text{ et } 0 = \sum_{k=0}^{m-1} \frac{P^{(k)}(a)}{k!}(X-a)^k.$$

En reconnaissant la composée du polynôme $\sum_{k=0}^{m-1} \frac{P^{(k)}(a)}{k!}X^k$ est de $(X-a)$, qui doit être égale au polynôme nul, on déduit que pour tout $k \in [\![0; m-1]\!]$: $\frac{P^{(k)}(a)}{k!} = 0$, donc $P^{(k)}(a) = 0$.
Par évaluation de Q en a, on trouve : $Q(a) = \frac{P^{(m)}(a)}{m!} \neq 0$, donc $P^{(m)}(a) \neq 0$. □

Corollaire III.21. *Si a est racine de P de multiplicité $m \geq 2$, alors a est racine de P' de multiplicité $(m-1)$.*

Démonstration. On a : $P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0$ et $P^{(m)}(a) \neq 0$.
Et donc : $P'(a) = (P')'(a) = \cdots = (P')^{(m-2)}(a) = 0$ et $(P')^{(m-1)}(a) \neq 0$. □

Remarque III.22. *On pouvait aussi le montrer par dérivée d'un produit. En notant $P = (X-a)^m Q$ avec $Q(a) \neq 0$, on a :*

$$P' = m(X-a)^{m-1}Q + (X-a)^m Q' = (X-a)^{m-1}\left(mQ + (X-a)Q'\right) = (X-a)^{m-1}\overline{Q}$$

où $\overline{Q} \in \mathbb{K}[X]$ vérifie : $\overline{Q}(a) = mQ(a) \neq 0$.

Corollaire III.23. *Si $A, B \in \mathbb{K}[X]$ avec $B \neq 0$, et que R est le reste de la division euclidienne de A par B, alors si a est une racine de B de multiplicité $m \in \mathbb{N}$: $\forall k \in [\![0; m-1]\!]$, $A^{(k)}(a) = R^{(k)}(a)$.*

Démonstration. Si $A = BQ + R$, alors a est racine de multiplicité m de BQ. Ainsi, en dérivant k fois et en évaluant en a, on obtient :

$$A^{(k)}(a) = (BQ)^{(k)}(a) + R^{(k)}(a)$$

ce qui donne bien le résultat pour $k \leq m-1$ car alors $(BQ)^{(k)}(a) = 0$. □

Remarque III.24. *Cela permet de calculer des restes de divisions euclidienne lorsque B possède des racines multiples.*

Exemple III.25. *Reprenons le polynôme $A_n = X^n \in \mathbb{K}[X]$, et posons R_n le reste de la division euclidienne de A_n par $B = (X-1)^2$. On a ainsi :*

$$R_n(1) = A_n(1) = 1 \text{ et } R_n'(1) = A_n'(1) = n$$

et donc par formule de Taylor, comme $\deg(R_n) \leq 1$ *:*

$$R_n = R_n(1) + R_n'(1)(X-1) = nX + (n-1).$$

Corollaire III.26. *Si $A, B, C \in \mathbb{K}[X]$ avec $A = BC$, et $a \in \mathbb{K}$. Notons m_A, m_B, m_C les multiplicités (éventuellement nulles) de a comme racine de A, B, C. Alors : $m_A = m_B + m_C$.*

Démonstration. Par définition de m_B et m_C, on a :

$$B(a) = \cdots = B^{(m_B-1)}(a) = C(a) = \ldots C^{(m_C-1)}(a) = 0 \text{ et } B^{(m_B)}(a), C^{(m_C)}(a) \neq 0.$$

Par la formule de Leibniz, on a pour tout $n \in \mathbb{N}$:

$$A^{(n)}(a) = \sum_{k=0}^{n} \binom{n}{k} B^{(k)}(a) C^{(n-k)}(a)$$

et donc :
- si $n \leq (m_B + m_C) - 1$: pour tout $k \in [\![0; n]\!]$, $k \leq m_B - 1$ ou $n - k \leq m_C - 1$, et donc $A^{(n)}(a) = 0$;
- si $n = m_B + m_C$: $A^{(n)}(a) = B^{(m_B)}(a)C^{(m_C)}(a) \neq 0$;

ce qui donne bien le résultat. □

III.3 Factorisation par les racines

Proposition III.27. *Si $P \in \mathbb{K}[X]$ est* ***non nul****, et $\lambda_1, \ldots, \lambda_r \in \mathbb{K}$ des racines deux-à-deux distinctes de P, de multiplicités respectives $m_1, \ldots, m_r \in \mathbb{N}^*$, alors P est divisible par $(X-\lambda_1)^{m_1} \ldots (X-\lambda_r)^{m_r}$.*

Démonstration. Prouvons par récurrence sur $k \in [\![1, r]\!]$ que P est divisible par $P_k = (X-\lambda_1)^{m_1} \ldots (X-\lambda_k)^{m_k}$.
- si $k = 1$: alors cela a déjà été prouvé, car λ_1 est racine de multiplicité m_1 de P.
- hérédité : supposons pour $k \in [\![1, r-1]\!]$ que P est divisible par P_k.
  On pose $Q \in \mathbb{K}[X]$ tel que $P = P_k Q$.
  Si on note n_1, n_2 les multiplicités de λ_{k+1} comme racines de P_k, Q, alors on a :
  - comme $P = P_k Q$, alors : $n_1 + n_2 = m_{k+1}$;
  - comme les λ_i sont deux-à-deux distincts, alors $P_k(\lambda_{k+1}) \neq 0$, donc $n_1 = 0$.

  Et donc $n_2 = m_{k+1}$, donc Q s'écrit : $Q = (X-\lambda_{k+1})^{m_{k+1}} A$ et finalement :

$$P = P_k (X-\lambda_{k+1})^{m_{k+1}} A = P_{k+1} A$$

  ce qui prouve l'hérédité.

D'où la récurrence. □

Remarque III.28. *On peut utiliser ce résultat dans l'autre sens : si $(X-\lambda_1)^{m_1} \ldots (X-\lambda_r)^{m_r}$ divise P, alors $\lambda_1, \ldots, \lambda_r$ sont racines de P de multiplicités respectives au moins $m_1, \ldots, m_r$.*

Corollaire III.29. *Si $\lambda_1, \ldots, \lambda_r \in \mathbb{K}$ sont deux à deux distincts, et $P \in \mathbb{K}[X]$, alors :*

$$P(\lambda_1) = \cdots = P(\lambda_r) = 0 \Leftrightarrow (X-\lambda_1) \ldots (X-\lambda_r) \text{ divise } P.$$

Exemple III.30. *On peut se demander pour quelles valeurs de $n \in \mathbb{N}$ le polynôme X^2+1 divise le polynôme X^n-1.*
Comme $X^2+1 = (X+i)(X-i)$, alors cela revient à chercher pour quelle valeur de n on a : $i^n - 1 = 0$ et $(-i)^n - 1 = 0$.
La première égalité impose que $n \equiv 0\ [4]$ et la seconde aussi. Et donc finalement $X^n - 1$ est divisible par X^2+1 si, et seulement si : $n \equiv 0\ [4]$.

Remarque III.31. *On retrouve le passage de la division sur $\mathbb{C}[X]$ à celle sur $\mathbb{R}[X]$. Il suffit de savoir si le polynôme X^2+1 divise X^n+1 dans $\mathbb{C}[X]$ pour avoir aussi la divisibilité sur $\mathbb{R}[X]$.*

Corollaire III.32. *Si $\lambda_1, \dots, \lambda_r$ sont des racines de P de multiplicité respectives $m_1, \dots, m_r$, alors :*

$$\sum_{k=1}^{r} m_k \leq \deg(P).$$

De plus, il y a égalité si, et seulement si, les polynômes P et $(X-\lambda_1)^{m_1} \dots (X-\lambda_r)^{m_r}$ sont associés.

Démonstration. Comme $(X-\lambda_1)^{m_1} \dots (X-\lambda_r)^{m_r}$ divise P, on peut noter $P = (X-\lambda_1)^{m_1} \dots (X-\lambda_r)^{m_r} Q$ pour $Q \in \mathbb{K}[X]$.
Et alors en regardant les degrés :
— $\deg((X-\lambda_1)^{m_1} \dots (X-\lambda_r)^{m_r}) \leq \deg(P)$, ce qui donne l'inégalité ;
— le cas d'égalité correspond au cas où $\deg(Q) = 0$, c'est-à-dire que Q est constant (non nul).
□

Corollaire III.33. *Un polynôme non nul a au plus autant de racines **comptées avec multiplicité** que sont degré.*
En particulier, si $P \in \mathbb{K}_n[X]$ possède plus de $(n+1)$ racines, alors $P = 0$.

Corollaire III.34. *Un polynôme qui possède une infinité de racines est nul.*

Remarque III.35. *Ce résultat peut être utilisé pour montrer que deux polynômes sont égaux : il suffit de voir qu'il prennent une infinité de valeurs communes.*

Exemple III.36. *Montrons que la fonction racine carrée n'est pas polynomiale.*
Par l'absurde, supposons qu'il existe $P \in \mathbb{C}[X]$ tel que : $\forall n \in \mathbb{N}, P(n) = \sqrt{n}$.
Alors : $\forall n \in \mathbb{N},\ P(n)^2 - n = 0$
Donc les polynômes P^2 et X sont égaux, donc ont même degré : $\deg(P^2) = 2\deg(P) = \deg(X) = 1$, ce qui est impossible.

III.4 Interpolation

Définition III.37. *Si $x_1, \dots, x_n \in \mathbb{K}$ sont deux-à-deux distincts et $i \in [\![1, n]\!]$, le **i-ème polynôme de Lagrange** associé à $(x_1, \dots, x_n)$ est le polynôme :*

$$L_i = \prod_{k \neq i} \frac{X - x_k}{x_i - x_k} = \frac{X-x_1}{x_i-x_1} \dots \frac{X-x_{i-1}}{x_i-x_{i-1}} \frac{X-x_{i+1}}{x_i-x_{i+1}} \dots \frac{X-x_n}{x_i-x_n}.$$

Remarque III.38. *Le point important est que les x_k sont deux à deux distincts, pour que L_i soit bien défini.*

Proposition III.39. *Avec les notations précédentes :*

$$\forall i, j \in [\![1, n]\!],\ L_i(x_j) = \delta_{i,j} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}.$$

Démonstration. Si $i, j \in [\![1, n]\!]$. Notons $P_k = \dfrac{X - x_k}{x_i - x_k}$ de sorte que $L_i = \prod_{k \neq i} P_k$:
— si $i \neq j$: $P_j(x_j) = 0$ apparaît dans le produit qui définit $L_i(x_j)$, donc $L_i(x_j) = 0$;
— si $i = j$: alors $P_k(x_i) = 1$ pour tout $k \neq i$, et donc $L_i(x_i) = 1$.

□

Proposition III.40. *Avec les mêmes notation, L_i est **l'unique** polynôme de $\mathbb{K}_{n-1}[X]$ vérifiant la propriété précédente.*

Démonstration. Si $P \in \mathbb{K}_{n-1}[X]$ vérifie cette propriété, alors pour tout $j \in [\![1, n]\!]$: $(P - L_i)(x_j) = 0$.
Donc le polynôme $P - L_i \in \mathbb{K}_{n-1}[X]$ possède n racines, donc il s'agit du polynôme nul, donc $P = L_i$. □

Théorème III.41 (Interpolation de Lagrange)**.** *Si $x_1, \dots, x_n \in \mathbb{K}$ sont deux-à-deux distincts, et $y_1, \dots, y_n \in \mathbb{K}$, alors il existe un unique polynôme $P \in \mathbb{K}_{n-1}[X]$ tel que : $\forall i \in [\![1, n]\!],\ P(x_i) = y_i$.*
Plus précisément, un tel P est donné par : $P = \sum_{i=1}^{n} y_i L_i$.

Démonstration. Montrons séparément l'existence et l'unicité.
— existence : posons $P = \sum_{i=1}^{n} y_i L_i$. Comme tous les L_i sont des éléments de $\mathbb{K}_{n-1}[X]$, alors P aussi. Et de plus pour tout $j \in [\![1, n]\!]$ on a :

$$P(x_j) = \sum_{i=1}^{n} y_i L_i(x_j) = \sum_{i=1}^{n} y_i \delta_{i,j} = y_j$$

ce qui montre que P convient.
— unicité : si P_1, P_2 conviennent, alors $Q = (P_1 - P_2) \in \mathbb{K}_{n-1}[X]$ vérifie :

$$Q(x_1) = \cdots = Q(x_n) = 0$$

et donc Q possède n racines, donc $Q = 0$. Et donc $P_1 = P_2$, ce qui assure l'unicité.

□

Remarque III.42. *Les polynômes L_i sont de degré $n - 1$, mais le polynôme donné par l'interpolation de Lagrange peut être de degré plus petit.*
Par exemple, si $x_i = y_i = i$, alors le polynôme obtenu est $P = X$ est est de degré 1.

Corollaire III.43. *Si $P \in \mathbb{K}_{n-1}[X]$, et $x_1, \dots, x_n \in \mathbb{K}$ sont deux-à-deux distincts, alors P s'écrit de manière unique comme combinaison linéaire en les L_i. Plus précisément : $P = \sum_{i=1}^{n} P(x_i) L_i$.*

Corollaire III.44. *Avec les notations précédentes, l'ensemble des polynômes Q tels que $\forall i \in [\![1, n]\!],\ Q(x_i) = y_i$ est exactement l'ensemble des polynômes de la forme :*

$$\left(\sum_{i=1}^{n} y_i L_i\right) + P \cdot \left(\prod_{i=1}^{n} (X - x_i)\right)$$

où $P \in \mathbb{K}[X]$.

Démonstration. Posons $Q_0 = \sum_{i=1}^{n} y_i L_i$. Pour $Q \in \mathbb{K}[X]$, on a donc :

$$\begin{aligned}
\forall i \in [\![1, n]\!],\ Q(x_i) = y_i &\Leftrightarrow \forall i \in [\![1, n]\!],\ Q(x_i) = Q_0(x_i) \\
&\Leftrightarrow \forall i \in [\![1, n]\!],\ (Q - Q_0)(x_i) = 0 \\
&\Leftrightarrow \left(\textstyle\prod_{i=1}^{n} (X - x_i)\right) | (Q - Q_0) \\
&\Leftrightarrow \exists P \in \mathbb{K}[X],\ P \cdot \left(\textstyle\prod_{i=1}^{n} (X - x_i)\right) = Q - Q_0 \\
&\Leftrightarrow \exists P \in \mathbb{K}[X],\ Q = Q_0 + P \cdot \left(\textstyle\prod_{i=1}^{n} (X - x_i)\right)
\end{aligned}$$

ce qui donne le résultat. □

Remarque III.45. *Avec les notations précédente, un tel polynôme Q a pour reste Q_0 dans la division euclidienne par $\left(\prod_{i=1}^{n} (X - x_i)\right)$. Donc si l'on possède un polynôme, on peut déduire Q_0 par division euclidienne et retrouver ensuite tous les polynômes voulus avec le résultat précédent.*

III.5 Polynômes scindés

Définition III.46. *On dit qu'un polynôme $P \in \mathbb{K}[X]$ non constant est **scindé** (sur $\mathbb{K}$) s'il possède autant de racines (comptées avec multiplicités) que son degré.*
*On dira de plus que P est **scindé simple** (ou scindé à racines simples) si toutes ses racines sont simples.*

Remarque III.47. *Le fait d'être scindé dépend du corps d'étude : par exemple, le polynôme X^2+1 est scindé sur $\mathbb{C}$ (car il a comme racines i et $-i$), mais pas sur $\mathbb{R}$ (car il n'a pas de racine dans $\mathbb{R}$).*

Proposition III.48. *Le polynôme $P \in \mathbb{K}[X]$ est scindé si, et seulement si, il existe $\lambda_1, \dots, \lambda_r \in \mathbb{K}$ (deux à deux distincts), $m_1, \dots, m_r \in \mathbb{N}^*$ et $\alpha \in \mathbb{K}^*$ tels que :*

$$P = \alpha(X-\lambda_1)^{m_1} \dots (X-\lambda_r)^{m_r}.$$

*Avec ces notations, les λ_i sont **les** racines de P, de multiplicité m_i.*
De plus P est de degré $\sum_{i=1}^r m_i$, et de coefficient dominant α.

Démonstration. Si P est scindé, en notant $\lambda_1, \dots, \lambda_r$ ses racines, de multiplicité $m_1, \dots, m_r$, alors $\sum_{i=1}^r m_i = \deg(P)$, et par le résultat précédent : P est associé à $(X-\lambda_1)^{m_1} \dots (X-\lambda_r)^{m_r}$, donc de la forme $\alpha(X-\lambda_1)^{m_1} \dots (X-\lambda_r)^{m_r}$ pour $\alpha \in \mathbb{K}^*$. Comme $(X-\lambda_1)^{m_1} \dots (X-\lambda_r)^{m_r}$ est unitaire, on trouve bien le coefficient dominant pour P.
Réciproquement, si $P = \alpha(X-\lambda_1)^{m_1} \dots (X-\lambda_r)^{m_r}$, alors $\lambda_1, \dots, \lambda_r$ sont des racines de P, de multiplicités $m_1, \dots, m_r$.
En effet, pour $k \in [\![1, r]\!]$, on a : $P = (X-\lambda_k)^{m_k} \cdot Q_k$, où $Q_k = \alpha \prod_{l \neq k}(X-\lambda_l)^{m_l}$, et la multiplicité vient du fait que $Q(\lambda_k) = \alpha \prod_{l \neq k}(\lambda_k - \lambda_l)^{m_l} \neq 0$.
Comme $\deg(P) = \sum_{k=1}^r m_i$, alors P est bien scindé. □

Proposition III.49. *Si $A, B \in \mathbb{K}[X]$ avec B **scindé**, alors :*

1. *si A divise B, alors A est scindé, et toutes les racines de A sont des racines de B avec des multiplicités plus petites que pour B ;*
2. *B divise A si, et seulement si, toutes les racines de B sont aussi des racines de A avec des multiplicités plus grandes que pour B.*

Démonstration. Notons $\lambda_1, \dots, \lambda_r$ les racines de B, et $m_1, \dots, m_r$ leurs multiplicité de sorte que $B = \alpha(X-\lambda_1)^{m_1} \dots (X-\lambda_r)^{m_r}$ pour $\alpha \in \mathbb{K}^*$.
Si A divise B : notons $Q \in \mathbb{K}[X]$ tel que $AQ = B$. Les racines de A et de Q sont exactement les mêmes racines que B. Notons $n_1, \dots, n_r$ et $n'_1, \dots, n'_r$ leurs multiplicités (éventuellement nulles) pour A et Q. Comme $AQ = B$, alors :

$$\forall k \in [\![1; r]\!],\ n_k + n'_k = m_k$$

et on a donc, en utilisant les degrés :

$$\deg(A) + \deg(Q) = \deg(B) = \sum_{k=1}^r m_k = \sum_{k=1}^r n_k + \sum_{k=1}^r n'_k \leq \deg(A) + \deg(Q)$$

et donc l'inégalité précédente est une égalité, ce qui impose que $\sum_{k=1}^r n_r = \deg(A)$, donc A est scindé (et Q aussi).
Si B divise A, alors $(X-\lambda_1)^{m_1} \dots (X-\lambda_r)^{m_r}$ divise A, donc chaque λ_k est racine de A de multiplicité au moins m_k.
Réciproquement, si tous les λ_k sont racines de A de multiplicité $n_k \geq m_k$, alors il existe un polynôme Q tel que :

$$A = (X-\lambda_1)^{n_1} \dots (X-\lambda_r)^{n_r} \cdot Q = \underbrace{(\alpha(X-\lambda_1)^{m_1} \dots (X-\lambda_r)^{m_r})}_{=B} \left(\frac{1}{\alpha}(X-\lambda_1)^{n_1-m_1} \dots (X-\lambda_r)^{n_r-m_r} Q\right)$$

et donc B divise A. □

Proposition III.50 (Formule de Viète, ou relation coefficients-racines)**.** *Soit $P = \sum a_k X^k$ un polynôme scindé de degré n, dont on note $x_1, \dots, x_n$ les racines (avec éventuellement des répétitions selon les multiplicités).*
On note, pour $k \in [\![1; n]\!]$, le scalaire σ_k comme le k-ème ***polynôme symétrique élémentaire*** *en les x_i, c'est-à-dire que :*

$$\sigma_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} x_{i_1} x_{i_2} \dots x_{i_k}.$$

Alors pour tout $k \in [\![1, k]\!]$, on a :

$$\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}.$$

Démonstration. Avec les notations, on a : $P = a_n(X - x_1) \dots (X - x_n) = \sum a_k X^k$.
L'égalité s'obtient en développant la première expression, et en identifiant les coefficient de même degré suivant les deux écritures. □

Remarque III.51. *Si l'expression de σ_k est compliquée dans le cas général, elle l'est beaucoup moins pour $k = 1$ ou n :*

$$\sigma_1 = \sum_{i=1}^{n} x_i \text{ et } \sigma_n = \prod_{i=1}^{n} x_i$$

ce qui se voit sur le polynôme P qui s'écrit :

$$P = a_n X^n - a_n(x_1 + \dots + x_n)X^{n-1} + a_n(x_1x_2 + \dots + x_{n-1}x_n)X^{n-2} - \dots + (-1)^n a_n x_1 x_2 \dots x_n.$$

Exemple III.52. *Si $n = 2$, notons $P = aX^2 + bX + c$, qui est scindé sur $\mathbb{C}$. Si on note x_1, x_2 ses racines, alors :*

$$x_1 + x_2 = -\frac{b}{a} \text{ et } x_1 x_2 = \frac{c}{a}$$

III.6 Racines et factorisation sur $\mathbb{R}$ ou $\mathbb{C}$

Théorème III.53 (Théorème de d'Alembert–Gauss, ou théorème fondamental de l'algèbre)**.** *Tout polynôme non constant de $\mathbb{C}[X]$ admet une racine.*

Démonstration. Admis. □

Corollaire III.54. *Tout polynôme non constant de $\mathbb{C}[X]$ est scindé.*

Démonstration. On procède par récurrence sur le degré de P.
- Si $\deg(P) = 1$: alors P possède une racine, et est de degré 1, donc P est scindé.
- Supposons le résultat acquis pour les polynômes de degré au plus n, pour $n \in \mathbb{N}$, et donnons-nous $P \in \mathbb{C}[X]$ avec $\deg(P) = n + 1$. Comme P possède une racine λ_{n+1}, alors il existe est divisible par $(X - \lambda_{n+1})$ donc il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - \lambda_{n+1})Q$.
  Comme Q est de degré n, il est scindé, donc on peut écrire $Q = \alpha(X - \lambda_1) \dots (X - \lambda_n)$, et ainsi : $P = \alpha(X - \lambda_1) \dots (X - \lambda_{n+1})$ est scindé.

□

Remarques III.55.

1. *En utilisant un résultat précédent, pour montrer que $B \in \mathbb{C}[X]$ divise $A \in \mathbb{C}[X]$, il suffit de regarder toutes les racines de B et de vérifier qu'elles sont racines de A de multiplicité plus grande ou égale.*
2. *On peut appliquer ce résultat à des polynômes de $\mathbb{R}[X]$, du fait de l'inclusion $\mathbb{R}[X] \subset \mathbb{C}[X]$, mais les polynômes seront alors scindés sur $\mathbb{C}$.*

Proposition III.56. *Soit $P \in \mathbb{R}[X]$. Si $\alpha \in \mathbb{C} \setminus \mathbb{R}$ est une racine de P de multiplicité m, alors :*

1. *$\overline{\alpha}$ est aussi une racine de P, de même multiplicité que α ;*
2. *P est divisible (dans $\mathbb{R}[X]$) par $(X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|^2)^m$.*

Démonstration. Notons $P = \sum a_k X^k$, où les a_k sont des réels.
Par propriété de la conjugaison complexe, on a :

$$P(\overline{\alpha}) = \sum a_k \overline{\alpha}^k = \sum \overline{a_k}\overline{\alpha^k} = \sum \overline{a_k \alpha^k} = \overline{\sum a_k \alpha^k} = \overline{P(\alpha)} = \overline{0} = 0$$

et donc α est racine de P.
Par le même raisonnement, comme $P', P'', \ldots, P^{(m)}$ sont aussi à coefficients réels, on trouve que pour $k \in \mathbb{N}$:

$$P^{(k)}(\overline{\alpha}) = \overline{P^{(k)}(\alpha)} \begin{cases} = & 0 \quad \text{si } k < m-1 \\ \neq & 0 \quad \text{si } k = m \end{cases}.$$

ce qui assure le premier résultat.
Comme $\alpha, \overline{\alpha}$ sont racines de multiplicité m, avec $\alpha \neq \overline{\alpha}$, alors P est divisible (sur $\mathbb{C}$ donc sur $\mathbb{R}$) par : $(X-\alpha)^m(X-\overline{\alpha})^m$. Le résultat découle alors de :

$$(X-\alpha)(X-\overline{\alpha}) = X^2 - 2(\alpha+\overline{\alpha})X + \alpha\overline{\alpha} = X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|^2.$$

□

Corollaire III.57. *Si $P \in \mathbb{R}[X]$, notons $\lambda_1, \ldots \lambda_r$ ses racines réelles, de multiplicités $m_1, \ldots, m_r$, et $\mu_1, \overline{\mu_1}, \ldots, \mu_p, \overline{\mu_p}$ ses racines complexes non réelles, de multiplicités $n_1, \ldots, n_p$. Alors :*

$$P = \alpha \prod_{k=1}^{r} (X - \lambda_k)^{m_k} \prod_{l=1}^{p} (X^2 - 2\mathrm{Re}(\mu_l)X + |\mu_l|^2)^{n_l}.$$

Démonstration. Découle de l'écriture de P comme polynôme scindé sur $\mathbb{C}$. □

Exemple III.58. *Soit $n \in \mathbb{N}^*$. Étudions le polynôme $P = X^n - 1$.*
Pour $z \in \mathbb{C}$, on a :

$$P(z) = 0 \Leftrightarrow z^n = 1 \Leftrightarrow z \in \mathbb{U}_n$$

donc les racines de P (dans $\mathbb{C}$) sont tous les éléments de $\mathbb{U}_n$.
Toutes ces racines sont simples : il y en a $n = \deg(P)$ (on peut aussi voir qu'aucune n'est racine de $P' = nX^{n-1}$).
Et comme P est unitaire, alors :

$$P = \prod_{k=1}^{n} \left(X - e^{\frac{2ik\pi}{n}}\right).$$

Les racines réelles de P sont 1 si n est impair, et 1 et -1 si n est pair. En regroupant $(X - e^{\frac{2ik\pi}{n}})$ avec $(X - e^{\frac{2i(n-k)\pi}{n}})$ pour $k \neq n, \frac{n}{2}$, on trouve la factorisation de P sur $\mathbb{R}[X]$:

$$P = \begin{cases} (X-1)\prod_{k=1}^{\frac{n-1}{2}} \left(X^2 - 2\cos\left(\frac{2k\pi}{n}\right)X + 1\right) & \text{si } n \text{ est impair} \\ (X-1)(X+1)\prod_{k=1}^{\frac{n}{2}-1} \left(X^2 - 2\cos\left(\frac{2k\pi}{n}\right)X + 1\right) & \text{si } n \text{ est pair} \end{cases}.$$

Et grâce aux relations coefficients-racines, on trouve :

$$\sigma_1 = \sum_{k=1}^{n} e^{\frac{2ik\pi}{n}} = 0 = \sigma_2 = \sum_{1 \leq k < l \leq n} e^{\frac{2i(k+l)\pi}{n}} = 0 = \ldots$$

et $\sigma_n = \prod_{k=1}^{n} e^{\frac{2ik\pi}{n}} = \prod_{z \in \mathbb{U}_n} z = (-1)^{n+1}$.

IV Arithmétique des polynômes

Les résultats qui suivent, sauf mention contraire, sont applicables à n'importe quel corps $\mathbb{K}$ ($\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}/p\mathbb{Z}$, etc.).

IV.1 PGCD et algorithme d'Euclide

Proposition-Définition IV.1. *Si $A, B \in \mathbb{K}[X]$ ne sont pas tous les deux nuls, on appelle **plus grand commun diviseur (PGCD)** de A et B tout polynôme qui divise A et B et qui est de degré maximal parmi les diviseurs communs de A et B.*
Si A et B sont nuls, on pose par convention que le polynôme nul est leur seul PGCD.

Démonstration. Par exemple, supposons que A est non nul. Alors l'ensemble $E = \{\deg(Q) \mid Q \in \mathbb{K}[X],\ Q \neq 0,\ Q|A,\ Q|B\}$ est un sous-ensemble non vide (il contient 1) et majoré (par $\deg(A)$) de $\mathbb{N}$ donc admet un plus grand élément. Ce qui justifie l'existence d'un diviseur de degré maximal. □

Remarque IV.2. *On n'a pas unicité du PGCD : plus précisément, si P est un PGCD de A et B, et $\lambda \in \mathbb{K}^*$, alors λP est aussi un PGCD de A et B comme le degré et la divisibilité sont conservés en multipliant par un scalaire.*

Exemple IV.3. *Traitons le cas où $B = 0$: les PGCD de A et 0 sont alors tous les polynômes associés à A. Comme tous les polynômes divisent 0, alors les diviseurs communs à A et 0 sont exactement les diviseurs de A. Et le plus grand degré pour un diviseur de A est $\deg(A)$ (réalisé pour A par exemple).*
Et si P divise A avec $\deg(P) = \deg(A)$, alors le degré du quotient est nul, donc P est associé à A. Ce qui montre le résultat.

Proposition IV.4. *Si $A, B, D \in \mathbb{K}[X]$ avec $B \neq 0$. Notons R le reste de la division euclidienne de A par B. Alors D est un diviseur de A et B si, et seulement si, c'est un diviseur de R et B.*

Démonstration. Si D divise A et B, alors il divise $R = A - QB$. Donc il divise R et B.
Réciproquement, si D divise B et R, alors il divise $A = BQ + R$. Donc il divise A et B. □

Corollaire IV.5. *Avec les mêmes notations, les PGCD de A et B sont ceux de B et R.*

Théorème IV.6 (Algorithme d'Euclide)**.** *Si $A, B \in \mathbb{K}[X]$ avec $\deg(Q) \geq \deg(B)$, on construit une suite finie de polynôme $R_1, \ldots, R_n$ suivant **l'algorithme d'Euclide** :*

1. *on pose R_1 le reste de la division euclidienne de A par B ;*
2. *si $R_1 \neq 0$, on pose pose R_2 le reste de la division euclidienne de B par R_1 ;*
3. *on continue en posant R_{k+1} le reste de la division euclidienne de R_{k-1} par R_k, tant que R_k est non nul.*

La suite des R_k est telle que la suite des degrés associée est une suite strictement décroissante d'entiers (ce qui assure bien que l'un des R_k est nul et que l'on s'arrête).
*Les diviseurs de A et B, de B et R_1, de R_1 et R_2 et ainsi de suite jusqu'à R_{n-1} et $R_n = 0$ sont les mêmes. Donc les PGCD de A et B sont les polynômes associés au **dernier reste non nul** dans l'algorithme d'Euclide.*

Proposition-Définition IV.7. *Si $A, B \in \mathbb{K}[X]$ ne sont pas tous les deux nuls, leurs PGCD sont associés deux-à-deux. En particulier, il en existe un unique qui est unitaire : on l'appelle **le PGCD unitaire** de A et B, et on le note $A \wedge B$.*
Par convention, on note $0 \wedge 0 = 0$.

Démonstration. Découle du résultat précédent. □

Corollaire IV.8. *Si $A, B \in \mathbb{K}[X]$, alors les diviseurs communs de A et B sont exactement les diviseurs de $A \wedge B$.*
Ainsi, les PGCD de A et B sont les plus grands diviseurs commun de A et B ***au sens de la divisibilité****, c'est-à-dire qu'un polynôme $D \in \mathbb{K}[X]$ est un PGCD de A et B si, et seulement si :*

$$\forall P \in \mathbb{K}[X],\ (P|A \text{ et } P|B) \Leftrightarrow P|D.$$

Démonstration. Si $A = B = 0$, alors 0 est le seul PGCD de A et B. Les résultats découlent alors du fait que 0 est divisible par tout polynôme, et que c'est le seul élément de $\mathbb{K}[X]$ vérifiant cette propriété.
Si A ou B est non nul : suivant les notations de l'algorithme d'Euclide, les diviseurs communs de A et B sont exactement les diviseurs de R_{n-1}, et donc de tous les polynômes qui lui sont associés, ce qui donne le premier résultat. Ceci montre que tout PGCD de A et B vérifie l'équivalence.
Inversement, si D vérifie l'équivalence précédente, alors il doit aussi la satisfaire :
— pour $P = A \wedge B$: alors $P|A$ et $P|B$ donc $P|D$, c'est-à-dire que $A \wedge B|D$;
— pour $P = D$: alors $P|A$ et $P|B$, donc $P|A \wedge B$ par le point précédent, c'est-à-dire que $D|A \wedge B$.
donc D est associé à $A \wedge B$ et est un PGCD de A et B. □

Théorème IV.9 (Identité de Bézout)**.** *Si $A, B \in \mathbb{K}[X]$, il existe $U, V \in \mathbb{K}[X]$ tels que : $A \wedge B = AU + BV$.*

Démonstration. Se fait comme pour l'identité de Bézout pour les entiers : soit par récurrence sur $\deg(B)$, soit par remontée dans l'algorithme d'Euclide (et on parle encore d'algorithme d'Euclide étendu) □

Corollaire IV.10. *Si $A, B \in \mathbb{K}[X]$ avec A ou B non nul, alors $A \wedge B$ est le polynôme unitaire de plus petit degré de la forme $AU + BV$ pour $U, V \in \mathbb{K}[X]$.*

Exemple IV.11. *Prenons $A = X^3 - 6X^2 + 11X - 6$ et $B = X^2 - X - 2$.*
On pourrait calculer le reste de la division euclidienne en évaluant A en les racines de B, mais on a besoin des quotients pour satisfaire l'identité de Bézout. On a :

$$\begin{array}{rrrr|l} X^3 & -6X^2 & +11X & -6 & X^2 \quad -X \quad -2 \\ \cline{5-5} -X^3 & +X^2 & +2X & & X \quad -5 \\ \cline{1-3} & -5X^2 & +13X & -6 & \\ & 5X^2 & -5X & -10 & \\ \cline{2-4} & & 8X & -16 & \end{array}$$

Donc $R_1 = 8X - 16$. Pour simplifier les calcule, on continue l'algorithme d'Euclide avec $\frac{1}{8}R_1 = X - 2$:

$$\begin{array}{rrr|l} X^2 & -X & -2 & X \quad -2 \\ \cline{4-4} -X^2 & +2X & & X \quad +1 \\ \cline{1-2} & X & -2 & \\ & -X & +2 & \\ \cline{2-3} & & 0 & \end{array}$$

Et donc $A \wedge B = X - 2$. Et :

$$X - 2 = \frac{1}{8}(8X - 16) = \frac{1}{8}\left((X^3 - 6X^2 + 11X - 6) - (X^2 - X - 2) \cdot (X - 5)\right) = \underbrace{\frac{1}{8}}_{=U} \cdot A + \underbrace{\left(-\frac{1}{8}X + \frac{5}{8}\right)}_{=V} \cdot B$$

Corollaire IV.12. *Si $A, B, C \in \mathbb{K}[X]$, alors :*

1. *$A \wedge (B \wedge C) = (A \wedge B) \wedge C$ (associativité du PGCD) ;*
2. *$(AC) \wedge (BC) = C(A \wedge B)$.*

Démonstration. On utilise l'équivalence précédente. □

IV.2 Polynômes premiers entre eux

Définition IV.13. *Deux polynômes $A, B \in \mathbb{K}[X]$ sont dits* ***premiers entre eux*** *si $A \wedge B = 1$ (ce qui revient à dire que tous leurs PGCD sont constants).*

Théorème IV.14 (de Bézout)**.** *Deux polynômes $A, B \in \mathbb{K}[X]$ sont premiers entre eux si, et seulement si, il existe $U, V \in \mathbb{K}[X]$ tels que : $AU + BV = 1$.*

Démonstration.
- si $A \wedge B = 1$: on utilise l'identité de Bézout ;
- si $AU + BV = 1$ pour $U, V \in \mathbb{K}[X]$: soit $D \in \mathbb{K}[X]$ un diviseur de A et B. Alors D divise $AU + BV = 1$, donc D est constant.

□

Corollaire IV.15. *Si $A, B_1, \ldots, B_n \in \mathbb{K}[X]$, alors A est premier avec le produit $B_1 \ldots B_n$ si, et seulement si, il est premier avec chacun des B_i.*

Démonstration. Prouvons le par récurrence sur $n \in \mathbb{N}^*$:
- si $n = 1$: c'est la définition ;
- si $n = 2$:
  - si $A \wedge B_1 B_2 = 1$: alors $AU + B_1 B_2 V = 1$, donc : $AU = B_1(B_2 V) = AU + B_2(B_1 V) = 1$ donc A est premier avec B_1 et avec B_2 ;
  - si $A \wedge B_1 = A \wedge B_2 = 1$: alors $AU_1 + B_1 V_1 = AU_2 + B_2 V_2 = 1$ pour $U_1, U_2, V_1, V_2 \in \mathbb{K}[X]$. Et donc :

$$1 = (AU_1 + B_1 V_1) \cdot (AU_2 + B_2 V_2) = A(AU_1 U_2 + U_1 B_2 V_2 + U_2 B_1 V_1) + (B_1 B_2)(V_1 V_2)$$

    donc A est premier avec $B_1 B_2$;
- hérédité : si A est premier avec $B_1, \ldots, B_n, B_{n+1}$, alors il est premier avec $B_1 \ldots B_n$ et B_{n+1}, donc avec leur produit ; réciproquement si A est premier avec $B_1 \ldots B_n B_{n+1}$, alors il l'est avec $B_1 \ldots B_n$ et avec B_{n+1}, donc avec chacun des B_i.

□

Proposition IV.16 (Lemme de Gauss)**.** *Si $A, B, C \in \mathbb{K}[X]$ tel que A divise BC et A est premier avec B, alors A divise C.*

Démonstration. Comme A et B sont premiers entre eux, il existe U, V tels que : $AU + BV = 1$. Et donc $AUC + BCV = C$.
Comme A divise AUC et BVC, alors A divise C. □

IV.3 PPCM

Proposition-Définition IV.17. *Si $A, B \in \mathbb{K}[X]$ non nuls, on appelle* ***plus petit commun multiple (PPCM)*** *de A et B tout multiple non nul de A et B de degré minimal parmi les multiples non nuls de A et B.*
Si A ou B est nul, on pose par convention que le polynôme nul est leur seul PPCM.

Démonstration. Si A et B sont non nuls, alors l'ensemble $E = \{\deg(Q) \,|\, Q \in \mathbb{K}[X],\ Q \neq 0,\ A|Q,\ B|Q\}$ est un sous-ensemble non vide (il contient AB) de $\mathbb{N}$ donc admet un plus petit élément. Ce qui justifie l'existence d'un multiple de degré minimal. □

Proposition-Définition IV.18. *Si $A, B \in \mathbb{K}[X]$ sont non nuls, leurs PPCM sont associés deux-à-deux. En particulier, il en existe un unique qui est unitaire : on l'appelle* ***le PPCM unitaire*** *de A et B, et on le note $A \vee B$.*
Par convention, on note $A \vee B = 0$ dès que A ou B est nul.

Démonstration. Soient M_1, M_2 deux PPCM de A et B.
Notons $M_1 = M_2Q + R$ la division euclidienne de M_1 par M_2. Alors : $R = M_1 - QM_2$ est un multiple de A et B de degré strictement inférieur à $\deg(M_2) = \deg(M_1)$. Par minimalité du degré du PPCM, on déduit que $R = 0$.
Donc $M_2|M_1$.
Par symétrie, on trouve que $M_1|M_2$, donc M_1 et M_2 sont associés.
Le reste est évident. □

Corollaire IV.19. *Si $A, B \in \mathbb{K}[X]$, alors les multiples communs de A et B sont exactement les multiples de $A \vee B$.*
Ainsi, les PPCM de A et B sont les plus petits multiples communs de A et B ***au sens de la divisibilité****, c'est-à-dire qu'un polynôme $M \in \mathbb{K}[X]$ est un PPCM de A et B si, et seulement si :*

$$\forall P \in \mathbb{K}[X],\ (A|P \text{ et } B|P) \Leftrightarrow M|P.$$

Démonstration. Si A ou B est nul, alors le résultat est immédiat comme 0 est le seul multiple de 0, et que tout polynôme non nul possède un multiple non nul.
Si A et B sont non nuls : posons $M = A \vee B$, et considérons N un multiple de A et B. On écrit $N = MQ + R$ la division euclidienne de N par M. Alors $R = N - MQ$ est aussi un multiple de A et B, qui vérifie $\deg(R) < \deg(M)$. Donc $R = 0$ par minimalité de M. Donc M divise N. Et tout PPCM de A et B est associé à M donc divise aussi N.
Inversement, si N vérifie l'équivalence précédente, alors il doit aussi la satisfaire :
— pour $P = M$: alors $A|P$ et $B|P$, donc $N|P$, c'est-à-dire $N|M$;
— pour $P = N$: alors $N|P$ donc $A|P$ et $B|P$, donc $M|P$ par le point précédent, c'est-à-dire que $M|N$;
donc N et M sont associés, et N est un PPCM de A et B. □

Proposition IV.20. *Si $A, B \in \mathbb{K}[X]$ sont* ***unitaires****, alors :*

$$AB = (A \wedge B)(A \vee B).$$

IV.4 PGCD d'un nombre fini de polynômes

Définition IV.21. *Si $A_1, \dots, A_n \in \mathbb{K}[X]$, on appelle PGCD de $A_1, \dots, A_n$ tout polynôme qui divise chacun des A_i de degré maximal.*
Un tel polynôme, s'il est unitaire, sera noté $A_1 \wedge \cdots \wedge A_n$ ou $\bigwedge_{i=1}^{n} A_i$.

Proposition IV.22. *Avec les mêmes notations, on a :*

$$\bigwedge_{i=1}^{n} A_i = (\dots((A_1 \wedge A_2) \wedge A_3) \cdots \wedge A_{n-1}) \wedge A_n.$$

Démonstration. Par récurrence, en utilisant le fait que : les diviseurs de A et B sont exactement les diviseurs de $A \wedge B$, donc les diviseurs de A, B, C sont les diviseurs de $A \wedge B$ et C. Et en prenant le diviseur de degré maximal on a bien le résultat. □

Proposition IV.23. *Si $A_1, \dots, A_n \in \mathbb{K}[X]$, alors il existe $U_1, \dots, U_n \in \mathbb{K}[X]$ tels que :*

$$\bigwedge_{i=1}^{n} A_i = \sum_{i=1}^{n} A_i U_i.$$

Démonstration. Par récurrence, avec l'identité de Bézout, comme pour les entiers. □

Définition IV.24. *Des polynômes $A_1, \dots, A_n \in \mathbb{K}[X]$ sont dits* ***premiers entre eux dans leur ensemble*** *si $\bigwedge_{i=1}^n A_i = 1$.*
On dit qu'ils sont ***deux-à-deux premiers entre eux*** *si, pour tous $i \neq j$, A_i est premier avec A_j.*

Proposition IV.25. *Les polynômes $A_1, \dots, A_n \in \mathbb{K}[X]$ sont premiers entre eux dans leur ensemble si, et seulement si, il existe $U_1, \dots, U_n \in \mathbb{K}[X]$ tels que : $\sum_{i=1}^n A_i U_i = 1$.*

Démonstration. Comme pour les entiers. □

Corollaire IV.26. *Des polynômes $A_1, \dots, A_n \in \mathbb{C}[x]$ sont premiers entre eux dans leur ensemble si, et seulement si, ils n'ont pas de racine commune.*

Démonstration. Supposons que $A_1, \dots, A_n$ soient premier entre eux. Par l'absurde, supposons que $A_1(\lambda) = \cdots = A_n(\lambda) = 0$ pour $\lambda \in \mathbb{C}$. Notons $U_1, \dots, U_n$ tels que $\sum_{i=1}^n A_i U_i = 1$. Alors en évaluant en λ on trouve : $0 = 1$, d'où la contradiction.
Inversement, si $A_1, \dots, A_n$ ne sont pas premiers entre eux, notons $D = \bigwedge_{i=1}^n A_i$, qui vérifie $\deg(D) \geq 1$. Et par théorème de d'Alembert–Gauss, D possède une racine $\lambda \in \mathbb{C}$, qui est donc une racine de chacun des A_i. □

IV.5 Polynômes irréductibles

Définition IV.27. *Un polynôme $P \in \mathbb{K}[X]$ non constant est dit* ***irréductible*** *si :*

$$\forall A, B \in \mathbb{K}[X],\ P = AB \Rightarrow (\deg(A) = 0 \text{ ou } \deg(B) = 0)\,.$$

Proposition IV.28 (Lemme d'Euclide)**.** *Un polynôme irréductible divise un produit si, et seulement si, il divise l'un des facteurs.*

Démonstration. On procède comme sur $\mathbb{Z}$ en constatant que, pour $P, A \in \mathbb{K}[X]$ avec P irréductible : P divise A si, et seulement si, P est A ne sont pas premiers entre eux. □

Proposition IV.29. *Tout polynôme non constant de $\mathbb{K}[X]$ s'écrit comme produit de polynômes irréductibles.*

Démonstration. Par récurrence forte sur $\deg(P) = n \in \mathbb{N}^*$:
- si $n = 1$: alors P est irréductible, car si $P = AB$ alors A ou B est constant ;
- supposons que tout polynôme non constant de $\mathbb{K}_{n-1}[X]$ s'écrit comme produit d'irréductibles pour $n \in \mathbb{N}^*$:
  - si P est irréductible : alors $P = P$;
  - sinon, on écrit $P = AB$ avec $\deg(A), \deg(B) > 0$; comme $\deg(A) + \deg(B) = n$, on a donc $A, B \in \mathbb{K}_{n-1}[X]$. Par hypothèse de récurrence, A et B s'écrivent comme produit d'irréductibles, donc $P = AB$ aussi.

  D'où l'hérédité.

D'où la récurrence. □

Remarque IV.30. *Dans la preuve apparaît un résultat important : tout polynôme de degré 1 est irréductible, et ce peu importe le corps $\mathbb{K}$ considéré.*

Théorème IV.31. *Si $A \in \mathbb{K}[X]$ non constant, alors il existe $\alpha \in \mathbb{K}^*$, des polynômes irréductibles* ***unitaires*** *deux-à-deux distincts $P_1, \dots, P_r$ et des entiers strictement positifs $m_1, \dots, m_r$ tels que :*

$$A = \alpha \prod_{i=1}^{r} P_i^{m_i}.$$

De plus cette décomposition est unique à l'ordre près des facteurs.

Démonstration. L'existence découle du résultat précédent.
L'unicité se déduit du lemme de Gauss en constatant que, pour P, Q irréductibles, alors $P|Q$ si, et seulement si P et Q sont associés. □

Théorème IV.32 (Décomposition en produit d'irréductibles sur $\mathbb{C}[X]$)**.** *Sur $\mathbb{C}[X]$:*

1. *les polynômes irréductibles sont exactement les polynômes de degré 1 ;*
2. *si P est non constant, sa factorisation en produit de facteurs irréductibles est :*

$$P = \alpha \prod_{k=1}^{r} (X - \lambda_k)^{m_k}$$

où α est le coefficient dominant de P, et les λ_k sont les racines distinctes de P, de multiplicité m_k.

Démonstration.

1. Il est clair que les polynômes de degré 1 sont irréductibles (par la remarque précédente).
   Réciproquement, si P est irréductible : il possède une racine $\lambda \in \mathbb{C}$, donc est divisible par $(X - \lambda)$, donc il existe $\alpha \in \mathbb{C}^*$ tel que $P = \alpha(X - \lambda)$ et $\deg(P) = 1$.
2. Si P est non constant, il est bien de la forme donnée. Et par le point précédent il s'agit bien de l'écriture en produit d'irréductibles.

□

Théorème IV.33 (Décomposition en produit d'irréductibles sur $\mathbb{R}[X]$)**.** *Sur $\mathbb{R}[X]$:*

1. *les polynômes irréductibles sont exactement les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle ;*
2. *si P est non constant, sa factorisation en produit de facteurs irréductibles est :*

$$P = \alpha \prod_{i=1}^{r} (X - \lambda_i)^{m_i} \prod_{j=1}^{p} \left((X^2 - 2\mathrm{Re}(\mu_j)X + |\mu_j|^2 \right)^{n_j}$$

*où α est le coefficient dominant de P, et les λ_i sont les racines **réelles** distinctes de P, de multiplicité m_i, et les $\mu_j, \overline{\mu_j}$ sont les racines complexes non réelles de P, de multiplicités n_j.*

Démonstration.

1. Il est à nouveau clair que les polynômes de degré 1 sont irréductibles. Pour les polynômes de degré 2, si un tel polynôme ne possède pas de racine réelle alors il n'est divisible par aucun polynôme de degré 1, donc il est aussi irréductible.
   Réciproquement, si $P \in \mathbb{R}[X]$ est un polynôme irréductible. Notons λ une racine complexe de P. Alors :
   — si $\lambda \in \mathbb{R}$: alors P est divisible par $(X - \lambda)$, donc est de la forme $\alpha(X - \lambda)$, donc de degré 1 ;
   — si $\lambda \notin \mathbb{R}$: alors $\overline{\lambda}$ est aussi racine de P, donc P est divisible (dans $\mathbb{C}[X]$ donc dans $\mathbb{R}[X]$) par : $(X - \lambda)(X - \overline{\lambda}) = X^2 - 2\mathrm{Re}(\lambda)X + |\lambda|^2$. Comme P est irréductible, il est de la forme $\alpha(X^2 - 2\mathrm{Re}(\lambda)X + |\lambda|^2)$, qui est bien un polynôme de degré 2 sans racine réelle.
2. Si P est non constant, il est bien de la forme donnée. Et par le point précédent il s'agit bien de l'écriture en produit d'irréductibles.

□

Remarque IV.34. *On a en fait un résultat légèrement plus fort que celui explicité ci-dessus pour les polynômes de degré 2, à savoir qu'un polynôme de degré 2 ou 3 est irréductible si, et seulement si, il n'a pas de racine (car s'il est non irréductible il a nécessairement un diviseur de degré 1).*
En revanche, selon les corps considérés, il existe des polynômes irréductible de degré arbitrairement grand. On peut voir par exemple que, pour p premier, le polynôme $1 + X + \cdots + X^{p-1}$ est irréductible sur $\mathbb{Q}[X]$.

V Fractions rationnelles

V.1 Le corps $K(X)$

Proposition-Définition V.1. *On définit sur $\mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$ la relation binaire $\sim$ définie par :*

$$(P_1, Q_1) \sim (P_2, Q_2) \Leftrightarrow P_1Q_2 = P_2Q_1.$$

Alors $\sim$ est une relation d'équivalence.
*L'ensemble $\mathbb{K}(X)$ des **fractions rationnelles sur** $\mathbb{K}$ est l'ensemble des classes d'équivalences pour la relation $\sim$.*

Démonstration. On vérifie les propriétés de $\sim$:
- réflexivité : si $(P, Q) \in \mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$, alors $PQ = PQ$ donc $(P, Q) \sim (P, Q)$;
- symétrie : si $(P_1, Q_1), (P_2, Q_2) \in \mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$, alors : $(P_1, Q_1) \sim (P_2, Q_2) \Leftrightarrow P_1Q_2 = P_2Q_1 \Leftrightarrow P_2Q_1 = P_1Q_2 \Leftrightarrow (P_2, Q_2) \sim (P_1, Q_1)$;
- transitivité : si $(P_1, Q_1), (P_2, Q_2), (P_3, Q_3) \in \mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$, avec $(P_1, Q_1) \sim (P_2, Q_2)$ et $(P_2, Q_2) \sim (P_3, Q_3)$, alors : $P_1Q_2 = P_2Q_1$ et $P_2Q_3 = P_3Q_2$. Et donc :
  - si $P_2 = 0$: alors $P_1 = P_3 = 0$, donc $P_1Q_3 = 0 = Q_1P_3$, donc $(P_1, Q_1) \sim (P_3, Q_3)$;
  - si $P_2 \neq 0$: alors $P_2Q_2 = 0$, et comme $P_1P_2Q_2Q_3 = P_2P_3Q_1Q_2$ alors $P_1Q_3 = P_3Q_1$, donc $(P_1, Q_1) \sim (P_3, Q_3)$.

Donc $\sim$ est bien une relation d'équivalence. □

Remarque V.2. *On notera plutôt $\dfrac{P}{Q}$ au lien de (P, Q) pour noter un élément de $\mathbb{K}(X)$. Inversement, on dira que (P, Q) est un **représentant** de la fraction $\dfrac{P}{Q}$.*

Les règles de calculs usuelles sur les fractions s'appliquent alors, car on a : $\dfrac{P_1}{Q_1} = \dfrac{P_2}{Q_2} \Leftrightarrow P_1Q_2 = P_2Q_1$.

Remarque V.3. *On pourrait construire $\mathbb{Q}$ de la même manière : ce serait l'ensemble des classes d'équivalences pour la relation $\sim$ définie sur $\mathbb{Z} \times \mathbb{Z}^*$ par :*

$$(p_1, q_1) \sim (p_2, q_2) \Leftrightarrow p_1q_2 = p_2q_1$$

ce qui correspond bien au fait que : $\dfrac{p_1}{q_1} = \dfrac{p_2}{q_2} \Leftrightarrow p_1q_2 = p_2q_1$.

Proposition-Définition V.4. *Tout élément $F \in \mathbb{K}(X)$ s'écrit sous la forme $F = \dfrac{P}{Q}$ avec $P \wedge Q = 1$. On dit alors que (P, Q) est un **représentant irréductible** de F, ou que $\dfrac{P}{Q}$ est irréductible.*

Démonstration. Posons $F = \dfrac{A}{B}$, et notons $D = A \wedge B$. Alors $A = DP$ et $B = DQ$ avec $P \wedge Q = 1$, et : $F = \dfrac{A}{B} = \dfrac{P}{Q}$, puisque $AQ = DPQ = PB$. □

Remarque V.5. *Une telle écriture n'est pas unique : si $\dfrac{A}{B}$ est irréductible, tous les autres représentants irréductibles sont les $\dfrac{\lambda A}{\lambda B}$, pour $\lambda \in \mathbb{K}^*$.*

Proposition-Définition V.6. *On muni $\mathbb{K}(X)$ des opérations $+$ et $\times$ définies par :*

$$\frac{P_1}{Q_1} + \frac{P_2}{Q_2} = \frac{P_1Q_2 + P_2Q_1}{Q_1Q_2} \text{ et } \frac{P_1}{Q_1} \times \frac{P_2}{Q_2} = \frac{P_1P_2}{Q_1Q_2}.$$

Muni de ces opérations, $(\mathbb{K}(X), +, \times)$ *est un corps (commutatif). Son élément neutre pour l'addition est* $0 = \dfrac{0}{1} = (0,1)$ *et celui pour la multiplication est* $1 = \dfrac{1}{1} = (1,1)$.
L'opposé de $F = \dfrac{A}{B}$ *est* $\dfrac{-A}{B}$, *tandis que son inverse est* $\dfrac{B}{A}$ *(pour* $A \neq 0$*).*

Démonstration. Il n'est pas compliqué, mais un peu long, de vérifier que $(\mathbb{K}(X), +, \times)$ est un anneau.
Le reste est immédiat par définition des opérations. □

Remarque V.7. *Les opérations ci-dessus correspondent en fait à l'addition et la multiplication de* $\mathbb{K}[X]$, *en confondant* $P \in \mathbb{K}[X]$ *avec* $\dfrac{P}{1} \in \mathbb{K}(X)$. *Ce qui fait de* $\mathbb{K}[X]$ *un sous-anneau de* $\mathbb{K}(X)$.
Plus précisément, on peut plonger $\mathbb{K}[X]$ *dans* $\mathbb{K}(X)$ *par le morphisme d'anneau injectif suivant :*

$$\varphi : \begin{cases} \mathbb{K}[X] & \to & \mathbb{K}(X) \\ P & \mapsto & \dfrac{P}{1} \end{cases}$$

Remarque V.8. *On pourrait généraliser cette construction à n'importe quel anneau* A ***intègre*** *: cela nous fournit un corps, appelé* ***corps des fractions*** *de* A, *qui est le plus petit corps contenant* A *comme sous-anneau.*

V.2 Degré, partie entières, zéros et pôles

Proposition-Définition V.9. *Si* $F \in \mathbb{K}(X)$, *alors la quantité* $\deg(A) - \deg(B)$ *ne dépend pas du représentant* $\frac{A}{B}$ *de* F.
On l'appelle le ***degré*** *de* F, *que l'on note* $\deg(F)$, *qui est un entier relatif si* $F \neq 0$ *et qui vaut* $-\infty$ *si* $F = 0$.

Démonstration. Si $\frac{A}{B}, \frac{C}{D}$ sont deux représentants de F, alors : $AD = BC$. Et donc : $\deg(A) + \deg(D) = \deg(B) + \deg(C)$, ce qui donne bien que $\deg(A) - \deg(B) = \deg(C) - \deg(D)$.
Le reste découle des valeurs possibles du degré d'un polynôme. □

Exemples V.10.

1. $\deg\left(\dfrac{X-1}{X^3+3}\right) = 1 - 3 = -2$;
2. $\deg\left(\dfrac{X^2+12}{X-7}\right) = 2 - 1 = 1$;
3. *si* $P \in \mathbb{K}[X]$ *:* $\deg(\frac{P}{1}) = \deg(P) - 0 = \deg(P)$.

Proposition V.11. *Si* $F, G \in \mathbb{K}(X)$, *alors :*

$$\deg(F+G) \leq \max(\deg(F), \deg(G)) \text{ et } \deg(FG) = \deg(F) + \deg(G).$$

Démonstration. Découle des propriétés du degré sur $\mathbb{K}[X]$ et de la définition des opérations de $\mathbb{K}(X)$. □

Définition V.12. *Soit* $F = \frac{A}{B}$ *une fraction rationnelle* ***sous forme irréductible****.*
On appelle ***zéro*** *de* F *toute racine de* A, *et* ***pôle*** *de* F *toute racine de* B.
On appelle ***ordre*** *(ou multiplicité) d'un zéro (resp. d'un pôle) de* F *sa multiplicité en tant que racine de* A *(resp. de* B*).*

Exemple V.13. *Considérons la fraction rationnelle* $F = \dfrac{X^3+3X^2}{X^3+3X^2-X-3}$. *Alors :*

$$F = \frac{X^2(X+3)}{(X^2-1)(X+3)} = \frac{X^2}{X^2-1}$$

et cette dernière écriture est irréductible.
Donc 0 *est un zéro double de* F, *et* 1 *et* -1 *sont ses pôles, qui sont simples.*

Définition V.14. *Si $F = \frac{A}{B}$ est une fraction rationnelle irréductible, on lui associe la* ***fonction rationnelle****, notée $\widetilde{F}$, comme la fonction définie sur $\mathbb{K}$ privé des pôles de F, par : $\widetilde{F} : x \mapsto \frac{A(x)}{B(x)}$.*

Remarque V.15. *L'intérêt de travailler avec une forme irréductible est que l'on définit $\widetilde{F}$ sur l'ensemble le plus grand possible. Avec une écriture non irréductible, les pôles qui apparaîtraient en plus serait des pôles* ***effaçables*** *: on pourrait prolonger $\widetilde{F}$ en ces points par continuité, et le prolongement obtenu serait même de classe $\mathcal{C}^\infty$.*

Proposition-Définition V.16. *Si $F \in \mathbb{K}(X)$, il existe un unique couple $(E, Q) \in \mathbb{K}[X] \times \mathbb{K}(X)$ avec $\deg(Q) < 0$ et $F = E + Q$.*
Le polynôme E est appelé la ***partie entière de*** *F.*

Démonstration. Pour l'existence, notons $F = \frac{A}{B}$. Alors, si $A = BE + R$ est la division euclidienne de A par B, le couple $(E, \frac{R}{B})$ convient.
Pour l'unicité : si $F = E_1 + Q_1 = E_2 + Q_2$, alors $E_1 - E_2 = Q_2 - Q_1$. Et donc $\deg(E_1 - E_2) = \deg(Q_2 - Q_1) \leq \max(\deg(Q_2), \deg(Q_1)) < 0$. Donc $E_1 - E_2 = 0$ (comme $E_1, E_2 \in \mathbb{K}[X]$), c'est-à-dire $E_1 = E_2$. Et finalement $Q_1 = Q_2$. □

V.3 Décomposition en éléments simples

Définition V.17. *Une fraction rationnelle de la forme $\frac{P}{Q^k}$ pour Q irréductible, $k \in \mathbb{N}^*$ et $\deg(P) < \deg(Q)$ est appelée* ***élément simple****.*
*Plus précisément, on parle d'élément simple de p-****ème espèce de degré*** *k, où $p = \deg(Q)$.*

Théorème V.18 (Décomposition en éléments simples)**.** *Si $F = \dfrac{A}{B}$ est une fraction rationnelle, elle s'écrit de manière unique comme somme d'un polynôme et d'éléments simples.*
Plus précisément, si F est irréductible et que $B = \alpha B_1^{b_1} \dots B_r^{b_r}$ est son écriture en produit de facteurs irréductibles, alors il existe une unique famille de polynômes $E, A_{1,1}, \dots, A_{1,b_1}, \dots, A_{r,1}, \dots, A_{r,b_r}$ tels que :

$$\begin{aligned} F &= E + \frac{A_{1,1}}{B_1} + \dots + \frac{A_{1,b_1}}{B_1^{b_1}} + \dots + \frac{A_{r,1}}{B_r} + \dots + \frac{A_{r,b_r}}{B_r^{b_r}} \\ &= E + \sum_{i=1}^{r} \sum_{j=1}^{b_i} \frac{A_{i,j}}{B_i^j} \end{aligned}$$

où : $\forall i, j,\ \deg(A_{i,j}) < \deg(B_i)$.

Démonstration. Admis. □

Corollaire V.19 (Décomposition en éléments simples sur $\mathbb{C}(X)$)**.** *Si $F = \dfrac{A}{B} \in \mathbb{C}(X)$ est irréductible, avec $B = \alpha \prod_{k=1}^{r} (X - \lambda_k)^{m_k}$ comme produit d'irréductibles, alors il existe un unique polynôme $E \in \mathbb{C}[X]$ et des complexes $\alpha_{1,1}, \dots, \alpha_{1,m_1}, \dots, \alpha_{r,1}, \dots, \alpha_{r,m_r}$ uniques tels que :*

$$F = E + \sum_{i=1}^{r} \sum_{j=1}^{m_i} \frac{\alpha_{i,j}}{(X - \lambda_i)^j}.$$

Corollaire V.20 (Décomposition en éléments simples sur $\mathbb{R}(X)$)**.** *Si $F = \dfrac{A}{B} \in \mathbb{R}(X)$ est irréductible, avec $B = \alpha \prod_{k=1}^{r} (X - \lambda_k)^{m_k} \prod_{l=1}^{s} (X^2 + b_l X + c_l)^{n_l}$ comme produit d'irréductibles, alors il existe un unique polynôme $E \in \mathbb{R}[X]$ et des réels $\alpha_{1,1}, \dots, \alpha_{1,m_1}, \dots, \alpha_{r,1}, \dots, \alpha_{r,m_r}, \beta_{1,1}, \dots, \beta_{1,n_1}, \dots, \beta_{s,1}, \dots, \beta_{s,n_s}, \gamma_{1,1}, \dots, \gamma_{1,n_1}, \dots$ uniques tels que :*

$$F = E + \left(\sum_{i=1}^{r} \sum_{j=1}^{m_i} \frac{\alpha_{i,j}}{(X - \lambda_i)^j} \right) + \left(\sum_{i=1}^{s} \sum_{j=1}^{n_i} \frac{\beta_{i,j} X + \gamma_{i,j}}{(X^2 + b_i X + c_i)^j} \right).$$

Exemple V.21. *La décomposition en élément simples de* $\dfrac{1}{X(X+1)}$ *est* $\dfrac{1}{X}-\dfrac{1}{X+1}$.

Remarque V.22. *On peut juste utiliser l'existence pour trouver les coefficients par identification, ou par évaluation.*
L'unicité permet en plus d'exploiter les symétries (comme la parité).

Exemple V.23. *Décomposons la fraction rationnelle* $F(X)=\dfrac{1}{X^2-1}$. *Les pôles sont* 1 *et* -1, *et on obtient une décomposition en éléments simples de la forme :*

$$F(X)=\frac{1}{X^2-1}=\frac{a}{X-1}+\frac{b}{X+1}$$

mais la fraction F *est paire ce qui donne :*

$$F(-X)=\frac{a}{-X-1}+\frac{b}{-X+1}=\frac{-a}{X+1}+\frac{-b}{X-1}$$

donc par unicité de la décomposition : $a=-b$ *(et* $b=-a$*).*
Donc on est ramené à déterminer le coefficient associé à un pôle simple.

Proposition V.24. *Si* $\lambda\in\mathbb{K}$ *est un pôle simple de* $F=\frac{P}{Q}\in\mathbb{K}(X)$ *(sous forme irréductible), alors l'élément simple associé à* $X-\lambda$ *dans la décomposition de* F *est :*

$$\frac{P(\lambda)}{Q'(\lambda)}\cdot\frac{1}{X-\lambda}.$$

Démonstration. Comme λ est un pôle simple de F, alors $Q=(X-\lambda)Q_1$, avec $Q_1(\lambda)\neq 0$.
Si on regroupe tous les autres éléments simples de F en une seule fraction G, on peut écrire : $F=\dfrac{\alpha}{X-\lambda}+G$.
En multipliant par $(X-\lambda)$, on déduit : $\dfrac{P}{Q_1}=\alpha+(X-\lambda)G$. En évaluant en λ (qui a bien un sens, comme λ n'est pas un pôle de G ou de $\frac{P}{Q_1}$), on trouve : $\alpha=\dfrac{P(\lambda)}{Q_1(\lambda)}$.
Comme $Q'=[(X-\lambda)Q_1]'=(X-\lambda)Q_1'+Q_1$, alors $Q'(\lambda)=Q_1(\lambda)$, et on a bien le résultat. □

Proposition V.25. *Si* $P\in\mathbb{K}[X]$ *est scindé, avec* $P=\alpha\prod_{k=1}^{r}(X-\lambda_k)^{m_k}$ *(décomposition en produit d'irréductibles), alors on a la décomposition en éléments simples :*

$$\frac{P'}{P}=\sum_{k=1}^{r}\frac{m_k}{X-\lambda_k}.$$

Démonstration. Par dérivée d'un produit, on a :

$$P'=\alpha\sum_{k=1}^{r}((X-\lambda_k)^{m_k})'\cdot\left(\prod_{l\neq k}(X-\lambda_l)^{m_l}\right)=\alpha\sum_{k=1}^{r}m_k(X-\lambda_k)^{m_k-1}\cdot\left(\prod_{l\neq k}(X-\lambda_l)^{m_l}\right)$$

et donc :

$$\frac{P'}{P}=\sum_{k=1}^{r}\frac{m_k}{X-\lambda_k}.$$

□

Remarque V.26. *Implicitement on voit apparaître que* $\dfrac{P'}{P}$ *n'a que des pôles simples. On a en fait, comme tout racine de multiplicité* m *de* P *est racine de multiplicité* $m-1$ *de* P', *que les racines de* $P\wedge P'$ *sont exactement les racines de* P, *de multiplicités diminuées de* 1. *Ainsi, le polynôme* $\dfrac{P}{P\wedge P'}$ *a exactement les mêmes racines que* P, *qui sont toutes simples.*

Remarque V.27. *Ce résultat se retrouve avec les fonctions rationnelles. Avec les mêmes notations, pour* $x \neq \lambda_1, \dots, \lambda_r$ *:* $P(x) \neq 0$ *et donc* $\ln(|P(x)|)$ *est bien défini et vaut :* $\sum_{k=1}^{r} m_k \ln(|x-\lambda_k|)$.
La fonction $x \mapsto \ln(|P(x)|)$ *est dérivable sur son ensemble de définition, de dérivée en* x *:* $\sum_{k=1}^{r} \frac{m_k}{x-\lambda_k}$.
Et on a bien la formule par dérivée d'une composée, comme $\ln(|P|)' = \frac{P'}{P}$.

V.4 Primitives de fonctions rationnelles

Méthode V.28. *Soit* $f = \widetilde{F}$ *une fonction rationnelle, pour* $F \in \mathbb{R}(X)$. *On écrit la décomposition en éléments simples de* F *:*

$$F = E + \left(\sum_{i=1}^{r} \sum_{j=1}^{m_i} \frac{\alpha_{i,j}}{(X-\lambda_i)^j} \right) + \left(\sum_{i=1}^{p} \sum_{j=1}^{n_i} \frac{\beta_{i,j} X + \gamma_{i,j}}{(X^2 + b_i X + c_i)^j} \right)$$

dont on calcule les primitives terme à terme :

- *la partie entière se traite directement (par primitive d'un polynôme) ;*
- *les éléments simples de première espèces se traitent en notant que :*

$$\int^x \frac{\mathrm{d}t}{t-\lambda} = \ln(|x-\lambda|) \text{ et } \int^x \frac{\mathrm{d}t}{(t-\lambda)^n} = \frac{-1}{n-1} \frac{1}{(x-\lambda)^{n-1}} \ (si\ n \neq 1) \ ;$$

- *les éléments simples de deuxième espèces se traitent de la manière suivante :*
  - *pour le degré* 1 *:*
    - *on écrit :*
    $$\frac{\beta x + \gamma}{x^2 + bx + c} = \frac{\frac{\beta}{2}(2x+b)}{x^2+bx+c} + \frac{-\frac{\beta}{2}b + \gamma}{x^2+bx+c};$$
    - *le premier terme a pour primitive (à un facteur près) :* $\ln(|x^2+bx+c|)$ *;*
    - *on écrit* $x^2 + bx + c = (x + \frac{b}{2})^2 + \lambda^2$ *(forme canonique) ; une primitive du second terme est (à un facteur près) :* $\frac{1}{\lambda} \mathrm{Arctan}\left(\frac{x+\frac{b}{2}}{\lambda} \right)$ *;*
  - *pour le degré* r *:*
    - *on écrit de même :*
    $$\frac{\beta x + \gamma}{(x^2+bx+c)^r} = \frac{\frac{\beta}{2}(2x+b)}{(x^2+bx+c)^r} + \frac{-\frac{\beta}{2}b + \gamma}{(x^2+bx+c)^r};$$
    - *le premier terme a pour primitive (à un facteur près) :* $\frac{1}{1-r} \frac{1}{(x^2+bx+c)^{r-1}}$ *;*
    - *on procède par intégration par parties pour diminuer l'exposant du dénominateur et se ramener au cas* $r = 1$.

Remarque V.29. *On peut ne traiter que des pôles de première espèce, quitte à travailler dans les complexes. Il faudra alors bien prendre garde au fait que, pour* $a, b \in \mathbb{R}$ *:*

$$\int^x \frac{1}{t-(a+ib)} \mathrm{d}t = \frac{1}{2} \ln\left((x-a)^2 + b^2\right) + i \mathrm{Arctan}\left(\frac{x-a}{b} \right).$$

Chapitre 18

Dérivabilité

I Nombre dérivé et fonction dérivée

Les résultats de cette partie restent valable si l'on suppose que f est à valeurs dans $\mathbb{C}$ (au lieu de $\mathbb{R}$).

I.1 Dérivabilité en un point

Définition I.1. *Soient $f : I \to \mathbb{R}$ et $a \in I$. On définit le* ***taux d'accroissement de f en*** *a, noté τ_a ou $\tau_{a,f}$, comme la fonction :*

$$\tau_{a,f} : \left\{ \begin{array}{ccc} I \setminus \{a\} & \to & \mathbb{R} \\ x & \mapsto & \dfrac{f(x)-f(a)}{x-a} \end{array} \right.$$

On dit alors que f est ***dérivable en*** *a si $\lim\limits_{x\to a} \tau_{a,f}(x)$* ***existe****, et est* ***finie****.*
On note cette limite $f'(a)$, et on l'appelle le ***nombre dérivé de f en*** *a.*

Remarque I.2. *De manière équivalente, cela revient à dire que $\lim\limits_{h\to 0} \dfrac{f(a+h)-f(a)}{h}$ existe et est fini, ce qui peut faciliter les calculs.*

Définition I.3. *Avec les mêmes notations, on dit que f est* ***dérivable sur*** *I si f est dérivable en tout $a \in I$.*
On note alors f' (ou Df, ou $\dfrac{\mathrm{d}f}{\mathrm{d}x}$) la fonction $a \mapsto f'(a)$, qui est définie sur I, et qu'on appelle ***fonction dérivée de*** *f.*

Proposition I.4. *Si $f : I \to \mathbb{R}$ et $a \in I$ avec f dérivable en a, alors f est continue en a.*

Démonstration. On a pour $x \in I \setminus \{a\}$:

$$f(x) - f(a) = \underbrace{\frac{f(x)-f(a)}{x-a}}_{\substack{\to \\ x\to a}\ f'(a)} \cdot \underbrace{(x-a)}_{\substack{\to \\ x\to a}\ 0} \underset{x\to a}{\to} 0$$

ce qui donne bien la continuité en a. □

Remarque I.5. *On n'a pas une équivalence, puisqu'il existe des fonctions continues non dérivables (par exemple $x \mapsto |x|$ en 0).*

Proposition I.6. *Si $f : I \to \mathbb{R}$ et $a \in I$, alors f est dérivable en a si, et seulement si, il existe une fonction ε définie sur $I - a = \{x - a \,|\, x \in I\}$ et $l \in \mathbb{R}$ tels que :*

$$\forall x \in I,\ f(x) = f(a) + l \cdot (x-a) + (x-a) \cdot \varepsilon(x-a) \text{ et } \varepsilon(h) \underset{h\to 0}{\to} 0.$$

Et sous ces conditions on a $l = f'(a)$.

Démonstration. Notons déjà qu'une telle fonction ε, si elle existe, est définie par :

$$\varepsilon : \left\{ \begin{array}{ccc} I-a & \to & \mathbb{R} \\ h=(x-a) & \mapsto & \left\{ \begin{array}{lll} 0 & \text{si} & h=0 \text{ c'est-à-dire } x=a \\ \frac{f(x)-f(a)}{x-a}-l & \text{si} & h\neq 0 \text{ c'est-à-dire } x\neq a \end{array} \right. \end{array} \right.$$

pour un certain $l \in \mathbb{R}$ à déterminer. Reste à faire le lien entre limite de ε et dérivabilité de f en a :

- si ε tend vers 0 en 0 : alors $\lim\limits_{x\to a} \frac{f(x)-f(a)}{x-a} - l = 0$, donc $\lim\limits_{x\to a} \frac{f(x)-f(a)}{x-a} = l$, c'est-à-dire que f est dérivable en a avec $f'(a) = l$;
- si f est dérivable en a : alors $\lim\limits_{x\to a} \frac{f(x)-f(a)}{x-a} = f'(a)$, donc $l = f'(a)$ convient.

□

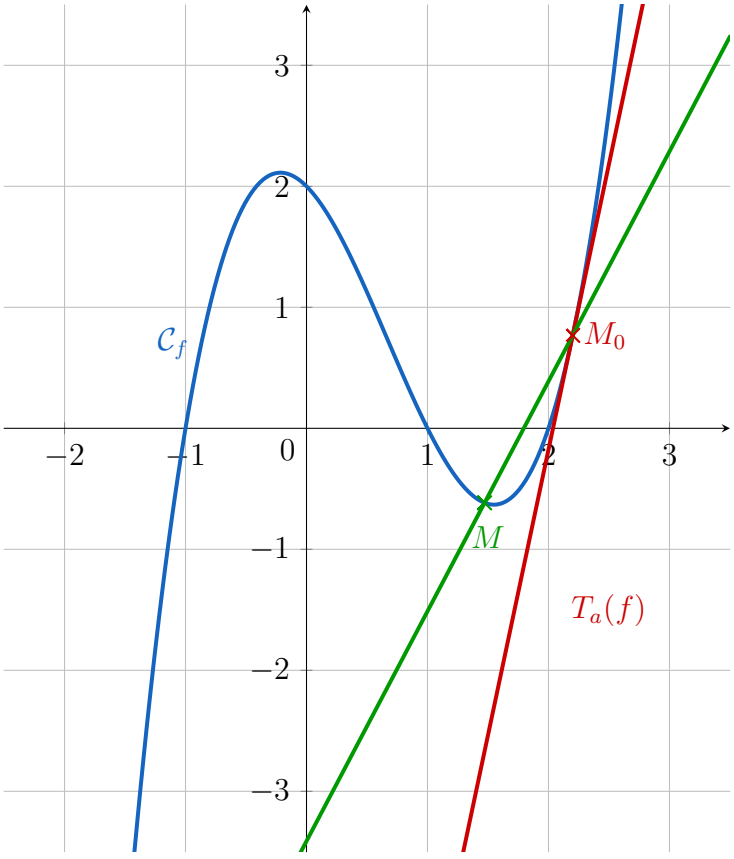
Remarque I.7. *On préfèrera travailler avec $h \to 0$ plutôt que $x \to a$ en général, et donc on écrira plutôt :*

$$f(a+h) = f(a) + f'(a)h + h\varepsilon(h) \text{ avec } \varepsilon(h) \underset{h\to 0}{\to} 0.$$

Corollaire I.8. *Avec les mêmes notations, si f est dérivable en a, alors la tangente $T_a(f)$ à la courbe de f en le point d'abscisse a a pour équation :*

$$T_a(f) : y = f(a) + (x-a)f'(a).$$

Démonstration. Si $M_0(a, f(a))$ et $M(x, f(x))$ pour $x \in I$, alors la droite (M_0M) est la droite passant par M_0 de pente $\tau_{a,f}(x)$. En faisant tendre x vers a, la droite (M_0M) tend bien vers la droite passant par M_0 de pente $f'(a)$.



□

Remarque I.9. *Si $\lim\limits_{x\to a} \tau_{a,f}(x) = \pm\infty$, alors la courbe de f admet une tangente verticale au point d'abscisse a.*

Exemple I.10. *Si $f : x \mapsto \sqrt{x}$, alors pour $x > 0$:*

$$\tau_{0,f}(x) = \frac{\sqrt{x} - \sqrt{0}}{x - 0} = \frac{1}{\sqrt{x}} \underset{x\to 0}{\to} +\infty$$

et on retrouve que la représentation graphique de f possède une tangente verticale en 0 (ce qu'on avait déjà vu comme cas particulier des fonctions $x \mapsto x^\alpha$ pour $\alpha \in]0;1[$).

I.2 Dérivabilité à gauche et à droite

Définition I.11. *Soit $f : I \to \mathbb{R}$ et $a \in \overset{\circ}{I}$. On dit que f est :*

1. ***dérivable à gauche en** a si $\lim\limits_{x\to a^-} \dfrac{f(x) - f(a)}{x - a}$ existe et est finie ; on note alors $f'_g(a)$ cette limite, appelée **dérivée à gauche de f en** a ;*
2. ***dérivable à droite en** a si $\lim\limits_{x\to a^+} \dfrac{f(x) - f(a)}{x - a}$ existe et est finie ; on note alors $f'_d(a)$ cette limite, appelée **dérivée à droite de f en** a.*

Proposition I.12. *Soit $f : I \to \mathbb{R}$, et $a \in \overset{\circ}{I}$. Alors f est dérivable en a si, et seulement si, f est dérivable à gauche et à droite en a avec $f'_g(a) = f'_d(a)$.*

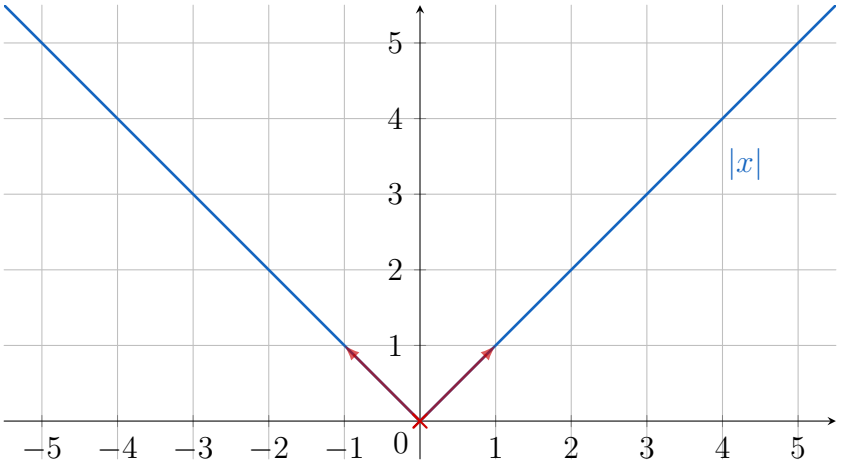
Démonstration. Découle de la limite du taux d'accroissement et du résultat sur les limites à gauche et à droite. □

Remarque I.13. *Comme les limites de taux d'accroissement considérées sont toujours privées de a, la valeur en a du taux n'a pas de sens. En particulier, une fonction peut être dérivable à droite et dérivable à gauche sans être dérivable.*

Exemple I.14. *Reprenons $f : x \mapsto |x|$ et regardons sa dérivabilité en 0. On a déjà vu que f n'est pas dérivable en 0, mais on peut voir que :*

- *si $x > 0$: $\tau_{0,f}(x) = \dfrac{|x| - 0}{x - 0} = 1$, donc f est dérivable à droite en 0 avec $f'_d(0) = 1$;*
- *si $x < 0$: $\tau_{0,f}(x) = \dfrac{|x| - 0}{x - 0} = -1$, donc f est dérivable à gauche en 0 avec $f'_g(0) = -1$.*

ce qui montre que f est dérivable à gauche et à droite en 0, sans y être dérivable comme $f'_g(0) \neq f'_d(0)$.



I.3 Opérations sur les dérivées

Proposition I.15. *Si $f, g : I \to \mathbb{R}$ sont dérivables en $a \in I$, alors :*

1. *pour tous $\lambda, \mu \in \mathbb{R}$: $(\lambda f + \mu g)$ est dérivable en a, avec $(\lambda f + \mu g)'(a) = \lambda f'(a) + \mu g'(a)$;*
2. *fg est dérivable en a avec $(fg)'(a) = f'(a)g(a) + f(a)g'(a)$;*
3. *si $g(a) \neq 0$, alors $\frac{1}{g}$ est dérivable en a, avec $\left(\frac{1}{g}\right)'(a) = \frac{-g'(a)}{(g(a))^2}$;*
4. *si $g(a) \neq 0$, alors $\frac{f}{g}$ est dérivable en a, avec $\left(\frac{f}{g}\right)'(a) = \frac{f'(a)g(a) - f(a)g'(a)}{(g(a))^2}$.*

Démonstration. Notons $\varepsilon_1, \varepsilon_2$ fonctions tendant vers 0 en 0 telles que :

$$\forall h \in I - a, \ \begin{cases} f(a+h) = f(a) + f'(a)h + h\varepsilon_1(h) \\ g(a+h) = g(a) + g'(a)h + h\varepsilon_2(h) \end{cases}$$

Et ainsi les dérivabilités et dérivées découlent des calculs suivants, pour $h \in I - a$:

1. $\lambda f(a+h) + \mu g(a+h) = (\lambda f(a) + \mu g(a)) + (\lambda f'(a) + \mu g'(a)) \cdot h + h \cdot (\lambda\varepsilon_1(h) + \mu\varepsilon_2(h))$
   avec $(\lambda\varepsilon_1(h) + \mu\varepsilon_2(h)) \underset{h\to 0}{\to} 0$;
2. $$\begin{aligned} f(a+h)g(a+h) &= (f(a) + f'(a)h + h\varepsilon_1(h))\,(g(a+h) = g(a) + g'(a)h + h\varepsilon_2(h)) \\ &= f(a)g(a) + (f'(a)g(a) + f(a)g'(a))h \\ &\quad + h\underbrace{(\varepsilon_1(h)g(a) + \varepsilon_2(h)f(a) + \varepsilon_1(h)g'(a)h + \varepsilon_2(h)f'(a)h + \varepsilon_1(h)\varepsilon_2(h)h)}_{=\varepsilon(h)} \end{aligned}$$
   avec $\varepsilon(h) \underset{h\to 0}{\to} 0$ par opérations sur les limites ;
3. $$\begin{aligned} \frac{1}{g(a+h)} &= \frac{1}{g(a) + g'(a)h + h\varepsilon_2(h)} \\ &= \frac{1}{g(a)} \frac{1}{1 + \frac{g'(a)}{g(a)}h + h\frac{\varepsilon_2(h)}{g(a)}} \\ &= \frac{1}{g(a)} \left(1 - \frac{g'(a)}{g(a)}h + h \cdot \frac{-\frac{\varepsilon_2}{g(a)} + h\frac{g'(a)^2}{g(a)^2} + h\frac{g'(a)\varepsilon_2}{g(a)^2}}{1 + \frac{g'(a)}{g(a)}h + h\frac{\varepsilon_2(h)}{g(a)}}\right) \\ &= \frac{1}{g(a)} - \frac{g'(a)}{g(a)^2}h + h\varepsilon(h) \end{aligned}$$
   avec $\varepsilon(h) \underset{h\to 0}{\to} 0$ par opérations sur les limites ;
4. le dernier cas découle de *3* et *4*.

□

Remarque I.16. *On peut aussi montrer tous les résultats précédents par des taux d'accroissements. Par exemple, pour le produit :*

$$\begin{aligned} \frac{f(a+h)g(a+h) - f(a)g(a)}{h} &= \frac{f(a+h)\,(g(a+h) - g(a)) + (f(a+h) - f(a))g(a)}{h} \\ &= f(a+h) \cdot \frac{g(a+h) - g(a)}{h} + \frac{f(a+h) - f(a)}{h}g(a) \\ &\underset{h\to 0}{\to} f(a)g'(a) + f'(a)g(a) \end{aligned}$$

On verra au prochain chapitre comment manipuler plus facilement encore les "fonctions ε", ce qui légitimera davantage leur utilisation.

Corollaire I.17. *Pour $I \subset \mathbb{R}$, l'ensemble $\mathcal{D}(I,\mathbb{R})$ est un sous-anneau de $\mathcal{C}(I,\mathbb{R})$, qui est stable par combinaison linéaire.*

Proposition I.18. *Si $f : I \to J$ et $g : J \to \mathbb{R}$, et $a \in I$ tel que f est dérivable en a et g est dérivable en $f(a)$, alors $g \circ f$ est dérivable en a avec :*

$$(g \circ f)'(a) = f'(a) \cdot g'(f(a)).$$

Démonstration. Montrons le par les taux d'accroissement. Pour $x \in I \setminus \{a\}$, on a :

$$\frac{g \circ f(x) - g \circ f(a)}{x - a} = \frac{g(f(x)) - g(f(a))}{f(x) - f(a)} \cdot \frac{f(x) - f(a)}{x - a}$$

dont le premier facteur tend vers $g'(f(a))$ par limite d'une composée, et le second vers $f'(a)$, ce qui donne le résultat voulu. □

Proposition I.19. *Soit $f : I \to J$ bijective et continue. On pose $a \in I$ tel que f est dérivable en a, et on note $b = f(a) \in J$. Alors f^{-1} est dérivable en b si, et seulement si, $f'(a) \neq 0$, et dans ce cas on a :*

$$(f^{-1})'(b) = \frac{1}{f'(a)} = \frac{1}{f'(f^{-1}(b))}.$$

Démonstration. Montrons les deux implications.
Supposons que f^{-1} est dérivable en b. Avec les mêmes notations, comme $f \circ f^{-1} = \mathrm{id}_J$, alors par dérivée d'une composée il vient que $(f^{-1})'(b) \cdot f'(a) = 1$, et donc $f'(a) \neq 0$ et $(f^{-1})'(b) = \dfrac{1}{f'(a)}$.
Réciproquement, si $f'(a) \neq 0$, alors pour tout $y \in J \setminus \{b\}$ on a :

$$\frac{f^{-1}(y) - f^{-1}(b)}{y - b} = \frac{f^{-1}(y) - f^{-1}(b)}{f(f^{-1}(y)) - f(f^{-1}(b))}.$$

Comme f est continue, alors f^{-1} aussi donc : $\lim\limits_{y \to b} f^{-1}(y) = f^{-1}(b) = a$. Et donc par composition de limites :

$$\lim_{y \to b} \frac{f(f^{-1}(y)) - f(f^{-1}(b))}{f^{-1}(y) - f^{-1}(b)} = f'(f^{-1}(b)) = f'(a)$$

puis en passant à l'inverse :

$$\lim_{y \to b} \frac{f^{-1}(y) - f^{-1}(b)}{y - b} = \frac{1}{f'(a)} = \frac{1}{f'(f^{-1}(b))}.$$

□

Remarque I.20. *Et on retrouve au passage le fait que la tangente à la courbe de f en a est la symétrique de la tangente à la courbe de f^{-1} en b.*

I.4 Dérivées d'ordre supérieur

Proposition-Définition I.21. *Pour $I \subset \mathbb{R}$ et $n \in \mathbb{N}$, on note $\mathcal{D}^n(I,\mathbb{R})$ l'ensemble des fonctions n-fois dérivables sur I, et $\mathcal{C}^n(I,\mathbb{R})$ l'ensemble des fonctions de classe $\mathcal{C}^n$ sur I. On note $\mathrm{C}^\infty(I,\mathbb{R})$ l'ensemble des fonctions infiniment dérivables sur I, aussi appelées fonctions de classe $\mathcal{C}^\infty$.*
Pour tout $n \in \mathbb{N}$, on a les inclusions strictes :

$$\mathcal{C}^\infty \subsetneq \mathcal{C}^{n+1}(I,\mathbb{R}) \subsetneq \mathcal{D}^{n+1}(I,\mathbb{R}) \subsetneq \mathcal{C}^n(I,\mathbb{R}) \subsetneq \mathcal{D}^n(I,\mathbb{R}).$$

Démonstration. Les inclusions viennent du fait qu'une fonction dérivable est continue. Le fait qu'elles soient strictes vient du fait qu'il existe des fonctions dérivables de dérivée non continue, ou continue non dérivable. □

Proposition I.22. *Soit $n \in \mathbb{N}^*$ et f, g de classe $\mathcal{C}^n$ sur I :*

1. *si $\lambda, \mu \in \mathbb{R}$, alors $\lambda f + \mu g$ est de classe $\mathcal{C}^n$ sur I, avec : $(\lambda f + \mu g)^{(n)} = \lambda f^{(n)} + \mu g^{(n)}$;*
2. *fg est de classe $\mathcal{C}^n$ sur I, avec :*

$$(fg)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(k)} g^{(n-k)} \text{ (Formule de Leibniz)};$$

3. *si g ne s'annule pas sur I, alors $\frac{1}{g}$ et $\frac{f}{g}$ sont de classe $\mathcal{C}^n$ sur I ;*
4. *si $f : I \to \mathbb{R}$ et $g : J \to \mathbb{R}$ sont composables, alors $g \circ f$ est de classe $\mathcal{C}^n$ sur I ;*
5. *si $f : I \to J$ est bijective, et que f' ne s'annule pas sur I, alors f^{-1} est de classe $\mathcal{C}^n$ sur J.*

Remarques I.23.

1. *Les énoncés restent valable en remplaçant "de classe $\mathcal{C}^n$" par "n-fois dérivable" ou "infiniment dérivable".*
2. *On prendra bien garde aux hypothèses très faibles (non annulation de g et non annulation de f'), pour les points 3 et5.*

Démonstration.
1. par récurrence, par linéarité de la dérivation ;
2. par récurrence, en utilisant le triangle de Pascal (à la manière de la démonstration du binôme) ;
3. par dérivée d'un produit, il suffit de la montrer pour $f = 1$, ce que l'on fait par récurrence.
   Pour l'hérédité : supposons que g est de classe $\mathcal{C}^{n+1}$ et que g ne s'annule pas. Alors $(\frac{1}{g})' = -\frac{g'}{g^2}$ est le produit des fonctions $-g'$ (qui est de classe $\mathcal{C}^n$) et des fonctions $\frac{1}{g}$ et $\frac{1}{g}$ (qui sont de classe $\mathcal{C}^n$ par hypothèse de récurrence). Et le résultat découle de celui sur les produits.

Les deux derniers résultats se montrent par récurrence de la même manière que le quotient. □

Corollaire I.24. *Pour $I \subset \mathbb{R}$, les ensembles $\mathcal{D}^n(I, \mathbb{R})$, $\mathcal{C}^n(I, \mathbb{R})$ et $\mathcal{C}^\infty(I, \mathbb{R})$ (pour $n \in \mathbb{N}$) sont des sous-anneaux de $\mathcal{C}(I, \mathbb{R})$, qui sont stable par combinaison linéaire.*

Corollaire I.25. *L'ensemble des fonctions polynomiales est un sous-anneau de $\mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$ stable par combinaisons linéaires.*

Démonstration. Découle du fait que $x \mapsto x$ est $\mathcal{C}^\infty$ □

II Propriétés générales des fonctions dérivables

II.1 Extremum d'une fonction dérivable

Définition II.1. *Soient $f : I \to \mathbb{R}$ et $a \in I$. On dit que f admet :*

1. *un **maximum** (resp. un **minimum**) en a si pour tout $x \in I$: $f(x) \leq f(a)$ (resp. $f(x) \geq f(a)$) ;*
2. *un **maximum local** (resp. **minimum local**) en a s'il existe $\eta > 0$ tel que pour tout $x \in I$: $|x - a| < \eta \Rightarrow f(x) \leq f(a)$ (resp. $f(x) \geq f(a)$) ;*
3. *un **point critique** en a si f est dérivable en a et que $f'(a) = 0$.*

Remarques II.2.

1. *Pour éviter toute ambiguïté, on parlera de maximum ou de maximum global dans le premier cas.*
2. *On parlera plus généralement d'extremums (locaux ou globaux) dans les deux premiers cas.*
3. *Des extremums seront qualifiés de* ***stricts*** *si on considère précédemment des inégalités strictes pour* $x \neq a$.

Proposition II.3. *Si f admet un maximum (resp. minimum) strict, celui-ci est unique.*

Démonstration. Supposons par l'absurde que f admette un maximum strict en a et b, avec $a \neq b$. Alors $f(a) > f(b)$ et $f(b) > f(a)$, d'où la contradiction. □

Proposition II.4. *Si $f : I \to \mathbb{R}$ et $a \in I$ tel que I est un voisinage de I et que f soit dérivable en a. Alors on a les implications :*

$$f \text{ a un extremum global en } a \Rightarrow f \text{ a un extremum local en } a \Rightarrow f \text{ a un point critique en } a.$$

Démonstration. La première implication est claire, du fait des définitions.

Supposons donc que f possède un maximum (local) en a. Notons $\eta > 0$ tel que : $\forall x \in I,\ |a - x| < \eta \Rightarrow f(x) \leq f(a)$.

Comme a est intérieur à I, alors, quitte à réduire η, on peut supposer que $]a - \eta; a + \eta[\subset I$. Et ainsi :

- si $x \in]a-\eta; a[$: $\dfrac{f(x) - f(a)}{x - a} \geq 0$, puis en passant à la limite pour x tendant vers a : $f'(a) = f'_g(a) \geq 0$;
- si $x \in]a; a+\eta[$: $\dfrac{f(x) - f(a)}{x - a} \leq 0$, puis en passant à la limite pour x tendant vers a : $f'(a) = f'_d(a) \leq 0$;

et donc $f'(a) = 0$, donc f a un point critique en a.

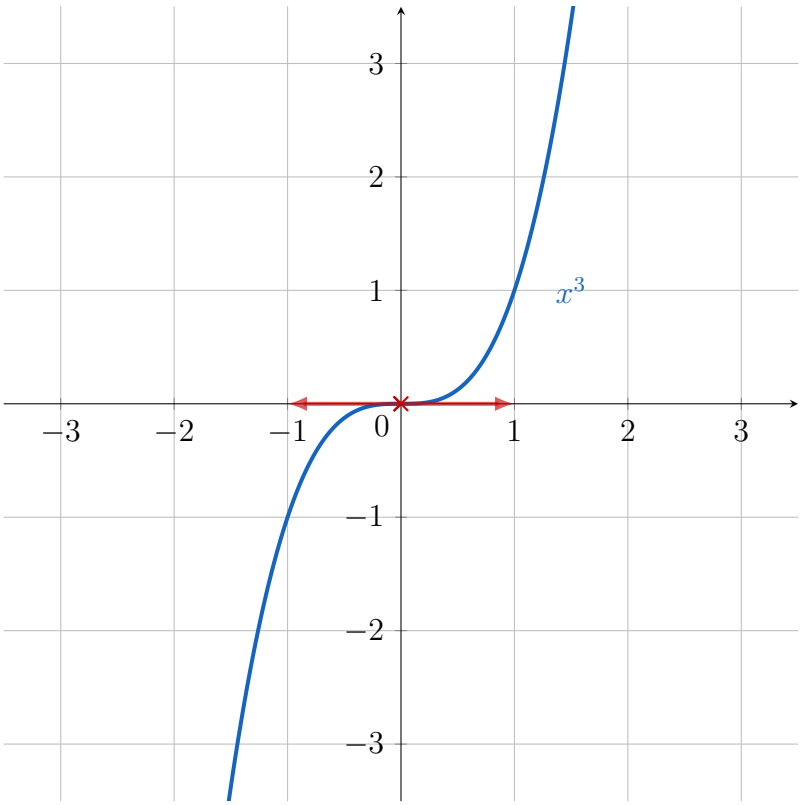
Le cas où f possède un minimum en a se traite de même. □

Remarque II.5. *Le fait que a soit intérieur est indispensable pour pouvoir travailler avec les dérivées à gauche et à droites. Le résultat devient faux sinon : par exemple, la restriction de la fonction $x \mapsto x$ à $[0; 1]$ admet un minimum en 0 et un maximum en 1, mais pas de point critique.*

En revanche, il donne une information importante sur la localisation des extrema : si f est dérivable sur $[a, b]$ ne possède pas de point critique, alors ses extrema sont en a ou b (en fait a et b).

De même, il faut imposer la dérivabilité en a : par exemple, la fonction $x \mapsto |x|$ admet un minimum en 0, qui n'est pas un point critique.

Remarque II.6. *Les réciproques des implications précédentes sont fausses. Par exemple, la fonction $x \mapsto x^3$ admet un point critique en 0, mais n'y admet pas d'extremum (local ou global), puisque pour tout $x > 0$ on a $x^3 > 0 = 0^3$ et pour tout $x < 0$ on a $x^3 < 0$.*



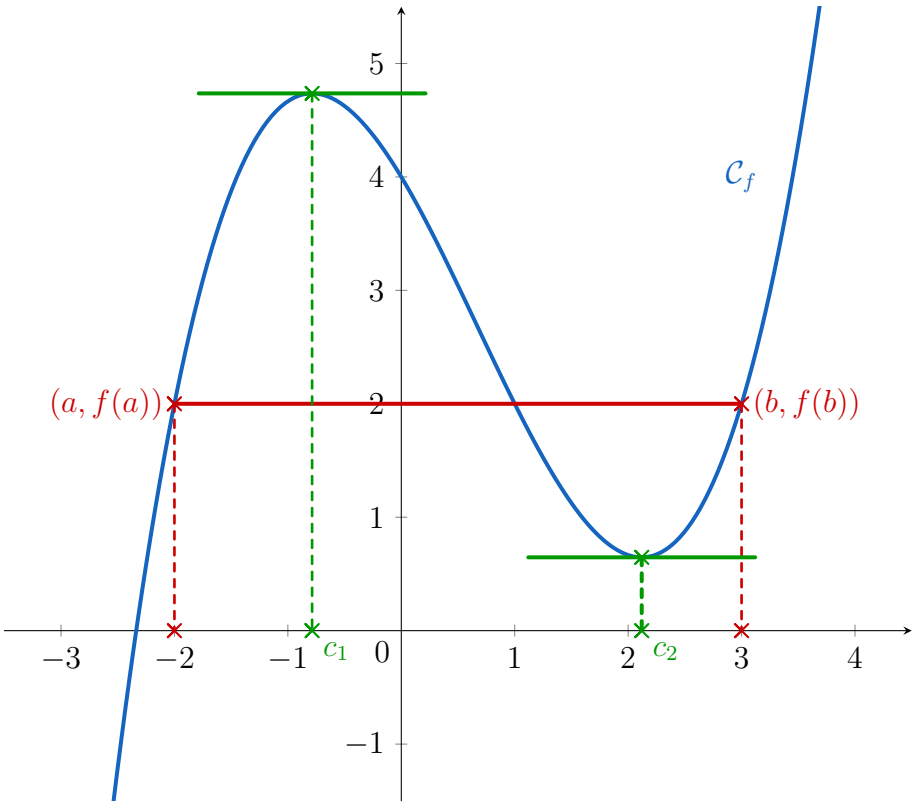
En revanche, ce résultat est utile pour sa contraposée : il permet de chercher les extremums d'une fonction en regardant ses points critiques puis en les étudiant de manière plus poussée.

II.2 Les théorèmes de Rolle et des accroissements finis

Théorème II.7 (Théorème de Rolle)**.** *Soit* $f : [a, b] \to \mathbb{R}$ *fonction :*

1. *continue sur* $[a; b]$ *;*
2. *dérivable sur* $]a; b[$ *;*
3. *telle que* $f(a) = f(b)$.

Alors il existe $c \in]a; b[$ *tel que* $f'(c) = 0$.



Démonstration. Comme f est continue sur le segment $[a, b]$, alors elle y est bornée et atteint ses bornes :
- si f est constante : alors $f' = 0$ sur $]a, b[$, donc tout élément de $]a, b[$ convient ;
- si f n'est pas constante : alors soit son minimum soit son maximum n'est pas atteint en a et b. Il est donc atteint en $x \in]a, b[$, qui est un extremum, donc un point critique.

□

Remarque II.8. *Comme le TVI, le résultat est faux si l'on travaille sur $\mathbb{C}$ au lieu de $\mathbb{R}$. On peut reprendre le même contre-exemple, avec la fonction $f : t \mapsto e^{it}$ sur $[0; 2\pi]$: elle est dérivable, avec $f(0) = 1 = f(2\pi)$, mais $f' : t \mapsto ie^{it}$ ne s'annule jamais.*

Corollaire II.9. *Si $P \in \mathbb{R}[X]$ de degré $n \geq 2$ est scindé simple, alors P' aussi. De plus, si on note $a_1 < \cdots < a_n$ les racines de P et $b_1 < \cdots < b_{n-1}$ celles de P', alors :*

$$a_1 < b_1 < a_2 < b_2 < \cdots < a_{n-1} < b_{n-1} < a_n.$$

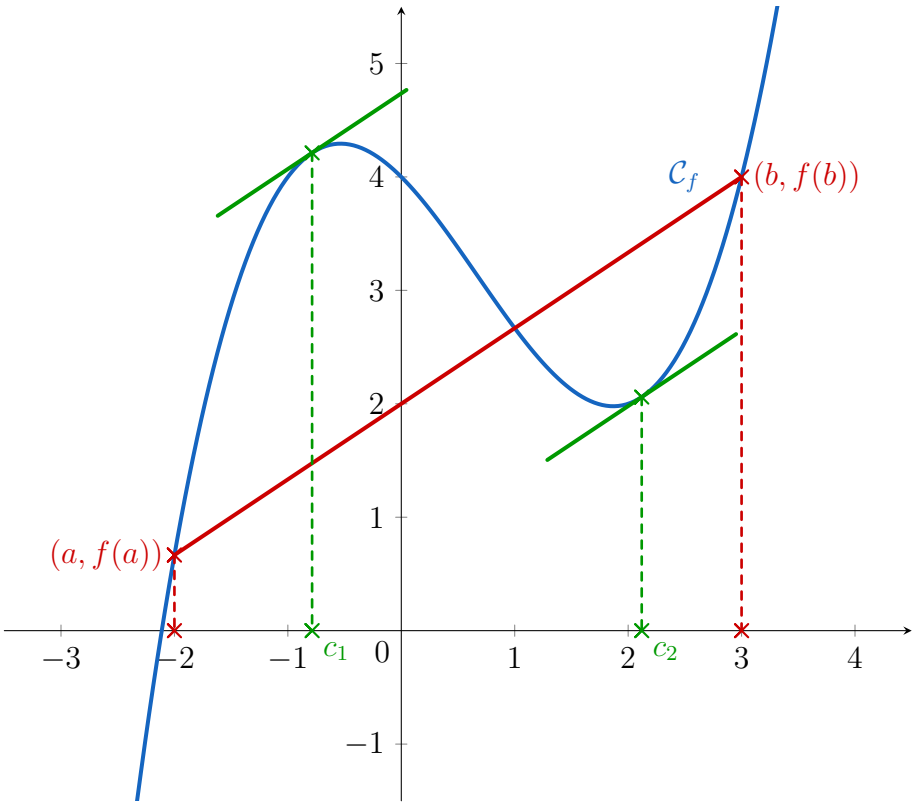
Démonstration. On applique le théorème de Rolle à P sur chaque intervalle de la forme $[a_i; a_{i+1}]$ ce qui assure l'existence d'une racine $b_i \in]a_i; a_{i+1}[$ pour P'. □

Corollaire II.10. *Si f est continue sur un intervalle I et dérivable sur $\mathring{I}$, telle que f' ne s'annule pas, alors f réalise une bijection continue strictement monotone de I sur $f(I)$.*

Démonstration. Par propriété des fonctions continues, il suffit de voir que f est injective. Par l'absurde, si $x, y \in I$ vérifient $f(x) = f(y)$ et $x < y$, alors par théorème de Rolle il existe $c \in]x, y[\subset \mathring{I}$ tel que $f'(c) = \frac{f(y)-f(x)}{y-x} = 0$, d'où la contradiction.
Donc f est injective, donc bijective sur $f(I)$, et sa continuité entraîne sa stricte monotonie. □

Théorème II.11 (Égalité des accroissements finis)**.** *Si $f : [a, b] \to \mathbb{R}$ continue sur $[a, b]$ et dérivable sur $]a, b[$, alors il existe $c \in]a, b[$ tel que :*

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



Démonstration. On considère la fonction g définie sur I par :

$$g(x) = f(x) - \frac{f(b) - f(a)}{b - a}(x - a) - f(a)$$

c'est-à-dire que g diffère de f d'une fonction affine et vérifie $g(a) = g(b) = 0$.
Alors g vérifie toutes les hypothèses du théorème de Rolle, et donc il existe $c \in]a, b[$ tel que $g'(c) = 0$. Mais la dérivée de g est donnée par :

$$g' : x \mapsto f'(x) - \frac{f(b) - f(a)}{b - a}$$

et donc il existe $c \in]a, b[$ tel que $f'(c) = \dfrac{f(b) - f(a)}{b - a}$. □

Remarques II.12.

1. *Pour pouvoir la manipuler plus facilement, on écrit parfois la dernière égalité :* $(b - a)f'(c) = f(b) - f(a)$.
2. *Pour mettre en évidence à quel point c est proche de a ou b, on peut aussi écrire qu'il existe $\theta \in]0; 1[$ tel que :* $f'(a + \theta(b - a)) = \dfrac{f(b) - f(a)}{b - a}$.

II.3 Inégalité des accroissements finis et fonctions lipschitziennes

Théorème II.13 (Inégalité des accroissements finis)**.** *Soit $f : I \to \mathbb{C}$ dérivable sur l'intervalle I. On suppose qu'il existe $M \in \mathbb{R}$ tel que : $\forall t \in I,\ |f'(t)| \leq M$. Alors :*

$$\forall x, y \in I,\ |f(x) - f(y)| \leq M|x - y|.$$

Démonstration. Soient $x, y \in I$. Le cas $x = y$ est clair (car les deux membres de l'inégalité à prouver son nuls). Supposons donc $x \neq y$. Quitte à échanger x et y, on peut supposer que $x < y$, et ainsi $[x, y] \subset I$.

— si f est à valeurs dans $\mathbb{R}$: alors par égalité des accroissements finis, il existe $c \in]x, y[$ tel que : $f'(c)(y-x) = f(y) - f(x)$. Comme $|f'(c)| \leq M$, alors en prenant la valeur absolue on déduit que :

$$|f(y) - f(x)| = |f'(c)| \cdot |y - x| \leq M|y - x|$$

ce qui est l'inégalité à prouver.

— si f est à valeurs complexes :

— si $f(y) - f(x) \in \mathbb{R}$: alors la fonction $\mathrm{Re}(f)$ est à valeurs réelles et vérifie $\mathrm{Re}(f)(y) - \mathrm{Re}(f)(x) = \mathrm{Re}\left(f(y) - f(x)\right) = f(y) - f(x)$. Par dérivée complexe, on a : $\left(\mathrm{Re}(f)\right)' = \mathrm{Re}(f')$, donc pour tout $t \in I$:

$$\left|\left(\mathrm{Re}(f)\right)'(t)\right| = \left|\mathrm{Re}(f'(t))\right| \leq |f'(t)| \leq M$$

donc en appliquant le résultat précédent à $\mathrm{Re}(f)$, on a :

$$|f(y) - f(x)| \leq M|y - x|$$

— si $f(y) - f(x) \notin \mathbb{R}$: on pose $\theta \in \mathbb{R}$ tel que $e^{i\theta}\left(f(y) - f(x)\right) \in \mathbb{R}$. Et on applique le résultat précédent à $g : t \mapsto e^{i\theta} f(t)$, puisque la fonction g est dérivable sur I, avec pour tout $t \in I$: $|g'(t)| = |e^{i\theta}| \cdot |f'(t)| = |f'(t)| \leq M$, et $g(y) - g(x) \in \mathbb{R}$. On a donc :

$$|g(y) - g(x)| \leq M|y - x|$$

et le résultat découle du fait que $|g(y) - g(x)| = \left|e^{i\theta}\left(f(y) - f(x)\right)\right| = |f(y) - f(x)|$.

□

Corollaire II.14. *Si $f : [a, b] \to \mathbb{C}$ est de classe $\mathcal{C}^1$, alors il existe $M \in \mathbb{R}$ tel que :*

$$\forall x, y \in [a, b],\ |f(x) - f(y)| \leq M|x - y|.$$

Démonstration. Si f est $\mathcal{C}^1$, alors $|f'|$ est continue sur le segment $[a, b]$ donc est majorée sur $[a, b]$ par un réel M, qui vérifie les hypothèses du théorème précédent. □

Remarque II.15. *En fait, on peut même démontrer plus rapidement le cas $\mathcal{C}^1$, car on a alors :*

$$\forall x, y \in [a, b],\ f(y) - f(x) = \int_x^y f'(t)\mathrm{d}t$$

et par "inégalité triangulaire" (version intégrale), on déduit que :

$$|f(y) - f(x)| = \left|\int_x^y f'(t)\mathrm{d}t\right| \leq \pm\int_x^y |f'(t)|\mathrm{d}t \leq \pm\int_x^y M\mathrm{d}t = M|y - x|$$

où le $\pm$ devant les intégrales permet de prendre en compte que $x < y$ ou $y < x$.

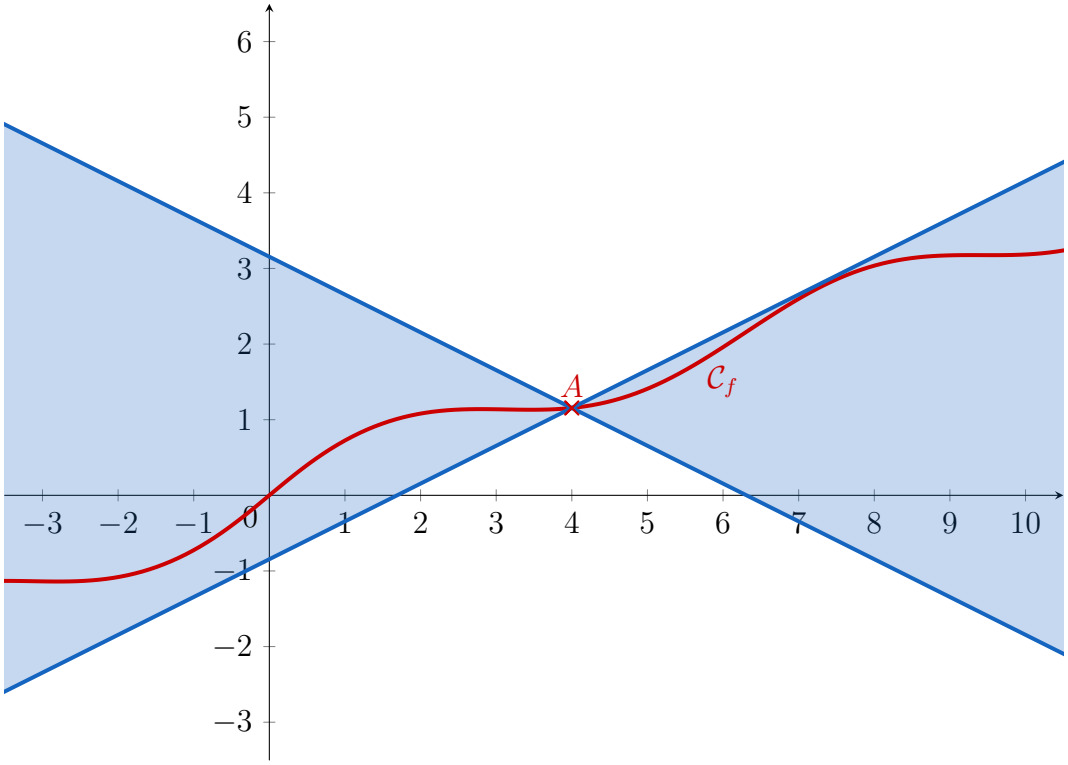
Exemple II.16. *Avec la fonction* sin*, on a $|\sin'| = |\cos| \leq 1$ sur $\mathbb{R}$. Et donc pour tous $x, y \in \mathbb{R}$:* $|\sin(x) - \sin(y)| \leq |x - y|$.
Avec $y = 0$, on retrouve l'inégalité classique : $\forall x \in \mathbb{R},\ |\sin(x)| \leq |x|$.

Définition II.17 (Fonctions Lipschitzienne)**.** *Si $I \subset \mathbb{R}$ et $k \in \mathbb{R}_+$, une fonction $f : I \to \mathbb{C}$ est dite k-**lipschitzienne** si :*

$$\forall x, y \in I,\ |f(y) - f(x)| \leq k \cdot |y - x|.$$

*Plus généralement, on dira que f est **lipschitzienne** s'il existe $k \geq 0$ tel que f est k-lipschitzienne.*

Remarque II.18. *Une fonction k-lipschitzienne se voit graphiquement : tous les taux d'accroissements sont entre $-k$ et k. Et donc si on se place au point $A(a, f(a))$, le cône délimité par les deux droites passant par A de pente $\pm k$ contient tous les points du graphe de f.*



Proposition II.19. *Une fonction lipschitzienne est continue.*

Démonstration. On applique la définition de la continuité.
Soit $f : I \to \mathbb{C}$ une fonction k-lipschitzienne, pour $k \in \mathbb{R}_+$. Si $k = 0$ alors f est constante (donc continue). Sinon, considérons $a \in I$ et $\varepsilon > 0$. En posant $\eta = \frac{\varepsilon}{k} > 0$, on a pour tout $x \in I$:

$$|x - a| \leq \eta \Rightarrow |f(x) - f(a)| \leq k \cdot \eta = \varepsilon$$

ce qui assure bien la continuité de f en $a \in I$. Comme ceci est valable pour tout $a \in I$, on déduit que f est continue sur I. □

Remarque II.20. *La réciproque est fausse. On peut par exemple considérer :*
- *la fonction $f : x \mapsto x^2$ sur $\mathbb{R}$: pour tout $k \in \mathbb{R}_+$, on a $f(k+1) - f(0) = (k+1)^2 > k \cdot |(k+1-0)$;*
- *la fonction $f : x \mapsto \sqrt{x}$ sur $[0;1]$: si elle était k-lipschitzienne, on aurait pour tout $x \in]0;1]$: $\sqrt{x} \leq kx$, et donc $1 \leq k\sqrt{x}$, ce qui devient faut en prenant $x = 1/2$ (si $k \leq 1$) ou $x = \frac{1}{k^4}$ (si $k > 1$).*

Proposition II.21. *Si f est dérivable sur un intervalle I, et que $|f'|$ est majorée par M, alors f est M-lipschitzienne.*
En particulier, si f est $\mathcal{C}^1$ sur le segment $[a, b]$, alors f est k-lipschitzienne avec $k = \max_{x \in [a,b]} |f'(x)|$.

Démonstration. Découle de l'inégalité des accroissements finis et de son corollaire. □

Remarque II.22. *Une fonction lipschitzienne n'étant pas nécessairement dérivable, cela donne un cadre plus large d'application de l'inégalité des accroissements finis. Par exemple la fonction $x \mapsto |x|$ n'est pas dérivable en 0, mais est 1-lipschitzienne, puisque l'inégalité triangulaire donne :*

$$\forall x, y \in \mathbb{R},\ ||x| - |y|| \leq 1 \cdot |x - y|.$$

II.4 Monotonie et dérivée

Proposition II.23. *Soient I intervalle et $f : I \to \mathbb{C}$ dérivable. Alors f est constante sur I si, et seulement si, pour tout $x \in I$: $f'(x) = 0$.*

Démonstration. Si f est constante, alors sa dérivée est nulle (car tous ses taux d'accroissement, donc leurs limites, sont nuls).
Réciproquement, si f' est nulle, alors par inégalité des accroissements finis, comme $|f'| = 0 \leq 0$, on a :

$$\forall x \in I,\ |f(x) - f(y)| \leq 0 \cdot |x - y| = 0$$

et donc f est constante. □

Remarque II.24. *Le résultat devient faux si on n'est pas sur un intervalle. Par exemple* $x \mapsto \text{Arctan}(x) + \text{Arctan}\left(\frac{1}{x}\right)$ *est bien de dérivée nulle sur* $\mathbb{R}^*$*, mais n'est pas constante comme :*

$$\text{Arctan}(x) + \text{Arctan}\left(\frac{1}{x}\right) = \begin{cases} \frac{\pi}{2} & si \quad x > 0 \\ -\frac{\pi}{2} & si \quad x < 0 \end{cases}.$$

Proposition II.25. *Soit* I *un intervalle de* $\mathbb{R}$*, et* $f : I \to \mathbb{R}$ *continue sur* I *et dérivable sur* $\overset{\circ}{I}$*. Alors* f *est croissante (resp. décroissante) si, et seulement si, pour tout* $x \in \overset{\circ}{I}$ *:* $f'(x) \geq 0$ *(resp.* $f'(x) \leq 0$*).*

Démonstration. Montrons le cas de la croissance.
Si f est croissante : soit $x \in \overset{\circ}{I}$ et $y \in I \setminus \{x\}$. Alors :

$$\frac{f(x) - f(y)}{x - y} \geq 0$$

et donc en passant à la limite pour $y \to x$: $f'(x) \geq 0$.
Réciproquement, si $f' \geq 0$ sur $\overset{\circ}{I}$, alors considérons $x, y \in I$ avec $x < y$. Par égalité des accroissements finis, il existe $c \in]x, y[\subset \overset{\circ}{I}$ tel que $f(y) - f(x) = f'(x)(y - x) \geq 0$. Et donc $f(x) \leq f(y)$. Donc f est croissante. □

Proposition II.26. *Soient* I *un intervalle et* $f : I \to \mathbb{R}$ *continue sur* I *et dérivable sur* $\overset{\circ}{I}$ *telle que :* $\forall x \in \overset{\circ}{I},\ f'(x) > 0$*. Alors* f *est strictement croissante sur* I*.*

Démonstration. En reprenant la preuve précédente, si $x, y \in I$ vérifient $x < y$, alors il existe $c \in \overset{\circ}{I}$ tel que : $f(y) - f(x) = f'(c)(y - x) > 0$, ce qui donne la strictement monotonie. □

Remarques II.27.

1. *On a bien sûr le résultat analogue pour les fonctions dérivables.*
2. *On peut faire mieux avec le théorème de Rolle : si* f' *ne s'annule pas sur* $\overset{\circ}{I}$ *alors* f *est strictement monotone, et le résultat précédent donne le sens de variations de* f*.*
3. *La réciproque est fausse : on peut reprendre* $x \mapsto x^3$ *qui est strictement croissante mais dont la dérivée s'annule en* 0*.*

Corollaire II.28. *Si* I *est un intervalle,* f *continue sur* I *et dérivable sur* $\overset{\circ}{I}$ *telle que* $f' \geq 0$*, ne s'annulant qu'en un nombre fini de réels, alors* f *est strictement croissante sur* I*.*

Démonstration. Soient $x, y \in I$ avec $x < y$. Notons $a_1, \ldots, a_n$ les éventuels réels de $]x, y[$ en lesquels f' s'annule, de sorte que $x < a_1 < \cdots < a_n < y$.
Par la proposition précédente, f' ne s'annulant sur aucun des intervalles $]x, a_1[$, $]a_i, a_{i+1}[$, $]a_n, y[$, alors on déduit que f est strictement croissante sur chacun des intervalles larges associés. Et donc :

$$f(x) < f(a_1) < \cdots < f(a_n) < f(y)$$

donc $f(x) < f(y)$. Donc f est strictement croissante. □

Remarques II.29.

1. *La réciproque est fausse : par exemple, la fonction $x \mapsto x + \sin(x)$ est dérivable sur $\mathbb{R}$ avec $f' : x \mapsto 1 - \cos(x)$, qui est bien positive ou nulle, et s'annule en tous les éléments de $2\pi\mathbb{Z}$.*
   Mais elle est strictement croissante car, sur chaque segment, f' n'a qu'un nombre fini de points d'annulations, donc on peut appliquer le théorème précédent.

2. *On a en fait l'équivalence qu'une fonction f continue sur un intervalle I et dérivable sur $\overset{\circ}{I}$ est strictement croissante si, et seulement si :*

$$\begin{cases} f' > 0 \text{ sur } \overset{\circ}{I} \\ \{x \in \overset{\circ}{I} \mid f'(x) = 0\} \text{ ne contient pas d'intervalle non trivial} \end{cases}.$$

II.5 Théorèmes de prolongement

Théorème II.30 (Théorème de la limite de la dérivée)**.** *Soit $f : [a, b] \to \mathbb{R}$ fonction :*

1. *continue sur $[a, b]$;*
2. *dérivable sur $]a, b]$;*
3. *telle que $\lim\limits_{x \to a^+} f'(x) = l \in \overline{\mathbb{R}}$.*

Alors : $\lim\limits_{x \to a^+} \dfrac{f(x) - f(a)}{x - a} = l$.
Sous ces conditions, la fonction f est dérivable en a si, et seulement si, $l \in \mathbb{R}$ et dans ce cas $f'(a) = l$ et f' est continue en a.

Démonstration. Soit $x \in]a, b]$. Par théorème des accroissements finis, comme f est dérivable sur $]a, x[$, il existe c_x (qui dépend de x) tel que : $f'(c_x) = \dfrac{f(x) - f(a)}{x - a}$.
Par théorème d'encadrement, comme $c_x \in]a, x[$, on a : $\lim\limits_{x \to a^+} c_x = a$. Et donc par composition :

$$\lim_{x \to a^+} \frac{f(x) - f(a)}{x - a} = \lim_{x \to a^+} f'(c_x) = l$$

ce qui donne bien le résultat précédent. □

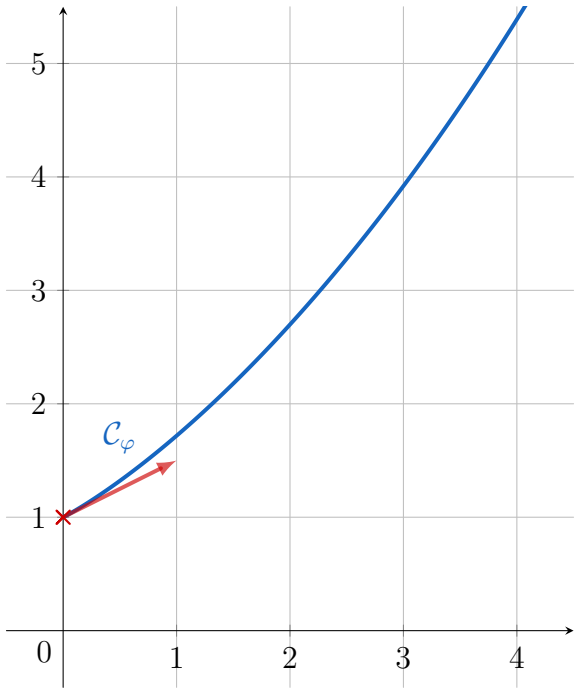
Corollaire II.31. *Si f est continue sur I et dérivable sur $I \setminus \{a\}$ telle que $\lim\limits_{\substack{x \to a \\ x \neq a}} f'(x) = l \in \mathbb{R}$, alors f est dérivable en a avec $f'(a) = l$.*

Démonstration. On applique le cas précédent en regardant la dérivabilité à gauche et à droite en a. □

Exemple II.32. *Regardons la fonction φ définie sur $\mathbb{R}_+$ par : $\forall x \in \mathbb{R}_+,\ \varphi(x) = e^{\sqrt{x}} - \sqrt{x}$. Alors φ est continue sur $\mathbb{R}_+$ et dérivable sur $\mathbb{R}_+^*$ avec :*

$$\forall x \in \mathbb{R}_+^*,\ \varphi'(x) = \frac{1}{2\sqrt{x}} e^{\sqrt{x}} - \frac{1}{2\sqrt{x}} = \frac{e^{\sqrt{x}} - 1}{2\sqrt{x}} \underset{x \to 0}{\to} \frac{1}{2}$$

donc φ est dérivable en 0, avec $\varphi'(0) = \dfrac{1}{2}$.



On peut en déduire que : $\dfrac{\varphi(x)-\varphi(1)}{x}$ *tend vers* $\dfrac{1}{2}$ *en* 0*, c'est-à-dire que :*

$$\lim_{x\to 0^+} \frac{e^{\sqrt{x}}-1-\sqrt{x}}{x} = \frac{1}{2}$$

et en faisant le changement de variable $X=\sqrt{x}$ *on déduit que :*

$$\lim_{x\to 0^+} \frac{e^{x}-1-x}{x^2} = \frac{1}{2}.$$

Corollaire II.33 (Théorème de prolongement $\mathcal{C}^1$)**.** *Si* f *est de classe* $\mathcal{C}^1$ *sur* $I\setminus\{a\}$ *telle que* f *et* f' *possèdent des limites finies en* a*, alors le prolongement par continuité de* f *en* a *définit une fonction de classe* $\mathcal{C}^1$ *sur* I*.*

Démonstration. Découle directement du résultat précédent en constatant que le prolongement par continuité a bien un sens et fournit une fonction continue sur I et dérivable sur $I\setminus\{a\}$.
La dérivabilité et le caractère $\mathcal{C}^1$ en a sont assurés par le résultat précédent. □

Corollaire II.34 (Théorème de prolongement $\mathcal{C}^k$)**.** *Si* $k\in\mathbb{N}^*$ *et* f *de classe* $\mathcal{C}^k$ *sur* $I\setminus\{a\}$ *telles que les quantités* $\lim\limits_{x\to a} f^{(i)}(x)$ *existent et sont finies pour tout* $i\in[\![0;k]\!]$*. Alors le prolongement par continuité de* f *en* a *définit une fonction de classe* $\mathcal{C}^k$ *sur* I*.*

Démonstration. Par récurrence.
Les cas $k=0$ et $k=1$ ont déjà été traités.
Supposons f de classe $\mathcal{C}^{k+1}$ vérifie les hypothèses précédentes, pour $k\in\mathbb{N}^*$. Alors :

- par le cas $k=1$: on déduit que le prolongement $\tilde{f}$ de f est $\mathcal{C}^1$ sur I ;
- $\tilde{f}'$ coïncide avec f' sur $I\setminus\{a\}$ et vérifie donc toutes les hypothèses du théorème au rang k, donc est de classe $\mathcal{C}^k$ sur I (en tant que seul prolongement continu de f') ;
- donc $\tilde{f}$ est de classe $\mathcal{C}^{k+1}$ sur I.

□

III Convexité

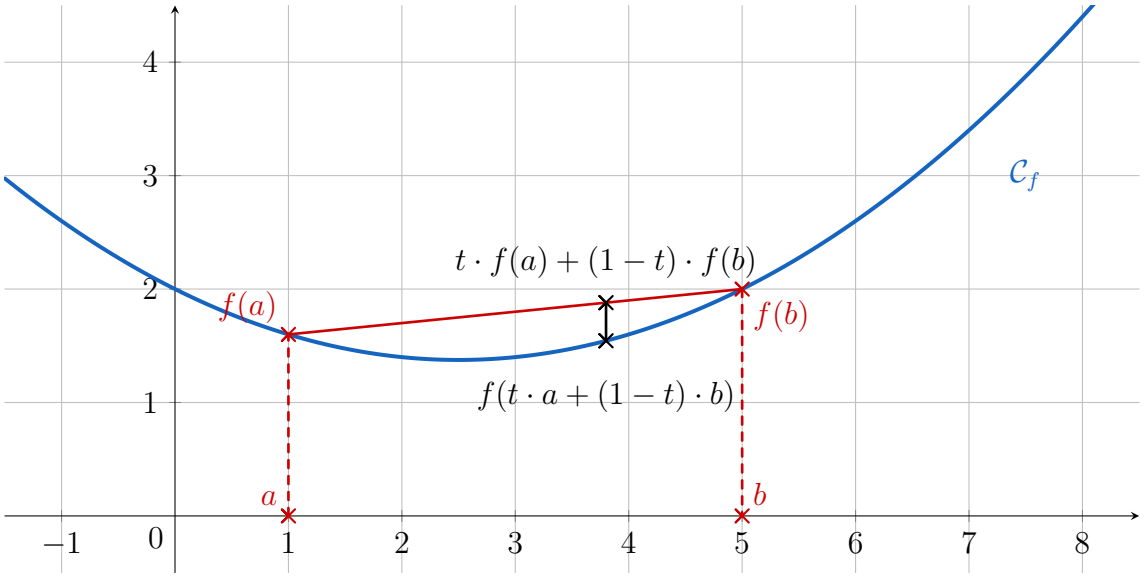
Définition III.1. *Si I est un intervalle, la fonction $f : I \to \mathbb{R}$ est dite* ***convexe*** *sur I si :*

$$\forall a, b \in I,\ \forall t \in [0;1],\ f(ta + (1-t)b) \leq tf(a) + (1-t)f(b).$$

On dira que la fonction f est ***concave*** *si $-f$ est convexe.*

Remarque III.2. *Notons que l'inégalité précédente a bien un sens. Comme I est un intervalle, alors I est un convexe de $\mathbb{R}$, donc pour tout $a, b \in I$ et tout $t \in [0,1]$ on a bien que $ta + (1-t)b \in I$.*

Remarque III.3. *Cela veut dire que toutes les cordes de f sont au-dessus de sa courbe*



Proposition III.4. *Si f est définie sur un intervalle I, alors f est convexe si, et seulement si, pour tout $a \in I$, la fonction :*

$$\tau_a : \left\{ \begin{array}{ccc} I \setminus \{a\} & \to & \mathbb{R} \\ x & \mapsto & \dfrac{f(x) - f(a)}{x - a} \end{array} \right.$$

est croissante.

Démonstration. Supposons que f est convexe. Fixons $a \in I$ et posons $x, y \in I \setminus \{a\}$ tels que $x < y$:

— si $x < y < a$: on écrit $y = tx + (1-t)a$ avec $t \in]0;1[$. On a ainsi : $y - a = t(x - a)$. Et donc :

$$\begin{array}{rcl} f \text{ convexe} & \Rightarrow & f(y) \leq tf(x) + (1-t)f(a) \\ & \Rightarrow & f(y) - f(a) \leq t\left(f(x) - f(a)\right) \\ & \Rightarrow & \dfrac{f(y) - f(a)}{y - a} \geq t \cdot \dfrac{f(x) - f(a)}{y - a} = \dfrac{f(x) - f(a)}{x - a} \end{array}$$

— si $x < a < y$: on écrit de même $a = tx + (1-t)y$ pour $t \in]0;1[$, et ainsi $t(a - x) = (1-t)(y - a)$. Et donc :

$$\begin{array}{rcl} f \text{ convexe} & \Rightarrow & f(a) \leq tf(x) + (1-t)f(y) \\ & \Rightarrow & t\left(f(a) - f(x)\right) \leq (1-t)\left(f(y) - f(a)\right) \\ & \Rightarrow & \dfrac{f(x) - f(a)}{x - a} = \dfrac{f(a) - f(x)}{a - x} \leq \dfrac{1-t}{t} \cdot \dfrac{f(y) - f(a)}{a - x} = \dfrac{f(y) - f(a)}{y - a} \end{array}$$

— si $a < x < y$: on écrit de même $x = at + (1-t)y$ pour $t \in]0;1[$, et ainsi $x - a = (1-t)(y-a)$. Et donc :

$$\begin{array}{rcl} f \text{ convexe} & \Rightarrow & f(x) \leq tf(a) + (1-t)f(y) \\ & \Rightarrow & f(x) - f(a) \leq (1-t)\left(f(y) - f(a)\right) \\ & \Rightarrow & \dfrac{f(x)-f(a)}{x-a} \leq (1-t) \cdot \dfrac{f(y)-f(a)}{x-a} = \dfrac{f(y)-f(a)}{y-a} \end{array}$$

Réciproquement, si toutes les fonctions τ_a sont croissantes : considérons $a, b \in I$ et $t \in [0;1]$. Montrons que $f(at + (1-t)b) \leq tf(a) + (1-t)f(b)$.
Les cas $t = 0$, $t = 1$ ou $a = b$ sont immédiats (l'inégalité est alors une égalité). Supposons donc $a < b$ et $t \in]0;1[$.
Quitte à échanger a et b et t par $1-t$, on peut supposer que $a < b$. Et ainsi : $a < ta + (1-t)b < b$. On a donc :

$$\begin{array}{rcl} \tau_a \text{ est croissante} & \Rightarrow & \dfrac{f(ta+(1-t)b)-f(a)}{ta+(1-t)b-a} \leq \dfrac{f(b)-f(a)}{b-a} \\ & \Rightarrow & \dfrac{f(ta+(1-t)b)-f(a)}{(1-t)(b-a)} \leq \dfrac{f(b)-f(a)}{b-a} \\ & \Rightarrow & f(ta+(1-t)b) \leq (1-t)\left(f(b)-f(a)\right) + f(a) \\ & \Rightarrow & f(ta+(1-t)b) \leq tf(a) + (1-t)f(b) \end{array}$$

ce qui prouve la convexité de f.

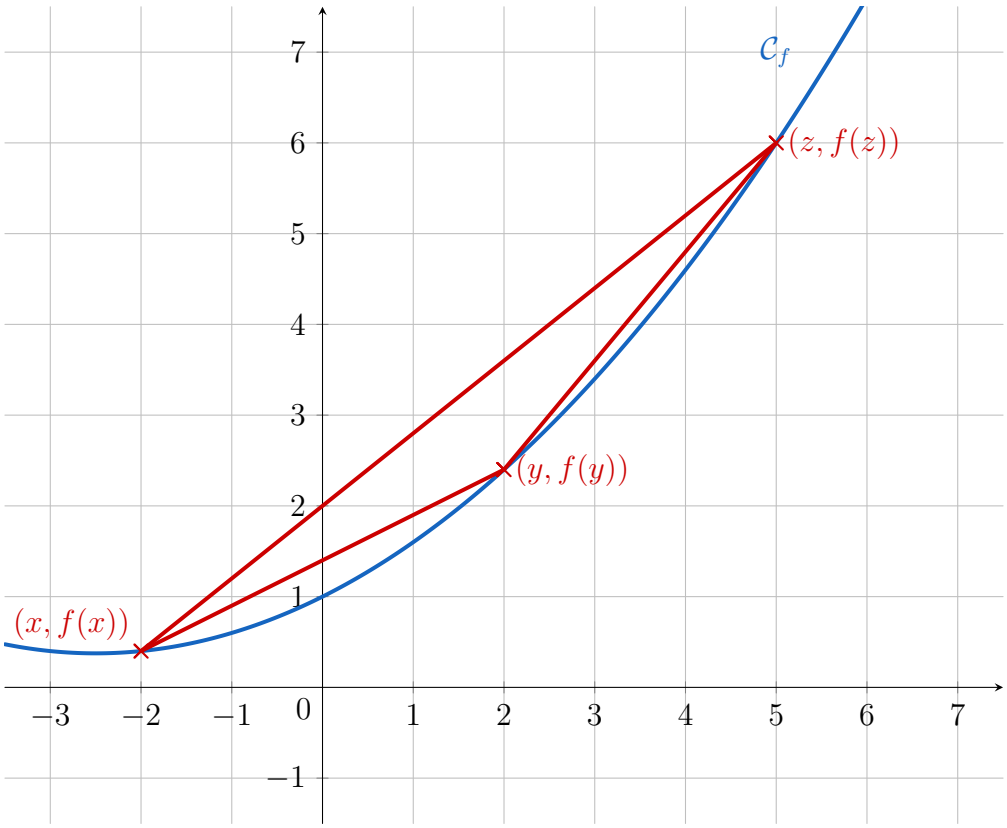
□

Corollaire III.5. *Une fonction f définie sur l'intervalle I est convexe si, et seulement si, elle vérifie l'une des trois assertions suivantes :*

1. *pour tous $x, y, z \in I$ avec $x < y < z$:* $\dfrac{f(y)-f(x)}{y-x} \leq \dfrac{f(z)-f(x)}{z-x}$;
2. *pour tous $x, y, z \in I$ avec $x < y < z$:* $\dfrac{f(z)-f(x)}{z-x} \leq \dfrac{f(z)-f(y)}{z-y}$;
3. *pour tous $x, y, z \in I$ avec $x < y < z$:* $\dfrac{f(y)-f(x)}{y-x} \leq \dfrac{f(z)-f(y)}{z-y}$.

Remarque III.6. *Ce résultat se comprend bien en terme de pentes. En combinant les trois inégalités précédentes, il vient que les pentes croissent de la manière suivante :*

$$\frac{f(y)-f(x)}{y-x} \leq \frac{f(z)-f(x)}{z-x} \leq \frac{f(z)-f(y)}{z-y}.$$



Corollaire III.7 (Convexité des fonctions dérivables)**.** *Une fonction f dérivable sur un intervalle I est convexe si, et seulement si, sa dérivée est croissante.*
En particulier, une fonction deux fois dérivable est convexe si, et seulement si, sa dérivée seconde est positive ou nulle.

Démonstration. On utilise la caractérisation précédente.
Si f est convexe : soient $a, b \in I$ avec $a < b$. Alors pour tout $x \in]a, b[$ on a :

$$\frac{f(a) - f(x)}{a - x} \leq \frac{f(a) - f(b)}{a - b} \leq \frac{f(b) - f(x)}{b - x}$$

puis en faisant tendre x vers a (dans le membre de gauche) et vers b (dans le membre de droite), on déduit que :

$$f'(a) \leq \frac{f(b) - f(a)}{b - a} \leq f'(b)$$

ce qui assure bien que f' est croissante.
Si f' est croissante. Considérons $a < x < b$. Alors par égalité des accroissements finis :

- il existe $c \in]a, x[$ tel que : $f'(c) = \dfrac{f(x) - f(a)}{x - a}$;
- il existe $d \in]x, b[$ tel que : $f'(d) = \dfrac{f(b) - f(x)}{b - x}$.

et par croissance de f' on déduit que : $\dfrac{f(x) - f(a)}{x - a} \leq \dfrac{f(b) - f(x)}{b - x}$. Donc f est bien convexe. □

Remarque III.8. *Ce résultat permet de savoir rapidement identifier une fonction convexe. Les autres propriétés s'utilisent dans un second temps pour exploiter la convexité.*

Exemple III.9. *La fonction* exp *est convexe sur* $\mathbb{R}$*, comme* $\exp'' = \exp \geq 0$.
Tout polynôme du second degré est convexe ou concave, selon le signe de son coefficient dominant. En effet, si $P = ax^2 + bx + c$ est un tel polynôme, alors $P'' = 2a$ est du signe de a.

Les fonctions affines sont les seules fonctions convexes et concaves.

La fonction ln *est deux fois dérivable sur* $\mathbb{R}_+^*$*, de dérivée* $x \mapsto \dfrac{1}{x}$ *qui est décroissante sur* $\mathbb{R}_+^*$ *(on peut voir aussi que* $\ln'' : x \mapsto -\dfrac{1}{x^2} \leq 0$*), donc elle est concave.*

Corollaire III.10. *Une fonction dérivable sur un intervalle* I *est convexe si, et seulement si, elle est au dessus de ses tangentes.*

Démonstration. Avec les notations précédentes, une fonction f est convexe si, et seulement si, toutes les fonctions τ_a sont croissantes.
Si f est dérivable, alors :

— τ_a est prolongeable par continuité en a ;
— τ_a est dérivable sur $I \setminus \{a\}$.

En particulier, elle elle croissante si, et seulement si, elle a une dérivée positive ou nulle. Mais si f est dérivable sur I, alors τ_a est dérivable sur $I \setminus \{a\}$ avec :

$$\forall x \in I \setminus \{a\},\ \tau_a'(x) = \frac{f'(x)(x-a) - (f(x) - f(a))}{(x-a)^2} = -\frac{f'(x)(a-x) + f(x) - f(a)}{(x-a)^2}$$

et ainsi f est convexe si, et seulement si, pour tous $x, a \in I$ tels que $x \neq a$:

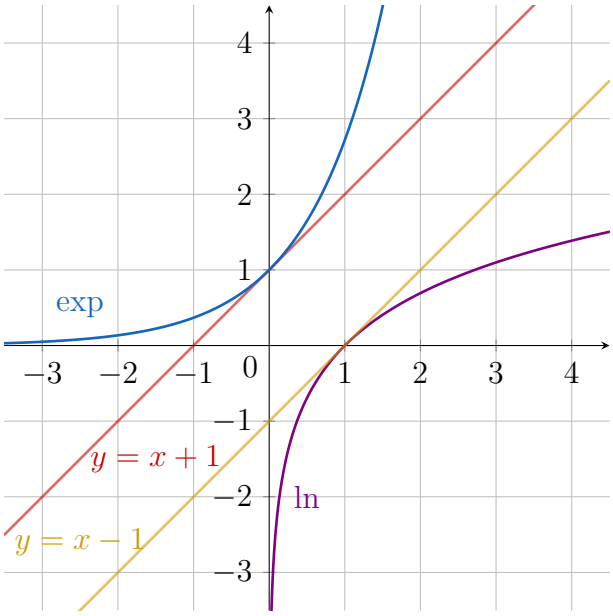
$$f(a) \geq f'(x)(a-x) + f(x)$$

c'est-à-dire que f est au dessus de ses tangentes. □

Remarque III.11. *On a en fait un résultat plus fort : en reprenant les monotonies des taux d'accroissements, on voit qu'une fonction convexe admet des dérivées à gauche et à droite en tout point intérieur à son ensemble de définition, et que le graphe d'une fonction convexe (même non dérivable) est au-dessus de ses demi-tangentes (qui sont alors bien définies.*

Exemple III.12. *La convexité de* exp *et la concavité de* ln*, en prenant leurs tangentes respectives en* 0 *et en* 1*, redonnent les inégalités classiques :*

$$\exp(x) \geq 1 + x \text{ et } \ln(1+x) \leq x$$



Proposition III.13 (Inégalité de Jensen)**.** *Soient f convexe sur un intervalle I, $n \in \mathbb{N}^*$ avec $n \geq 2$ $x_1, \ldots, x_n \in I$ et $\lambda_1, \ldots, \lambda_n \in \mathbb{R}_+$ tels que $\sum_{i=1}^n \lambda_i = 1$. Alors :*

$$f\left(\sum_{i=1}^n \lambda_i x_i\right) \leq \sum_{i=1}^n \lambda_i f(x_i).$$

Démonstration. Montrons par récurrence sur $n \geq 2$ que pour de tels $x_1, \ldots, x_n, \lambda_1, \ldots, \lambda_n$ on a :

$$\sum_{i=1}^n \lambda_i x_i \in I \text{ et } f\left(\sum_{i=1}^n \lambda_i x_i\right) \leq \sum_{i=1}^n \lambda_i f(x_i)$$

Si $n = 2$: c'est le fait que I est un intervalle (donc convexe) et la définition de la convexité de f avec $\lambda_1 = t$, $\lambda_2 = 1 - t$.
Supposons le résultat acquis au rang $n-1$ pour $n \geq 3$. Si $\lambda_1 = \cdots = \lambda_{n-1} = 0$, alors nécessairement $\lambda_n = 1$, donc on cherche à montrer que :

$$x_n \in I \text{ et } f(x_n) \leq f(x_n)$$

ce qui est vrai.
Sinon, posons :

$$t = \sum_{i=1}^{n-1} \lambda_i > 0, \ x = \sum_{i=1}^{n-1} \frac{\lambda_i}{t} x_i$$

avec $x \in I$ par hypothèse de récurrence (comme $\sum_{i=1}^{n-1} \frac{\lambda_i}{t} = 1$).
On a alors $\lambda_n = 1 - t$, ce qui assure déjà que :

$$\sum_{i=1}^{n-1} \lambda_i x_i = tx + (1-t)x_n \in I$$

Et par convexité de f :

$$f\left(\sum_{i=1}^n \lambda_i x_i\right) = f\left(tx + (1-t)x_n\right) \leq tf(x) + (1-t)f(x_n)$$

et par hypothèse de récurrence on a : $f(x) \leq \sum_{i=1}^{n-1} \frac{\lambda_i}{t} f(x_i)$. Donc finalement :

$$f\left(\sum_{i=1}^n \lambda_i x_i\right) \leq \sum_{i=1}^n \lambda_i f(x_i).$$

□

Exemple III.14. *On peut appliquer l'inégalité de Jensen pour comparer des moyennes.*
Pour $n \in \mathbb{N}^*$ et $x_1, \ldots, x_n \in \mathbb{R}_+^*$, on définit leurs moyennes :

- *arithmétique (appelée plus simplement "moyenne") : $M_a = \dfrac{x_1 + \cdots + x_n}{n}$;*
- *harmonique : $M_h = \dfrac{n}{\frac{1}{x_1} + \cdots + \frac{1}{x_n}}$ (l'inverse de la moyenne harmonique est la moyenne des inverses) ;*
- *géométrique : $M_g = \sqrt[n]{x_1 \ldots x_n}$ (le logarithme de la moyenne géométrique est la moyenne des logarithmes) ;*
- *quadratique : $M_q = \sqrt{\dfrac{x_1^2 + \cdots + x_n^2}{n}}$ (le carré de la moyenne quadratique est la moyenne des carrés).*

On a alors les inégalités :

$$M_h \leq M_g \leq M_a \leq M_q$$

avec égalité si, et seulement si, tous les x_i *sont égaux.*
Montrons les trois inégalités :

— *par concavité de la fonction* ln, *on trouve que :*

$$\ln\left(\frac{1}{M_h}\right) \geq \frac{1}{n}\sum_{i=1}^{n} \ln\left(\frac{1}{x_i}\right)$$

et donc :

$$\ln(M_h) \leq \frac{1}{n}\sum_{i=1}^{n} \ln(x_i) = \ln(M_g)$$

ce qui donne la première inégalité par croissance de ln *;*

— *par concavité de la fonction* ln, *on a de même :*

$$\ln(M_g) = \frac{1}{n}\sum_{i=1}^{n} \ln(x_i) \leq \ln\left(\frac{1}{n}\sum_{i=1}^{n} x_i\right) = \ln(M_a)$$

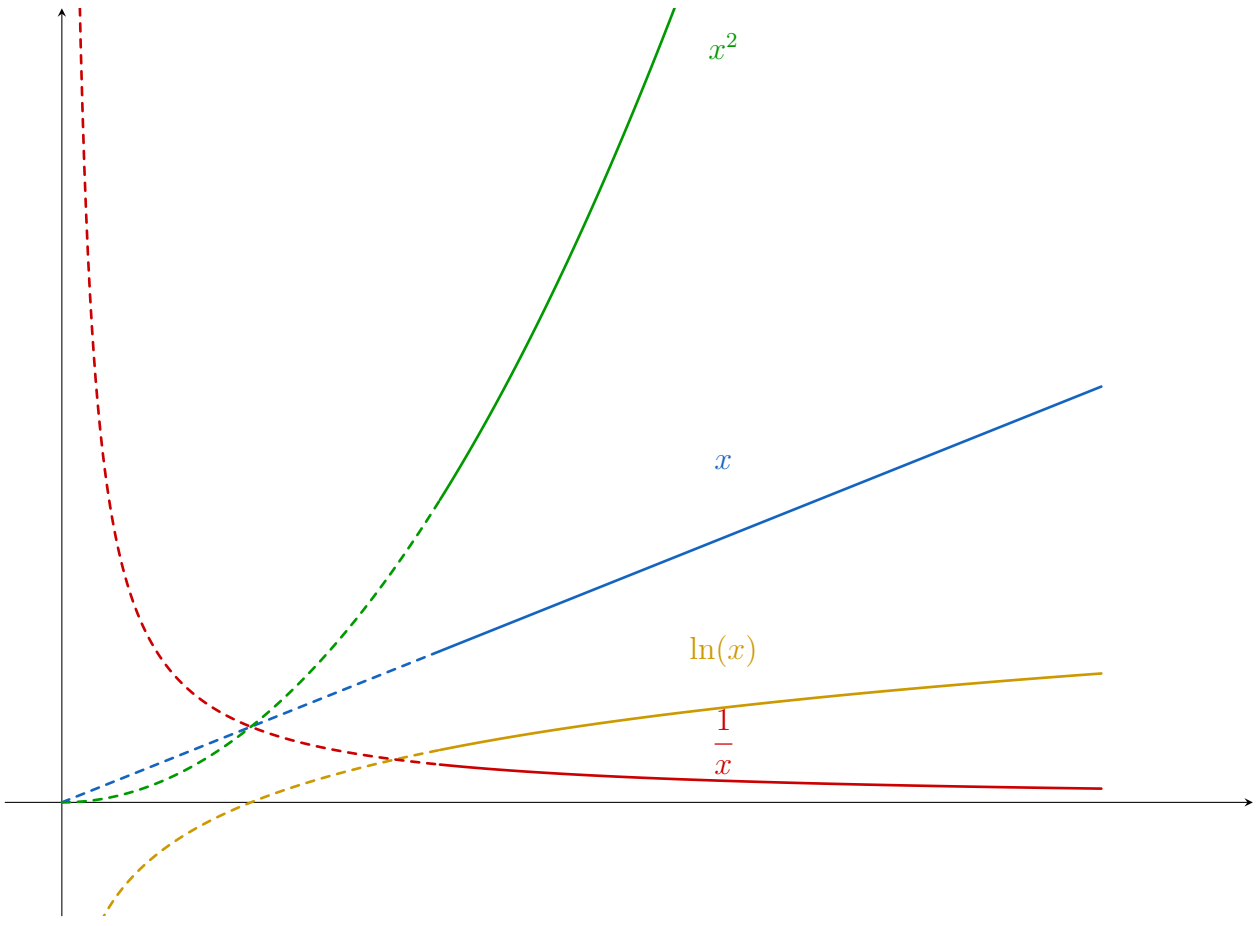
et donc par croissance de ln *on a la deuxième inégalité ;*

— *par convexité de la fonction carré, on a :*

$$M_a^2 = \left(\frac{1}{n}\sum_{i=1}^{n} x_i\right) \leq \frac{1}{n}\sum_{i=1}^{n} x_i^2 = M_q^2$$

d'où l'inégalité par croissance de $x \mapsto x^2$ *sur* $\mathbb{R}_+$.

En fait, ces moyenne sont triées dans le même ordre que les fonctions qui leur correspondent au voisinage de $+\infty$.



Chapitre 19

Analyse asymptotique

Pour tout ce chapitre, on considère I un sous-ensemble de $\mathbb{R}$, et $a \in \overline{\mathbb{R}}$ adhérent à I.

I Relations de comparaisons

I.1 Négligeabilité, domination et équivalence

Définition I.1. *Soient f et g deux fonctions définies sur I. On dit que :*

1. *f est **négligeable devant** g **au voisinage de** a, ce que l'on note $f(x) \underset{x\to a}{=} \mathrm{o}(g(x))$, s'il existe une fonction ε définie sur un voisinage V_a de a, qui tend vers 0 en a, telle que : pour tout $x \in I \cap V_a$, $f(x) = \varepsilon(x)g(x)$;*
2. *f est **dominée par** g **au voisinage de** a, ce que l'on note $f(x) \underset{x\to a}{=} \mathrm{O}(g(x))$, s'il existe une fonction M définie sur un voisinage V_a de a, bornée, telle que : pour tout $x \in I \cap V_a$, $f(x) = M(x)g(x)$.*

Remarque I.2. *Pour la domination, cela revient à imposer l'existence de $M \in \mathbb{R}_+$ tel que, sur un voisinage de a : $|f(x)| \leq M \cdot |g(x)|$.*

Exemples I.3.

1. *si $a = +\infty$, on a vu que $x \underset{x\to+\infty}{=} \mathrm{o}(e^x)$ et que $\ln(x) \underset{x\to+\infty}{=} \mathrm{o}(x)$.*
2. *si f et g sont deux fonctions continues en $a \in \mathbb{R}$, avec g qui ne s'annule pas, alors : $f(x) \underset{x\to a}{=} \mathrm{o}(g(x))$ si, et seulement si, $f(a) = 0$; et peu importe la valeur de f on a toujours $f(x) \underset{x\to a}{=} \mathrm{O}(g(x))$*

Remarques I.4.

1. *Quant il n'y aura pas d'ambiguïté sur la valeur de a, on pourra écrire plus simplement $f(x) = \mathrm{o}(g(x))$ (ou O). On prendra bien garde à cette notation comme la relation entre deux fonctions dépend du point en lequel on les compare. Par exemple :*

$$\cos(x) \underset{x\to\pm\infty}{=} \mathrm{o}(x) \text{ mais } x \underset{x\to 0}{=} \mathrm{o}(\cos(x)).$$

2. *Comme une fonction ayant une limite finie est bornée, la notion de o est plus forte que celle de O dans le sens où :*

$$f(x) \underset{x\to a}{=} \mathrm{o}(g(x)) \Rightarrow f(x) \underset{x\to a}{=} \mathrm{O}(g(x)).$$

Proposition I.5. *Si f, g sont définies sur I et que g ne s'annule pas sur $I \setminus \{a\}$, alors :*

1. $f(x) \underset{x\to a}{=} \mathrm{o}(g(x)) \Leftrightarrow \lim\limits_{x\to a} \dfrac{f(x)}{g(x)} = 0$;

2. $f(x) \underset{x\to a}{=} \mathrm{O}(g(x)) \Leftrightarrow \dfrac{f(x)}{g(x)}$ *est bornée sur un voisinage de* a.

Démonstration. Pour un tel g, les fonctions ε ou M de la définition coïncident avec la fonction $\frac{f}{g}$. □

Corollaire I.6 (Comparaison à des fonctions constantes)**.** *On note* 1 *la fonction constante de valeur* 1 *définie sur* I. *Pour* f *définie sur* I, *on a :*

1. $f(x) \underset{x\to a}{=} \mathrm{o}(1)$ *si, et seulement si,* $\lim\limits_{x\to a} f(x) = 0$;
2. $f(x) \underset{x\to a}{=} \mathrm{O}(1)$ *si, et seulement si,* f *est bornée sur un voisinage de* a.

Définition I.7. *Si* f *et* g *sont deux fonctions définies sur* I, *on dit que* f ***est équivalente à*** g ***au voisinage de*** a, *ce que l'on note* $f(x) \underset{x\to a}{\sim} g(x)$, *si* $f(x) \underset{x\to a}{=} g(x) + \mathrm{o}(g(x))$.

Remarque I.8. *On peut aussi dire que* $f(x) - g(x) \underset{x\to a}{=} \mathrm{o}(g(x))$, *ce qui revient au même.*

Proposition I.9. *Si* f, g *sont définies sur* I *et que* g *ne s'annule pas sur* $I \setminus \{a\}$, *alors :*

$$f(x) \underset{x\to a}{\sim} g(x) \Leftrightarrow \lim_{x\to a} \frac{f(x)}{g(x)} = 1.$$

Démonstration. Découle du résultat sur les "o". □

Exemple I.10. *On a :* $\sin(x) \underset{x\to 0}{\sim} x$, *comme on avait vu que :* $\lim\limits_{x\to 0} \dfrac{\sin(x)}{x} = 1$.
De même, on a : $(e^x - 1) \underset{x\to 0}{\sim} x$ *par limite classique.*

Remarque I.11. *Cette caractérisation, comme celle sur les* o *et* O, *est beaucoup plus pratique pour comprendre les relations entre deux fonctions. D'autant plus que le fait d'imposer que* g *ne s'annule pas ne réduit que très peu le cadre d'utilisation.*
En revanche, l'utilisation des o *et des* O, *comme on le verra après, se comporte très bien avec les calculs, ce qui n'est pas toujours le cas des équivalents, qui ne sont pas aussi précis.*

Proposition I.12. *Si* f, g *sont définies sur* I, *et* $\lambda \in \mathbb{R}$, *alors :*

$$\Big(f(x) \underset{x\to a}{=} \mathrm{o}(g(x)) \text{ ou } f(x) \underset{x\to a}{\sim} \lambda g(x)\Big) \Rightarrow f(x) \underset{x\to a}{=} \mathrm{O}(g(x)).$$

Démonstration. Dans l'une ou l'autre des situations, on écrit $f(x) = h(x)g(x)$ avec $h(x)$ qui a une limite finie, donc h est bornée au voisinage de a. □

Remarque I.13. *La réciproque est fausse : il existe des fonctions dominées qui ne sont ni négligeables ni des équivalents. Mais l'idée est que ces deux cas extrêmes couvrent déjà beaucoup de situations, ce qui fait qu'on ne travaillera pas beaucoup avec des* O.

Proposition I.14. *Si* $l \in \mathbb{R}^*$, *et* f *une fonction définie sur* I, *alors* $f(x) \underset{x\to a}{\sim} l$ *si, et seulement si,* $\lim\limits_{x\to a} f(x) = l$.

Démonstration. Comme $l \neq 0$, on peut utiliser la caractérisation de l'équivalence par quotient, et on a :

$$f(x) \underset{x\to a}{\sim} l \Leftrightarrow \frac{f(x)}{l} \underset{x\to a}{\to} 1 \Leftrightarrow f(x) \underset{x\to a}{\to} l$$

□

Proposition I.15. *La relation* $\underset{x\to a}{\sim}$ *est une relation d'équivalence sur l'ensemble des fonctions définies sur* I.

Démonstration. Soit f, g, h définies sur I :
- avec $\varepsilon = 0$, on trouve que $0 = \mathrm{o}(f(x))$ et donc $f(x) = f(x) + 0 = f(x) + \mathrm{o}(f(x)) \sim f(x)$.
- si $f(x) \sim g(x)$, en notant ε qui tend vers 0 tel que $f(x) = g(x) + \varepsilon(x)g(x) = (1+\varepsilon(x))g(x)$. Comme ε tend vers 0, alors quitte à restreindre le voisinage de a considéré on peut supposer que $1 + \varepsilon$ ne s'annule pas. Et donc :
$$g(x) = \frac{f(x)}{1+\varepsilon(x)} = f(x) + f(x) \cdot \underbrace{\frac{-\varepsilon(x)}{1+\varepsilon(x)}}_{=\varepsilon'(x)}$$
avec ε' qui tend vers 0, donc $g(x) \sim f(x)$;
- si $f(x) \sim g(x)$ et $g(x) \sim h(x)$, en notant $\varepsilon_1, \varepsilon_2$ qui tendent vers 0 tels que $f(x) = g(x)(1+\varepsilon_1)$ et $g(x) = h(x)(1+\varepsilon_2)$, alors $f(x) = (1+\varepsilon_1)(1+\varepsilon_2)h(x)$ donc $f(x) \sim h(x)$.

Ce qui montre bien la réflexivité, la symétrie et la transitivité : on a bien une relation d'équivalence. □

Remarque I.16. *On voit au passage que c'est plus $(1 + \varepsilon)$ qui compte pour les équivalents, et donc on utilisera parfois la définition équivalente que f et g sont équivalentes s'il existe une fonction θ définie sur un voisinage V_a de a, qui tend vers 1 en a, telle que : pour tout $x \in I \cap V_a$, $f(x) = \theta(x)g(x)$.*

Proposition I.17. *Si $f(x) \underset{x\to a}{\sim} g(x)$, alors sur un voisinage de a les fonctions f et g ont le même signe.*

Démonstration. On écrit $f(x) = \theta(x)g(x)$, pour θ tendant vers 1 au voisinage de a. Alors par définition de la limite, pour un voisinage V_a de a, on a : $\theta(x) \in [\frac{1}{2}; \frac{3}{2}]$. Et donc $\theta(x) > 0$ dans un voisinage de a, ce qui donne bien le résultat. □

Proposition I.18. *Si $f(x) \underset{x\to a}{=} \mathrm{O}(g(x))$ et $g(x) \underset{x\to a}{=} \mathrm{o}(h(x))$, alors $f(x) \underset{x\to a}{=} \mathrm{o}(h(x))$*

Démonstration. On écrit au voisinage de a : $f(x) = M(x)g(x)$ et $g(x) = \varepsilon(x)h(x)$, de sorte que $f(x) = \underbrace{M(x)\varepsilon(x)}_{=\varepsilon'(x)} h(x)$, où $\varepsilon'(x)$ tend vers 0 par encadrement. □

Remarque I.19. *Comme un* o *est aussi un* O*, alors le résultat est vrai avec un* o*.*

Proposition I.20. *Si $f(x) \underset{x\to a}{\sim} g(x)$, alors f a une limite en a si, et seulement si, g en a une, et dans ce cas les limites sont égales.*

Démonstration. Comme $\sim$ est une relation d'équivalence, il suffit de montrer une implication.
Si g possède une limite, comme $f = \theta \cdot g$, avec θ qui tend vers 1, alors par opération sur les limites f a même limite que g. □

Proposition I.21. *Si f, g, h sont définies sur I avec $f \leq g \leq h$ et $f(x) \underset{x\to a}{\sim} h(x)$, alors $g(x) \underset{x\to a}{\sim} f(x)$.*

Démonstration. Par l'inégalité vérifiée par f, g, h on a :
$$0 \leq g - f \leq h - f$$
et donc par encadrement : $g(x) - f(x) \underset{x\to a}{=} \mathrm{O}(h(x) - f(x)) \underset{x\to a}{=} \mathrm{o}(f(x))$. Ce qui donne la relation d'équivalence. □

I.2 Opérations sur les relations de comparaison

Remarque I.22. *Les* o *ou les* O *ne se valent pas : par exemple, au voisinage de l'infini, on a que* $x = \mathrm{o}(e^x)$ *et* $\ln(x) = \mathrm{o}(e^x)$*, mais* x *et* $\ln(x)$ *ne sont pas du tout égaux (et même* $\ln(x)$ *est négligeable devant* x*).*

Proposition I.23 (Opérations sur les o et les O)**.** *Soient* f, g, h *des fonctions définies sur* I*. Alors :*

1. *si* $\lambda \in \mathbb{R}^*$ *et* $f(x) \underset{x\to a}{=} \mathrm{o}(g(x))$*, alors* $f(x) \underset{x\to a}{=} \mathrm{o}(\lambda g(x))$ *et* $\lambda f(x) \underset{x\to a}{=} \mathrm{o}(g(x))$ *;*
2. *si* $f(x) \underset{x\to a}{=} \mathrm{o}(h(x))$ *et* $g(x) \underset{x\to a}{=} \mathrm{o}(h(x))$*, alors* $f(x) + g(x) \underset{x\to a}{=} \mathrm{o}(h(x))$ *;*
3. *si* $f(x) \underset{x\to a}{=} \mathrm{o}(g(x))$ *et* $g(x) \underset{x\to a}{=} \mathrm{o}(h(x))$*, alors* $f(x) \underset{x\to a}{=} \mathrm{o}(h(x))$ *(transitivité) ;*
4. *si* $f_1(x) \underset{x\to a}{=} \mathrm{o}(g_1(x))$ *et* $f_2(x) \underset{x\to a}{=} \mathrm{o}(g_2(x))$*, alors* $f_1(x)f_2(x) \underset{x\to a}{=} \mathrm{o}(g_1(x)g_2(x))$ *;*
5. *si* $n \in \mathbb{N}^*$ *et* $f(x) \underset{x\to a}{=} \mathrm{o}(g(x))$*, alors* $f(x)^n \underset{x\to a}{=} \mathrm{o}(g(x)^n)$ *;*
6. *si* $f(x) \underset{x\to a}{=} \mathrm{o}(g(x))$*, alors* $f(x)h(x) \underset{x\to a}{=} \mathrm{o}(g(x)h(x))$ *;*
7. *si* f *et* g *ne s'annulent pas, alors :* $f(x) \underset{x\to a}{=} \mathrm{o}(g(x)) \Leftrightarrow \dfrac{1}{g(x)} \underset{x\to a}{=} \mathrm{o}\left(\dfrac{1}{f(x)}\right)$ *;*
8. $f(x) \underset{x\to a}{=} \mathrm{o}(g(x)) \Leftrightarrow |f(x)| \underset{x\to a}{=} \mathrm{o}(|g(x)|)$.

Démonstration.

1. On pose ε qui tend vers 0 en a telle que $f(x) = \varepsilon(x)g(x)$ sur V_a. Alors, selon le cas considéré, $\frac{\varepsilon}{\lambda}$ ou $\lambda\varepsilon$ convient, ce qui montre le résultat.
2. On pose $\varepsilon_1, \varepsilon_2$ qui tendent vers 0 en a telles que $f(x) = \varepsilon_1(x)h(x)$ sur V_a et $g(x) = \varepsilon_2(x)h(x)$ sur W_a. Alors, sur $V_a \cap W_a$ on a : $(f(x) + g(x)) = (\varepsilon_1(x) + \varepsilon_2(x))h(x)$, avec $\varepsilon_1 + \varepsilon_2$ qui tend bien vers 0 en a (par limite d'une somme).
3. En notant $\varepsilon_1, \varepsilon_2$ qui tendent vers 0 en a telles que $f(x) = \varepsilon_1(x)g(x)$ sur V_a et $g(x) = \varepsilon_2(x)h(x)$ sur W_a. Alors, sur $V_a \cap W_a$ on a : $f(x) = (\varepsilon_1(x) \cdot \varepsilon_2(x))h(x)$, avec $\varepsilon_1 \cdot \varepsilon_2$ qui tend bien vers 0 en a (par limite d'un produit).

   Et les autres points se montrent pareil. Notons qu'on peut simplifier nettement les démonstrations dans le cas où les fonctions ne s'annulent pas, car il suffit de calculer des limites de quotients.

□

Remarque I.24. *Tous les résultats ci-dessus restent valables en changeant les* o *en des* O*. Mais en pratique on utilisera surtout des* o *(qui sont plus précis, même s'ils conduisent parfois à des calculs un peu plus lourds).*
Dans cette optique d'alléger les calculs, on essaiera le plus possible de regrouper les termes dans les o *: aussi bien les différents* o *qui interviennent, que certains termes qui seraient en dehors.*

Corollaire I.25. *Si* f *est définie sur* I*, alors :*

1. $1 \underset{x\to a}{=} \mathrm{O}(f(x))$ *si, et seulement si,* $\left|\dfrac{1}{f(x)}\right|$ *est majorée sur un voisinage de* a *;*
2. $1 \underset{x\to a}{=} \mathrm{o}(f(x))$ *si, et seulement si,* $|f|$ *tend vers* $+\infty$ *en* a*.*

Remarque I.26. *On prend bien garde à sommer* ***les*** o *et pas* ***dans les*** o*. Par exemple, on a* $\ln(x) \underset{x\to+\infty}{=} \mathrm{o}(x)$ *et* $\ln(x) \underset{x\to+\infty}{=} \mathrm{o}(-x)$*. Mais* $2\ln(x) \underset{x\to+\infty}{\neq} \mathrm{o}(x - x) \underset{x\to+\infty}{=} \mathrm{o}(0)$.
De fait, pour sommer des o *différents, il faudra d'abord les exprimer comme des* o *d'une même quantité.*

Exemple I.27. *On considère f, g deux fonctions définies sur $\mathbb{R}$ telles que $f(x) \underset{x\to+\infty}{=} 4 + \frac{1}{x} + \mathrm{o}\left(\frac{1}{x^2}\right)$ et $g(x) \underset{x\to+\infty}{=} 3x + 2 + \mathrm{o}(1)$. Alors :*

$$\begin{aligned} f(x)g(x) &\underset{x\to+\infty}{=} \left(4 + \frac{1}{x} + \mathrm{o}\left(\frac{1}{x}\right)\right) \cdot (3x + 2 + \mathrm{o}(1)) \\ &\underset{x\to+\infty}{=} 12x + 11 + \underbrace{\frac{2}{x} + \mathrm{o}(1) + \mathrm{o}\left(\frac{1}{x}\right)}_{=\mathrm{o}(1)} \end{aligned}$$

qui ne peut pas être davantage simplifiée comme expression, comme ni $12x$ ni 11 ne tendent vers 0 en $+\infty$ (donc ne sont des $\mathrm{o}(1)$).

Proposition I.28 (Opérations sur les équivalents)**.** *Soient f, g, h des fonctions définies sur I. Alors :*

1. *si $f_1(x) \underset{x\to a}{\sim} g_1(x)$ et $f_2(x) \underset{x\to a}{\sim} g_2(x)$, alors $f_1(x)f_2(x) \underset{x\to a}{\sim} g_1(x)g_2(x)$;*
2. *si $n \in \mathbb{N}^*$ et $f(x) \underset{x\to a}{\sim} g(x)$, alors $f(x)^n \underset{x\to a}{\sim} g(x)^n$;*
3. *si $f(x) \underset{x\to a}{\sim} g(x)$, alors $f(x)h(x) \underset{x\to a}{\sim} g(x)h(x)$;*
4. *si f ou g ne s'annule pas, alors $f(x) \underset{x\to a}{\sim} g(x) \Leftrightarrow \frac{1}{f(x)} \underset{x\to a}{\sim} \frac{1}{g(x)}$;*
5. *si f ou g est positive, et $f(x) \underset{x\to a}{\sim} g(x)$, alors pour tout $\alpha \in \mathbb{R}$: $f(x)^\alpha \underset{x\to a}{\sim} g(x)^\alpha$.*

Démonstration. Comme pour les o. Notons juste que le dernier résultat n'apparaissait pas pour les o, parce qu'il est faux en général. Pour les équivalents, il vient du fait que :

$$\frac{f(x)^\alpha}{g(x)^\alpha} = \left(\frac{f(x)}{g(x)}\right)^\alpha$$

et donc, par continuité de $x \mapsto x^\alpha$ pour tout $\alpha \in \mathbb{R}$, si $\frac{f(x)}{g(x)}$, tend vers 1, alors $\left(\frac{f(x)}{g(x)}\right)^\alpha$ tend vers $1^\alpha = 1$. □

Remarque I.29. *On ne somme **jamais** des équivalents : pour avoir un équivalent d'une somme, on est obligé de repasser par les* o.
Par exemple : $x + 1 \underset{x\to+\infty}{\sim} x$ et $-x + 1 \underset{x\to+\infty}{\sim} -x$, mais $x + 1 - x + 1 = 2 \underset{x\to+\infty}{\not\sim} 0 = x - x$.

Proposition I.30. *Si f, g, h sont définie sur I avec $f \underset{x\to a}{=} \mathrm{o}(g(x))$ et $g(x) \underset{x\to a}{\sim} h(x)$, alors $f \underset{x\to a}{=} \mathrm{o}(h(x))$.*

Démonstration. On écrit $f(x) = \varepsilon(x)g(x)$ et $g(x) = \theta(x)h(x)$ avec ε qui tend vers 0 en a et θ qui tend vers 1.
Alors $f(x) = \underbrace{(\varepsilon(x)\theta(x))}_{=\varepsilon'(x)} h(x)$, avec $\varepsilon'(x)$ qui tend vers 0.
D'où le résultat. □

Proposition I.31 (Composition à droite)**.** *On considère $\varphi : J \to I$ et $b \in \overline{J}$ tel que $\lim_{x\to b} \varphi(x) = a$. Alors pour f, g définies sur I :*

1. *si $f(x) \underset{x\to a}{=} \mathrm{o}(g(x))$, alors $(f \circ \varphi)(x) \underset{x\to b}{=} \mathrm{o}((g \circ \varphi)(x))$;*
2. *si $f(x) \underset{x\to a}{\sim} g(x)$, alors $(f \circ \varphi)(x) \underset{x\to b}{\sim} (g \circ \varphi)(x)$.*

Démonstration. Par composition des limites. Les fonctions ε et θ que l'on utilise dans les hypothèses se substituent aux fonctions $\varepsilon \circ \varphi$ et $\theta \circ \varphi$ qui donnent les résultats. □

Remarques I.32.

1. *Dans le premier résultat, on peut remplacer les* o *par des* O.
2. *Un cas très utile est lorsque φ est une translation : on peut ainsi ramener l'étude locale d'une fonction f au voisinage de $a \neq 0$ en étudiant en 0 la fonction $x \mapsto f(x+a)$.*
3. *Les compositions à gauche se comportent moins bien en général. On ne donnera que quelques cas particuliers.*

Exemple I.33. *On a vu que* $\sin(x) \underset{x\to 0}{\sim} x$. *Comme* $\lim_{x\to 0} x\cdot\ln(x) = 0$, *alors on déduit que :*

$$\sin(x\cdot\ln(x)) \underset{x\to 0}{\sim} x\cdot\ln(x).$$

Et on déduit ainsi que :

$$\frac{\sin(x\cdot\ln(x))}{x} \underset{x\to 0}{\sim} \ln(x) \text{ donc } \lim_{x\to 0}\frac{\sin(x\cdot\ln(x))}{x} = -\infty.$$

De même, comme $\lim_{x\to+\infty}\dfrac{\ln(x)}{x} = 0$, *alors :*

$$\sin\left(\frac{\ln(x)}{x}\right) \underset{x\to+\infty}{\sim} \frac{\ln(x)}{x}.$$

Et on déduit ainsi que :

$$\sqrt{x}\sin\left(\frac{\ln(x)}{x}\right) \underset{x\to+\infty}{\sim} \frac{\ln(x)}{\sqrt{x}} \text{ donc } \lim_{x\to+\infty}\sqrt{x}\sin\left(\frac{\ln(x)}{x}\right) = 0.$$

Proposition I.34. *Si f, g sont définies sur I, alors :*

1. $e^{f(x)} \underset{x\to a}{\sim} e^{g(x)}$ *si, et seulement si,* $\lim_{x\to a}(f(x)-g(x)) = 0$;
2. *si* $f(x) \underset{x\to a}{\sim} g(x)$, *avec f (ou g) positive, tendant vers $l \in \overline{\mathbb{R}}\setminus\{1\}$ en a, alors :* $\ln(f(x)) \underset{x\to a}{\sim} \ln(g(x))$.

Démonstration.

1. Par équivalences, on a, comme l'exponentielle ne s'annule jamais :

$$\begin{aligned} e^{f(x)} \underset{x\to a}{\sim} e^{g(x)} &\Leftrightarrow \frac{e^{f(x)}}{e^{g(x)}} \underset{x\to a}{\to} 1 \\ &\Leftrightarrow e^{f(x)-g(x)} \underset{x\to a}{\to} 1 \\ &\Leftrightarrow f(x)-g(x) \underset{x\to a}{\to} 0 \end{aligned}$$

   par continuité de exp et de ln pour la dernière équivalence.

2. Avec les conditions imposées, on a que $\dfrac{f(x)}{g(x)} \underset{x\to a}{\to} 1$ et $\ln(g(x)) \to \ln(l) \neq 0$. Donc $\ln(g(x))$ ne s'annule pas sur un voisinage de a et sur ce voisinage :

$$\frac{\ln(f(x))}{\ln(g(x))} = \frac{\ln(g(x))+\ln(f(x))-\ln(g(x))}{\ln(g(x))} = 1+\frac{\ln\left(\frac{f(x)}{g(x)}\right)}{\ln(g(x))} \underset{x\to a}{\to} 1+\frac{0}{\ln(l)} = 1$$

   d'où le résultat.

□

Remarques I.35.

1. *Le cas de* exp *a une utilité assez limitée en fait puisque :*
   — *avec* $f(x) = x$ *et* $g(x) = x+1$, *on a* $f(x) \underset{x\to+\infty}{\sim} g(x)$ *mais* $e^{f(x)} \underset{x\to+\infty}{\not\sim} e^{g(x)}$;
   — *avec* $f(x) = \frac{1}{x}$ *et* $g(x) = \frac{1}{x^2}$ *on a* $e^{f(x)} \underset{x\to0}{\sim} e^{g(x)}$ *mais* $f(x) \underset{x\to0}{\not\sim} g(x)$.
2. *Pour le logarithme, il faut bien faire attention à ce que la limite ne soit pas* 1, *et la réciproque est fausse :*
   (a) *avec* $f(x) = 1+x$ *et* $g(x) = 1+x^2$, *on a* $f(x) \underset{x\to0}{\sim} g(x) \underset{x\to0}{\sim} 1$, *mais* $\ln(f(x)) \underset{x\to0}{\sim} x \underset{x\to0}{\not\sim} x^2 \underset{x\to0}{\sim} \ln(g(x))$;
   (b) *avec* $f(x) = x$ *et* $g(x) = 2x$, *on a* $\ln(f(x)) = \ln(x) \underset{x\to+\infty}{\sim} \ln(x) + \ln(2) = \ln(g(x))$ *mais* $f(x) \underset{x\to+\infty}{\not\sim} g(x)$.

I.3 Exemples fondamentaux

Remarque I.36. *Si on travaille avec des fonctions continues, le cas intéressant est lorsque les limites considérées sont nulles, ou infinies : dans les autres cas, les relations de comparaison n'apportent pas grand chose dans la compréhension des fonctions.*
C'est justement là où les relations de comparaisons sont importantes : elles lèvent les formes indéterminées en disant plus précisément à quel point une quantité est grande ou petite.

Théorème I.37 (Croissances comparées en $+\infty$)**.** *On a les relation de comparaisons suivantes :*

1. *si* $\alpha, \beta \in \mathbb{R}$ *:* $\alpha < \beta \Leftrightarrow x^\alpha \underset{x\to+\infty}{=} x^\beta$;
2. *si* $a, b \in \mathbb{R}_+^*$ *:* $a < b \Leftrightarrow a^x \underset{x\to+\infty}{=} \mathrm{o}(b^x)$;
3. *si* $\alpha, \beta \in \mathbb{R}_+^*$ *:* $(\ln(x))^\alpha \underset{x\to+\infty}{=} \mathrm{o}\left(x^\beta\right)$;
4. *si* $\alpha, \beta \in \mathbb{R}_+^*$ *:* $x^\alpha \underset{x\to+\infty}{=} \mathrm{o}\left(e^{\beta x}\right)$.

Démonstration. Découle des limites classiques et des croissances comparées. Dans chaque cas, comme les fonctions ne s'annulent pas, on peut étudier la limite du quotient. □

Théorème I.38 (Croissances comparées en 0)**.** *On a les relations de comparaisons suivantes :*

1. *si* $\alpha, \beta \in \mathbb{R}$, *alors :* $\alpha > \beta \Leftrightarrow x^\alpha \underset{x\to0}{=} \mathrm{o}\left(x^\beta\right)$;
2. *si* $\alpha > 0$ *et* $\beta \in \mathbb{R}$ *:* $x^\alpha \underset{x\to0}{=} \mathrm{o}\left(|\ln(x)|^\beta\right)$.

Démonstration. Idem. □

Corollaire I.39. *Une fonction polynomiale non nulle est équivalente à son monôme de plus haut degré en* $\pm\infty$ *et à son monôme de plus petit degré en* 0. *Concrètement, si* $f : x \mapsto a_n x^n + a_{n-1}x^{n-1} + \cdots + a_m x^m$, *avec* $m \leq n$ *et* $a_n, a_m \neq 0$, *alors :*

$$f(x) \underset{x\to\pm\infty}{\sim} a_n x^n \text{ et } f(x) \underset{x\to0}{\sim} a_m x^m.$$

Démonstration. Avec les mêmes notations, il vient que :
— pour tout $k > m$: $x^k \underset{x\to0}{=} \mathrm{o}(x^m)$;
— pour tout $k < n$: $x^k \underset{x\to\pm\infty}{=} \mathrm{o}(x^n)$;
et ainsi en sommant :

$$f(x) \underset{x\to0}{=} a_m x^m + \mathrm{o}(x^m) \underset{x\to0}{\sim} a_m x^m \text{ et } f(x) \underset{x\to\pm\infty}{=} a_n x^n + \mathrm{o}(x^n) \underset{x\to\pm\infty}{\sim} a_n x^n.$$

□

Proposition I.40. *Si f est dérivable en a, alors :*

$$f(x) \underset{x\to a}{=} f(a) + f'(a)(x-a) + \mathrm{o}(x-a).$$

En particulier, si $f'(a) \neq 0$, alors :

$$f(x) - f(a) \underset{x\to a}{\sim} f'(a)\cdot(x-a).$$

Démonstration. Démontré au chapitre précédent. □

Remarque I.41. *Inversement, si on peut trouver une écriture du type $f(x) \underset{x\to a}{=} f(a) + l(x-a) + \mathrm{o}(x-a)$, on avait vu que f est dérivable en a, de dérivée $f'(a) = l$.*
Et la version avec des équivalents aussi peut s'utiliser dans l'autre sens.

Corollaire I.42. *On a les équivalents suivants en 0 :*

1. $e^x - 1 \underset{x\to 0}{\sim} x$;
2. $\dfrac{1}{1+x} - 1 \underset{x\to 0}{\sim} -x$;
3. $\ln(1+x) \underset{x\to 0}{\sim} x$;
4. *si* $\alpha \in \mathbb{R}^*$: $(1+x)^\alpha - 1 \underset{x\to 0}{\sim} \alpha x$;
5. $\sin(x) \underset{x\to 0}{\sim} x$;
6. $\tan(x) \underset{x\to 0}{\sim} x$;
7. $\mathrm{Arcsin}(x) \underset{x\to 0}{\sim} x$;
8. $\mathrm{Arccos}(x) - \frac{\pi}{2} \underset{x\to 0}{\sim} -x$;
9. $\mathrm{Arctan}(x) \underset{x\to 0}{\sim} x$;
10. $\mathrm{sh}(x) \underset{x\to 0}{\sim} x$;
11. $\mathrm{th}(x) \underset{x\to 0}{\sim} x$.

Démonstration. Découle des calculs de dérivées en 0. □

Remarque I.43. *Pour $\alpha = \frac{1}{2}$, on trouve que $\sqrt{1+x} - 1 \underset{x\to 0}{\sim} \frac{x}{2}$, ou que $\sqrt{1+x} = 1 + \frac{x}{2} + \mathrm{o}(x)$.*
Avec $\alpha = -1$, on retrouve le cas de $\dfrac{1}{1+x}$.

Remarque I.44. *Si $f'(a) = 0$, on ne peut pas avoir l'équivalent de $f(x) - f(a)$ aussi facilement. Par exemple, pour* cos *en 0, la méthode précédente ne donnerait pas d'équivalent, mais seulement que :*

$$\cos(x) \underset{x\to 0}{=} 1 + \mathrm{o}(x).$$

Exemple I.45. *Déterminons un équivalent de* $\cos(x)-1$ *en 0. Pour cela, on utilise que* $\cos(x) = 1-2\sin^2\left(\frac{x}{2}\right)$. *Et par le fait que* $\sin(x) \underset{x\to 0}{=} x + \mathrm{o}(x)$, *on déduit que :*

$$\cos(x) \underset{x\to 0}{=} 1 - 2\left(\frac{x}{2} + \mathrm{o}(x)\right)^2$$

Mais on a :

$$\left(\frac{x}{2} + \mathrm{o}(x)\right)^2 = \left(\frac{x}{2}\cdot(1+\mathrm{o}(1))\right)^2 = \left(\frac{x}{2}\right)^2\cdot(1+\mathrm{o}(1))^2 = \frac{x^2}{4}\cdot(1+\mathrm{o}(1)) = \frac{x^2}{4} + \mathrm{o}(x^2)$$

et donc en réinjectant cette valeur :

$$\cos(x) \underset{x\to 0}{=} 1 - \frac{x^2}{2} + \mathrm{o}(x^2)$$

c'est-à-dire que : $\cos(x) - 1 \underset{x\to 0}{\sim} -\dfrac{x^2}{2}$.

Exemple I.46. *Calculons la limite en* $+\infty$ *de* $f : x \mapsto \sqrt[3]{x^3+x^2} - \sqrt[3]{x^3-2x^2}$.
On pourrait utiliser des quantités conjuguées, en notant que $\sqrt[3]{a} - \sqrt[3]{b} = \dfrac{a-b}{\sqrt[3]{a^2}+\sqrt[3]{ab}+\sqrt[3]{b^2}}$, *mais les calculs deviennent rapidement compliqués. On va plutôt utiliser des* o *:*

$$\begin{aligned} f(x) &= \sqrt[3]{x^3+x^2} - \sqrt[3]{x^3-2x^2} = x\cdot\left(\sqrt[3]{1+\tfrac{1}{x}} - \sqrt[3]{1-\tfrac{2}{x}}\right) \underset{x\to+\infty}{=} x\cdot\left(\frac{1}{3x} + \mathrm{o}\left(\tfrac{1}{x}\right) - \frac{-2}{x} + \mathrm{o}\left(\tfrac{1}{x}\right)\right) \\ &\underset{x\to+\infty}{\sim} x\cdot\frac{3}{3x} = 1 \end{aligned}$$

et donc $\lim\limits_{x\to+\infty} f(x) = 1$.

I.4 Comparaison de suites

Définition I.47. *Soient* (u_n), (v_n) *deux suites. On dit que* (u_n) *est* ***négligeable devant*** (v_n) *(resp.* ***dominée par*** (v_n), ***équivalente à*** (v_n)*) s'il existe un rang* n_0 *et une suite* (w_n) *qui tend vers* 0 *(resp. qui est bornée, qui tend vers* 1*) telle que :*

$$\forall n \geq n_0,\ u_n = w_n v_n.$$

On note alors $u_n = \mathrm{o}(v_n)$ *(resp.* $u_n = \mathrm{O}(v_n)$, $u_n \sim v_n$*).*

Remarque I.48. *Il s'agit donc de la même définition que pour les fonctions, en considérant uniquement le cas où* $a = +\infty$ *(dont on a vu que c'est le seul point adhérent important pour les suites). Cela justifie au passage que l'on ne fasse pas apparaître le* $n \to +\infty$ *dans les notations.*
De fait, tous les résultats précédents restent valables, notamment les liens entre les relations et les manières de les manipuler.

Proposition I.49. *Si* u, v *sont deux suites telles que* v *ne s'annule pas à partir d'un certain rang, alors :*

1. $u_n = \mathrm{O}(v_n)$ *si, et seulement si,* $\dfrac{u_n}{v_n}$ *est bornée à partir d'un certain rang ;*
2. $u_n = \mathrm{o}(v_n)$ *si, et seulement si,* $\dfrac{u_n}{v_n}$ *tend vers* 0 *;*
3. $u_n \sim v_n$ *si, et seulement si,* $\dfrac{u_n}{v_n}$ *tend vers* 1.

Démonstration. Comme pour les fonctions. □

Proposition I.50. *Si* u, v *sont deux suites telles que* $u_n = \mathrm{o}(v_n)$ *(resp.* $u_n = \mathrm{O}(v_n)$, $u_n \sim v_n$*) et* φ *est une extractrice, alors* $u_{\varphi(n)} = \mathrm{o}(v_{\varphi(n)})$ *(resp.* $u_{\varphi(n)} = \mathrm{O}(v_{\varphi(n)})$, $u_{\varphi(n)} \sim v_{\varphi(n)}$*).*

Démonstration. Il suffit de voir une extraction comme une composition à droite. □

Proposition I.51. *Si* f, g *sont deux fonctions définies sur* I*, et* (u_n) *une suite d'éléments de* I *qui tend vers* a*, alors :*

1. *si* $f(x) \underset{x\to a}{=} \mathrm{o}(g(x))$*, alors* $f(u_n) = \mathrm{o}(g(u_n))$ *;*
2. *si* $f(x) \underset{x\to a}{=} \mathrm{O}(g(x))$*, alors* $f(u_n) = \mathrm{O}(g(u_n))$ *;*
3. *si* $f(x) \underset{x\to a}{\sim} g(x)$*, alors* $f(u_n) \sim g(u_n)$.

Démonstration. Par caractérisation séquentielle de la limite. Qu'on peut aussi voir comme un cas particulier de composition à droite. □

II Développements limités et formules de Taylor

Pour toute la suite, on suppose que $a \in \mathbb{R}$.

II.1 Développements limités

Définition II.1. *Si f est définie sur I et $n \in \mathbb{N}$, on dit que f possède un* ***développement limité d'ordre*** *n (abrégé dl n)* ***au voisinage de*** *a s'il existe des réels $c_0, \dots, c_n$ tels que :*

$$f(x) \underset{x\to a}{=} c_0 + c_1(x-a) + \cdots + c_n(x-a)^n + \mathrm{o}\left((x-a)^n\right)$$

Remarque II.2. *Un développement limité d'ordre n est une approximation de f par un polynôme P de $\mathbb{R}_n[X]$ de la forme $f(x) \underset{x\to a}{=} P(x-a) + \mathrm{o}\left((x-a)^n\right)$.*

Remarque II.3. *En pratique, on essaiera de se ramener à des dl en 0. Comme les* o *se comportent bien avec les compositions, cela revient à considérer l'application $x \mapsto f(a+x)$ en 0 au lieu de l'application f en a.*

Exemple II.4. *Si $x \neq 1$, par somme géométrique, on trouve que :*

$$1 + x + \cdots + x^n = \frac{1-x^{n+1}}{1-x}$$

et donc :

$$\frac{1}{1-x} = 1 + x + \cdots + x^n + \frac{x^{n+1}}{1-x}$$

Mais on a aussi que :

$$\frac{x^{n+1}}{1-x} \underset{x\to 0}{\sim} \frac{x^{n+1}}{1} = x^{n+1} \underset{x\to 0}{=} \mathrm{o}(x^n).$$

Et ainsi : $\dfrac{1}{1-x}$ admet le dl n en 0 suivant :

$$\frac{1}{1-x} \underset{x\to 0}{=} 1 + x + \cdots + x^n + \mathrm{o}(x^n).$$

Proposition II.5 (Troncature)**.** *Si $n, m \in \mathbb{N}$ avec $m \leq n$, et que f possède un dl n au voisinage de a, alors f possède un dl m au voisinage de a dont les coefficients coïncident.*
Concrètement, si on a :

$$f(x) \underset{x\to a}{=} c_0 + c_1(x-a) + \cdots + c_n(x-a)^n + \mathrm{o}\left((x-a)^n\right)$$

alors le dl m de f est :

$$f(x) \underset{x\to a}{=} c_0 + c_1(x-a) + \cdots + c_m(x-a)^m + \mathrm{o}\left((x-a)^m\right).$$

Démonstration. Il suffit de voir que, pour $k > m$: $(x-a)^k \underset{x\to a}{=} \mathrm{o}\left((x-a)^m\right)$ et ainsi que :

$$c_{m+1}(x-a)^{m+1} + \cdots + c_n(x-a)^n + \mathrm{o}\left((x-a)^n\right) \underset{x\to a}{=} \mathrm{o}\left((x-a)^m\right).$$

□

Proposition II.6. *Un développement limité est unique, dans le sens où, si $n \in \mathbb{N}$ et que :*

$$f(x) \underset{x\to a}{=} c_0 + c_1(x-a) + \cdots + c_n(x-a)^n + \mathrm{o}\left((x-a)^n\right) \underset{x\to a}{=} b_0 + b_1(x-a) + \cdots + b_n(x-a)^n + \mathrm{o}\left((x-a)^n\right)$$

alors pour tout $i \in [\![0; n]\!]$ on a : $b_i = c_i$.

Démonstration. Supposons par l'absurde que les deux dl soient différents. Notons k le plus petit entier de $[\![0;n]\!]$ tel que $b_k \neq c_k$. Il vient alors, en tronquant les dl de f à l'ordre k que :

$$f(x) \underset{x\to a}{=} c_k(x-a)^k + \mathrm{o}\left((x-a)^k\right) \underset{x\to a}{=} b_k(x-a)^k + \mathrm{o}\left((x-a)^k\right)$$

et donc $(b_k - c_k)\cdot(x-a)^k = \mathrm{o}\left((x-a)^k\right)$. Et donc $b_k - c_k = \mathrm{o}(1)$.
D'où la contradiction avec le fait que $b_k - c_k \neq 0$. □

Définition II.7. *Si f admet le dl n suivant :*

$$f(x) \underset{x\to a}{=} c_0 + c_1(x-a) + \cdots + c_n(x-a)^n + \mathrm{o}\left((x-a)^n\right)$$

alors la fonction polynomiale $x \mapsto c_0 + c_1(x-a) + \cdots + c_n(x-a)^n$ est appelée ***partie régulière*** *du dl n de f en a.*

Proposition II.8. *Si f est définie sur I est possède le développement limité en a suivant :*

$$f(x) \underset{x\to a}{=} c_0 + c_1(x-a) + \cdots + c_n(x-a)^n + \mathrm{o}\left((x-a)^n\right)$$

alors en notant k le plus petit entier de $[\![0;n]\!]$ tel que $c_k \neq 0$, on a :

$$f(x) \underset{x\to a}{\sim} c_k(x-a)^k.$$

Démonstration. Par troncature, on a :

$$f(x) = c_k(x-a)^k + \mathrm{o}\left((x-a)^k\right)$$

ce qui donne directement le résultat. □

Remarque II.9. *L'idée derrière est que l'on peut très rapidement avoir des équivalents (donc des limites) à condition de pousser les développements limités suffisamment loin : c'est-à-dire jusqu'à avoir un terme non nul dans la partie régulière.*

Exemple II.10. *La fonction* exp *admet en* 0 *le dl* 2 *suivant :*

$$e^x \underset{x\to 0}{=} 1 + x + \frac{x^2}{2} + \mathrm{o}(x^2).$$

Et ainsi on peut retrouver que la fonction φ définie sur $\mathbb{R}_+$ par $\varphi(x) = e^{\sqrt{x}} - \sqrt{x}$ est dérivable en 0 *car pour $x > 0$ on a :*

$$\frac{\varphi(x)-\varphi(0)}{x} = \frac{e^{\sqrt{x}} - \sqrt{x} - 1}{x} \underset{x\to 0}{=} \frac{1 + \sqrt{x} + \frac{\sqrt{x}^2}{2} + \mathrm{o}(x) - 1 - \sqrt{x}}{x} \underset{x\to 0}{=} \frac{\frac{x}{2} + \mathrm{o}(x)}{x} \underset{x\to 0}{=} \frac{1}{2} + \mathrm{o}(1) \underset{x\to 0}{\to} \frac{1}{2}$$

ce qui donne bien la dérivabilité en 0, *avec* $\varphi'(0) = \dfrac{1}{2}$.

En prenant le dl 1 *de* exp, *on aurait seulement obtenu que* $\dfrac{\varphi(x)-\varphi(0)}{x} = \mathrm{o}\left(\frac{1}{\sqrt{x}}\right)$, *ce qui ne montrerait même pas la dérivabilité.*

Corollaire II.11. *Avec les mêmes notations, on trouve que :*

- *si k est pair : alors f est du signe de c_k au voisinage de a ;*
- *si k est impair : alors f est du signe de $-c_k$ sur un voisinage à gauche de a, et du signe de c_k sur un voisinage à droite de a.*

Démonstration. Découle de la conservation du signe par équivalent, et du tableau de signe de $x \mapsto c_k(x-a)^k$ au voisinage de a. □

Proposition II.12. *Si f est définie sur I et $a \in I$, alors :*

1. *f admet un dl 0 en a si, et seulement si, f est continue en a, et dans ce cas : $f(x) \underset{x\to a}{=} f(a)+\mathrm{o}(1)$;*
2. *f admet un dl 1 en a si, et seulement si, f est dérivable en a, et dans ce cas : $f(x) \underset{x\to a}{=} f(a) + f'(a)(x-a)+\mathrm{o}(x-a)$.*

Démonstration.

1. f admet un dl 0 si, et seulement si, f admet une limite en a, ce qui revient bien à la continuité comme $a \in I$;
2. déjà montré au chapitre précédent.

□

Remarque II.13. *Le résultat n'est plus vrai aux ordres supérieurs : il existe notamment des fonctions qui admettent un dl 2 en 0 sans être deux fois dérivable en 0.*
Par exemple, considérons la fonction :

$$f : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \left\{ \begin{array}{cc} x^3 \sin\left(\frac{1}{x}\right) & si\ x \neq 0 \\ 0 & si\ x = 0 \end{array} \right. \end{array} \right.$$

On constate par encadrement que f est continue sur $\mathbb{R}$.
De plus, f est dérivable sur $\mathbb{R}^*$ avec :

$$\forall x \in \mathbb{R}^*,\ f'(x) = 3x^2 \cdot \sin\left(\frac{1}{x}\right) - x \cdot \cos\left(\frac{1}{x}\right)$$

qui tend vers 0 en 0 (par encadrement), donc par théorème de prolongement des fonctions dérivables on déduit que f est dérivable en 0 avec $f'(0) = 0$.
Pour la dérivée seconde en 0, on utilise le taux d'accroissement de f' : pour $x \neq 0$, on a :

$$\frac{f'(x) - f'(0)}{x - 0} = 3x \cdot \sin\left(\frac{1}{x}\right) - \cos\left(\frac{1}{x}\right)$$

qui n'admet pas de limite quand x tend vers 0, donc f n'est pas deux fois dérivable en 0.
En revanche, comme $x^3 \underset{x\to 0}{=} \mathrm{o}(x^2)$, on déduit par encadrement que $f(x) \underset{x\to 0}{=} \mathrm{o}(x^2)$. Et donc f admet un dl 2 en 0, à savoir :

$$f(x) \underset{x\to 0}{=} 0 + 0 \cdot x + 0 \cdot x^2 + \mathrm{o}(x^2).$$

On verra plus tard que les dl se comportent bien avec les primitives, ce qui fournira, en primitivant $n-2$ fois f, des exemples de fonctions admettant des dl n sans être n-fois dérivables.

Proposition II.14. *On suppose que f est définie sur $\mathbb{R}$, et que f possède un développement limité d'ordre n en 0 de la forme :*

$$f(x) \underset{x\to 0}{=} c_0 + \cdots + c_n x^n + \mathrm{o}(x^n).$$

Alors :

1. *si f est paire : tous les coefficients de degré impair de son dl sont nuls : si k est impair, alors $c_k = 0$;*
2. *si f est impaire : tous les coefficients de degré pair de son dl sont nuls : si k est pair, alors $c_k = 0$;*

Démonstration. On utilise la composition à droite par la fonction $x \mapsto -x$ sur les o, ce qui assure que :

$$f(-x) \underset{x\to 0}{=} c_0 + c_1(-x) \cdots + c_n(-x)^n + \mathrm{o}((-x)^n) \underset{x\to 0}{=} c_0 - c_1 x \cdots + (-1)^n c_n x^n + \mathrm{o}(x^n)$$

donc la fonction $g : x \mapsto f(-x)$ admet le dl n ci-dessus.
Si f est paire : alors $f = g$, et par unicité du dl on déduit que :

$$c_0 = c_0,\ c_1 = -c_1,\ c_2 = c_2,\ c_3 = -c_3,\ \ldots$$

ce qui donne bien la nullité des coefficients de degré impair.
Si f est impaire, alors $f = -g$, et par unicité on trouve de même que les coefficients de degré pair sont nuls. □

Remarque II.15. *On peut supposer que f est seulement définie sur un ensemble I symétrique par rapport à 0, tel que 0 est adhérent à I et le résultat tient toujours.*
Les autres symétries rencontrées, tant qu'elles sont locales, se voient sur les dl : par exemple une symétrie centrale pourra se lire sur les coefficients, mais pas la périodicité.

Corollaire II.16. *Avec les mêmes notations, si on note f_1, f_2 les fonctions respectivement paires et impaires telles que $f = f_1 + f_2$, alors f_1 et f_2 admettent les dl n suivant en 0 :*

$$f_1(x) \underset{x\to 0}{=} c_0 + c_2 x^2 + \cdots + \mathrm{o}(x^n) \underset{x\to 0}{=} \sum_{k=0}^{\lfloor n/2 \rfloor} c_{2k} x^{2k} + \mathrm{o}(x^n)\,;$$

$$f_2(x) \underset{x\to 0}{=} c_1 x + c_3 x^3 + \cdots + \mathrm{o}(x^n) \underset{x\to 0}{=} \sum_{k=0}^{\lfloor n-1/2 \rfloor} c_{2k+1} x^{2k+1} + \mathrm{o}(x^n);$$

II.2 Formules de Taylor

Proposition II.17. *Soit f une fonction continue sur un intervalle I admettant un dl n au voisinage de a. Si F est une primitive de f sur I, alors F admet un dl $n+1$ au voisinage de a.*
Plus précisément, si :

$$f(x) \underset{x\to a}{=} c_0 + c_1(x-a) + \cdots + c_n(x-a)^n + \mathrm{o}\left((x-a)^n\right)$$

alors :

$$F(x) \underset{x\to a}{=} F(a) + c_0(x-a) + \frac{c_1}{2}(x-a)^2 + \cdots + \frac{c_n}{n+1}(x-a)^{n+1} + \mathrm{o}\left((x-a)^{n+1}\right).$$

Remarque II.18. *Il y a certaines précautions à prendre avec ce résultat : déjà il faut prendre en compte $F(a)$ quand on primitive f, et surtout il faut considérer f continue sur I (pas seulement en a, ce qui serait acquis par l'existence du dl) pour que F ait bien un sens, et que I soit un intervalle pour utiliser le théorème des accroissements finis.*

Démonstration. Avec les mêmes notations, considérons la fonction

$$\varphi : x \mapsto F(x) - F(a) - \sum_{k=0}^{n} \frac{c_k}{k+1}(x-a)^{k+1}.$$

Par construction, la fonction φ est dérivable sur I, et sa dérivée est donnée par :

$$\forall x \in I,\ \varphi'(x) = f(x) - \sum_{k=0}^{n} c_k (x-a)^k$$

et ainsi $\varphi'(x) \underset{x\to a}{=} \mathrm{o}\left((x-a)^n\right)$.
Si $x \in I$, par théorème des accroissements finis, il existe c_x entre x et a tel que : $\varphi(x)-\varphi(a) = \varphi'(c_x)(x-a)$.
Par composition, comme $c_x \underset{x\to a}{\to} a$ (par encadrement), alors : $\varphi'(c_x) \underset{x\to a}{=} \mathrm{o}((c_x-a)^n)$.
Comme $|c_x - a| \leq |x-a|$, alors $\varphi'(c_x) \underset{x\to a}{=} \mathrm{o}\left((x-a)^n\right)$.
Et finalement : $\varphi(x) - \underbrace{\varphi(a)}_{=0} = \mathrm{o}\left((x-a)^{n+1}\right)$ de sorte que, en remplaçant φ par son expression :

$$F(x) \underset{x\to a}{=} F(a) + \sum_{k=0}^{n} \frac{c_k}{k+1}(x-a)^{k+1} + \mathrm{o}\left((x-a)^{n+1}\right).$$

□

Remarque II.19. *Cela veut dire qu'on peut primitiver un dl terme à terme : ce qui se comprend bien par croissance de l'intégrale, dans la mesure ou primitiver un quantité petite donnera aussi une quantité petite. En revanche, on ne dérive pas un dl : ce n'est pas parce qu'une fonction prend des petites valeurs que sa dérivée aussi (par exemple* cos *est toujours entre les fonctions constantes de valeurs* 1 *et* -1*, mais cette inégalité ne passe pas à la dérivation.*
On peut en revanche dire que, si une fonction f possède un dl n, celui-ci est donné par la dérivée du dl $n+1$ d'une de ses primitives (par unicité du dl).

Corollaire II.20. *La fonction* tan *admet le développement limité suivant en* 0 *:*

$$\tan(x) \underset{x\to 0}{=} x + \frac{x^3}{3} + \mathrm{o}(x^3).$$

Démonstration. On a déjà montré que $\tan(x) \underset{x\to 0}{=} x + \mathrm{o}(x)$. Et ainsi :

$$\tan^2(x) \underset{x\to 0}{=} (x+\mathrm{o}(x))^2 \underset{x\to 0}{=} x^2 \underbrace{(1+\mathrm{o}(1))^2}_{=1+\mathrm{o}(1)} \underset{x\to 0}{=} x^2 + \mathrm{o}(x^2)$$

et donc, comme $\tan' = 1+\tan^2$, on déduit par intégration le dl de tan suivant :

$$\tan(x) \underset{x\to 0}{=} \tan(0) + x + \frac{x^3}{3} + \mathrm{o}(x^3) = x + \frac{x^3}{3} + \mathrm{o}(x^3).$$

□

Remarque II.21. *On peut réitérer cette méthode pour obtenir de dl de* tan *à tout ordre : un dl n de* tan *donne un dl $n+1$ de $1+\tan^2$, qui donne un dl $n+2$ de* tan*, etc.*
Notons au passage que, tan *étant impaire, ses coefficients de degré pair sont nuls.*

Théorème II.22 (Formule de Taylor–Young)**.** *Si f est une fonction de classe $\mathcal{C}^n$ (pour $n \in \mathbb{N}$) sur un intervalle I, et $a \in I$, alors f admet un développement limité à l'ordre n en a, donné par :*

$$f(x) \underset{x\to a}{=} \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k + \mathrm{o}\left((x-a)^n\right).$$

Démonstration. On procède par récurrence sur $n \in \mathbb{N}$.
Si $n = 0$ ou $n = 1$: les résultats ont déjà été montrés.
Supposons le résultat vrai pour tout fonction de classe $\mathcal{C}^n$ (pour $n \in \mathbb{N}$), et considérons f de classe $\mathcal{C}^{n+1}$.
Comme f' est de classe $\mathcal{C}^n$, alors par hypothèse de récurrence :

$$f'(x) \underset{x\to a}{=} \sum_{k=0}^{n} \frac{f'^{(k)}(a)}{k!}(x-a)^k + \mathrm{o}((x-a)^n) \underset{x\to a}{=} \sum_{k=0}^{n} \frac{f^{(k+1)}(a)}{k!}(x-a)^k + \mathrm{o}\left((x-a)^n\right)$$

et ainsi en primitivant le dl ci-dessus :

$$\begin{aligned} f(x) &\underset{x\to a}{=} f(a) + \textstyle\sum_{k=0}^{n} \dfrac{f^{(k+1)}}{k!}\dfrac{(x-a)^{k+1}}{k+1} + \mathrm{o}\left((x-a)^{n+1}\right) \\ &\underset{x\to a}{=} f(a) + \textstyle\sum_{k=0}^{n} \dfrac{f^{(k+1)}}{(k+1)!}(x-a)^{k+1} + \mathrm{o}\left((x-a)^{n+1}\right) \\ &\underset{x\to a}{=} \textstyle\sum_{k=0}^{n+1} \dfrac{f^{(k)}(a)}{k!}(x-a)^{k} + \mathrm{o}\left((x-a)^{n+1}\right) \end{aligned}$$

ce qui conclut l'hérédité.
D'où le résultat. □

Remarques II.23.

1. *Les dérivées successives d'une fonction en un point a se lisent dont sur les coefficients de son développement limité en a.*
2. *Si f est de classe $\mathcal{C}^\infty$, elle admet donc des développements limités à tout ordre en tout point.*
3. *Cette formule coïncide avec la formule de Taylor polynomiale, en ayant poussé suffisamment l'ordre du développement pour que toutes les dérivées suivantes soient nulles.*
4. *Il existe d'autres formules de Taylor (Taylor–Lagrange et Taylor avec reste intégral) qui permettent d'estimer plus précisément le $\mathrm{o}((x-a)^n)$ en fonction de la $(n+1)$-ème dérivée de la fonction.*

II.3 Développements limités usuels

Théorème II.24 (Développements limités usuels en 0)**.** *Pour $n \in \mathbb{N}^*$, on a :*

1. $e^x \underset{x\to 0}{=} \displaystyle\sum_{k=0}^{n} \frac{x^k}{k!} + \mathrm{o}(x^n) = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \cdots + \frac{x^n}{n!} + \mathrm{o}(x^n)$;
2. $\sin(x) \underset{x\to 0}{=} \displaystyle\sum_{k=0}^{\lfloor n-1/2\rfloor} (-1)^k \frac{x^{2k+1}}{(2k+1)!} + \mathrm{o}(x^n) = x - \frac{x^3}{6} + \frac{x^5}{120} - \cdots + \mathrm{o}(x^n)$;
3. $\cos(x) \underset{x\to 0}{=} \displaystyle\sum_{k=0}^{\lfloor n/2\rfloor} (-1)^k \frac{x^{2k}}{(2k)!} + \mathrm{o}(x^n) = 1 - \frac{x^2}{2} + \frac{x^4}{24} - \cdots + \mathrm{o}(x^n)$;
4. $\mathrm{sh}(x) \underset{x\to 0}{=} \displaystyle\sum_{k=0}^{\lfloor n-1/2\rfloor} \frac{x^{2k+1}}{(2k+1)!} + \mathrm{o}(x^n) = x + \frac{x^3}{6} + \frac{x^5}{120} + \cdots + \mathrm{o}(x^n)$;
5. $\mathrm{ch}(x) \underset{x\to 0}{=} \displaystyle\sum_{k=0}^{\lfloor n/2\rfloor} \frac{x^{2k}}{(2k)!} + \mathrm{o}(x^n) = 1 + \frac{x^2}{2} + \frac{x^4}{24} + \cdots + \mathrm{o}(x^n)$;
6. $\dfrac{1}{1-x} \underset{x\to 0}{=} \displaystyle\sum_{k=0}^{n} x^k + \mathrm{o}(x^n) = 1 + x + x^2 + \cdots + x^n + \mathrm{o}(x^n)$;
7. $\dfrac{1}{1+x} \underset{x\to 0}{=} \displaystyle\sum_{k=0}^{n} (-x)^k + \mathrm{o}(x^n) = 1 - x + x^2 - x^3 + \cdots + (-1)^n x^n + \mathrm{o}(x^n)$;
8. $\ln(1+x) \underset{x\to 0}{=} \displaystyle\sum_{k=1}^{n} (-1)^{k-1} \frac{x^k}{k} + \mathrm{o}(x^n) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots + (-1)^{n-1}\frac{x^n}{n} + \mathrm{o}(x^n)$;
9. $\mathrm{Arctan}(x) \underset{x\to 0}{=} \displaystyle\sum_{k=0}^{\lfloor n-1/2\rfloor} (-1)^k \frac{x^{2k+1}}{2k+1} + \mathrm{o}(x^n) = x - \frac{x^3}{3} + \frac{x^5}{5} - \cdots + \mathrm{o}(x^n)$;

10. si $\alpha \in \mathbb{R}$:

$$(1+x)^\alpha \underset{x\to 0}{=} \sum_{k=0}^{n} \frac{\alpha(\alpha-1)\dots(\alpha-k+1)}{k!}x^k + \mathrm{o}(x^n)$$
$$\underset{x\to 0}{=} 1 + \alpha x + \frac{\alpha(\alpha-1)}{2}x^2 + \dots + \frac{\alpha(\alpha-1)\dots(\alpha-n+1)}{n!}x^n + \mathrm{o}(x^n)$$

Démonstration. Pour e^x, sin et cos on utilise la formule de Taylor–Young, et il suffit donc de calculer les dérivées successives de ces fonctions en 0. Pour $n \in \mathbb{N}$, on a :

— $\exp^{(n)}(x) = \exp(x)$, donc $\exp^{(n)}(0) = 1$;

— $\sin^{(n)}(x) = \sin(x + n\frac{\pi}{2})$, donc $\sin^{(n)}(0) = \begin{cases} 0 & \text{si } n \text{ est pair} \\ (-1)^{n-1/2} & \text{si } n \text{ est impair} \end{cases}$;

— $\cos^{(n)}(x) = \cos(x + n\frac{\pi}{2})$, donc $\cos^{(n)}(0) = \begin{cases} 0 & \text{si } n \text{ est impair} \\ (-1)^{n/2} & \text{si } n \text{ est pair} \end{cases}$.

Pour sh et ch, on prend les parties respectivement impaire et paire de exp.

Le cas de $\dfrac{1}{1-x}$ a déjà été traité (par somme géométrique). On déduit le cas de $\dfrac{1}{1+x}$ en changeant x en $-x$ dans le dl (par opération sur les o).
On déduit alors le dl de $x \mapsto \ln(1+x)$ par primitivation du dl précédent, en notant que $\ln(1+0) = \ln(1) = 0$.

Pour Arctan, on remplace x par x^2 dans le dl de $\dfrac{1}{1+x}$, ce qui donne le dl de $\dfrac{1}{1+x^2}$, qu'on primitive pour avoir celui de Arctan en notant que $\mathrm{Arctan}(0) = 0$.

Pour $(1+x)^\alpha$, la dérivée n-ème est donnée par $\alpha(\alpha-1)\dots(\alpha-n+1)(1+x)^{\alpha-n}$, qui vaut donc $\alpha(\alpha-1)\dots(\alpha-n+1)$ en 0. Et on conclut en appliquant la formule de Taylor–Young. □

Remarque II.25. *Pour $(1+x)^\alpha$, si $\alpha \in \mathbb{N}$ on trouve que :*

$$\frac{\alpha(\alpha-1)\dots(\alpha-n+1)}{n!} = \binom{\alpha}{n}$$

et le dl de $(1+x)^\alpha$ correspond à la troncature de la formule donnée par le binôme en développant $(1+x)^\alpha$. On retrouve aussi que, pour $k > \alpha$, le coefficient d'indice k dans le dl est nul, à la manière de ce qu'on avait pour la formule de Taylor polynomiale.

Exemple II.26. *À la manière de ce qu'on a fait pour* Arctan*, on peut donner les dl en 0 des fonctions* Arcsin *et* Arccos.
Par exemple pour Arcsin*, on utilise que :*

$$\mathrm{Arcsin}'(x) = \frac{1}{\sqrt{1-x^2}} = (1-x^2)^{1/2} \underset{x\to 0}{=} 1 + \frac{x^2}{2} = \frac{3x^4}{8} + \dots + \frac{1\cdot 3\cdot\dots\cdot(2n-1)}{2^n\cdot n!}x^{2n} + \mathrm{o}(x^{2n+1})$$

où on a utilisé que, pour $\alpha = -\frac{1}{2}$:

$$\alpha(\alpha-1)(\alpha-2)\dots(\alpha-n+1) = \frac{-1}{2}\cdot\frac{-3}{2}\cdot\dots\cdot\frac{-(2n-1)}{2} = (-1)^n\cdot\frac{1\cdot 3\cdot\dots\cdot(2n-1)}{2^n}.$$

La dernière expression se simplifie en notant que :

$$1\cdot 3\cdot\dots\cdot(2n-1) = \frac{1\cdot 2\cdot 3\cdot\dots\cdot(2n-1)\cdot 2n}{2\cdot 4\cdot\dots\cdot 2n} = \frac{(2n)!}{2^n\cdot n!}.$$

En primitivant ce dl (comme $\mathrm{Arcsin}(0)=0$*), on déduit que :*

$$\begin{array}{rcl}\mathrm{Arcsin}(x) & \underset{x\to 0}{=} & x+\dfrac{x^3}{6}+\dfrac{3x^5}{40}+\cdots+\dfrac{1\cdot 3\cdot\cdots\cdot(2n-1)}{2^n\cdot n!\cdot(2n+1)}x^{2n+1}+\mathrm{o}(x^2n+2)\\ & \underset{x\to 0}{=} & \displaystyle\sum_{k=1}^{n}\frac{1}{4^k(2k+1)}\binom{2k}{k}x^{2k+1}+\mathrm{o}(x^{2n+2})\end{array}.$$

Et on peut calculer le dl de Arccos *de la même manière, ou utiliser que* $\mathrm{Arcsin}+\mathrm{Arccos}=\frac{\pi}{2}$.

II.4 Opérations sur les développements limités

Remarque II.27. *Les développements limités héritent des règles de calcul sur les* o*, et sont donc compatibles avec somme, produit, quotient et composition.*
La subtilité résidera dans l'optimisation de ces calculs, et notamment le fait de ne pas faire des dl d'ordre plus grand que nécessaire, et de les tronquer au fur et à mesure pour éviter de manipuler trop de termes dans les calculs.

Méthode II.28. *Pour obtenir le dl* n *d'une combinaison linéaire, il suffit de prendre les dl* n *de chacune des fonctions et de les regrouper terme à terme.*

Exemple II.29. *Donnons le dl* 3 *de* $f:x\mapsto e^x-\ln(1+x)$ *en* 0*. On a :*

$$e^x\underset{x\to 0}{=}1+x+\frac{x^2}{2}+\frac{x^3}{6}+\mathrm{o}(x^3)\ \text{et}\ \ln(1+x)=x-\frac{x^2}{2}+\frac{x^3}{3}+\mathrm{o}(x^3)$$

et ainsi :

$$f(x)\underset{x\to 0}{=}1+x^2-\frac{x^3}{6}+\mathrm{o}(x^3).$$

Méthode II.30. *Pour obtenir un dl* n *d'un produit, il suffit de multiplier les dl* n *de chaque facteur, en tronquant dès que l'on distribue.*

Exemple II.31. *Donnons le dl* 4 *de* $f:x\mapsto e^x\cos(x)$ *en* 0*. On a :*

$$e^x\underset{x\to 0}{=}1+x+\frac{x^2}{2}+\frac{x^3}{6}+\frac{x^4}{24}+\mathrm{o}(x^4)\ \text{et}\ \cos(x)=1-\frac{x^2}{2}+\frac{x^4}{24}+\mathrm{o}(x^4)$$

et ainsi :

$$\begin{array}{rcl}f(x) & \underset{x\to 0}{=} & \left(1+x+\dfrac{x^2}{2}+\dfrac{x^3}{6}+\dfrac{x^4}{24}+\mathrm{o}(x^4)\right)\cdot\left(1-\dfrac{x^2}{2}+\dfrac{x^4}{24}+\mathrm{o}(x^4)\right)\\ & \underset{x\to 0}{=} & \left(1+x+\dfrac{x^2}{2}+\dfrac{x^3}{6}+\dfrac{x^4}{24}+\mathrm{o}(x^4)\right)+\left(-\dfrac{x^2}{2}-\dfrac{x^3}{2}-\dfrac{x^4}{4}+\mathrm{o}(x^4)\right)+\left(\dfrac{x^4}{24}+\mathrm{o}(x^4)\right)+\mathrm{o}(x^4)\\ & \underset{x\to 0}{=} & 1+x-\dfrac{x^3}{3}-\dfrac{x^4}{6}+\mathrm{o}(x^4)\end{array}$$

Méthode II.32. *Pour obtenir le dl* n *d'un produit, on commence par factoriser chaque facteur par son équivalent, ce qui fait sortir un facteur de la forme* $(x-a)^k$*, et on utilise ensuite des dl* $n-k$ *des deux facteurs restants.*

Exemple II.33. *Déterminons le dl* 5 *de* $f:x\mapsto\sin(x)\mathrm{Arcsin}(x)$ *en* 0*.*
Comme $\sin(x)\underset{x\to 0}{\sim}x$ *et que* $\mathrm{Arcsin}(x)\underset{x\to 0}{\sim}x$*, alors on peut factoriser par* x^2 *le produit des dl, et il suffit d'avoir le dl* 3 *de* $\dfrac{\sin(x)}{x}$ *et de* $\dfrac{\mathrm{Arcsin}(x)}{x}$*, donc le dl* 4 *de* $\sin(x)$ *et de* $\mathrm{Arcsin}(x)$*. Par imparité, ceux-ci sont directement donnés par les dl* 3*.*

On a :

$$\sin(x) \underset{x\to 0}{=} x - \frac{x^3}{6} + \mathrm{o}(x^4) \text{ et } \mathrm{Arcsin}(x) \underset{x\to 0}{=} x + \frac{x^3}{6} + \mathrm{o}(x^4)$$

et ainsi :

$$\begin{array}{rcl} f(x) & = & \sin(x)\mathrm{Arcsin}(x) \underset{x\to 0}{=} \left(x - \frac{x^3}{6} + \mathrm{o}(x^4)\right)\cdot\left(x + \frac{x^3}{6} + \mathrm{o}(x^4)\right) \\ & \underset{x\to 0}{=} & x^2\cdot\left(1 - \frac{x^2}{6} + \mathrm{o}(x^3)\right)\cdot\left(1 + \frac{x^2}{6} + \mathrm{o}(x^3)\right) \\ & \underset{x\to 0}{=} & x^2\cdot\left(1 + \frac{x^2}{6} + \mathrm{o}(x^3) - \frac{x^2}{6} + \mathrm{o}(x^3) + \mathrm{o}(x^3)\right) \\ & \underset{x\to 0}{=} & x^2\cdot(1 + \mathrm{o}(x^3)) \\ & \underset{x\to 0}{=} & x^2 + \mathrm{o}(x^5) \end{array}$$

Remarque II.34. *Pour les puissances, le résultat reste le même : si* $f \underset{x\to a}{\sim} (x-a)^k$ *(à une constante multiplicative près), pour déterminer le dl* n *de* f^l*, il suffit de connaître le dl* $(n - k(l-1))$ *de* f*.*
Par exemple, le dl 1 *de* sin *donne le dl* n *de* $\sin^n$ *pour tout* n*. En revanche, pour* cos*, il faut le dl* n *de dl* n *de* cos *pour avoir celui d'une de ses puissances.*

Méthode II.35. *Pour obtenir le dl* n *de la composée* $g \circ f$*, on commence par exprimer le dl de* g*, dans lequel on remplace la variable par* f*, puis par le dl de* f*. Le constat sur les puissances permet de savoir jusqu'à quel ordre donner les dl de* f *et* g*.*

Exemple II.36. *Donnons le dl* 4 *en* 0 *de* $f : x \mapsto \ln(1+\sin(x))$ *en* 0*.*
On a :

$$\ln(1+x) \underset{x\to 0}{=} x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \mathrm{o}(x^4)$$

et donc par composition :

$$f(x) \underset{x\to 0}{=} \sin(x) - \frac{\sin(x)^2}{2} + \frac{\sin(x)^3}{3} - \frac{\sin(x)^4}{4} + \mathrm{o}(\sin(x)^4)$$

Comme $\sin(x) \underset{x\to 0}{\sim} x$*, on a déjà que* $\mathrm{o}(\sin(x)^4) \underset{x\to 0}{=} \mathrm{o}(x^4)$*. Reste donc à trouver les dl* 4 *en* 0 *des puissances de* $\sin(x)$*.*
On a déjà :

$$\sin(x) \underset{x\to 0}{=} x - \frac{x^3}{6} + \mathrm{o}(x^4) = x\cdot\left(1 - \frac{x^2}{6} + \mathrm{o}(x^2)\right)$$

On déduit que :

$$\sin^2(x) \underset{x\to 0}{=} x^2\cdot\left(1 - \frac{x^2}{6} + \mathrm{o}(x^3)\right)^2 = x^2\cdot\left(1 - \frac{x^2}{3} + \mathrm{o}(x^3)\right) = x^2 - \frac{x^4}{3} + \mathrm{o}(x^4).$$

Pour les autres puissances, on pourrait faire de même en calculant les dl par produit, mais on peut se contenter d'équivalents, comme on sait déjà que $\sin^3$ *et* $\sin^4$ *admettent des dl à tout ordre :*

- *on a :* $\sin^3(x) \underset{x\to 0}{\sim} x^3$*, donc* $\sin^3(x) \underset{x\to 0}{=} x^3 + ax^4 + \mathrm{o}(x^4)$*. Mais* $x \mapsto \sin^3(x)$ *est impaire, donc* $a = 0$*, et finalement :*

$$\sin^3(x) \underset{x\to 0}{=} x^3 + \mathrm{o}(x^4).$$

- *on a :* $\sin^4(x) \underset{x\to 0}{\sim} x^4$*, donc :*

$$\sin^4(x) \underset{x\to 0}{=} x^4 + \mathrm{o}(x^4).$$

Et en réinjectant ces dl, on est ramené au dl d'une combinaison linéaire :

$$\begin{array}{rcl} f(x) & \underset{x\to 0}{=} & x - \dfrac{x^3}{6} - \dfrac{1}{2}\left(x^2 - \dfrac{x^4}{3}\right) + \dfrac{x^3}{3} - \dfrac{x^4}{4} + \mathrm{o}(x^4) \\ & \underset{x\to 0}{=} & x - \dfrac{x^2}{2} + \dfrac{1}{3}x^3 - \dfrac{x^4}{12} + \mathrm{o}(x^4) \end{array}.$$

Méthode II.37. *Pour calculer le dl n de l'inverse d'une fonction, on se ramène à une composée avec $x \mapsto \dfrac{1}{1 \pm x}$ en 0 en divisant la fonction par une constante pour qu'elle tende vers 1.*
Le dl d'un quotient se déduit alors par produit.

Exemple II.38. *Déduisons le dl de* tan *en* 0 *de ceux de* sin *et* cos. *Par exemple pour le dl* 5.
Estimons d'abord les ordres des dl à faire. Comme on veut écrire :

$$\tan(x) = \sin(x) \cdot \frac{1}{\cos(x)}$$

et que $\sin(x) \underset{x\to 0}{\sim} x$ *et* $\cos(x) \underset{x\to 0}{\sim} 1$, *alors pour avoir le dl* 5 *de* tan *il faut le dl* 4 *de* $\dfrac{\sin(x)}{x}$ *et de* $\dfrac{1}{\cos(x)}$, *donc le dl* 5 *de* $\sin(x)$ *et le dl* 4 *de* $\dfrac{1}{\cos(x)}$.
On utilise que :

$$\cos(x) \underset{x\to 0}{=} 1 - \frac{x^2}{2} + \frac{x^4}{24} + \mathrm{o}(x^4)$$

Et on utilise ensuite que :

$$\frac{1}{1+u} = 1 - u + u^2 - u^3 + \cdots + (-1)^n u^n + \mathrm{o}(u^n)$$

que l'on va appliquer avec $u = -\frac{x^2}{2} + \frac{x^4}{24} + \mathrm{o}(x^4) \underset{x\to 0}{=} \mathrm{O}(x^2)$.
Comme on veut le dl 4 *de* $\dfrac{1}{\cos(x)}$, *alors on veut le dl en* u *à l'ordre* 2. *On a alors :*

$$\begin{array}{rcl} \dfrac{1}{\cos(x)} & \underset{x\to 0}{=} & \dfrac{1}{1 - \frac{x^2}{2} + \frac{x^4}{24} + \mathrm{o}(x^4)} \\ & \underset{x\to 0}{=} & 1 - \left(\dfrac{-x^2}{2} + \dfrac{x^4}{24} + \mathrm{o}(x^4)\right) + \left(\dfrac{-x^2}{2} + \dfrac{x^4}{24} + \mathrm{o}(x^4)\right)^2 + \mathrm{o}\left(\left(\dfrac{-x^2}{2} + \dfrac{x^4}{24} + \mathrm{o}(x^4)\right)^2\right) \\ & \underset{x\to 0}{=} & 1 + \dfrac{x^2}{2} - \dfrac{x^4}{24} + \dfrac{x^4}{4} + \mathrm{o}(x^4) \\ & \underset{x\to 0}{=} & 1 + \dfrac{x^2}{2} + \dfrac{5x^4}{24} + \mathrm{o}(x^4) \end{array}$$

et par produit :

$$\begin{array}{rcl} \tan(x) & \underset{x\to 0}{=} & \left(x - \dfrac{x^3}{6} + \dfrac{x^5}{120} + \mathrm{o}(x^5)\right) \cdot \left(1 + \dfrac{x^2}{2} + \dfrac{5x^4}{24} + \mathrm{o}(x^4)\right) \\ & \underset{x\to 0}{=} & x + \dfrac{x^3}{2} + \dfrac{5x^5}{24} - \dfrac{x^3}{6} - \dfrac{x^5}{12} + \dfrac{x^5}{120} + \mathrm{o}(x^5) \\ & \underset{x\to 0}{=} & x + \dfrac{x^3}{3} + \dfrac{2x^5}{15} + \mathrm{o}(x^5) \end{array}$$

Exemple II.39. *Donnons le dl* 3 *en* 0 *de* $\dfrac{1}{2 + e^x}$. *On a :*

$$2 + e^x \underset{x\to 0}{=} 2 + 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \mathrm{o}(x^3) = 3 \cdot \left(1 + \frac{x}{3} + \frac{x^2}{6} + \frac{x^3}{18} + \mathrm{o}(x^3)\right)$$

et donc :

$$\frac{1}{2+e^x} \underset{x\to 0}{=} \frac{1}{3}\cdot\frac{1}{1+\dfrac{x}{3}+\dfrac{x^2}{6}+\dfrac{x^3}{18}+\mathrm{o}(x^3)}$$

et par composition, on a :

$$\begin{aligned}\frac{1}{1+\dfrac{x}{3}+\dfrac{x^2}{6}+\dfrac{x^3}{18}+\mathrm{o}(x^3)} &\underset{x\to 0}{=} 1-\left(\frac{x}{3}+\frac{x^2}{6}+\frac{x^3}{18}\right)+\left(\frac{x}{3}+\frac{x^2}{6}\right)^2-\left(\frac{x}{3}\right)^3+\mathrm{o}(x^3)\\ &\underset{x\to 0}{=} 1-\left(\frac{x}{3}+\frac{x^2}{6}+\frac{x^3}{18}\right)+\left(\frac{x^2}{9}+\frac{x^3}{9}\right)-\left(\frac{x^3}{27}\right)\\ &\underset{x\to 0}{=} 1-\frac{x}{3}-\frac{x^2}{18}+\frac{x^3}{54}+\mathrm{o}(x^3)\end{aligned}$$

et finalement :

$$f(x) \underset{x\to 0}{=} \frac{1}{3}-\frac{x}{9}-\frac{x^2}{54}+\frac{x^3}{162}+\mathrm{o}(x^3).$$

Méthode II.40. *Pour calculer un dl ailleurs qu'en* 0*, on peut ou bien utiliser la formule de Taylor–Young en calculant les dérivées successives, ou bien de ramener à des dl usuels en* 0 *par changement de variable affine.*

Exemple II.41. *Donnons le dl* 2 *de* e^x *au voisinage de* 2*. On peut procéder de deux manières :*

— *Avec la formule de Taylor–Young : il suffit de calculer les dérivées successives de la fonction exponentielle en* 2*, ce qui donne :*

$$\forall k\in\mathbb{N},\ \exp^{(k)}(2)=\exp(2)=e^2$$

et en réinjectant dans la formule de Taylor–Young, on obtient :

$$e^x \underset{x\to 2}{=} \sum_{k=0}^{2}\frac{\exp^{(k)}(2)}{k!}(x-2)^k+\mathrm{o}\left((x-2)^3\right)=e^2+e^2(x-2)+\frac{e^2}{2}(x-2)^2+\mathrm{o}((x-2)^2).$$

— *Avec une composée : on écrit* $x=2+h$*, avec* h *qui tend vers* 0*. Et alors :*

$$\begin{aligned}e^x &= e^{2+h}=e^2\cdot e^h\\ &\underset{x\to 2}{=} e^2\cdot\left(1+h+\frac{h^2}{2}+\mathrm{o}(h^2)\right)\\ &\underset{x\to 2}{=} e^2+e^2(x-2)+\frac{e^2}{2}(x-2)^2+\mathrm{o}((x-2)^2)\end{aligned}$$

Dans un cas comme dans l'autre, il n'est pas difficile d'adapter la méthode à des ordres arbitrairement grands.

III Applications

III.1 Développement limité d'une fonction réciproque

Méthode III.1. *Étant donnée une fonction* f *bijective de classe* $\mathcal{C}^n$ *dont la réciproque* f^{-1} *est de classe* $\mathcal{C}^n$*, on peut déterminer un dl de* f^{-1} *en composant un dl hypothétique par* f*, et en utilisant que* $f\circ f^{-1}(y)=y \underset{y\to 0}{=} y+\mathrm{o}(y^n)$ *pour tout* $n\in\mathbb{N}^*$*.*

Remarque III.2. *On peut aussi utiliser que* $f^{-1}\circ f=\mathrm{id}$*, mais les calculs peuvent devenir plus compliqués.*

Exemple III.3. *On considère la fonction f définie sur $\mathbb{R}$ par : $f(x) = x\exp(x^2)$.*
Alors la fonction f est dérivable sur $\mathbb{R}$, de dérivée :

$$f'(x) = (2x^2+1)\exp(x^2) > 0$$

donc f est continue strictement croissante sur $\mathbb{R}$, avec $\lim\limits_{x\to+\infty} f(x) = +\infty$ et $\lim\limits_{x\to-\infty} f(x) = -\infty$, donc f réalise une bijection strictement croissante de $\mathbb{R}$ sur $\mathbb{R}$.
Comme f' ne s'annule jamais, et que f est de classe $\mathcal{C}^\infty$, alors f^{-1} est aussi de classe $\mathcal{C}^\infty$, donc admet en tout point des dl de tout ordre.
Calculons le dl 4 de f^{-1} en 0. On l'écrit sous la forme :

$$f^{-1}(y) = a + by + cy^2 + dy^3 + ey^4 + o(y^4)$$

Comme f est impaire, alors f^{-1} aussi, donc on a déjà : $a = c = e = 0$.
De plus, par les dl classiques, on a le dl suivant pour f :

$$f(x) \underset{x\to0}{=} x\cdot(1+x^2+o(x^3)) \underset{x\to0}{=} x + x^3 + o(x^4).$$

Soient $x, y \in \mathbb{R}$. On a alors :

$$f\circ f^{-1}(y) \underset{y\to0}{=} (by+dy^3) + (by+dy^3)^3 + o(y^4) \underset{y\to0}{=} by + (b^3+d)y^3 + o(y^4)$$

$$f^{-1}\circ f(x) \underset{x\to0}{=} b(x+x^3) + d(x+x^3)^3 + o(x^4) \underset{x\to0}{=} bx + (b+d)x^3 + o(x^4)$$

et ainsi :

- *en utilisant que $f\circ f^{-1}(y) = y \underset{y\to0}{=} y + o(y^4)$, on trouve par unicité d'un dl que $b = 1$ et $b^3 + d = 0$, donc $d = -1$;*
- *en utilisant que $f^{-1}\circ f(x) = x \underset{x\to0}{=} x + o(x^4)$, on trouve par unicité d'un dl que $b = 1$ et $b + d = 0$ donc $d = -1$.*

Dans les deux cas on retrouve le même dl 4 de f^{-1} en 0, à savoir :

$$f^{-1}(y) \underset{x\to0}{=} y - y^3 + o(y^4)$$

III.2 Calcul de limites ou d'équivalents

Méthode III.4. *Pour calculer une limite ou un équivalent d'une fonction, on peut effectuer son développement limité jusqu'au premier ordre où la partie régulière est non nulle : on déduit ainsi un équivalent de la fonction, donc sa limite éventuelle.*

Exemple III.5. *Déterminons la limite en 0 de la fonction $f : x \mapsto \dfrac{1+\ln(1+x)-e^x}{1-\cos(x)}$.*
On effectue séparément les dl du numérateur et du dénominateur jusqu'au premier terme non nul :

- *pour le numérateur, un ordre 2 suffit :*

$$1+\ln(1+x)-e^x \underset{x\to0}{=} 1 + x - \frac{x^2}{2} - 1 - x - \frac{x^2}{2} + o(x^2) \underset{x\to0}{=} -x^2 + o(x^2) \underset{x\to0}{\sim} -x^2$$

- *c'est pareil pour le dénominateur :*

$$1-\cos(x) \underset{x\to0}{=} 1 - 1 + \frac{x^2}{2} + o(x^2) \underset{x\to0}{=} \frac{x^2}{2} + o(x^2) \underset{x\to0}{\sim} \frac{x^2}{2}$$

et ainsi :

$$f(x) \underset{x\to 0}{\sim} \frac{-x^2}{x^2/2} = -2$$

donc f tend vers -2 en 0.

Remarque III.6. *Il ne faudra pas pour autant systématiquement utiliser des dl : même si cela va aboutir, les calculs sont souvent assez lourds (plus que des équivalents ou des théorèmes d'encadrement).*
Par exemple, pour calculer la limite en 0 de $x \mapsto \dfrac{e^{\sin(x)} - e^{\tan(x)}}{\sin(x) - \tan(x)}$, on préfère y voir un taux d'accroissement de $\exp$ entre deux quantités qui tendent vers 0, et qui tend donc vers $\exp'(0) = 1$ par théorème des accroissements finis.

Remarque III.7. *On pourra aussi parfois travailler avec des dl nuls mais tout de même avoir des résultats. Par exemple, pour $f : x \mapsto \dfrac{x - \sin(x)}{\ln(1+x)}$, on trouve :*

$$f(x) \underset{x\to 0}{=} \frac{\mathrm{o}(x)}{x + \mathrm{o}(x)} \underset{x\to 0}{=} \mathrm{o}(1) \underset{x\to 0}{\to} 0.$$

mais dans ce cas on a seulement la limite (et pas un équivalent).

III.3 Position d'une courbe par rapport à sa tangente

Proposition III.8. *Soit f définie au voisinage de a, qui admet un développement limité de la forme :*

$$f(x) \underset{x\to a}{=} f(a) + f'(a)(x-a) + \alpha(x-a)^n + \mathrm{o}\left((x-a)^n\right)$$

pour $n \geq 2$ et $\alpha \neq 0$, alors :

1. *si n est pair : alors la courbe de f est au-dessus de sa tangente en a si $\alpha > 0$ et en dessous sinon ;*
2. *si n est impair : alors la courbe de f traverse sa tangente en a, et on a un point d'inflexion.*

Démonstration. L'équation de la tangente à la courbe de f est a est $y = f(a) + f'(a)(x-a)$. Donc la position de la courbe de f par rapport à cette courbe est donné par le signe de $f(x) - f(a) - f'(a)(x-a)$ au voisinage de a. D'après le dl de f, on a :

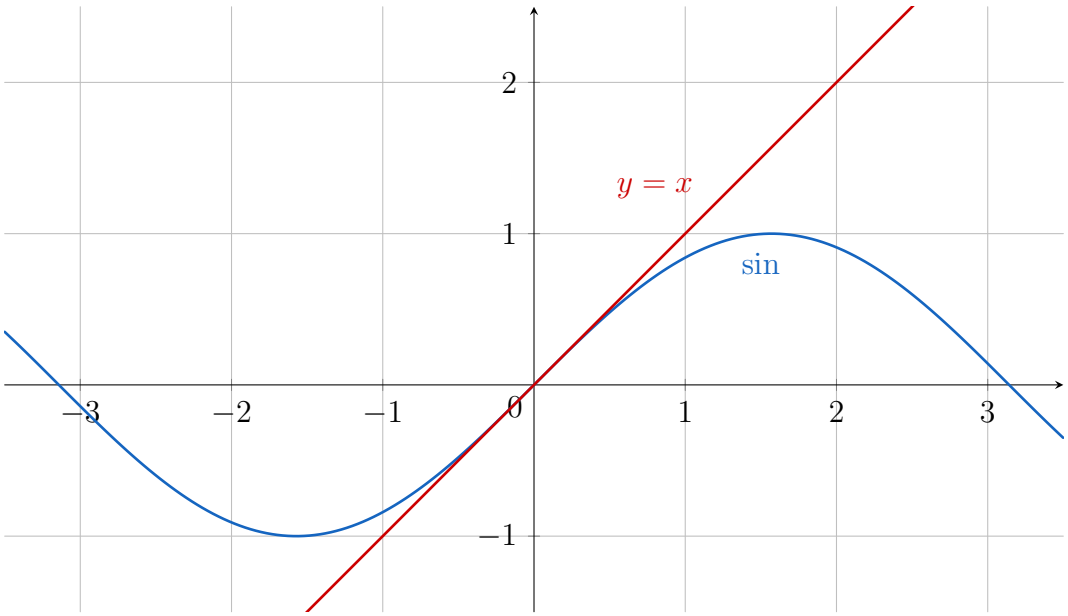
$$f(x) - f(a) - f'(a)(x-a) \underset{x\to a}{\sim} \alpha(x-a)^n$$

qui est donc du signe de $\alpha(x-a)^n$ d'après les propriétés des équivalents, ce qui donne le résultat selon les valeurs de α et n. □

Exemple III.9. *Au voisinage de 0, on a le dl suivant :*

$$\sin(x) \underset{x\to 0}{=} x - \frac{x^3}{6} + \mathrm{o}(x^3)$$

donc la courbe de $\sin$ admet un point d'inflexion en 0.



Corollaire III.10. *Avec les mêmes notations, si f possède un point critique en a, alors :*

1. *si n est pair : f possède un maximum en a si $\alpha < 0$ ou un minimum si $\alpha > 0$;*
2. *si n est impair : f n'admet pas d'extremum en a.*

III.4 Développements asymptotique

Remarque III.11. *Les dl s'inscrivent dans un cadre restrictif d'approximation par des polynômes. Plus généralement, on pourra utiliser des* ***développements asymptotiques*** *: des écritures de la forme :*

$$f(x) \underset{x\to a}{=} g_0(x) + g_1(x) + \cdots + g_n(x) + \mathrm{o}(g_n(x))$$

*où les fonctions g_i vérifient que pour $k > l$: $g_k(x) \underset{x\to a}{=} \mathrm{o}(g_l(x))$, et seront systématiquement des produits ou puissances de fonctions usuelles (*exp, ln *ou puissances de x).*
Et les mêmes types de développements s'appliquerait aussi pour des suites.
Ces développements sont d'autant plus intéressants quand les fonctions n'ont pas d'équivalent polynomial, ou lorsqu'on se place en $\pm\infty$ (car alors les $\mathrm{o}(x^n)$ ne donnent pas beaucoup d'information sur la fonction). Dans ce dernier cas, un développement asymptotique peut prendre la forme d'un développement limité en $\frac{1}{x}$ ou en e^{-x} (dont le calcul passe par celui d'un développement limité classique).

Exemples III.12.

1. *au voisinage de 0, on a :*

$$\ln(x)\sin(x) \underset{x\to 0}{=} x\ln(x) - \frac{x^3\ln(x)}{6} + \frac{x^5\ln(x)}{120} + \mathrm{o}(5\ln(x))$$

2. *au voisinage de $+\infty$:*

$$\begin{aligned}
\frac{x+2}{x^2-1} &= \frac{1}{x}\frac{1+\frac{2}{x}}{1-\frac{1}{x^2}} \\
&\underset{x\to+\infty}{=} \frac{1}{x}\left(1+\frac{2}{x}\right)\left(1+\frac{1}{x^2}+\frac{1}{x^4}+\mathrm{o}\left(\frac{1}{x^4}\right)\right) \\
&\underset{x\to+\infty}{=} \frac{1}{x}+\frac{2}{x^2}+\frac{1}{x^3}+\frac{2}{x^4}+\frac{1}{x^5}+\mathrm{o}\left(\frac{1}{x^5}\right)
\end{aligned}$$

3. au voisinage de $+\infty$:

$$\ln(1+e^{-x}) \underset{x\to+\infty}{=} e^{-x} - \frac{e^{-2x}}{2} + \frac{e^{-3x}}{3} + \mathrm{o}(e^{-3x}).$$

Exemple III.13. *Un développement asymptotique célèbre trouve ses origines dans la* ***formule de Stirling****, qui donne un équivalent pour la factorielle :*

$$n! \ \sim \ n^n e^{-n}\sqrt{2\pi n}.$$

On a ainsi que : $\dfrac{n!}{n^n e^{-n}\sqrt{2\pi n}} \underset{n\to+\infty}{\to} 1$, *donc* $\ln\left(\dfrac{n!}{n^n e^{-n}\sqrt{2\pi n}}\right) = \mathrm{o}(1)$, *et ainsi* $\ln(n!)$ *a pour développement asymptotique :*

$$\ln(n!) = n\ln(n) - n + \frac{\ln(n)}{2} + \frac{\ln(2\pi)}{2} + \mathrm{o}(1).$$

Méthode III.14. *Pour trouver l'asymptote d'une fonction f en $\pm\infty$, on peut chercher un développement asymptotique de la forme :*

$$f(x) \underset{x\to\pm\infty}{=} \alpha x + \beta + \mathrm{o}(1).$$

Dans ce cas, la droite d'équation $y = \alpha x + \beta$ est asymptote à f, et la position de la courbe de f par rapport à l'asymptote est donnée par le signe de $f(x) - \alpha x - \beta$, dont il suffit donc de trouver un équivalent.

Exemple III.15. *Étudions les asymptotes éventuelles de la fonction définie sur $\mathbb{R}\setminus]-1;1[$ par : $f(x) = \sqrt{x^2+1} + \sqrt{x^2-1}$.*
On se ramène tout d'abord au dl de $\sqrt{1+u}$ en 0, à savoir :

$$\sqrt{1+u} \underset{u\to0}{=} 1 + \frac{u}{2} - \frac{u^2}{8} + \frac{u^3}{16} + \mathrm{o}(u^3)$$

Et ainsi on déduit que :

$$\sqrt{x^2+1} = |x|\sqrt{1+\frac{1}{x^2}} \underset{x\to\pm\infty}{=} |x|\left(1 + \frac{1}{2x^2} - \frac{1}{8x^4} + \mathrm{o}\left(\frac{1}{x^4}\right)\right)$$

$$\sqrt{x^2-1} = |x|\sqrt{1-\frac{1}{x^2}} \underset{x\to\pm\infty}{=} |x|\left(1 - \frac{1}{2x^2} - \frac{1}{8x^4} + \mathrm{o}\left(\frac{1}{x^4}\right)\right)$$

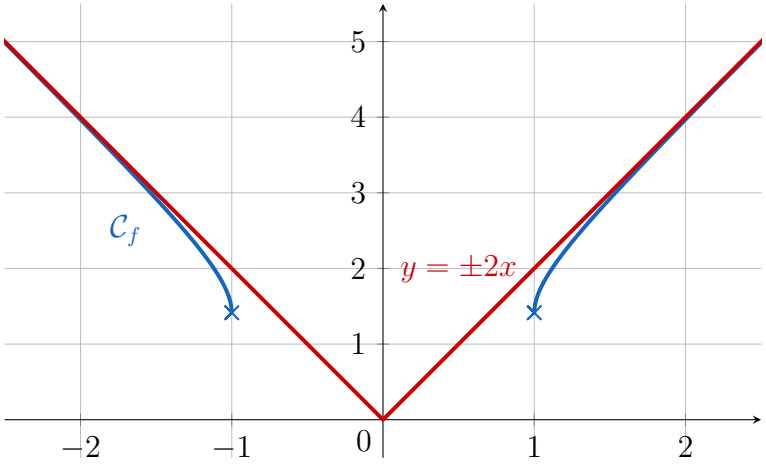
ce qui donne le développement asymptotique pour f :

$$f(x) \underset{x\to\pm\infty}{=} |x|\left(2 - \frac{1}{4x^4} + \mathrm{o}\left(\frac{1}{x^4}\right)\right)$$

et donc :

- *en $+\infty$: $f(x) \underset{x\to+\infty}{=} 2x - \dfrac{1}{4x^3} + \mathrm{o}(1/x^3)$, donc f admet la droite d'équation $y = 2x$ pour asymptote, et la courbe de f est en dessous de son asymptote ;*
- *en $-\infty$: $f(x) \underset{x\to-\infty}{=} -2x + \dfrac{1}{4x^3} + \mathrm{o}(1/x^3)$, donc f admet la droite d'équation $y = -2x$ pour asymptote, et la courbe de f est en dessous de son asymptote.*

Et notons au passage que la parité de f permet de se contenter d'une étude en $+\infty$ ou $-\infty$ pour avoir les deux résultats.



Méthode III.16. *On peut déterminer un développement asymptotique récursivement :*
- *on détermine un équivalent de la fonction f ou de la suite (u_n) ;*
- *on retranche cet équivalent ;*

et on répète les étapes précédentes : les équivalents ainsi trouvés constituent les termes du développement asymptotique.

Remarque III.17. *Un méthode qui ressemble beaucoup consiste à calculer des développements asymptotiques que l'on réinjecte dans une égalité (une équation fonctionnelle par exemple) pour gagner des ordres à chaque fois.*

Exemple III.18. *On considère la suite (u_n) définie par le fait que, pour tout $n \geq 3$, u_n est la plus petite solution de l'équation $e^x = nx$.*
Les variations de $f_n : x \mapsto e^x - nx$ montrent que $u_n \in]0; \dfrac{3}{n}[$, donc (u_n) tend vers 0. Mais on peut voir à quelle vitesse.
Comme (u_n) tend vers 0, alors $u_n = \mathrm{o}(1)$. Mais comme $f_n(u_n) = 0$, alors :

$$u_n = \frac{e^{u_n}}{n} = \frac{e^{\mathrm{o}(1)}}{n} = \frac{1}{n} + \mathrm{o}\left(\frac{1}{n}\right)$$

et en réinjectant ce développement plus poussé on trouve :

$$u_n = \frac{e^{\frac{1}{n}+\mathrm{o}\left(\frac{1}{n}\right)}}{n} = \frac{1 + \frac{1}{n} + \mathrm{o}\left(\frac{1}{n}\right)}{n} = \frac{1}{n} + \frac{1}{n^2} + \mathrm{o}\left(\frac{1}{n^2}\right)$$

et on recommence :

$$u_n = \frac{e^{\frac{1}{n}+\frac{1}{n}^2+\mathrm{o}\left(\frac{1}{n^2}\right)}}{n} = \frac{1 + \frac{1}{n} + \frac{1}{n^2} + \frac{1}{2n^2} + \mathrm{o}\left(\frac{1}{n^2}\right)}{n} = \frac{1}{n} + \frac{1}{n^2} + \frac{3}{2n^2} + \mathrm{o}\left(\frac{1}{n^3}\right)$$

et on pourrait continuer sans se lasser...

Chapitre 20

Espaces vectoriels et applications linéaires

Dans tout ce chapitre, on désigne $\mathbb{K}$ un corps (par exemple $\mathbb{R}$ ou $\mathbb{C}$), dont les éléments seront appelés scalaires.

I Espaces vectoriels

I.1 La structure d'espace vectoriel

Définition I.1. *Si E, F sont deux ensembles non vides, une **loi de composition externe** (abrégée en lce) de F sur E est une application de $F \times E$ sur E.*

Remarque I.2. *Si $\cdot$ est une lce, on notera plus simplement $\lambda \cdot x$ au lieu de $\cdot(\lambda, x)$.*

Définition I.3. *Si E est un ensemble muni d'une lci $+$ et d'une lce $\cdot$ de $\mathbb{K}$ sur E, on dit que $(E, +, \cdot)$ est un $\mathbb{K}$-**espace vectoriel** (ou **espace vectoriel sur** $\mathbb{K}$, abrégé parfois $\mathbb{K}$-ev) si :*

1. *$(E, +)$ est un groupe abélien (qu'on notera additivement), et dont l'élément neutre 0_E est appelé le **vecteur nul** ;*
2. *$\forall x \in E, 1 \cdot x = x$;*
3. *$\forall \lambda \in \mathbb{K},\ \forall x, y \in E,\ \lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$;*
4. *$\forall \lambda, \mu \in \mathbb{K},\ \forall x \in E,\ (\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot y$;*
5. *$\forall \lambda, \mu \in \mathbb{K},\ \forall x \in E,\ (\lambda\mu) \cdot x = \lambda \cdot (\mu \cdot x)$.*

*Dans ce cas, les éléments de E sont appelés **vecteurs**.*

Exemples I.4.

1. *Sur $\mathbb{K}$, on peut voir la multiplication comme une lce, ce qui fournit à $\mathbb{K}$ une structure d'espace vectoriel. On peut même faire agir un sous-corps par multiplication sur $\mathbb{K}$: par exemple, $\mathbb{C}$ est un espace vectoriel sur $\mathbb{C}$, sur $\mathbb{R}$ ou sur $\mathbb{Q}$.*
2. *Plus généralement, pour $n \in \mathbb{N}^*$, la multiplication de toutes les coordonnées d'un élément de $\mathbb{K}^n$ par un élément de $\mathbb{K}$ munit $\mathbb{K}^n$ d'une structure d'espace vectoriel sur $\mathbb{K}$.*
3. *La multiplication scalaire munit $\mathcal{M}_{n,p}(\mathbb{K})$ d'une structure de $\mathbb{K}$-espace vectoriel, tout comme la multiplication par une constante dans $\mathbb{K}[X]$ ou $\mathbb{K}(X)$.*
4. *L'ensemble des solutions d'une équation différentielle linéaire homogène est aussi un $\mathbb{K}$-ev, comme l'ensemble des solutions d'un système linéaire homogène.*

Proposition I.5 (Espace produit)**.** *Si E, F sont deux $\mathbb{K}$-ev, alors l'ensemble $E \times F$ muni des opérations :*

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2) \text{ et } \lambda \cdot (x, y) = (\lambda \cdot x, \lambda \cdot y)$$

est un $\mathbb{K}$-ev.

Démonstration. On avait déjà vu que le produit de deux groupes est un groupe. Reste à vérifier les propriétés de la lce, qui découlent de celles pour E et F.
Pour $(x,y) \in E \times F$, on a : $1 \cdot (x,y) = (1 \cdot x, 1 \cdot y) = (x,y)$.
Si $\lambda \in \mathbb{K}$ et $x_1, x_2 \in E$, $y_1, y_2 \in F$, alors :

$$\begin{aligned} \lambda \cdot ((x_1,y_1)+(x_2,y_2)) &= \lambda \cdot (x_1+x_2, y_1+y_2) = (\lambda \cdot (x_1+x_2), \lambda \cdot (y_1+y_2)) \\ &= (\lambda \cdot x_1 + \lambda \cdot x_2, \lambda \cdot y_1 + \lambda \cdot y_2) = (\lambda \cdot x_1, \lambda \cdot y_1) + (\lambda \cdot x_2, \lambda \cdot y_2) \\ &= \lambda \cdot (x_1,y_1) + \lambda \cdot (x_2,y_2) \end{aligned}$$

□

Remarque I.6. *Le résultat se généralise à un nombre fini de $\mathbb{K}$-ev. Par exemple on retrouve que $\mathbb{K}^n = \mathbb{K} \times \cdots \times \mathbb{K}$ est un espace vectoriel, de vecteur nul $(0,\ldots,0)$.*

Proposition I.7. *Si Ω est un ensemble non vide et E est un $\mathbb{K}$-espace vectoriel, on munit $\mathcal{F}(\Omega,E)$ de la lci $+$ et de la lce $\cdot$ suivantes :*

$$\forall f,g \in \mathcal{F}(\Omega,E),\ f+g : \left\{ \begin{array}{ccc} \Omega & \to & E \\ x & \mapsto & f(x)+g(x) \end{array} \right. ;$$

$$\forall f \in \mathcal{F}(\Omega,E),\ \forall \lambda \in \mathbb{K},\ \lambda \cdot f : \left\{ \begin{array}{ccc} \Omega & \to & E \\ x & \mapsto & \lambda \cdot f(x) \end{array} \right. .$$

Alors $(\mathcal{F}(\Omega,E),+,\cdot)$ est un $\mathbb{K}$-espace vectoriel.

Démonstration. On vérifie facilement que $(\mathcal{F}(\Omega,E),+)$ est un groupe : les propriétés de la loi $+$ sur E sont aussi vérifiées par les éléments de $\mathcal{F}(\Omega,E)$. La fonction $x \mapsto 0_E$ est son élément neutre, et l'opposé d'une fonction f est la fonction $x \mapsto -f(x)$.
De même, il est clair que les propriétés de $\cdot$ sur E sont aussi vérifiées sur $\mathcal{F}(\Omega,E)$.
Et finalement on a bien un $\mathbb{K}$-ev. □

Remarques I.8.

1. *La situation la plus simple est lorsque $E = \mathbb{K}$: la multiplication et l'addition sont directement celles de $\mathbb{K}$ comme corps.*
2. *L'ensemble Ω n'a besoin d'aucune structure, comme toutes les opérations se font sur les images d'éléments de Ω.*
3. *Dans le cas particulier où $\Omega = \mathbb{N}$ et $E = \mathbb{K}$, on trouve que l'ensemble des suites à valeurs dans $\mathbb{K}$ est un $\mathbb{K}$-espace vectoriel. Plus généralement, l'ensemble des suites à valeurs dans E est aussi un $\mathbb{K}$-ev.*

Proposition I.9. *Si $(E,+,\cdot)$ est un $\mathbb{K}$-ev, alors :*

1. *pour tous $\lambda \in \mathbb{K}$ et $x \in E$: $\lambda \cdot x = 0_E \Leftrightarrow (\lambda = 0$ ou $x = 0_E)$;*
2. *pour tout $x \in E$: $(-1) \cdot x = -x$.*

Démonstration.

1. Si $x = 0_E$, alors $0_E + 0_E = 0_E$ donc $\lambda \cdot 0_E = \lambda \cdot 0_E + \lambda \cdot 0_E$, donc $\lambda \cdot 0_E = 0_E$.
   De même, si $\lambda = 0$: $0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x$ donc $0 \cdot x = 0_E$.
   Inversement, si $\lambda \neq 0$, alors :
   $$\lambda \cdot x = 0_E \Rightarrow \left(\frac{1}{\lambda}\lambda\right) \cdot x = 0_E \Rightarrow x = 0_E$$
   ce qui montre bien l'équivalence.
2. Pour $x \in E$, on a :
   $$(-1) \cdot x + x = (-1) \cdot x + 1 \cdot x = (-1+1) \cdot x = 0 \cdot x = 0_E$$
   ce qui montre bien que $(-1) \cdot x$ est l'opposé de x, c'est-à-dire $-x$.

□

I.2 Sous-espaces vectoriels

Définition I.10. *Si $(E,+,\cdot)$ est un $\mathbb{K}$-ev et F est une partie de E, on dit que F est un **sous-espace vectoriel** (abrégé sev) de E si F est stable par les lois $+$ et $\cdot$ et que $(F,+,\cdot)$ est un $\mathbb{K}$-ev.*

Remarque I.11. *Les ensembles $\{0_E\}$ et E sont toujours des sev de E, qu'on appelle **sous-espaces vectoriels triviaux**.*

Proposition I.12. *Si $(E,+,\cdot)$ est un $\mathbb{K}$-ev et F est une partie de E, alors F est un sev de E si, et seulement si :*

1. *F est non-vide ;*
2. *F est stable par combinaison linéaire : $\forall x,y\in F,\ \forall\lambda\in\mathbb{K},\lambda\cdot x+y\in F$.*

Démonstration. Par définition d'un sev, il est clair que, si F est un sev, alors il vérifie les deux propriétés. Réciproquement, si F est non vide et stable par combinaison linéaire. Alors :

- en prenant $\lambda=-1$, on déduit déjà que : pour tous $x,y\in F$, on a $x-y\in F$. Comme F est non vide, ceci assure déjà que F est un groupe abélien (c'est un sous-groupe de E, qui est abélien) ; ainsi F est stable par la loi $+$;
- donc $0_E\in F$, et en prenant $y=0_E$, on trouve que pour tout $\lambda\in\mathbb{K}$ et tout $x\in F$: $\lambda\cdot x\in F$; ainsi F est stable par la loi $\cdot$;
- reste à vérifier que les propriétés qui relient les lois $+$ et $\cdot$ sont bien celles d'un $\mathbb{K}$-ev, mais celles-ci découle du fait que F est une partie de E, donc les propriétés vérifiées pour les éléments de E le sont aussi pour les éléments de F.

D'où le résultat. □

Remarque I.13. *Comme pour les sous-groupes, un sev contient toujours 0_E, donc en pratique on montrera que $0_E\in F$ pour s'assurer que F est non vide.*
De même, pour des raisons de symétrie des rôles de x et y, on écrit parfois les combinaisons linéaires sous la forme $\lambda x+\mu y$, mais le résultat reste le même.

Exemples I.14.

1. *Pour tout $n\in\mathbb{N}$, l'ensemble $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$.*
2. *Dans $\mathcal{M}_n(\mathbb{K})$, les ensembles de matrices triangulaires supérieures, triangulaires inférieures, diagonales, symétriques ou antisymétriques sont des sous-espaces vectoriels de $\mathcal{M}_n(\mathbb{K})$.*
3. *Dans $\mathbb{K}^{\mathbb{N}}$, l'ensemble des suites de limite nulle est un sev. Plus généralement, l'ensemble des suites de limite finie est aussi un sev de $\mathbb{K}^{\mathbb{N}}$. Ce sont eux-même des sev du $\mathbb{K}$-ev de l'ensemble des suites bornées. Ce n'est en revanche pas le cas de :*
   - *l'ensemble des suites de limite infinie : car, pour une telle suite (u_n), $(0\cdot u_n)$ tend vers 0, donc il n'est pas stable par $\cdot$;*
   - *l'ensemble des suites ayant une limite : avec $u_n=n+\sin(n)$ et $v_n=-n$, on trouve que $u_n+v_n=\sin(n)$ qui n'a pas de limite, donc il n'est pas stable par somme.*
4. *Dans $\mathbb{R}^2$, les points de la droite d'équation $ax+by=0$ (pour $a,b\in\mathbb{R}$ non tous nuls) est un sev de $\mathbb{R}^2$ qu'on appelle **droite vectorielle**.*
5. *Dans $\mathbb{R}^3$, les points du plan d'équation $ax+by+cz=0$ (pour $a,b,c\in\mathbb{R}$ non tous nuls) est un sev de $\mathbb{R}^3$ qu'on appelle **plan vectoriel**.*

Proposition I.15. *Si $(F_i)_{i\in I}$ est une famille de sev de E, alors $F=\cap_{i\in I}F_i$ est un sev de E.*

Démonstration. Comme $0_E\in F_i$ pour tout $i\in I$, alors $0_E\in F$ et ainsi $F\neq\emptyset$.
Si $x,y\in F$, $\lambda\in\mathbb{K}$ et $i\in I$: alors $x,y\in F_i$, qui est un espace vectoriel, donc $\lambda\cdot x+y\in F_i$. Comme ceci est vrai pour tout i, on déduit que $\lambda\cdot x+y\in F$.
Donc F est un sev de E. □

Remarque I.16. *Comme pour les groupes, l'union ne se comporte pas bien avec les espaces vectoriels (notamment à cause de leur structure de groupe).*

Exemple I.17. *On peut ainsi voir de deux manières que l'ensemble des solutions d'un système linéaire homogène est un espace vectoriel :*

- *soit directement comme on a vu que c'est un ensemble non-vide (le vecteur nul est toujours solution) stable par combinaison linéaire) ;*
- *soit en constatant que les solutions de chaque équation du système forme un sev de $\mathbb{R}^p$: l'ensemble solution du système complet est donc l'intersection de n sev de $\mathbb{R}^p$, et est donc un sev de $\mathbb{R}^p$.*

Corollaire I.18. *Si $A \subset E$ est non vide, alors :*

$$\bigcap_{\substack{F \text{ sev de } E \\ A \subset F}} F$$

est le plus petit espace vectoriel contenant A.

II Famille de vecteurs

II.1 Combinaisons linéaires et sous-espaces engendrés

Définition II.1. *Si $x_1, \dots, x_n \in E$, on dit que $x \in E$ est une* ***combinaison linéaire de*** *$x_1, \dots, x_n$ s'il existe $\lambda_1, \dots, \lambda_n \in \mathbb{K}$ tels que : $x = \sum_{i=1}^n \lambda_i \cdot x_i$.*
L'ensemble des combinaisons linéaires de $x_1, \dots, x_n$ est noté $\mathrm{Vect}(x_1, \dots, x_n)$, c'est-à-dire que :

$$\mathrm{Vect}(x_1, \dots, x_n) = \left\{ \sum_{i=1}^n \lambda_i \cdot x_i \,|\, \lambda_1, \dots, \lambda_n \in \mathbb{K} \right\}.$$

Exemple II.2. *On se place dans $\mathbb{R}^3$ est on considère les vecteurs $x_1 = (1, -1, 0)$, $x_2 = (0, 1, -1)$ et $x_3 = (-1, 0, 1)$. Alors :*

$$\mathrm{Vect}(x_1, x_2, x_3) = \{\lambda x_1 + \mu x_2 + \nu x_3 \,|\, \lambda, \mu, \nu \in \mathbb{R}\}.$$

Mais pour $\lambda, \mu, \nu \in \mathbb{R}$ on a :

$$\lambda \cdot x_1 + \mu \cdot x_2 + \nu \cdot x_3 = (\lambda, -\lambda, 0) + (0, \mu, -\mu) + (-\nu, 0, \nu) = (\lambda - \nu, \mu - \lambda, \nu - \mu).$$

Et ainsi un élément $(x, y, z) \in \mathbb{R}^3$ est dans $\mathrm{Vect}(x_1, x_2, x_3)$ si, et seulement si, il existe $\lambda, \mu, \nu \in \mathbb{R}$ tels que :

$$\begin{cases} \lambda - \nu &= x \\ \mu - \lambda &= y \\ \nu - \mu &= z \end{cases}$$

que l'on peut résoudre comme un système en λ, μ, ν. En échelonnant, on trouve que le système est équivalent à :

$$\begin{cases} \lambda & & - & \nu &= x \\ & \mu & - & \nu &= x + y \\ & - \mu & + & \nu &= z \end{cases}$$

qui admet donc une solution si, et seulement si $x + y = -z$, c'est-à-dire $x + y + z = 0$.
Et donc $\mathrm{Vect}(x_1, x_2, x_3)$ est le plan d'équation $x + y = z = 0$.

Remarque II.3. *La définition précédente se généralise à des familles ou des parties quelconques (éventuellement infinies ou même vide) de E :*

— *si $A \subset E$: on note* $\mathrm{Vect}(A)$ *l'ensemble des combinaisons linéaires d'un nombre* ***fini*** *d'éléments de A :*

$$\mathrm{Vect}(A) = \left\{ \sum_{i=1}^{n} \lambda_i \cdot x_i \,|\, n \in \mathbb{N},\ x_1, \dots, x_n \in A,\ \lambda_1, \dots, \lambda_n \in \mathbb{K} \right\}.$$

— *si $(a_i)_{i \in I}$ est une famille d'éléments de E :*

$$\mathrm{Vect}(a_i)_{i \in I} = \left\{ \sum_{\substack{j \in J \\ J \subset I \text{ fini}}} \lambda_j \cdot x_j \,|\, (\lambda_j) \in J^{\mathbb{K}} \right\}.$$

Dans tous les cas, on travaille avec des sommes ***finies*** *et on utilise plutôt la notion de* ***famille presque nulle*** *(ou* ***famille à support fini****) : étant donné A (fini ou non), c'est une famille $(\lambda_a)_{a \in A}$ telle que $\{a \in A \,|\, \lambda_a \neq 0\}$ est fini. Et alors :*

$$\mathrm{Vect}(A) = \left\{ \sum_{a \in A} \lambda_a \cdot A \,|\, (\lambda_a) \text{ à support fini} \right\}.$$

Exemple II.4. *D'après la formule de Taylor polynomiale, on a pour tout $a \in \mathbb{K}$ que :*

$$\mathrm{Vect}\left((X-a)^k\right)_{k \in [\![0;n]\!]} = \mathbb{K}_n[X] \text{ et } \mathrm{Vect}\left((X-a)^k\right)_{k \in \mathbb{N}} = \mathbb{K}[X].$$

Proposition-Définition II.5. *Étant donnée A une partie de E :*

1. $\mathrm{Vect}(A)$ *est un sev de E.*
2. *C'est le plus petit sev de E contenant A, dans le sens où : si F est un sev contenant A, alors il contient* $\mathrm{Vect}(A)$.

On appellera ainsi $\mathrm{Vect}(A)$ *le* ***sous-espace vectoriel engendré par*** *A.*

Démonstration.

1. La combinaison linéaire nulle (obtenue ou bien avec la famille vide ou avec les scalaires tous nuls) est dans $\mathrm{Vect}(A)$, donc $0_E \in \mathrm{Vect}(A) \neq \emptyset$.
   Si $x, y \in \mathrm{Vect}(A)$: quitte à rajouter des termes nuls dans les sommes qui suivent, on peut supposer que :
   $$x = \sum_{i=1}^{n} \lambda_i \cdot a_i \text{ et } \sum_{i=1}^{n} \mu_i \cdot a_i$$
   pour $\lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_n \in \mathbb{K}$ et $a_1, \dots, a_n \in A$.
   Et ainsi, pour tout $\nu \in \mathbb{K}$:
   $$\nu \cdot x + y = \sum_{i=1}^{n} (\nu\lambda_i + \mu_i) \cdot a_i \in \mathrm{Vect}(A)$$
   et donc $\mathrm{Vect}(A)$ est stable par combinaison linéaire.
   Donc $\mathrm{Vect}(A)$ est un sev de E.
2. Soit F un sev de E contenant A. Soit $x \in \mathrm{Vect}(A)$. On écrit $x = \sum_{i=1}^{n} \lambda_i \cdot a_i$ pour $\lambda_1, \dots, \lambda_n \in \mathbb{K}$ et $a_1, \dots, a_n \in A$.
   Et alors :
   — comme F contient A, il contient tous les a_i ;
   — comme F est stable par $\cdot$, il contient tous les $\lambda_i \cdot a_i$;
   — comme F est stable par $+$, il contient x.

Et donc $\text{Vect}(A) \subset F$.

□

Corollaire II.6. *Si A, B sont deux parties de E, alors :*

1. *si $A \subset B$, alors $\text{Vect}(A) \subset \text{Vect}(B)$;*
2. *si $A \subset \text{Vect}(B)$, alors $\text{Vect}(A \cup B) = \text{Vect}(B)$.*

Démonstration.

1. Comme $B \subset \text{Vect}(B)$ et que $A \subset B$, alors $A \subset \text{Vect}(B)$, donc $\text{Vect}(A) \subset \text{Vect}(B)$.
2. On a déjà que $\text{Vect}(B) \subset \text{Vect}(A \cup B)$ comme $B \subset A \cup B$.
   Mais on a aussi que $B \subset \text{Vect}(B)$ et $A \subset \text{Vect}(B)$, donc $A \cup B \subset \text{Vect}(B)$, puis $\text{Vect}(A \cup B) \subset \text{Vect}(B)$.
   Et l'égalité découle par double inclusion.

□

Remarque II.7. *On pratique, on pourra utiliser ce résultat avec des familles finies. Par exemples, en considérant les vecteurs $x_1, \dots, x_n$, ce résultat dit que :*

1. *si $m \leq n$: $\text{Vect}(x_1, \dots, x_m) \subset \text{Vect}(x_1, \dots, x_n)$;*
2. *si $x_n \in \text{Vect}(x_1, \dots, x_{n-1})$, alors $\text{Vect}(x_1, \dots, x_{n-1}) = \text{Vect}(x_1, \dots, x_n)$.*

Exemple II.8. *Si on reprend les vecteurs $x_1 = (1, -1, 0), x_2 = (0, 1, -1), x_3 = (-1, 0, 1)$, on a $x_1 + x_2 + x_3 = 0$, et donc : $x_3 = -x_1 - x_2 \in \text{Vect}(x_1, x_2)$.*
Et donc $\text{Vect}(x_1, x_2, x_3) = \text{Vect}(x_1, x_2)$.
On peut le retrouver en notant qu'un élément $(x, y, z) \in \mathbb{R}^3$ est dans $\text{Vect}(x_1, x_2)$ si, et seulement si, il existe $\lambda, \mu \in \mathbb{R}$ tels que :

$$\begin{cases} \lambda &= x \\ \mu - \lambda &= y \\ -\mu &= z \end{cases}$$

qu'on résout pour obtenir le système équivalent :

$$\begin{cases} \lambda &= x \\ \mu &= -z \\ 0 &= x + y + z \end{cases}$$

qui a donc une solution si, et seulement si, $x + y + z = 0$, et on retrouve le plan d'équation $x + y + z = 0$.

II.2 Familles génératrices

Définition II.9 (Famille génératrice)**.** *Une famille A (ou une partie) de E est dite **génératrice** si $\text{Vect}(A) = E$, c'est-à-dire si tout vecteur de E peut s'écrire comme combinaison linéaire d'éléments de A.*

Remarque II.10. *On dit aussi que A **engendre** E.*

Exemples II.11.

1. *La famille $(1, X, \dots, X^n)$ (pour $n \in \mathbb{N}$) est une famille génératrice de $\mathbb{K}_n[X]$, tout comme les familles $(1, X - a, \dots, (X - a)^n)$ pour $a \in \mathbb{K}$ (par les formules de Taylor). Plus généralement, la famille infinie $(1, X - a, \dots, (X - a)^n, \dots)$ engendre $\mathbb{K}[X]$.*
2. *Les matrices élémentaires de taille $n \times p$ engendrent $\mathcal{M}_{n,p}(\mathbb{K})$.*

Définition II.12 (Droite vectorielle)**.** *Un sev engendré par un unique vecteur non nul est appelé **droite vectorielle**.*

Exemple II.13. *Reprenons dans $\mathbb{R}^2$ la droite d'équation $ax+by=0$, et montrons qu'il s'agit d'une droite vectorielle au sens de la définition précédente.*
Le vecteur $(x,y)\in\mathbb{R}^2$ est un élément de la droite si, et seulement si, $ax+by=0$, et donc :
— *si $a\neq 0$: alors $x=-\frac{b}{a}y$, donc $(x,y)=\left(-\frac{b}{a}y,y\right)=y\cdot\left(-\frac{b}{a},1\right)=-\frac{y}{a}\cdot(b,-a)$;*
— *si $a=0$: on a $b\neq 0$, donc $y=0$, donc $(x,y)=(x,0)=\frac{x}{b}\cdot(b,-a)$.*
et donc dans les deux cas $(x,y)\in\mathrm{Vect}((b,-a))$: on a donc bien une droite vectorielle.

II.3 Familles libres

Définition II.14 (Famille libre)**.** *Une famille $A=(a_i)_{i\in I}$ de E est dite **libre** si pour toute famille $(\lambda_i)_{i\in I}$ à support fini d'éléments de $\mathbb{K}$:*

$$\sum_{i\in I}\lambda_i\cdot a_i=0_E\Rightarrow\forall i\in I,\ \lambda_i=0$$

c'est-à-dire si la seule combinaison linéaire nulle a tous ses coefficients nuls.
En particulier, si $A=(a_1,\dots,a_n)$ est une famille finie, alors A est libre si :

$$\forall\lambda_1,\dots,\lambda_n\in\mathbb{K},\ \sum_{i=1}^{n}\lambda_i\cdot a_i=0\Rightarrow\lambda_1=\cdots=\lambda_n=0.$$

Remarques II.15.

1. *Il s'agit en fait d'une équivalence, mais la réciproque est toujours vérifiée.*
2. *On dit aussi que les éléments de A sont **linéairement indépendants**.*
3. *Une famille qui n'est pas libre est dite **liée**.*
4. *Ce résultat se transpose aux parties de E, mais l'intérêt des familles est qu'elles permettent d'exprimer des redondances.*
5. *Comme les combinaisons linéaires sont à support fini, une famille infinie est libre si, et seulement si, toutes ses sous-familles finies sont libres.*

Exemples II.16.

1. *Dans $\mathbb{R}^3$, la famille formée des vecteurs $x_1=(1,-1,0),x_2=(0,1,-1),x_3=(-1,0,1)$ est liée, puisque :*

$$0=x_1+x_2+x_3=1\cdot x_1+1\cdot x_2+1\cdot x_3$$

et que $(1,1,1)\neq(0,0,0)$.

2. *Une famille formée d'un seul vecteur x est libre si, et seulement si, x est non nul :*
— *si $x=0$: alors $1\cdot x=0$, donc on a une combinaison linéaire nulle dont tous les coefficients ne sont pas nuls ;*
— *si $x\neq 0$: alors pour tout $\lambda\in\mathbb{K}$: $\lambda\cdot x=0\Rightarrow\lambda=0$, donc la famille est libre.*

3. *Sur $\mathcal{M}_{n,p}(\mathbb{K})$, les matrices élémentaires forment une famille libre, du fait de l'unicité de l'écriture : le seul moyen d'écrire la matrice nulle comme combinaison linéaire de matrices élémentaires est que tous les coefficients soient nuls.*

4. *Si $A\in\mathcal{M}_n(\mathbb{K})$, dont on note $A_1,\dots,A_n$ les colonnes, on a pour tous $\lambda_1,\dots,\lambda_n$:*

$$\lambda_1A_1+\cdots+\lambda_nA_n=A\cdot\begin{pmatrix}\lambda_1\\ \vdots\\ \lambda_n\end{pmatrix}$$

et ainsi un combinaison linéaire nulle correspond à une solution à l'équation $AX=0$ (d'inconnue $X\in\mathcal{M}_{n,1}(\mathbb{K})$). Et donc la matrice A est inversible si, et seulement si, cette équation a pour seule solution $X=0$, c'est-à-dire si, et seulement si, les colonne de A forment une famille libre de $\mathcal{M}_{n,1}(\mathbb{K})$.

Proposition II.17. *Une famille est liée si, et seulement si, l'un de ses vecteurs s'exprime comme combinaison linéaire d'autres de ses vecteurs.*
Pour $A = (a_i)_{i\in I}$, cela revient à dire que :

$$\exists i_0 \in I, \exists (\lambda_i) \in \mathbb{K}^{I\setminus\{i_0\}} \text{ à support fini, } a_{i_0} = \sum_{i\neq i_0} \lambda_i \cdot a_i.$$

Démonstration. Si A est liée, notons $(\mu_i)_{i\in I}$ famille non nulle à support finie telle que $\sum_{i\in I} \mu_i \cdot a_i = 0$.
Comme (μ_i) n'est pas nulle, il existe $i_0 \in I$ tel que $\mu_{i_0} \neq 0$. Ainsi, en posant pour tout $i \neq i_0$: $\lambda_i = -\frac{\mu_i}{\mu_{i_0}}$, alors la famille (λ_i) est bien définie, à support fini, et vérifie :

$$a_{i_0} = -\sum_{i\in I\setminus\{i_0\}} \frac{\mu_i}{\mu_{i_0}} \cdot a_i = \sum_{i\neq i_0} \lambda_i \cdot a_i$$

ce qui montre la première implication.
Réciproquement, si $a_{i_0} = \sum_{i\neq i_0} \lambda_i \cdot a_i$, alors en posant $\mu_i = \lambda_i$ si $i \neq i_0$ et $\mu_{i_0} = -1$, on a :

$$\sum_{i\in I} \mu_i \cdot a_i = \sum_{i\neq i_0} \lambda_i \cdot a_i - a_{i_0} = 0$$

et la famille (μ_i) est bien à support fini (comme les λ_i, comme on change seulement la valeur pour i_0) et non nulle (comme $\mu_{i_0} = 1 \neq 0$), donc la famille est liée. □

Proposition-Définition II.18 (Vecteurs colinéaires)**.** *On dit que les vecteurs $x, y \in E$ sont **colinéaires** si la famille (x, y) est liée. C'est le cas si, et seulement si :*

$$\exists \lambda \in \mathbb{K},\ x = \lambda \cdot y \text{ ou } y = \lambda \cdot x.$$

En particulier, si x est non nul, l'ensemble des vecteurs colinéaires à x constitue la droite vectorielle $\mathrm{Vect}(x)$.

Démonstration. Le début découle du point précédent.
Pour l'ensemble des vecteurs colinéaires à x, par le point précédent, on a déjà qu'il contient $\mathrm{Vect}(x)$ (comme ce sont exactement les combinaisons linéaires de x).
Inversement, si y est colinéaire à x, alors :
— soit $y = \lambda \cdot x$: et alors $y \in \mathrm{Vect}(x)$ par définition ;
— soit $x = \lambda \cdot y$: mais, comme $x \neq 0$, alors $\lambda \neq 0$ et donc $y = \frac{1}{\lambda} \cdot x \in \mathrm{Vect}(x)$.
d'où l'autre inclusion, et donc le résultat. □

Remarques II.19.

1. *Le vecteur nul est colinéaire à tout autre vecteur.*
2. *Si x, y sont non nuls, alors ils sont colinéaires si, et seulement si, $x = \lambda \cdot y$ pour $\lambda \in \mathbb{K}^*$.*
   En particulier, la relation "être colinéaire à" définit une relation d'équivalence sur $E \setminus \{0\}$, et deux éléments $x, y \in E \setminus \{0\}$ sont dans la même classe si, et seulement si : $\mathrm{Vect}(x) = \mathrm{Vect}(y)$.

Corollaire II.20. *Une famille qui contient le vecteur nul, ou deux vecteurs colinéaires (par exemple deux vecteurs égaux) est liée.*

Proposition II.21. *Soient A, B deux familles avec $A \subset B$:*

1. *si A est liée, alors B est liée ;*
2. *si B est libre, alors A est libre.*

Démonstration. On pourrait montrer l'une ou l'autre des assertions, dans la mesure où elles sont contraposées l'une de l'autre.

1. si A est liée : notons une combinaison linéaire nulle d'éléments de A à coefficients non tous nuls. C'est donc (par l'inclusion $A \subset B$) une combinaison linéaire nulle à coefficients non tous nuls d'éléments de B. Donc B est liée.
2. si B est libre : considérons une combinaison linéaire nulle d'éléments de A. Alors c'est une combinaison linéaire nulle d'éléments de B (par l'inclusion $A \subset B$), donc tous ses coefficients sont nuls (comme B est libre). Donc A est libre.

□

Corollaire II.22. *La famille $A = (a_i)_{i\in I}$ est libre si, et seulement si, pour n'importe quel $i_0 \in I$:*

1. *la famille $A_{i_0} = (a_i)_{i\neq i_0}$ est libre ;*
2. *$a_{i_0} \notin \mathrm{Vect}(A_{i_0})$.*

Remarque II.23. *Ici, on peut librement interpréter le "n'importe quel" comme un quantificateur existenciel ou universel et le résultat reste vrai.*

Démonstration. Si A est libre : toute sous-famille de A est libre, donc pour tout $i_0 \in I$ la famille A_{i_0} est libre, et aucun élément de A ne s'exprime comme combinaison linéaire des autres, donc $a_{i_0} \notin \mathrm{Vect}(A_{i_0})$.

Inversement, si A est liée, notons $\sum_i \lambda_i a_i$ une combinaison linéaire nulle à support fini où tous les λ_i ne sont pas nul, et considérons $i_0 \in I$:

— si $\lambda_{i_0} = 0$: alors la famille A_{i_0} est liée, car l'un au moins des autres λ_i est non nul et $\sum_{i\neq i_0} \lambda_i a_i$;

— si $\lambda_{i_0} \neq 0$: alors $a_{i_0} = \dfrac{-1}{\lambda_{i_0}} \sum_{i\neq i_0} \lambda_i a_i \in \mathrm{Vect}(A_{i_0})$.

D'où l'équivalence. □

Corollaire II.24. *Si A est une famille et a est un vecteur, la famille $A \cup \{a\}$ est libre si, et seulement si, la famille A est libre et que $a \notin \mathrm{Vect}(A)$.*

Proposition II.25. *Une famille de polynômes de degrés deux-à-deux distincts est libre.*

Démonstration. Soient $P_1, \ldots, P_n$ polynômes de degrés deux-à-deux distincts et $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ tels que $\sum_{i=1}^n \lambda_i P_i = 0$.
Quitte à renuméroter les polynômes, on peut supposer que $\deg(P_1) < \deg(P_2) < \cdots < \deg(P_n)$.
Mais alors :

$$\lambda_n P_n = -\sum_{i=1}^{n-1} \lambda_i P_i$$

et en passant au degré on déduit que $\lambda_n = 0$ car sinon on aurait :

$$\deg(P_n) \leq \max\{\deg(P_1), \ldots, \deg(P_{n-1})\}.$$

Et en itérant ce processus on trouve que tous les λ_i sont nuls, donc la famille est libre. □

Remarque II.26. *On a vu avec les polynômes de Lagrange qu'il existe des familles libres dont tous les polynômes ont même degré.*

Proposition II.27. *Une famille A est libre si, et seulement si, tout élément de $\mathrm{Vect}(A)$ s'écrit de manière unique comme combinaison linéaire d'éléments de A.*

Démonstration. Si A est libre, notons $x \in \text{Vect}(A)$. Quitte à rajouter des coefficients nuls dans les sommes qui suivent, cela revient à dire qu'il existe $a_1, \dots, a_n \in A$, $\lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_n \in \mathbb{K}$ tels que :

$$x = \sum_{i=1}^{n} \lambda_i \cdot a_i = \sum_{i=1}^{n} \mu_i \cdot a_i$$

et donc :

$$0 = \sum_{i=1}^{n} (\lambda_i - \mu_i) \cdot a_i$$

et comme A est libre, on déduit que pour tout i : $\lambda_i - \mu_i = 0$, c'est-à-dire $\lambda_i = \mu_i$. D'où l'unicité.

Réciproquement, comme $0 \in \text{Vect}(A)$, si tout élément de $\text{Vect}(A)$ s'écrit de manière unique, alors 0 aussi. Et comme 0 s'écrit comme combinaison linéaire dont tous les coefficients sont nuls, toute combinaison linéaire nulle a ses coefficients nuls : donc A est libre. □

Remarque II.28. *Ce résultat est surtout utile dans le sens direct : à la manière des systèmes linéaires, il suffit de traiter le problème en 0 (l'analogue du problème homogène) pour avoir le résultat partout.*
Par exemple, quand on a montré l'unicité de l'écriture pour les fonctions polynomiales, on aurait pu se contenter de voir que la fonction nulle s'écrit de manière unique.

II.4 Bases

Définition II.29 (Bases)**.** *Une famille qui est à la fois libre et génératrice est appelée une* ***base****.*

Exemples II.30.

1. *la famille* $1, X - a, \dots (X - a)^n$ *est une base de* $\mathbb{K}^n$ *;*
2. *la famille des matrices élémentaires de taille* $n \times p$ *est une base de* $\mathcal{M}_{n,p}(\mathbb{K})$ *;*
3. *la famille* $((1, -1, 0), (0, 1, -1))$ *est une base du plan de* $\mathbb{R}^3$ *d'équation* $x + y + z = 0$*.*

Proposition II.31. *Une famille A est une base de E si, et seulement si, tout élément de E s'écrit* ***de manière unique*** *comme combinaison linéaire d'éléments de A.*

Démonstration. L'existence vient du côté "génératrice" et l'unicité du côté "libre". □

Définition II.32. *Étant donnée une base $\mathcal{B} = (e_i)_{i \in I}$ d'un espace E et $x \in E$ qu'on écrit $x = \sum_{i \in I} x_i \cdot e_i$, on dit que les x_i sont les* ***coordonnées*** *de x* ***dans la base $\mathcal{B}$***

Remarque II.33. *En pratique, on travaillera avec une base ordonnée, puisque les coordonnées ne sont pas échangeable. Et on indicera souvent les éléments d'une base par l'ensemble $[\![1; n]\!]$, et plus rarement $[\![0; n]\!]$ ou $\mathbb{N}$, mais en faisant toujours attention à l'ordre.*
Et une base n'est pas unique (on l'a vu avec $\mathbb{K}_n[X]$ ou $\mathbb{K}[X]$ par exemple). Donc les coordonnées dépendent de la base choisie.

Exemples II.34. *Certains espaces vectoriels, qui reviennent souvent, on des bases standardisées, souvent plus naturelles, appelées* ***bases canoniques*** *: celle-ci est unique, et soumise à de nombreuses conventions, donc n'est pas à improviser mais à connaître. En voici quelques exemples :*

1. *pour* $\mathbb{K}^n$ *:* $((1, 0, \dots, 0), (0, 1, \dots, 0), \dots, (0, 0, \dots, 1))$ *;*
2. *pour* $\mathbb{K}_n[X]$ *:* $(1, X, X^2, \dots, X^n)$ *;*
3. *pour* $\mathbb{K}[X]$ *:* $(1, X, X^2, \dots, X^n, X^{n+1}, \dots)$ *;*
4. *pour* $\mathcal{M}_{n,p}$ *:* $(E_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}}$

Proposition II.35. *Si $P_0, \dots, P_n \in \mathbb{K}[X]$ vérifient pour tout i : $\deg(P_i) = i$, alors la famille (P_i) est une base de $\mathbb{K}_n[X]$.*
*On parle alors de famille de polynômes de **degrés échelonnés**.*

Démonstration. Comme les polynômes sont de degrés deux-à-deux distincts, on a déjà que la famille est libre.
On montre qu'elle est génératrice en montrant par récurrence sur $k \in [\![0; n]\!]$ que $\mathbb{K}_k[X] = \text{Vect}(P_i)_{0 \leq i \leq k}$:
- si $k = 0$: si $P \in \mathbb{K}_0[X]$, alors P est constant (éventuellement nul) ; comme $\deg(P_0) = 0$, alors P_0 est constant (non nul) donc $P = \frac{P}{P_0} \cdot P_0 \in \text{Vect}(P_0)$;
- hérédité : si $P \in \mathbb{K}_{k+1}[X]$ pour $k \in [\![0, n-1]\!]$, notons $\lambda \in \mathbb{K}$ le coefficient (éventuellement nul) de P de degré $k+1$, et μ celui (non nul) de P_{k+1}. Alors $P - \frac{\lambda}{\mu} P_{k+1} \in \mathbb{K}_k[X] = \text{Vect}(P_0, \dots P_k)$, donc $P \in \text{Vect}(P_0, \dots, P_k, P_{k+1})$.

D'où la récurrence. □

III Sommes de sous-espaces

III.1 Somme de deux sous-espaces vectoriels

Définition III.1. *Si F, G sont deux sev de E, on définit leur **somme**, notée $F + G$, comme l'ensemble des somme d'éléments de F et de G :*

$$F + G = \{x + y \,|\, x \in F, y \in G\}.$$

Exemple III.2. *Dans les matrices carrées, on a déjà vu que $\mathcal{S}_n(\mathbb{K}) + \mathcal{A}_n(\mathbb{K}) = \mathcal{M}_n(\mathbb{K})$.*
Si on note $\mathcal{T}^+(\mathbb{K})$ et $\mathcal{T}^-(\mathbb{K})$ les ensembles de matrices respectivement triangulaires supérieures et inférieures de taille n, alors : $\mathcal{T}^+(\mathbb{K}) + \mathcal{T}^-(\mathbb{K}) = \mathcal{M}_n(\mathbb{K})$.

Proposition III.3. *Étant donnés F, G deux sev de E, alors $F + G$ est un sev de E. C'est même le plus petit sev de E contenant F et G, dans le sens où tout sev de E contenant F et G contient aussi $F + G$.*

Démonstration. On a : $0 = \underbrace{0}_{\in F} + \underbrace{0}_{\in G} \in F + G$ donc $F + G$ est non vide.
Si $z_1, z_2 \in F + G$ et $\lambda \in \mathbb{K}$: notons $z_1 = x_1 + y_1$ et $z_2 = x_2 + y_2$ pour $x_1, x_2 \in F$, $y_1, y_2 \in G$. Alors :

$$\lambda \cdot z_1 + z_2 = \lambda \cdot (x_1 + y_1) + (x_2 + y_2) = \underbrace{\lambda \cdot (x_1 + x_2)}_{\in F} + \underbrace{(y_1 + y_2)}_{\in G} \in F + G$$

ce qui montre que $F + G$ est bien un sev de E.

Si H est un sev de E qui contient F et G, considérons $z = x + y \in F + G$, avec $x \in F$ et $y \in G$. Alors $x, y \in H$, et donc $z = x + y \in H$. Donc $F + G \subset H$. □

Remarque III.4. *Une autre manière de formuler ce résultat est de dire que $\text{Vect}(F \cup G) = F + G$.*

Corollaire III.5. *Si A, B sont deux parties de E, alors : $\text{Vect}(A \cup B) = \text{Vect}(A) + \text{Vect}(B)$.*
En particulier, si A engendre F et B engendre G, alors $A \cup B$ engendre $F + G$.

III.2 Somme directe de deux sev

Définition III.6. *Deux sev F, G de E sont dits en **somme directe** si tout élément de $F + G$ s'écrit de manière unique comme somme d'un élément de F et d'un élément de G, c"est-à-dire si :*

$$\forall x_1, x_2 \in F,\ \forall y_1, y_2 \in G,\ x_1 + y_1 = x_2 + y_2 \Rightarrow x_1 = x_2 \text{ et } y_1 = y_2.$$

Dans ce cas, on notera $F \oplus G$ au lieu de $F + G$.

Exemples III.7. *Si on reprend les exemples précédents dans les matrices carrées, alors :*

- *les espaces $\mathcal{S}_n(\mathbb{K})$ et $\mathcal{A}_n(\mathbb{K})$ sont en somme directe : on avait montré l'unicité dans le chapitre sur les matrices ;*
- *les espaces $\mathcal{T}^+(\mathbb{K})$ et $\mathcal{T}^-(\mathbb{K})$ ne sont pas en somme directe : comme on matrice diagonale est à la fois triangulaire supérieure et inférieure, on a par exemple : $I_n = \underbrace{I_n}_{\in\mathcal{T}^+(\mathbb{K})} + \underbrace{0}_{\in\mathcal{T}^-(\mathbb{K})} = \underbrace{0}_{\in\mathcal{T}^+(\mathbb{K})} + \underbrace{I_n}_{\in\mathcal{T}^-(\mathbb{K})}$.*

  Donc l'écriture n'est pas unique.

Proposition III.8. *Pour F, G deux sev de E, il y a équivalence entre :*

1. *F et G sont en somme directe ;*
2. *si $x \in F$ et $y \in G$ vérifient $x + y = 0$, alors $x = y = 0$;*
3. *$F \cap G = \{0\}$.*

Démonstration. Montrons que $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$ ce qui montrera l'équivalence.
Pour $1 \Rightarrow 2$: comme tout élément de $F + G$ s'écrit d'une seule manière, alors c'est le cas pour 0. Si $x \in F$ et $y \in G$ vérifient $x + y = 0$, alors on a : $x + y = 0 = \underbrace{0}_{\in F} + \underbrace{0}_{\in G}$ donc par unicité on déduit que $x = y = 0$.
Pour $2 \Rightarrow 3$: comme $F \cap G$ est un sev de E, alors $0 \in F \cap G$; réciproquement, si $x \in F \cap G$, alors on a aussi que $-x \in F \cap G$ (comme $F \cap G$ est un ev), et alors : $0 = \underbrace{x}_{\in F} + \underbrace{-x}_{\in G}$, et donc $x = -x = 0$. Et finalement $F \cap G = \{0\}$.
Pour $3 \Rightarrow 1$: soit $z \in F + G$, que l'on écrit $z = x_1 + y_1 = x_2 + y_2$ pour $x_1, x_2 \in F$ et $y_1, y_2 \in G$. Alors on déduit que : $\underbrace{x_1 - x_2}_{\in F} = \underbrace{y_2 - y_1}_{\in G} \in F \cap G = \{0\}$, donc $x_1 - x_2 = y_2 - y_1 = 0$, donc $x_1 = x_2$ et $y_1 = y_2$. D'où l'unicité de l'écriture de z, donc F et G sont en somme directe.

□

Remarque III.9. *Comme pour le fait d'être libre, on peut ramener le problème d'une combinaison linéaire à un combinaison linéaire nulle.*

III.3 Sous-espaces supplémentaires

Définition III.10. *Deux sev F, G de E sont dits **supplémentaires (dans E)** si $E = F \oplus G$, c'est-à-dire si tout élément de E s'écrit de manière unique comme somme d'un élément de F et d'un élément de G.*

Remarque III.11. *Il y a en fait deux propriétés à vérifier : que F et G soient en somme directe, et que leur somme soit égale à E.*

Exemples III.12.

1. *Dans $\mathcal{M}_n(\mathbb{K})$, les espaces $\mathcal{S}_n(\mathbb{K})$ et $\mathcal{A}_n(\mathbb{K})$ sont supplémentaires.*
2. *Sur $\mathbb{C}$, vu comme $\mathbb{R}$-espace vectoriel, les sev $\mathbb{R}$ et $i\mathbb{R}$ sont supplémentaires.*
3. *Dans $\mathcal{F}(\mathbb{R}, \mathbb{R})$, les ensembles des fonctions paires et des fonctions impaires sont des espaces vectoriels supplémentaires.*
4. *Par division euclidienne, si $B \in \mathbb{K}[X]$ est un polynôme non nul, alors les espaces $\mathbb{K}_{\deg(B)-1}[X]$ (avec la convention $\mathbb{K}_{-1}[X] = \{0\}$) et $B \cdot \mathbb{K}[X] = \{B \cdot P \mid P \in \mathbb{K}[C]\}$ sont supplémentaires dans $\mathbb{K}[X]$. De mêmes, les espaces $\mathbb{K}_{\deg(B)-1}[X]$ et $B \cdot \mathbb{K}_{n-\deg(B)}[X]$ sont supplémentaires dans $\mathbb{K}_n[X]$.*

Remarque III.13. *À part pour des sev triviaux, un supplémentaire n'est jamais unique. Plus précisément : si $F = \{0\}$ (resp. E), alors son seul supplémentaire est E (resp. $\{0\}$), et dans les autres cas il n'y a pas unicité.*
Par exemple, dans le plan, deux droites vectorielles distinctes (donc engendrées par des vecteurs non colinéaires) sont toujours supplémentaires. Dans l'espace, un plan vectoriel et une droite vectorielle n'appartenant pas à ce plan sont toujours supplémentaires.

Exemple III.14. *Reprenons le plan d'équation $x+y+z=0$ dans $\mathbb{R}^3$ que l'on note F. Considérons $u=(a,b,c)\notin F$, et posons $G=\mathrm{Vect}(u)$ la droite vectorielle engendrée par u. Montrons que F et G sont supplémentaires car :*

- *F et G sont en somme directe : on peut voir que $F\cap G=\{0\}$, car si $(x,y,z)\in F\cap G$, alors il existe $\lambda\in\mathbb{R}$ tel que : $(x,y,z)=(\lambda a,\lambda b,\lambda c)$ et alors $x+y+z=0\Leftrightarrow\lambda(a+b+c)=0\Leftrightarrow\lambda=0$ (comme $u\notin F$, donc $a+b+c\neq 0$).*
- *F et G engendrent $E=\mathbb{R}^3$: si $v=(x,y,z)\in\mathbb{R}^3$, posons $\lambda=\dfrac{x+y+z}{a+b+c}$. Alors :*

$$v=\underbrace{(v-\lambda\cdot u)}_{\in F}+\underbrace{\lambda\cdot u}_{\in G}$$

où le seul point subtile est que $v-\lambda\cdot u\in F$, et qui vient du fait qu'il est égal à $(x-\lambda a,y-\lambda b,z-\lambda x)$, donc la somme de ses coordonnées vaut :

$$(x+y+z)-\lambda(a+b+c)=(x+y+z)-(x+y+z)=0.$$

Et donc on a bien que $F\oplus G=\mathbb{R}^3$.

Proposition III.15. *Si F et G sont supplémentaires dans E, que A est une base de F et que B est une base de G, alors $A\cup B$ est une base de E.*

Démonstration. Montrons que $A\cup B$ est libre et génératrice.
Comme A engendre F et B engendre G, alors $A\cup B$ engendre $F+G=E$, donc est génératrice.
Donnons-nous une combinaison linéaire nulle de $A\cup B$, à partir de deux familles $(\lambda_a)\in\mathbb{K}^A$ et $(\mu_b)\in\mathbb{K}^B$ à supports finis :

$$\sum_{a\in A}\lambda_a\cdot a+\sum_{b\in B}\mu_b\cdot b=0.$$

Et donc :

$$\underbrace{\sum_{a\in A}\lambda_a\cdot a}_{\in F}=\underbrace{-\sum_{b\in B}\mu_b\cdot b}_{\in G}=0.$$

comme F et G sont en somme directe, donc $F\cap G=\{0\}$.
Et comme A,B sont libres, on déduit que (λ_a) et (μ_b) sont nulles, donc la combinaison linéaire initiale a tous ses coefficients nuls, donc la famille $A\cup B$ est libre.
Et finalement : $A\cup B$ est une base de E. □

Remarque III.16. *On a même une équivalence : F et G sont supplémentaire dans E si, et seulement si, toute (une) concaténation d'une base de F et d'une base de G est une base de E. Le résultat se montre de manière très proche : on relie la liberté de la famille au fait d'avoir une somme direct, et le caractère générateur de la famille à celui de la somme des espaces vectoriels.*

III.4 Généralisation à un nombre fini d'espaces vectoriels

Définition III.17. *Pour $n\in\mathbb{N}^*$ et $F_1,\dots,F_n$ des sev de E, on définit de même leur **somme** comme l'ensemble des sommes d'éléments de $F_1,\dots,F_n$:*

$$F_1+\cdots+F_n=\sum_{i=1}^{n}F_i=\left\{\sum_{i=1}^{n}x_i\,|\,(x_1,\dots,x_n)\in F_1\times\cdots\times F_n\right\}.$$

On parlera de somme directe, que l'on notera $F_1\oplus\cdots\oplus F_n$ ou $\bigoplus_{i=1}^{n}F_i$, si toute écriture comme somme d'éléments de $F_1,\dots,\dots F_n$ est unique.

Proposition III.18. *Avec les mêmes notations, $\sum_{i=1}^{n} F_i$ est un sev de E : c'est même le plus petit sev de E contenant chacun des F_i.*

Démonstration. Comme pour deux espaces, ou par récurrence sur le nombre d'espaces. □

Proposition III.19. *Avec les mêmes notations, il y a équivalence entre :*

1. *$F_1, \dots, F_n$ sont en somme directe ;*
2. *si $(x_1, \dots, x_n) \in F_1 \times \cdots \times F_n$ vérifie $x_1 + \cdots + x_n = 0$, alors $x_1 = \cdots = x_n = 0$;*
3. *pour tout $k \in [\![1; n]\!]$: $F_k \cap \left(\sum_{i \neq k} F_i\right) = \{0\}$.*

Démonstration. Comme pour deux espaces, par implications circulaires. □

Remarque III.20. *Que ce soit pour 2 ou davantage d'espaces, la somme des F_i est directe si, et seulement si, l'application φ ci-dessous est bijective :*

$$\varphi : \left\{ \begin{array}{ccc} F_1 \times \cdots \times F_n & \to & E \\ (x_1, \dots, x_n) & \mapsto & x_1 + \cdots + x_n \end{array} \right.$$

et on verra d'autres manières de caractériser la bijectivité, donc d'autre manière de caractériser les sommes directes.

IV Applications linéaires

IV.1 Généralités

Définition IV.1. *Soient E, F deux $\mathbb{K}$-ev. Une application $f : E \to F$ est appelée **application linéaire** si :*

$$\forall x, y \in E,\ \forall \lambda \in \mathbb{K},\ f(\lambda \cdot x + y) = \lambda \cdot f(x) + f(y).$$

On note $\mathcal{L}(E, F)$ l'ensemble des applications linéaires de E dans F.

Remarques IV.2.

1. *En prenant $\lambda = 1$, on déduit qu'une application linéaire est aussi un morphisme de groupe (et la réciproque est fausse). En particulier, on aura toujours $f(0_E) = 0_F$.*
2. *Comme un $\mathbb{C}$-espace vectoriel est aussi un $\mathbb{R}$-espace vectoriel, alors on précisera parfois le corps considéré en disant qu'une application est $\mathbb{K}$-linéaire.*

Exemples IV.3.

1. *Sur $\mathbb{R}$ (vu comme une droite vectorielle), les applications linéaires sont exactement celles qu'on avait appelées ainsi avant : les applications $x \mapsto ax$ pour $a \in \mathbb{R}$.*
2. *Sur $\mathbb{C}$, les similitudes qui fixent O sont $\mathbb{C}$-linéaires ; la conjugaison complexe n'est pas $\mathbb{C}$-linéaire mais elle est $\mathbb{R}$-linéaire, tout comme les applications $z \mapsto \mathrm{Re}(z)$ ou $z \mapsto \mathrm{Im}(z)$.*
3. *Sur les matrices, la transposition est une application linéaire de $\mathcal{M}_{n,p}(\mathbb{K})$ dans $\mathcal{M}_{p,n}(\mathbb{K})$.*
4. *Si $A \in \mathcal{M}_{n,p}(\mathbb{K})$, l'application $f_A : \left\{ \begin{array}{ccc} \mathcal{M}_{p,1}(\mathbb{K}) & \to & \mathcal{M}_{n,1}(\mathbb{K}) \\ X & \mapsto & AX \end{array} \right.$ est un application linéaire, qu'on appelle application linéaire canoniquement associée à A.*
5. *Peu importe F, l'application $x \mapsto 0_F$ définie de E vers F est linéaire : c'est la seule application linéaire constante.*

Proposition IV.4. *Si $f \in \mathcal{L}(E,F)$, $\lambda_1,\dots,\lambda_n \in \mathbb{K}$ et $x_1,\dots,x_n \in E$, alors :*

$$f\left(\sum_{i=1}^{n} \lambda_i \cdot x_i\right) = \sum_{i=1}^{n} \lambda_i \cdot f(x_i).$$

Démonstration. Par récurrence sur $n \in \mathbb{N}^*$. □

Proposition IV.5. *L'ensemble $\mathcal{L}(E,F)$ est un sev de $\mathcal{F}(E,F)$.*

Démonstration. On a déjà dit que l'application nulle est linéaire, donc $\mathcal{L}(E,F)$ est non vide.
Si $f,g \in \mathcal{L}(E,F)$ et $\lambda \in \mathbb{K}$, alors pour tous $x,y \in E$ et $\mu \in \mathbb{K}$ on a :

$$\begin{array}{rcl}(\lambda \cdot f + g)(\mu \cdot x + y) &=& \lambda \cdot f(\mu \cdot x + y) + g(\mu \cdot x + y)\\ &=& \lambda \cdot (\mu \cdot f(x) + f(y)) + \mu \cdot g(x) + g(y)\\ &=& \mu \cdot (\lambda \cdot f(x) + g(x)) + (\lambda \cdot f(y) + g(y))\\ &=& \mu \cdot (\lambda \cdot f + g)(x) + (\lambda \cdot f + g)(y)\end{array}.$$

□

Proposition IV.6. *La composée de deux applications linéaires est une application linéaire, c'est-à-dire que, si E,F,G sont des $\mathbb{K}$-ev, $f \in \mathcal{L}(E,F)$ et $g \in \mathcal{L}(F,G)$, alors $g \circ f \in \mathcal{L}(E,G)$.*

Démonstration. Si $x,y \in E$ et $\lambda \in \mathbb{K}$, alors :

$$(g \circ f)(\lambda \cdot x + y) = g\left(\lambda \cdot f(x) + f(y)\right) = \lambda \cdot g(f(x)) + g(f(y)) = \lambda \cdot (g \circ f)(x) + (g \circ f)(y).$$

□

Proposition IV.7. *La composition est une application bilinéaire, dans le sens où, si E,F,G sont des espaces vectoriels, et $f_0 \in \mathcal{L}(E,F)$, $g_0 \in \mathcal{L}(F,G)$, alors les applications :*

$$\varphi : \left\{\begin{array}{rcl}\mathcal{L}(E,F) &\to& \mathcal{L}(E,G)\\ f &\mapsto& g_0 \circ f\end{array}\right. \quad \text{et } \psi : \left\{\begin{array}{rcl}\mathcal{L}(E,G) &\to& \mathcal{L}(E,G)\\ g &\mapsto& g \circ f_0\end{array}\right.$$

sont des applications linéaires.

Démonstration. Immédiat par le calcul. □

Définition IV.8. *Une application linéaire bijective est appelée un* ***isomorphisme****.*

Remarque IV.9. *Étant donnés E,F deux espaces vectoriels, il n'existe pas toujours d'isomorphisme de E vers F. Mais si un tel isomorphisme existe, on dira que E et F sont* ***isomorphes****.*

Proposition IV.10. *Si f est un isomorphisme de E sur F, alors f^{-1} est un isomorphisme de F sur E.*

Démonstration. La seule chose à vérifier est que la réciproque d'une application linéaire bijective est aussi linéaire.
Soient $x,y \in F$ et $\lambda \in \mathbb{K}$. Alors :

$$f(\lambda \cdot f^{-1}(x) + f^{-1}(y)) = \lambda f(f^{-1}(x)) + f(f^{-1}(y)) = \lambda \cdot x + y$$

et ainsi $\lambda \cdot f^{-1}(x) + f^{-1}(y)$ est l'unique antécédent de $\lambda \cdot x + y$ par f, c'est-à-dire : $f^{-1}(\lambda \cdot x + y) = \lambda \cdot f^{-1}(x) + f^{-1}(y)$. D'où la linéarité. □

IV.2 Images directes et images réciproques

Proposition IV.11. *Si $f \in \mathcal{L}(E,F)$, alors :*

1. *si A est un sev de E, alors $f(A)$ est un sev de F ;*
2. *si B est un sev de F, alors $f^{-1}(B)$ est un sev de E.*

Démonstration.

1. Comme A est un sev de E, alors $0 \in A$ donc $f(0) = 0 \in f(A)$, donc A est non vide.
   Si $y_1, y_2 \in f(A)$, notons $x_1, x_2 \in A$ tels que $f(x_1) = y_1, f(x_2) = y_2$. Alors pour $\lambda \in \mathbb{K}$:
   $$\lambda y_1 + y_2 = \lambda f(x_1) + f(x_2) = f(\lambda x_1 + x_2) \in f(A)$$
   comme A est un espace vectoriel. Donc $f(A)$ est bien un sev.
2. Comme B est un sev de F, alors $0 = f(0) \in B$, donc $0 \in f^{-1}(B)$.
   Si $x_1, x_2 \in f^{-1}(B)$ et $\lambda \in \mathbb{K}$, alors $f(x_1), f(x_2) \in B$, donc $\lambda f(x_1) + f(x_2) = f(\lambda x_1 + x_2) \in B$. Et ainsi $\lambda x_1 + x_2 \in f^{-1}(B)$.
   Donc $f^{-1}(B)$ est bien un espace vectoriel.

□

Corollaire IV.12. *Soit $f \in \mathcal{L}(E,F)$:*

1. *en tant que morphisme de groupe, son noyau $\mathrm{Ker} f = f^{-1}(\{0\})$ est bien défini, et est un sev de E ;*
2. *en tant qu'application, son image $\mathrm{Im} f = f(E)$ est bien définie, et est un sev de F.*

Exemple IV.13. *Ce résultat permet rapidement de montrer qu'un ensemble est un espace vectoriel en le voyant comme l'image ou le noyau d'une application linéaire. Par exemple, si on considère sur $\mathcal{M}_n(\mathbb{K})$ l'application linéaire $\varphi : M \mapsto \dfrac{M + M^T}{2}$ (qui est linéaire comme combinaison d'applications linéaires, par linéarité de la transposition). Et ainsi :*

- *$\mathcal{S}_n(\mathbb{K}) = \mathrm{Im}\varphi$ est un sev de $\mathcal{M}_n(\mathbb{K})$;*
- *$\mathcal{A}_n(\mathbb{K}) = \mathrm{Ker}\varphi$ est un sev de $\mathcal{M}_n(\mathbb{K})$.*

et on aurait pu aussi utiliser l'application $\psi : M \mapsto \dfrac{M - M^T}{2}$.
On pouvait simplifier aussi en ne divisant par par 2 dans ψ et φ, d'après le résultat qui suit.

Exemple IV.14. *Si $q \in \mathbb{K}$, l'ensemble des suites géométriques de raison q est un espace vectoriel : c'est le noyau de l'application :*
$$\varphi : \left\{ \begin{array}{ccc} \mathbb{K}^{\mathbb{N}} & \to & \mathbb{K}^{\mathbb{N}} \\ (u_n) & \mapsto & (u_{n+1} - q \cdot u_n) \end{array} \right.$$
Et on pourrait faire le même genre de raisonnements pour d'autres classes de suites.
Par exemple, si $a, b \in \mathbb{K}$, l'ensemble des suites linéaires récurrentes d'ordre 2 définies par la relation : $u_{n+2} + au_{n+1} + bu_n = 0$ forment le noyau de l'application $(u_n) \mapsto (u_{n+2} + au_{n+1} + bu_n)$.
On peut aussi retrouver que $\mathbb{R}_n[x]$ est un sev de $\mathcal{C}^\infty(\mathbb{R},\mathbb{R})$, en tant que noyau de l'application $f \mapsto f^{(n+1)}$.

Proposition IV.15. *Si $f \in \mathcal{L}(E,F)$ et $\lambda \in \mathbb{K}^*$, alors :*
$$\mathrm{Ker}(\lambda f) = \mathrm{Ker}(f) \text{ et } \mathrm{Im}(\lambda f) = \mathrm{Im} f.$$

Démonstration. Comme $\lambda \neq 0$, on a les équivalences suivantes :
$$\lambda y = 0 \Leftrightarrow y = 0 \text{ et } \lambda x \in E \Leftrightarrow x \in E$$
et donc :

— en appliquant la première avec $y = f(x)$ pour $x \in E$:

$$x \in \mathrm{Ker} f \Leftrightarrow f(x) = 0 \Leftrightarrow \lambda f(x) = 0 \Leftrightarrow x \in \mathrm{Ker}(\lambda f)$$

— en appliquant la seconde avec $x \in E$:

$$y \in \mathrm{Im}(\lambda f) \Leftrightarrow \exists x \in E, y = \lambda f(x) = f(\lambda x) \Leftrightarrow \exists x' \in E, y = f(x') \Leftrightarrow y \in \mathrm{Im} f.$$

□

Proposition IV.16. *Si $f \in \mathcal{L}(E, F)$, alors :*

1. *f est injective si, et seulement si,* $\mathrm{Ker} f = \{0\}$ *;*
2. *f est surjective si, et seulement si,* $\mathrm{Im} f = F$.

Démonstration. Découle des résultats pour les morphismes de groupe (pour le noyau) et pour les applications (pour l'image). □

Proposition IV.17. *Si $f \in \mathcal{L}(E, F)$ et que $(x_i)_{i\in I}$ est une famille génératrice de E, alors la famille $(f(x_i))_{i\in I}$ engendre* $\mathrm{Im} f$.

Démonstration. On veut montrer que $\mathrm{Im} f = \mathrm{Vect}(f(x_i))_{i\in I}$, ce que l'on fait par double inclusion.
Comme les x_i sont dans E, alors les $f(x_i)$ sont des éléments de $\mathrm{Im} f$, qui est un espace vectoriel, donc $\mathrm{Vect}(f(x_i))_{i\in I} \subset \mathrm{Im} f$.
Inversement, si $y \in \mathrm{Im} f$, notons $x \in E$ tel que $f(x) = y$. Comme $(x_i)_{i\in I}$ engendre E, alors il existe une famille $(\lambda_i)_{i\in I}$ à support fini telle que : $x = \sum_{i\in I} \lambda_i x_i$. Et alors :

$$y = f(x) = f\left(\sum_{i\in I} \lambda_i x_i\right) = \sum_{i\in I} \lambda_i f(x_i) \in \mathrm{Vect}(f(x_i))_{i\in I}$$

ce qui donne l'autre inclusion.
D'où le résultat. □

IV.3 Endomorphismes

Définition IV.18. *Une application linéaire de E dans E est appelée un* ***endomorphisme*** *de E. On note $\mathcal{L}(E)$ l'ensemble des endomorphismes de E.*
Un endomorphisme bijectif de E est appelé un ***automoprhisme****. On note* $\mathrm{GL}(E)$ *l'ensemble des automorphismes de E.*

Exemple IV.19. *L'application identité* id_E *est un endomorphisme de E, et c'est même un automorphisme. Les applications de la forme $\lambda \cdot \mathrm{id}_E$ pour $\lambda \in \mathbb{K}^*$ aussi : ce sont les homothéties de E.*

Proposition IV.20. $(\mathcal{L}(E), +, \circ)$ *est un anneau.*

Démonstration. Comme $(\mathcal{L}(E), +, \cdot)$ est un ev, alors $(\mathcal{L}(E), +)$ est un groupe abélien, dont l'élément neutre est l'application nulle.
La composition laisse stable $\mathcal{L}(E)$, est associative, et possède pour élément neutre l'application $\mathrm{id}_E \in \mathcal{L}(E)$.
La bilinéarité assure la distributivité de $\circ$ par rapport à $+$. □

Remarque IV.21. *En particulier on pourra utiliser toutes les règles de calcul dans les anneaux : puissances, binômes (en cas de commutativité), nilpotence, etc. Pour la composition, si $f, g \in \mathcal{L}(E)$, on notera plus simplement gf au lieu de $g \circ f$, et f^k (pour $k \in \mathbb{N}$) au lieu de $\underbrace{f \circ \cdots \circ f}_{k \text{ fois}}$. Si de plus $f \in \mathrm{GL}(E)$, alors on notera f^k pour $k \in \mathbb{Z}$, défini f^k si $k \in \mathbb{N}$ et $(f^{-1})^{-k}$ si $k < 0$.*
De plus, dès lors que E n'est pas une droite ou $\{0\}$, alors $\mathcal{L}(E)$ n'est pas commutatif.

Corollaire IV.22. $(\mathrm{GL}(E), \circ)$ *est un groupe.*
En particulier, c'est un sous-groupe de $\mathfrak{S}(E)$.

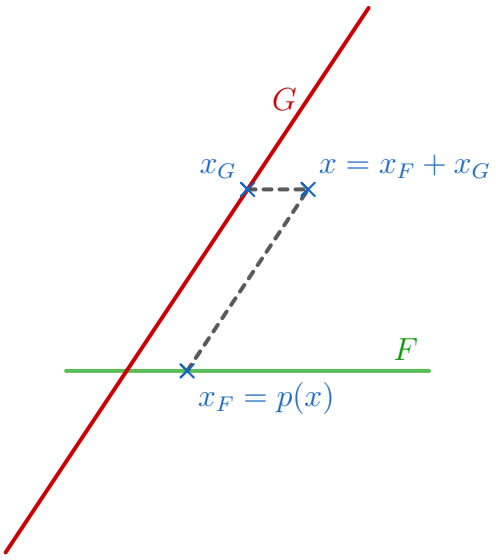
Démonstration. Il s'agit du groupe des inversibles de l'anneau $(\mathcal{L}(E), +, \circ)$. □

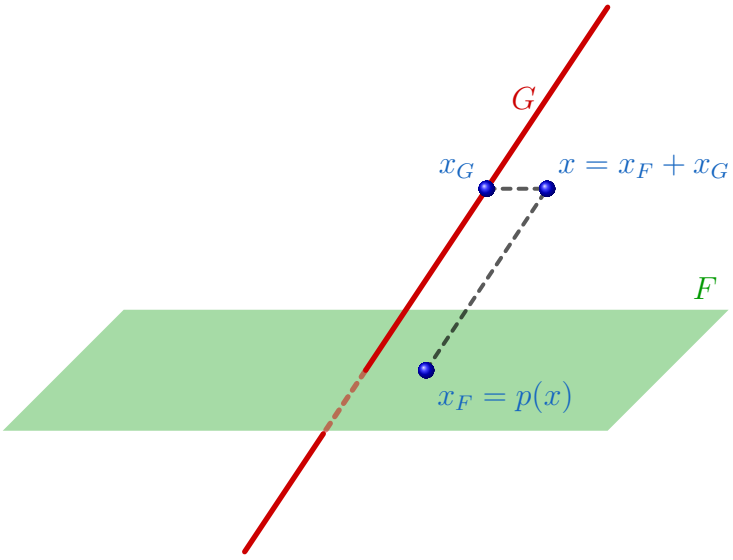
IV.4 Projecteurs et symétries

Définition IV.23. *Soit E un espace vectoriel, et F, G deux sev supplémentaires dans E. On appelle alors le **projecteur sur F parallèlement à G** l'application :*

$$p : \left\{ \begin{array}{rcl} E & \to & E \\ x = x_F + x_G & \mapsto & x_F \end{array} \right.$$

où l'écriture $x = x_F + x_G$ est l'unique écriture d'un élément de E comme somme d'un élément de F et d'un élément de G.





Remarques IV.24.

1. *Le fait que F et G soient supplémentaires permet d'avoir une application bien définie : la somme directe permet qu'elle soit bien définie sur $F+G$, et le fait que $F+G = E$ permet donc de la définir sur E entier.*
2. *Si on inverse les rôles de F et G, on obtient un autre projecteur q tel que $p + q = \mathrm{id}_E$.*

Proposition IV.25. *Avec les mêmes notations, p est un endomorphisme **idempotent** de E, c'est-à-dire tel que $p \circ p = p$.*

Démonstration. La linéarité vient de l'unicité de l'écriture : si $x, y \in E$ avec $x = x_F + x_G$ et $y = y_F + y_G \in E$ leurs décompositions, et $\lambda \in \mathbb{K}$, alors :

$$\lambda \cdot x + y = \lambda \cdot (x_F + x_G) + (y_F + y_G) = \underbrace{\lambda \cdot x_F + y_F}_{\in F} + \underbrace{\lambda \cdot x_G + y_G}_{\in G}$$

et donc par définition de p on a : $p(\lambda \cdot x + y) = \lambda \cdot x_F + y_F = \lambda \cdot p(x) + p(y)$. Donc $p \in \mathcal{L}(E)$.
De plus, on a :

$$p(x) = x_F = \underbrace{x_F}_{\in F} + \underbrace{0}_{\in G}$$

donc $p(p(x)) = x_F = p(x)$. Et comme ceci est vrai pour tout x, on a bien $p \circ p = p$. □

Théorème IV.26. *Les projecteurs de E sont **exactement** les endomorphismes idempotents p de E. Pour un tel p, il s'agit plus précisément de la projection sur $\mathrm{Im}p$ parallèlement à $\mathrm{Ker}p$.*

Démonstration. On a déjà vu qu'un projecteur est un endomorphisme idempotent.
Réciproquement, soit $p \in \mathcal{L}(E)$ vérifie $p \circ p = p$. Montrons que $\mathrm{Im}p$ et $\mathrm{Ker}p$ sont supplémentaires, et que p est le projecteur sur $\mathrm{Im}p$ parallèlement à $\mathrm{Ker}p$.

— si $x \in E$, alors $x = \underbrace{p(x)}_{=x_1} + \underbrace{x - p(x)}_{=x_2}$ avec :
  — par définition, $x_1 \in \mathrm{Im}p$;
  — par linéarité et idempotence de p : $p(x_2) = p(x) - p \circ p(x) = 0$, donc $x_2 \in \mathrm{Ker}p$.
  Donc Imp et Ker$p$ engendrent E.
— si $x \in \mathrm{Im}p \cap \mathrm{Ker}p$, alors il existe $y \in E$ tel que $p(y) = x$ et $p(x) = 0$. Mais, par idempotence, on a :

$$x = p(y) = p \circ p(y) = p(x) = 0$$

  donc Im$p \cap$ Ker$p = \{0\}$, donc Imp et Ker$p$ sont en somme directe.
Donc Imp et Ker$p$ sont supplémentaires.
Mais alors, on a pour tout $x \in E$:

$$x = \underbrace{p(x)}_{\in \mathrm{Im}p} + \underbrace{(x - p(x))}_{\in \mathrm{Ker}p}$$

donc p est l'application qui associe à x sa composante suivant Imp associé à la décomposition $E = \mathrm{Im}p \oplus \mathrm{Ker}p$: c'est donc le projecteur sur Imp parallèlement à Ker$p$. □

Remarque IV.27. *Comme* Imp *et* Ker$p$ *sont supplémentaires, on déduit que l'on a l'équivalence :* $\mathrm{Im}p = E \Leftrightarrow \mathrm{Ker}p = \{0\}$. *Ainsi, on a équivalence entre : p injectif, p surjectif et p bijectif (ce qu'on avait déjà vu avec les applications idempotentes), et que dans ce cas* $p = \mathrm{id}$.

Proposition IV.28. *Si* $p \in \mathcal{L}(E)$, *alors p est un projecteur si, et seulement si :*

$$\mathrm{Im}p = \mathrm{Ker}(p - \mathrm{id}_E).$$

Remarque IV.29. *Pour* $x \in E$, *on a :*

$$x \in \mathrm{Ker}(p - \mathrm{id}_E) \Leftrightarrow (p - \mathrm{id}_E)(x) = 0 \Leftrightarrow p(x) = x$$

et plus généralement, pour $f \in \mathcal{L}(E)$ *et* $\lambda \in \mathbb{K}$, *on a :*

$$x \in \mathrm{Ker}(f - \lambda \mathrm{id}_E) \Leftrightarrow f(x) = \lambda \cdot x$$

et ces ensembles ont un rôle très important pour analyser des endomorphismes.

Démonstration. Si p est un projecteur :
— comme $p \circ p = p$, alors pour tout $x \in \mathrm{Im}p$, on a : $p(x) = x$ donc $\mathrm{Im}p \subset \mathrm{Ker}(p - \mathrm{id}_E)$;
— réciproquement, si $p(x) = x$, alors : x est sa propre image donc $x \in \mathrm{Im}p$.
ce qui montre bien l'égalité.
Si $\mathrm{Im}p = \mathrm{Ker}(p - \mathrm{id}_E)$, alors pour tout $x \in E$, on a $p(x) \in \mathrm{Im}p = \mathrm{Ker}(p - \mathrm{id}_E)$, et donc : $p(p(x)) = x$.
Donc p est idempotent : c'est un projecteur. □

Remarque IV.30. *Dans la démonstration, on voit que seule l'inclusion* $\mathrm{Im}p \subset \mathrm{Ker}(p - \mathrm{id}_E)$ *est liée au fait d'avoir un projecteur : l'autre inclusion est en fait toujours vérifiée.*

Exemple IV.31. *Considérons l'application* $\varphi \in \mathcal{L}(\mathcal{M}_n(\mathbb{K}))$ *telle que* $\varphi : M \mapsto \dfrac{M + M^T}{2}$.
Alors φ *est le projecteur sur* $\mathcal{S}_n(\mathbb{K})$ *parallèlement à* $\mathcal{A}_n(\mathbb{K})$. *On a en effet :*

$$\forall M \in \mathcal{M}_n(\mathbb{K}), \varphi \circ \varphi(M) = \frac{\frac{M+M^T}{2} + \left(\frac{M+M^T}{2}\right)^T}{2} = \frac{\frac{M+M^T+M^T+M}{2}}{2} = \frac{M + M^T}{2} = \varphi(M)$$

donc φ *est une application linéaire involutive : c'est un projecteur.*
De plus, on a pour tout $M \in \mathcal{M}_n(\mathbb{K})$ *:*

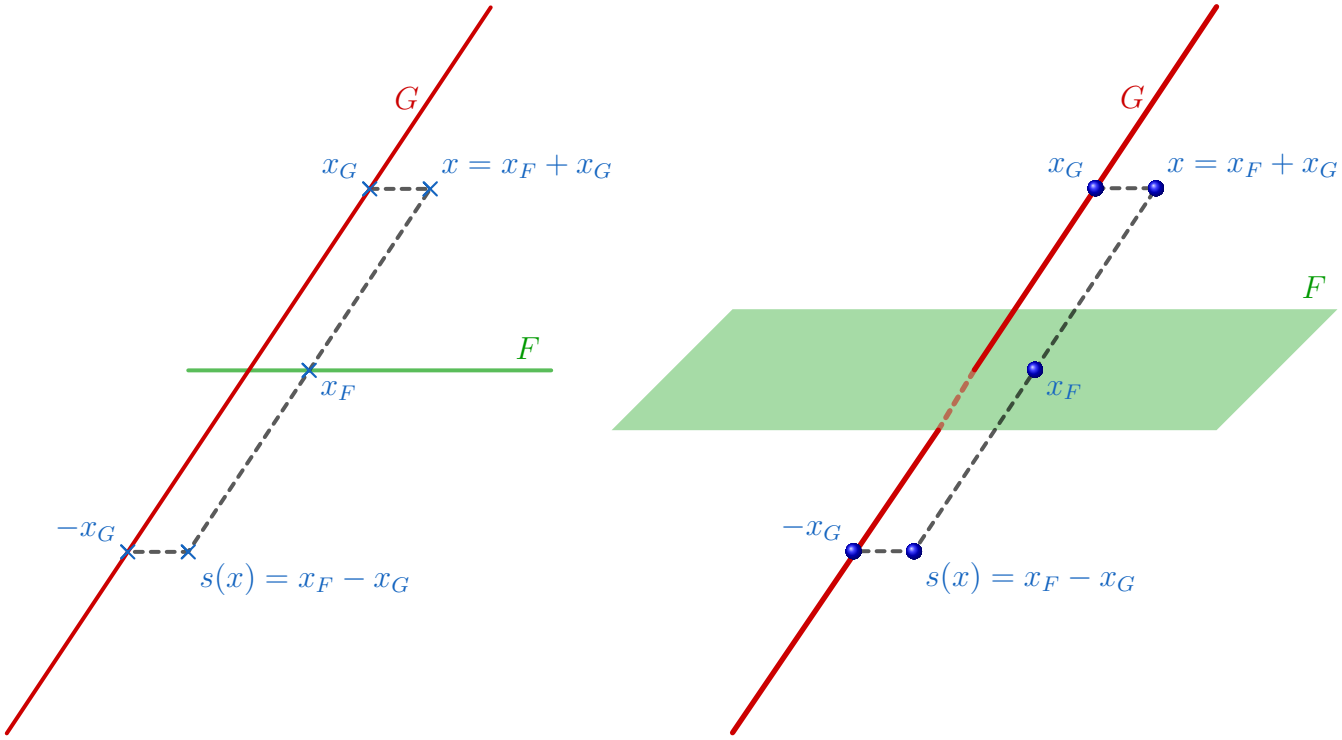
— $M \in \mathrm{Ker}\varphi \Leftrightarrow \frac{M+M^T}{2} = 0 \Leftrightarrow M + M^T = 0 \Leftrightarrow M \in \mathcal{A}_n(\mathbb{K})$, *donc* $\mathrm{Ker}\varphi = \mathcal{A}_n(\mathbb{K})$;

— $M \in \mathrm{Im}\varphi \Leftrightarrow M \in \mathrm{Ker}(\varphi - \mathrm{id}) \Leftrightarrow \varphi(M) = M \Leftrightarrow \dfrac{M + M^T}{2} = M \Leftrightarrow M = M^T \Leftrightarrow M \in \mathcal{S}_n(\mathbb{K})$.

Définition IV.32. *Soit E un espace vectoriel, et F, G deux sev supplémentaires de E. On appelle alors* ***symétrie par rapport à F parallèlement à G*** *l'application :*

$$s : \left\{ \begin{array}{ccc} E & \to & E \\ x = x_F + x_G & \mapsto & x_F - x_G \end{array} \right.$$

où l'écriture $x = x_F + x_G$ est l'unique écriture d'un élément de E comme somme d'un élément de F et d'un élément de G.



Proposition IV.33. *Avec les mêmes notations, si p désigne le projecteur sur F parallèlement à G, alors : $s = 2p - \mathrm{id}_E$.*

Démonstration. En gardant les notations, si $x \in E$, alors :

$$(2p - \mathrm{id}_E)(x) = 2x_F - (x_F + x_G) = x_F - x_G = s(x).$$

□

Corollaire IV.34. *Avec les mêmes notations, s est un endomorphisme de E involutif, c'est-à-dire tel que $s \circ s = \mathrm{id}_E$.*

Démonstration. Comme $s = 2p - \mathrm{id}_E$, on a déjà que $s \in \mathcal{L}(E)$. Et comme p et id_E commutent, on a :

$$s^2 = (2p - \mathrm{id}_E)^2 = 4p^2 - 4p + \mathrm{id}_E = \mathrm{id}_E$$

en utilisant quand $p^2 = p$. □

Théorème IV.35. *Les symétries de E sont* ***exactement*** *les endomorphismes involutifs s de E.*
Pour un tel s, il s'agit plus précisément de la symétrie par rapport à $\mathrm{Ker}(s - \mathrm{id}_E)$ parallèlement à $\mathrm{Ker}(s + \mathrm{id}_E)$.

Démonstration. On a déjà vu qu'une symétrie est un endomorphisme involutif.
Réciproquement, soit $s \in \mathcal{L}(E)$ tel que $s \circ s = \mathrm{id}_E$. Notons $p = \dfrac{s + \mathrm{id}_E}{2}$. Alors :

$$p \circ p = \frac{s^2 + 2s + \mathrm{id}_E}{4} = \frac{s + \mathrm{id}_E}{2} = p.$$

Donc p est le projecteur sur $\mathrm{Im}p$ parallèlement à $\mathrm{Ker}p$, et $s = 2p - \mathrm{id}_E$ est la symétrie par rapport à $\mathrm{Im}p$ parallèlement à $\mathrm{Ker}p$.
Mais on a aussi que :

— $\mathrm{Im}p = \mathrm{Ker}(p - \mathrm{id}_E) = \mathrm{Ker}\left(\dfrac{s - \mathrm{id}_E}{2}\right) = \mathrm{Ker}(s - \mathrm{id}_E)$;

— $\mathrm{Ker}p = \mathrm{Ker}\left(\dfrac{s + \mathrm{id}_E}{2}\right) = \mathrm{Ker}(s + \mathrm{id}_E)$.

Et finalement, s est la symétrie par rapport à $\mathrm{Ker}(s - \mathrm{id}_E)$ parallèlement à $\mathrm{Ker}(s + \mathrm{id}_E)$. □

Remarque IV.36. *On peut réécrire ces deux noyaux de la manière suivante :*

$$\mathrm{Ker}(s - \mathrm{id}_E) = \{x \in E \,|\, s(x) = x\} \text{ et } \mathrm{Ker}(s + \mathrm{id}_E) = \{x \in E \,|\, s(x) = -x\}.$$

IV.5 Détermination d'une application linéaire

Proposition IV.37. *Étant données $(x_i)_{i\in I}$ une base de E, et $(y_i)_{i\in I}$ une famille quelconque d'éléments de F, il existe une unique application linéaire $f \in \mathcal{L}(E, F)$ telle que :*

$$\forall i \in I,\ f(x_i) = y_i.$$

Démonstration. Si une telle application f existe : considérons $x \in E$, que l'on écrit $x = \sum_{i\in I} \lambda_i x_i$ (pour (λ_i) famille de scalaires à support fini). Et alors par linéarité :

$$f(x) = f\left(\sum_{i\in I} \lambda_i \cdot x_i\right) = \sum_{i\in I} \lambda_i \cdot f(x_i) = \sum_{i\in I} \lambda_i y_i$$

où l'écriture a bien un sens comme l'écriture de x comme combinaison linéaire des x_i existe, et est unique. Donc f est donnée par la formule précédente.
Reste à montrer que f est linéaire : si $x = \sum_{i\in I} \lambda_i x_i$ et $x' = \sum_{i\in I} \mu_i x_i$. Alors pour tout $\lambda \in \mathbb{K}$ on a :

$$\lambda x + x' = \sum_{i\in I} (\lambda\lambda_i + \mu_i) \cdot x_i$$

et ainsi :

$$f(\lambda \cdot x + x') = \sum_{i\in I} (\lambda \cdot \lambda_i + \mu_i) y_i = \lambda \cdot \left(\sum_{i\in I} \lambda_i \cdot x_i\right) + \left(\sum_{i\in I} \mu_i \cdot x_i\right) = \lambda \cdot f(x) + f(x')$$

et donc une telle application f est bien linéaire. □

Remarque IV.38. *On voit bien qu'on a besoin d'une base tant pour l'aspect libre (pour que f soit bien définie) que générateur (pour qu'elle soit définie partout).*

Corollaire IV.39. *Si $\mathcal{B}$ est une base de E, deux applications de $\mathcal{L}(E, F)$ sont égales si, et seulement si, elles coïncident sur $\mathcal{B}$.*

Démonstration. Par l'unicité dans la proposition précédente. □

Remarque IV.40. *Notons qu'il faut a priori avoir une base de E pour utiliser ce résultat, ce qui n'est pas toujours le cas.*

Théorème IV.41. *Étant données $(x_i)_{i\in I}$ une base de E et $(y_i)_{i\in I}$ une famille de E, alors l'application $f \in \mathcal{L}(E,F)$ qui vérifie pour tout $i \in I$ que $f(x_i) = y_i$ est :*

1. *injective si, et seulement si, $(y_i)_{i\in I}$ est libre ;*
2. *surjective si, et seulement si, $(y_i)_{i\in I}$ engendre F ;*
3. *bijective si, et seulement si, $(y_i)_{i\in I}$ est une base de F.*

Démonstration. Comme une famille est une base si, et seulement si, elle est libre et génératrice, et qu'une application est bijective si, et seulement si, elle est injective et surjective, alors il suffit de montrer les deux premiers points.

1. Si f est injective : alors $\mathrm{Ker}(f) = \{0\}$. Considérons (λ_i) à support fini telle que $\sum_{i\in I} \lambda_i y_i = 0$. Alors, en posant $x = \sum_{i\in I} \lambda_i x_i$, on a :
$$f(x) = \sum_{i\in I} \lambda_i y_i = 0$$
donc $x \in \mathrm{Ker} f$, donc $x = \sum_{i\in I} \lambda_i x_i = 0$. Mais la famille (x_i) est une base de E, donc elle est libre, et donc la famille (λ_i) est nulle, donc la famille (y_i) est libre.
Réciproquement, si (y_i) est libre : soit $x \in \mathrm{Ker} f$. On écrit $x = \sum_{i\in I} \lambda_i x_i$, de telle sorte que :
$$f(x) = 0 = \sum_{i\in I} \lambda_i y_i$$
et comme la famille (y_i) est libre, on déduit que (λ_i) est la famille nulle, donc $x = 0$. Ce qui montre l'autre implication.
2. On a déjà vu que l'image d'une famille génératrice engendre l'image d'un application linéaire. Et ainsi on a : $\mathrm{Im} f = \mathrm{Vect}(f(x_i)) = \mathrm{Vect}(y_i)$. Et donc f est surjective si, et seulement si, $\mathrm{Vect}(y_i) = F$, c'est-à-dire que (y_i) engendre F.
3. Découle des deux points précédents.

□

Exemple IV.42. *Considérons E un espace vectoriel, $(e_1, \dots, e_n)$ famille d'éléments de E. On pose l'application :*
$$\varphi : \left\{ \begin{array}{ccc} \mathbb{K}^n & \to & E \\ (\lambda_1, \dots, \lambda_n) & \mapsto & \sum_{i=1}^n \lambda_i e_i \end{array} \right. .$$
Suivant les notations précédentes, l'application φ n'est autre que l'unique application linéaire de $\mathbb{K}^n$ dans E qui envoie les vecteurs de la base canonique sur la famille (e_i). On trouve ainsi que la famille (e_i) est une base de E si, et seulement si, l'application φ est bijective.
Et c'est bien ce qu'on avait trouvé pour les bases, puisque la bijectivité de φ revient à dire que tout élément de E a un unique antécédent par φ dans $\mathbb{K}^n$, c'est-à-dire que tout élément de E s'écrit de manière unique comme combinaison linéaire d'éléments de la famille (e_i).

Proposition IV.43. *Soient F, G deux sev de E supplémentaires, et soit H un $\mathbb{K}$-ev.*
Pour tout couple $(f,g) \in \mathcal{L}(F,H) \times \mathcal{L}(G,H)$, il existe une unique application linéaire $h \in \mathcal{L}(E,H)$ telle que : $h|_F = f$ et $h|_G = g$.

Démonstration. Si un tel h existe, il est nécessairement défini par le fait que :
$$\forall x \in E,\ x = \underbrace{x_F}_{\in F} + \underbrace{x_G}_{\in G} \Rightarrow h(x) = h(x_F) + h(x_G) = f(x_F) + g(x_G)$$
ce qui assure l'unicité.
Montrons qu'une telle application répond bien au problème :

— h ainsi définie est linéaire : si $x, y \in E$ se décomposent en $x = x_F + x_G, y = y_F + y_G$, et $\lambda \in \mathbb{K}$, alors :

$$\lambda \cdot x + y = \underbrace{\lambda \cdot x_F + y_F}_{\in F} + \underbrace{\lambda \cdot x_G + y_G}_{\in G}$$

donc :

$$\begin{aligned} h(\lambda x + y) &= f(\lambda x_F + y_F) + g(\lambda x_G + y_G) \\ &= \lambda f(x_F) + f(y_F) + \lambda g(x_G) + g(y_G) \\ &= \lambda h(x) + h(y) \end{aligned}$$

ce qui assure la linéarité de h.

— si $x \in F$: alors $x = \underbrace{x}_{\in F} + \underbrace{0}_{\in G}$ donc $h(x) = f(x) + g(0) = f(x)$, donc $h|_F = f$.

— de même $h|_G = g$.

Ce qui montre l'existence. □

IV.6 Formes linéaires et hyperplans

Définition IV.44. *Si E est un $\mathbb{K}$-ev, une application linéaire de E dans $\mathbb{K}$ est appelée une **forme linéaire**. On notera E^* au lieu de $\mathcal{L}(E, \mathbb{K})$ l'ensemble des formes linéaires sur E.*

Exemples IV.45.

1. *Si on se place sur $\mathbb{R}^3$, l'application : $(x, y, z) \mapsto x + y + z$ est une forme linéaire.*
   On peut même voir que, comme une application linéaire est entièrement définie par l'image d'une base, toute forme linéaire sur $\mathbb{R}^3$ est de la forme $(x, y, z) \mapsto ax + by + cz$, où a, b, c sont les images respectives des vecteurs de la base canonique de $\mathbb{R}^3$.
2. *Sur $\mathbb{K}_n[X]$, on peut considérer les applications $\varphi : P \mapsto P(a)$ (pour $a \in \mathbb{K}$) ou encore $\psi : P \mapsto \int_0^1 P(t)\mathrm{d}t$: ce sont deux formes linéaires, que l'on peut aussi chercher à exprimer à l'aide des images des vecteurs de la base canonique.*
   Pour φ : si $k \in [\![0; n]\!]$, alors $\varphi(X^k) = a^k$ et on retrouve que $\varphi(\sum_{k=0}^n a_k X^k) = \sum_{k=0}^n a_k a^k$, donc pas très instructif.
   Pour ψ : si $k \in [\![0; n]\!]$, alors $\psi(X^k) = \frac{1}{k+1}$, et donc : $\psi(\sum_{k=0}^n a_k X^k) = \sum_{k=0}^n \frac{a_k}{k+1}$, ce qui facilite les calculs.
3. *Plus généralement, les applications φ et ψ peuvent s'étendre en des formes linéaires sur $\mathcal{F}(\Omega, \mathbb{K})$ et $\mathcal{C}^0(\mathbb{R}, \mathbb{K})$ respectivement, mais on perd alors l'existence de base.*

Définition IV.46. *Si E est un $\mathbb{K}$-ev et H est un sev de E, on dira que H est un **hyperplan (vectoriel)** s'il existe une forme linéaire φ non nulle telle que $H = \mathrm{Ker}\varphi$.*

Exemples IV.47.

1. *Dans $\mathbb{R}^3$, l'ensemble $\{(x, y, z) \in \mathbb{R}^3 \,|\, x + y + z = 0\}$ est un hyperplan, en tant que noyau de la forme linéaire $(x, y, z) \mapsto x + y + z$, qui est non nulle. Plus généralement, si $a, b, c \in \mathbb{R}$ sont non tous nuls, l'ensemble $\{(x, y, z) \in \mathbb{R}^3 \,|\, ax + by + cz = 0\} = \mathrm{Ker}((x, y, z) \mapsto ax + by + cz)$ est un hyperplan.*
2. *Si Ω est une ensemble quelconque et $a \in \Omega$, l'ensemble $\{f \in \mathcal{F}(\Omega, \mathbb{R}) \,|\, f(a) = 0\} = \mathrm{Ker}(f \mapsto f(a))$ est un hyperplan. Par exemple, si $\Omega = \mathbb{N}$: pour tout $n_0 \in \mathbb{N}$, l'ensemble $\{(u_n) \in \mathbb{K}^{\mathbb{N}} \,|\, u_{n_0} = 0\}$ est un hyperplan.*
3. *L'ensemble $\{f \in \mathcal{C}^0([a, b], \mathbb{K}) \,|\, \int_a^b f(t)\mathrm{d}t = 0\}$ est un hyperplan de $\mathcal{C}^0([a, b], \mathbb{K})$. Si E est l'ensemble des fonctions continues 2π-périodiques, alors l'hyperplan $\{f \in E \,|\, \int_0^{2\pi} f(t)\mathrm{d}t = 0\}$ est l'ensemble des fonctions continues 2π-périodiques dont les primitives sont périodiques.*

Théorème IV.48. *Un sev H de E est un hyperplan si, et seulement si, c'est un supplémentaire d'une droite.*
Dans ce cas, c'est même un supplémentaire de toute droite qu'il ne contient pas.

Démonstration. Soit H un hyperplan : notons $\varphi \in E^*$ tel que $H = \text{Ker}\varphi$. Comme $\varphi \neq 0$, il existe $u \in E$ tel que $\varphi(u) \neq 0$ (et donc nécessairement $u \notin H$). Montrons que $E = H \oplus D$, où $D = \text{Vect}(u)$:

— soit $x \in E$: alors $x = \underbrace{x - \dfrac{\varphi(x)}{\varphi(u)}u}_{=x_H} + \underbrace{\dfrac{\varphi(x)}{\varphi(u)}u}_{=x_D}$, avec $x_H \in H$ comme par linéarité $\varphi(x_H) = \varphi(x) - \dfrac{\varphi(x)}{\varphi(u)}\varphi(u) = 0$ et $x_D \in D$ par construction. Donc $E = H + D$.

— soit $x \in H \cap D$: alors $x = \lambda u$, pour $\lambda \in \mathbb{K}$, et $\varphi(x) = 0$. Donc par linéarité : $0 = \varphi(x) = \lambda \cdot \underbrace{\varphi(u)}_{\neq 0}$ donc $\lambda = 0$, puis $x = 0$. Donc $H \cap D = \{0\}$.

Et finalement $E = H \oplus D$.
La seule propriété utilisée pour u est que $\varphi(u) \neq 0$, on peut le remplacer pour tout élément de $E \setminus H$, ce qui montre le dernier résultat (comme contenir un vecteur est équivalent à contenir la droite qu'il engendre pour un espace vectoriel).

Si H est le supplémentaire d'une droite D. Notons $u \in E$ tel que $D = \text{Vect}(u)$. Alors l'application :

$$\varphi : \left\{ \begin{array}{rcl} E & \to & \mathbb{K} \\ x = x_H + \lambda \cdot u & \mapsto & \lambda \end{array} \right.$$

est une forme linéaire telle que $H = \text{Ker}\varphi$: en effet, on a :

$$x \in \text{Ker}\varphi \Leftrightarrow \lambda = 0 \Leftrightarrow x = x_H \in H$$

et donc H est un hyperplan. □

Exemples IV.49.

1. *Pour l'hyperplan H d'équation $x+y+z = 0$ dans $\mathbb{R}^3$, on a déjà montré que tout vecteur n'appartenant pas à H engendre un supplémentaire de H dans $\mathbb{R}^3$.*
2. *Dans $\mathbb{R}^2$, toute droite vectorielle est donnée par une équation de la forme $ax + by = 0$ (avec a ou b non nul) : c'est donc un hyperplan ! En particulier, deux droites de $\mathbb{R}^2$ sont supplémentaires si, et seulement si, elles sont distinctes.*

Proposition IV.50. *Deux formes linéaires donnent le même hyperplan si, et seulement si, elles sont colinéaires.*

Démonstration. On considère φ, ψ deux formes linéaires non nulles : leurs hyperplans associés sont $H_1 = \text{Ker}\varphi$ et $H_2 = \text{Ker}\psi$; et elles sont colinéaires si, et et seulement si, il existe $\lambda \in \mathbb{K}^*$ tel que $\varphi = \lambda\psi$ (comme elles sont non nulles).
On a déjà vu que $\text{Ker}(\lambda\psi) = \text{Ker}\psi$ donc deux formes linéaires colinéaires donnent le même hyperplan.
Réciproquement, si $H_1 = H_2$: notons $u \notin H_1$. Alors $\varphi(u), \psi(u) \neq 0$. Posons $\lambda = \dfrac{\varphi(u)}{\psi(u)} \in \mathbb{K}^*$.
Si $x \in E$, posons $x = \underbrace{x_H}_{\in H_1} + \mu \cdot u$. Alors :

$$\varphi(x) = \mu \cdot \varphi(u) \text{ et } \lambda\psi(x) = \frac{\varphi(u)}{\psi(u)} \cdot \mu \cdot \varphi(u) = \mu \cdot \varphi(u)$$

et ainsi : $\varphi = \lambda\psi$, donc φ et ψ sont colinéaires. □

V Sous-espaces affines d'un espace vectoriel

V.1 Points, vecteurs et sous-espaces affines

Un espace vectoriel E peut être traité de manière affine : on distingue alors les points (notés par des lettre majuscules : $A, B, C, etc.$) des vecteurs (notés avec des flèches : $\overrightarrow{a}$, $\overrightarrow{b}$, $\overrightarrow{c}$, *etc.*, ou pas d'ailleurs).

Définition V.1. *Un **point** est un élément d'un espace affine.*

Définition V.2 (Translations)**.** *Si $\overrightarrow{a} \in E$, on appelle **translation de vecteur** $\overrightarrow{a}$ l'application :*

$$\tau_{\overrightarrow{a}} : \left\{ \begin{array}{ccc} E & \to & E \\ x & \mapsto & x + \overrightarrow{a} \end{array} \right.$$

Remarque V.3. *Les translations permettent de faire le lien entre points et vecteurs, dans le sens où le point A et le vecteur $\overrightarrow{a}$ décrivent le même élément de E si :*

$$\tau_{\overrightarrow{a}}(0) = A.$$

Pour A, B deux points et $\overrightarrow{u}$ un vecteur, on notera $B = A + \overrightarrow{u}$ ou $\overrightarrow{AB} = \overrightarrow{u}$ si $B = \tau_{\overrightarrow{u}}(A)$.
La correspondance entre un point A et son vecteur $\overrightarrow{a}$ est donnée par : $\overrightarrow{OA} = \overrightarrow{a}$ (où O est le point associé au vecteur nul).

Définition V.4. *On appelle **sous-espace affine** de E tout sous-ensemble $\mathcal{F}$ de E de la forme $\mathcal{F} = \tau_{\overrightarrow{a}}(F) = \{x + \overrightarrow{a} \,|\, x \in F\}$, pour F un sev de E.*
*On note plus simplement $\mathcal{F} = F + \overrightarrow{a}$ (ou $F + a$). Et on dira que $\mathcal{F}$ est **le sous-espace affine de** E **passant par** a **de direction** F.*

Proposition-Définition V.5. *Dans l'écriture précédente, le choix de F est unique, mais pas celui de a. Plus précisément, les espaces affines $F + a$ et $F' + a'$ sont égaux si, et seulement si : $F = F'$ et $(a - a') \in F$.*
*L'espace vectoriel F est appelé **la direction** de l'espace affine $F + a$.*

Démonstration.
— si $a + F = a' + F'$: alors $a' \in a' + F = a + F$ donc $a' = a + x$ pour $x \in F$, et donc $a' - a = x \in F$.
Si $x \in F'$, alors $a' + x \in a' + F = a + F$, donc il existe $y \in F$ tel que : $a' + x = a + y$. Et alors :

$$x = a + y - a' = \underbrace{(a - a')}_{\in F} + \underbrace{y}_{\in F} \in F$$

donc $F' \subset F$. Et par raisonnement analogue on trouve $F \subset F'$. Et donc $F = F'$.
— si $a' - a \in F$, montrons que $a + F = a' + F$:
— si $u \in a + F$: on pose $x \in F$ tel que $u = a + x$. Et alors :

$$u = a' + (a + x) - a' = a' + \underbrace{(a - a') + x}_{\in F} \in a' + F$$

donc $a + F \subset a + F'$.
— comme $a - a' \in F$, en échangeant les rôles de a et a', on trouve que :$a' + F \subset a + F$.
et ainsi $a + F = a' + F$.

□

Corollaire V.6. *Si $\mathcal{F}$ est un espace affine de direction F, alors pour tout $a \in \mathcal{F}$ on a : $\mathcal{F} = F + a$. En particulier, si $a, b \in \mathcal{F}$, alors $b - a \in F$.*

Définition V.7. *Un espace affine dont la direction est une droite (resp. un hyperplan) est appelé une* ***droite affine*** *(resp. un* ***hyperplan affine****).*

Exemples V.8.

1. *Dans $\mathbb{R}^2$, toute droite affine est donnée par une équation de la forme $ax + by + c = 0$, avec a ou b non nul. La direction d'une telle droite est la droite vectorielle d'équation $ax + by = 0$.*
2. *Dans $\mathbb{R}^3$, les hyperplans vectoriels sont donnés par des équations de la forme $ax + by + xz + d = 0$, avec a, b, c non tous nuls, et la direction d'un tel hyperplan est l'hyperplan vectoriel d'équation $ax + by + xz = 0$.*

V.2 Intersection de sous-espaces affines

Proposition V.9. *Une intersection d'espaces affines est soit vide, soit un espace affine dirigée par l'intersection de leurs directions.*

Démonstration. Soient $(\mathcal{F}_i)_{i\in I}$ une famille d'espaces affines. Supposons que $\bigcap_{i\in I} \mathcal{F}_i$ est non vide, et notons a un de ses éléments, de sorte que a appartient à chaque $\mathcal{F}_i$, et donc :

$$\forall i \in I,\ \mathcal{F}_i = F_i + a$$

où F_i est la direction de $\mathcal{F}_i$.
On a ainsi les équivalences :

$$\begin{array}{rcl} x \in \bigcap_{i\in I} \mathcal{F}_i & \Leftrightarrow & \forall i \in I,\ x \in \mathcal{F}_i = F_i + a \\ & \Leftrightarrow & \forall i \in I,\ \exists x_i \in F_i,\ x = x_i + a \\ & \Leftrightarrow & \forall i \in I,\ \exists x_i \in F_i,\ x - a = x_i \\ & \Leftrightarrow & \forall i \in I,\ x - a \in F_i \\ & \Leftrightarrow & x - a \in \bigcap_{i\in I} F_i \\ & \Leftrightarrow & x \in \bigcap_{i\in I} F_i + a \end{array}$$

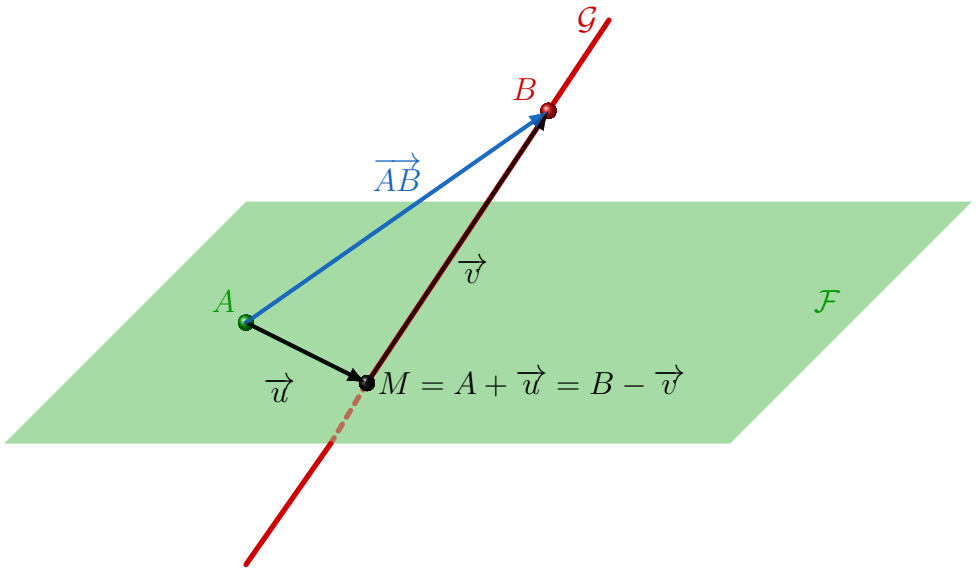
et ainsi : $\bigcap_{i\in I} \mathcal{F}_i = \left(\bigcap_{i\in I} F_i\right) + a$. □

Proposition V.10. *Étant donnés $\mathcal{F} = A + F$ et $\mathcal{G} = B + G$ deux sous-espaces affines de E, alors $\mathcal{F} \cap \mathcal{G}$ est non vide si, et seulement si, $\overrightarrow{AB} \in F + G$.*

Démonstration. Si $\mathcal{F} \cap \mathcal{G} \neq \emptyset$, notons M un de ses points. Alors $\overrightarrow{AM} \in F$ et $\overrightarrow{MB} \in G$. Et donc : $\overrightarrow{AB} = \overrightarrow{AM} + \overrightarrow{MB} \in F + G$.
Réciproquement, si $\overrightarrow{AB} = \underbrace{\overrightarrow{u}}_{\in F} + \underbrace{\overrightarrow{v}}_{\in G}$. Notons $M = A + \overrightarrow{u}$. Alors :

- $M \in \mathcal{F}$ par construction ;
- $\overrightarrow{BM} = \overrightarrow{BA} + \overrightarrow{AM} = -\overrightarrow{u} - \overrightarrow{v} + \overrightarrow{u} = -\overrightarrow{v} \in G$, donc $M \in \mathcal{G}$.

donc $\mathcal{F} \cap \mathcal{G}$ contient M, donc est non vide.



□

Exemple V.11. *Dans $\mathbb{R}^2$, deux droites vectorielles distinctes sont supplémentaires, donc engendrent tout l'espace. Ainsi, deux droites qui ne se coupent pas ont nécessairement la même direction : elles sont parallèles.*

V.3 Sous-espaces affines et équation linéaires

Définition V.12. *Une **équation linéaire** est une équation de la forme $f(x) = y$, où $f \in \mathcal{L}(E, F)$ et $y \in F$ sont les paramètres, et $x \in E$ est l'inconnue.*

Proposition V.13. *Si E, F sont deux espaces vectoriels, $f \in \mathcal{L}(E, F)$, et $y \in F$, alors l'ensemble des solutions de l'équation linéaire $f(x) = y$ est soit l'ensemble vide, soit un sous-espace affine de E dirigé par* $\mathrm{Ker} f$.

Démonstration. Supposons que l'ensemble des solutions soit non vide, et notons $a \in E$ tel que $f(a) = y$. Alors pour tout $x \in E$:

$$f(x) = y \Leftrightarrow f(x) = f(a) \Leftrightarrow f(x - a) = 0 \Leftrightarrow x - a \in \mathrm{Ker} f \Leftrightarrow x \in a + \mathrm{Ker} f.$$

□

Exemples V.14.

1. *si $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et $B \in \mathcal{M}_{n,1}(\mathbb{K})$, alors les solutions du système $AX = B$, si elles existent, forment un espace affine dirigé par* $\mathrm{Ker}(X \mapsto AX)$, *c'est-à-dire dirigé par l'espace vectoriel des solutions de l'équation homogène.*
2. *les solutions d'une équation différentielle linéaire forment un espace affine dirigé par l'espace vectoriel des solutions de l'équation homogène associée. Pour le premier degré, on a en effet que, pour f dérivable : $f' + af = b \Leftrightarrow \varphi(f) = b$, où $\varphi : f \mapsto f' + af$ est une application linéaire. Et c'est pareil pour les degrés plus grands.*
3. *si $a, b \in \mathbb{K}$ avec $a \neq 1$, l'ensemble des suites arithmético-géométriques telles que $u_{n+1} = au_n + b$ est un espace affine, contenant la suite constante de valeur $\dfrac{b}{1-a}$ et dirigée par l'espace vectoriel des suites géométriques de raison a.*
4. *Si $x_1, \ldots, x_n$ sont des scalaires deux-à-deux distincts, et $y_1, \ldots, y_n$ sont des scalaires (quelconques), alors l'ensemble $\{P \in \mathbb{K}[X] \,|\, \forall i \in [\![1, n]\!],\ P(x_i) = y_i\}$ est un sous-espace affine dirigé par $F = \{(X - x_1) \ldots (X - x_n)P \,|\, P \in \mathbb{K}[X]\}$.*

Remarques V.15.

1. *Si $E = \mathbb{K}$, alors f est une forme linéaire, donc si $f \neq 0$ on obtient un hyperplan affine.*
2. *Si $y = 0$, on retrouve directement $\mathrm{Ker} f$, qui est un espace vectoriel. C'est en fait le seul cas car si l'ensemble solution est un espace vectoriel, il contient 0 donc $y = f(0) = 0$.*

Chapitre 21

Espaces vectoriels de dimension finie

Dans tout ce chapitre, on désigne $\mathbb{K}$ un corps (par exemple $\mathbb{R}$ ou $\mathbb{C}$), dont les éléments seront appelés scalaires.

I Dimension et base d'un espace vectoriel

I.1 Dimension d'un espace vectoriel

Définition I.1. *Un espace vectoriel E est dit **de dimension finie** s'il possède une famille génératrice de cardinal fini.*
Dans le cas contraire, on dira que E est de dimension infinie.

Exemples I.2.

1. *Les espaces $\mathbb{K}^n$, $\mathbb{K}_n[X]$ ou $\mathcal{M}_{n,p}(\mathbb{K})$ sont de dimension finie, puisque l'on a donné des familles génératrices (et même des bases) finies.*
2. *L'espaces $\mathbb{K}[X]$ est de dimension infinie, car on peut voir qu'aucune famille finie n'est génératrice (en raisonnant sur les degrés). On verra que les espaces $\mathbb{K}^{\mathbb{N}}$ et $\mathcal{F}(\mathbb{R},\mathbb{K})$ sont également de dimension infinie.*

Proposition I.3. *Soit E un espace vectoriel de dimension finie, engendré par une famille à n éléments. Alors toute famille libre possède au plus n éléments.*

Remarque I.4. *On utilisera souvent la contraposée, à savoir que toute famille de cardinal strictement plus grand que n est liée.*

Démonstration. Montrons la contraposée. Comme une famille contenant une famille liée est elle-même liée, il suffit de montrer que toute famille de cardinal $n+1$ est liée.
Montrons par récurrence sur n que : si E possède une famille génératrice de cardinal n, toute famille de cardinal $n+1$ d'éléments de E est liée :

— si $n=0$: alors E est engendré par une famille vide, donc $E=\{0\}$. Une famille à 1 élément contient un élément de E, donc 0, donc est liée ;
— supposons le résultat vrai pour $n\in\mathbb{N}$. Soit $(x_1,\dots,x_{n+1})$ une famille qui engendre E, et $(y_1,\dots,y_{n+2})$ une famille d'éléments de E (de cardinal $n+2$). Posons $F=\text{vect}(x_1,\dots,x_n)$, et écrivons pour tout $i\in[\![1;n+2]\!]$:

$$y_i = z_i + \lambda_i x_{n+1}$$

avec $z_i\in F$ et $\lambda_i\in\mathbb{K}$, qui existent bien comme la famille (x_i) engendre E.
Si tous les λ_i sont nuls, alors tous les y_i sont des éléments de F et on applique directement l'hypothèse de récurrence (comme F est engendré par n éléments), et la famille $(y_1,\dots,y_{n+2})$ est liée.

Sinon, il existe i tel que $\lambda_i \neq 0$. Quitte à renuméroter les y_i, on peut supposer que $\lambda_1 \neq 0$. Posons alors pour tout $i \in [\![2; n+2]\!]$:

$$z'_i = y_i - \frac{\lambda_i}{\lambda_1} y_1$$

Alors pour un tel i on a :

$$z'_i = z_i + \lambda_i x_{n+1} - \frac{\lambda_i}{\lambda_1}(z_1 + \lambda_1 x_{n+1}) = z_i - \frac{\lambda_i}{\lambda_1} z_1 \in F.$$

Par hypothèse de récurrence, la famille $(z'_2, \dots z'_{n+2})$ est liée (possédant $n+1$ éléments dans un espace engendré par n éléments). Donc il existe $\mu_2, \dots, \mu_{n+2}$ non tous nuls tels que :

$$\sum_{i=2}^{n+2} \mu_i z'_i = 0.$$

Et donc en remplaçant dans l'expression précédente :

$$0 = \sum_{i=2}^{n+2} \mu_i z'_i = \underbrace{\left(- \sum_{i=2}^{n+2} \mu_i \frac{\lambda_i}{\lambda_1} \right)}_{=\mu_1} y_1 + \sum_{i=2}^{n+2} \mu_i y_i = \sum_{i=1}^{n+2} \mu_i y_i$$

où les μ_i sont non tous nuls (par construction). Donc la famille $(y_1, \dots, y_{n+2})$ est liée, ce qui prouve l'hérédité.

D'où le résultat par récurrence. □

Théorème-Définition I.5 (Dimension d'un espace vectoriel)**.** *Si E est un espace vectoriel de dimension finie, toutes ses bases ont même cardinal fini. Ce cardinal est appelé* ***dimension*** *de E, que l'on note* $\dim E$ *(ou* $\dim_{\mathbb{K}} E$ *quand on veut préciser le corps).*

Démonstration. Soient $\mathcal{B}_1 = (x_1, \dots, x_n)$ et $\mathcal{B}_2 = (y_1, \dots, y_m)$ deux bases de E. Notons déjà que, en tant que familles libres dans un espace de dimension fini, ces bases sont finies.
Par la proposition précédente :

— comme $\mathcal{B}_1$ est génératrice et $\mathcal{B}_2$ est libre, alors $m \leq n$;
— comme $\mathcal{B}_2$ est génératrice et $\mathcal{B}_1$ est libre, alors $n \leq m$.

Et donc $m = n$. □

Remarques I.6.

1. *Ce théorème ne donne pas l'existence de base, mais celles-ci existent toujours en dimension finie comme on le verra plus loin. Il dit en revanche que la dimension est le nombre de coordonnées, c'est-à-dire concrètement le nombre de degrés de liberté (ou de paramètres) pour décrire un espace vectoriel de dimension finie.*
2. *On parlera de manière analogue d'un espace affine de dimension finie, si sa direction est un espace de dimension finie, et sa dimension sera alors la dimension de l'espace affine.*

Exemples I.7.

1. $\dim \mathbb{K}^n = n$;
2. $\dim \mathbb{K}_n[X] = n+1$;
3. $\dim \mathcal{M}_{n,p}(\mathbb{K}) = n \times p$ *(et en particulier* $\dim \mathcal{M}_n(\mathbb{K}) = n^2$*)* ;
4. $\dim_{\mathbb{C}} \mathbb{C} = 1$ *mais* $\dim_{\mathbb{R}} \mathbb{C} = 2$*. Plus généralement, si E est un espace vectoriel de dimension finie sur $\mathbb{C}$, c'est aussi un espace vectoriel de dimension finie sur $\mathbb{R}$ avec :* $\dim_{\mathbb{R}} E = 2 \cdot \dim_{\mathbb{C}} E$.

Définition I.8. *On appelle* ***droite vectorielle*** *tout espace vectoriel de dimension* 1.
On appelle ***plan vectoriel*** *tout espace vectoriel de dimension* 2.

Exemples I.9.

1. *L'ensemble des solutions homogènes d'une équation différentielle linéaire d'ordre n est un espace vectoriel de dimension n : il s'agit donc d'une droite vectorielle pour les équations de degré* 1, *et d'un plan vectoriel pour celles de degré* 2.
2. *L'ensemble des suites linéaires vérifiant une* ***même*** *relation de récurrence linéaire d'ordre* 2 *est un plan vectoriel.*

Proposition I.10. *Si E, F sont deux espaces vectoriels de dimension finie, alors $E \times F$ est un espace vectoriel de dimension finie avec* $\dim(E \times F) = \dim E + \dim F$.

Démonstration. On admet l'existence de bases (pour le moment). On considère $(e_1, \dots, e_n)$ base de E et $(f_1, \dots, f_m)$ base de F. Alors la famille $((e_1, 0), \dots, (e_n, 0), (0, f_1), \dots, (0, f_m))$ est une base de $E \times F$:

1. elle est génératrice : si $(x, y) \in E \times F$, comme (e_i) et (f_j) sont génératrices, on peut écrire $x = \sum_i x_i e_i$ et $y = \sum_j y_j f_j$ de sorte que :
$$(x, y) = \sum_i x_i (e_i, 0) + \sum_j y_j (0, f_j);$$
2. elle est libre : si $\sum_i \lambda_i (e_i, 0) + \sum_j \mu_j (0, f_j) = 0$, alors en regardant coordonnée par coordonnée on trouve :
$$\sum_i \lambda_i e_i = 0 \text{ et } \sum_j \mu_j f_j = 0$$
et donc, comme les familles (e_i) et (f_j) sont libres, les familles (λ_i) et (μ_j) sont nulles ; donc on a bien une famille libre.

Et le résultat sur la dimension en découle naturellement. □

Corollaire I.11. *Si $E_1, \dots, E_n$ sont des espaces de dimensions finies, alors $E_1 \times \cdots \times E_n$ est de dimension finie avec :* $\dim(E_1 \times \cdots \times E_n) = \sum_i \dim(E_i)$.

Démonstration. Par récurrence sur n. □

I.2 Bases dans un espace de dimension finie

Proposition I.12. *Soit E un espace vectoriel de dimension fini engendré par $(x_1, \dots, x_n)$. Si la famille $(x_1, \dots, x_p)$ (pour un certain $p \in [\![1; n]\!]$) est libre, alors il existe des éléments $x'_{p+1}, \dots, x'_r$ parmi $x_{p+1}, \dots x_n$ tels que la famille $(x_1, \dots, x_p, x'_{p+1}, \dots, x'_r)$ est une base de E.*

Démonstration. On va construire, à partir de $(x_1, \dots, x_p)$ une famille libre maximale.
Pour cela, on considère : $A = \{\text{card}(J) \mid [\![1; p]\!] \subset J \subset [\![1; n]\!] \text{ et } (x_i)_{i \in J} \text{ est libre}\}$.
Alors A est une partie non vide de $\mathbb{N}$, donc possède un plus grand élément. Notons J un sous-ensemble réalisant ce maximum. Montrons que $(x_i)_{i \in J}$ est une base de E. Comme par construction elle est déjà libre, il suffit de voir qu'elle est génératrice. Pour cela, on pose $F = \text{vect}(x_i, i \in J)$ et on va montrer que $E = F$. On a déjà que $F \subset E$. Et de plus, comme $E = \text{vect}(x_i, i \in [\![1, n]\!])$, il suffit de montrer que tous les x_i sont dans F. Soit $i_0 \in [\![1; n]\!]$:

— si $i_0 \in J$: alors c'est clair que $x_i \in F$ par construction ;

— si $i_0 \notin J$: $\text{card}(J \cup \{i_0\}) > \text{card}(J)$; par maximalité de J, on déduit que la famille $(x_i)_{i\in J\cup\{i_0\}}$ est liée. Ainsi il existe $(\lambda_i)_{i\in J}$ et λ_0 non tous nuls tels que : $\lambda_0 x_{i_0} + \sum_{i\in J} \lambda_i x_i = 0$.
Nécessairement on a $\lambda_0 \neq 0$ (sinon la famille $(x_i)_{i\in J}$ serait liée). Et donc :

$$x_{i_0} = -\frac{1}{\lambda_0} \sum_{i\in J} \lambda_i x_i \in F$$

ce qui montre bien le résultat.

Et finalement $E = F$, donc $(x_i)_{i\in J}$ est bien une base de E. □

Corollaire I.13 (Théorème de la base extraite)**.** *Si $E \neq \{0\}$ est un espace vectoriel de dimension finie, de toute famille génératrice finie de E on peut extraire une base de E.*

Démonstration. Soit $(x_1, \ldots, x_n)$ qui engendre E. Comme $E \neq \{0\}$ alors l'un des x_i (au moins) est non nul. Quitte à les renuméroter, on peut supposer que $x_1 \neq 0$, de sorte que la famille (x_1) est libre et on peut appliquer le résultat précédent. □

Corollaire I.14. *Tout espace vectoriel de dimension finie admet une base.*

Corollaire I.15 (Théorème de la base incomplète)**.** *Toute famille libre d'un espace vectoriel E de dimension finie peut être complétée en une base de E.*

Démonstration. On considère $(x_1, \ldots, x_m)$ une famille libre de E (nécessairement finie comme E est de dimension finie), et $(y_1, \ldots, y_n)$ famille génératrice de E. On applique alors le résultat précédente à la famille $(x_1, \ldots, x_m, y_1, \ldots, y_n)$. □

I.3 Familles finies dans un espace de dimension finie

Proposition I.16. *Soit E un espace vectoriel de dimension $n \in \mathbb{N}^*$ et $(x_1, \ldots, x_m)$ (pour $m \in \mathbb{N}^*$) une famille d'éléments de E. Alors :*

1. *si (x_i) est libre, alors $m \leq n$;*
2. *si (x_i) est génératrice, alors $m \geq n$.*

Démonstration.

1. Déjà prouvé.
2. Si $(x_1, \ldots, x_m)$ est génératrice, on peut en extraire une base, qui sera de cardinal n (comme toutes les bases de E), donc $n \leq m$.

□

Proposition I.17. *Soit E un espace vectoriel de dimension $n \in \mathbb{N}^*$, et (x_i) une famille de cardinal n. Alors on a l'équivalence :*

$$(x_i) \text{ est libre } \Leftrightarrow (x_i) \text{ est génératrice} \Leftrightarrow (x_i) \text{ est une base.}$$

Démonstration. Il suffit de montrer que, si (x_i) est libre ou génératrice alors c'est une base (les réciproques étant évidentes). On a en effet :

— si (x_i) est libre : on peut la compléter en une base ; mais comme (x_i) est de cardinal n, sa base complétée aura même cardinal, donc (x_i) sera sa propre base complétée, donc est bien une base ;
— si (x_i) est génératrice : on peut en extraire une base ; mais comme (x_i) est de cardinal n, sa base extraite aura même cardinal, donc (x_i) sera sa propre base extraite, donc est bien une base.

□

Remarque I.18. *En pratique, étant donné un espace vectoriel dont on connaît la dimension, pour montrer qu'une famille en est une base, on montrera qu'elle est libre et a le bon cardinal. On pourra montrer qu'elle est génératrice (au lieu de libre), mais c'est en général plus difficile.*

Exemple I.19. *Soient $a \neq b \in \mathbb{C}$. Montrons que la famille $\left((X-a)^k(X-b)^{n-k}\right)_{k\in[\![0;n]\!]}$ est une base de $\mathbb{C}_n[X]$.*
Comme $\dim \mathbb{C}_n[X] = n+1$, alors la famille considéré a bon cardinal : il suffit de montrer qu'elle est libre ou génératrice pour avoir que c'est une base.
Et elle est libre : si $\lambda_0, \dots, \lambda_n \in \mathbb{C}$ vérifient $\sum_{k=0}^n \lambda_k (X-a)^k (X-b)^{n-k} = 0$, alors :
- *en évaluant en a, il vient $\lambda_0 (a-b)^n = 0$, donc $\lambda_0 = 0$;*
- *en simplifiant par $(X-a)$ puis en évaluant à nouveau en a, il vient : $\lambda_1 = 0$;*
- *et en continuant à diviser par $(X-a)$ et évaluer en a, on trouve $\lambda_0 = \lambda_1 = \cdots = \lambda_n = 0$.*

Donc la famille est libre : donc c'est une base de $\mathbb{C}_n[X]$.
On peut aussi montrer qu'elle est génératrice, ce qui se fait bien par récurrence sur $n \in \mathbb{N}$:
- *si $n = 0$: alors la famille possède pour seul élément le polynôme constant de valeur 1, qui engendre bien $\mathbb{C}_0[X]$ (l'ensemble des polynômes constants), et dont c'est même la base canonique ;*
- *soit $n \in \mathbb{N}$ tel que la famille au rang n engendre $\mathbb{C}_n[X]$. Considérons la famille au rang $(n+1)$, et montrons qu'elle engendre $C_{n+1}[X]$.*
  Pour cela, soit $P \in \mathbb{C}_{n+1}[X]$. Alors, comme $a \neq b$, on peut considérer le polynôme :

$$Q = P - \frac{P(a)}{(a-b)^{n+1}} \cdot (X-b)^{n+1}$$

  qui est un élément de $\mathbb{C}_{n+1}[X]$ qui vérifie :

$$Q(a) = P(a) - \frac{P(a)}{(a-b)^{n+1}} \cdot (a-b)^{n+1} = 0$$

  donc Q est divisible par $(X-a)$. On écrit $Q = (X-a)\cdot R$, avec $R \in \mathbb{C}_n[X]$.
  Par hypothèse de récurrence, on peut écrire R comme combinaison linéaires des $(X-a)^k(X-b)^{n-k}$ pour $k \in [\![0;n]\!]$. On peut alors écrire :

$$R = \sum_{k=0}^{n} \lambda_k (X-a)^k (X-b)^{n-k}$$

  et en réinjectant dans l'expression de Q puis de P, on trouve :

$$P = \frac{P(a)}{(a-x)^{n+1}} \cdot (X-b)^{n+1} + \sum_{k=0}^{n} \lambda_k (X-a)^{k+1}(X-b)^{n-k} = \frac{P(a)}{(a-x)^{n+1}} \cdot (X-b)^{n+1} + \sum_{l=1}^{n+1} \lambda_k (X-a)^l (X-b)^{n+1-}$$

  qui est bien un combinaison linéaire des $(X-a)^k(X-b)^{n+1-k}$ pour $k \in [\![0;n+1]\!]$.
  D'où la récurrence.

Et ainsi on a bien montré que la famille est génératrice.

II Sous-espaces vectoriels en dimension finie

II.1 Dimension d'un sous-espace et rang d'une famille

Proposition II.1. *Si E est un espace vectoriel de dimension finie, alors tout sous-espace vectoriel F de E est également de dimension finie.*
De plus, on a $\dim F \leq \dim E$, avec égalité si, et seulement si, $F = E$.

Démonstration. Si $F = \{0\}$ alors le résultat est vérifié.
Sinon, on considère l'ensemble $A = \{n \in \mathbb{N}^* \mid \exists (x_1, \dots, x_n) \in F^n \text{ libre}\}$ (l'ensemble des cardinaux de familles libres construites à partir d'éléments de F). Alors A est une partie non vide (comme $F \neq \{0\}$)

majorée (par $\dim E$, comme toute famille libre d'éléments de F est une famille libre d'éléments de E) donc admet un plus grand élément n.
Notons $(x_1, \dots, x_n)$ famille libre de F. Montrons que c'est une base. Il suffit de prouver qu'elle est génératrice.
Soit $x \in F$. La famille $(x_1, \dots, x_n, x)$ est de cardinal $(n+1)$, donc liée (par définition de n), et comme $(x_1, \dots, x_n)$ est libre cela veut donc dire que x est combinaison linéaire de $x_1, \dots, x_n$: la famille (x_i) est donc bien génératrice.
Donc finalement F admet une base de cardinal $n \leq \dim E$, ce qui prouve le résultat.
Si $\dim E = \dim F$, toute base de F est également une base de E (en tant que famille libre d'élément de E de "bon" cardinal), donc $E = F$ (en tant qu'espace engendré par cette base). □

Remarques II.2.

1. *Le résultat est faux en dimension infinie. Par exemple, si $E = \mathbb{R}[X]$ et $F = \{P \in \mathbb{R}[X] \,|\, P(0) = 0\}$, alors F est un sev de E, et F et E ont même dimension (infinie) mais $F \neq E$.*
2. *Ce résultat dit aussi que l'application :*

$$\varphi : \left\{ \begin{array}{ccc} \{F \text{ sev de } E\} & \to & \mathbb{N} \\ F & \mapsto & \dim F \end{array} \right.$$

est une application strictement croissante (où on prend comme relations d'ordre l'inclusion au départ, et la relation d'ordre usuelle à l'arrivée).

Exemples II.3.

1. *Dans $\mathbb{R}^2$, les sous-espaces non triviaux sont les espaces de dimension 1 (donc les droites).*
2. *Dans $\mathbb{R}^3$, ce sont les espaces de dimension 1 ou 2, donc les plans et les droites.*

Définition II.4. *Étant donnée une famille $(x_i)_{i\in I}$ (finie ou non) d'un espace vectoriel E de dimension finie, on appelle **rang** de la famille (x_i) la dimension de l'espace $\mathrm{vect}((x_i)_{i\in I})$, que l'on notera $\mathrm{rg}((x_i)_{i\in I})$.*

Remarque II.5. *Pour une famille finie $(x_1, \dots, x_n)$, on notera $\mathrm{rg}(x_1, \dots, x_n)$ son rang.*
On peut généraliser à une famille finie dans un espace quelconque : on raisonne alors dans l'espace vectoriel engendré, qui est de dimension finie.

Proposition II.6. *On considère $(x_i)_{i\in I}$ famille d'éléments de E. Alors :*

1. *si E est de dimension finie : (x_i) est génératrice si, et seulement si, $\mathrm{rg}((x_i)) = \dim E$;*
2. *si I est fini : $\mathrm{rg}((x_i)) \leq \mathrm{card}(I)$, avec égalité si, et seulement si, la famille (x_i) est libre.*

Démonstration. On pose $F = \mathrm{Vect}(x_i)$, de sorte que $\dim(F) = \mathrm{rg}(x_i)$. Et alors :

1. (x_i) est génératrice si, et seulement si, $E = F$, c'est-à-dire $\dim(E) = \dim(F) = \mathrm{rg}(x_i)$ si E est de dimension finie ;
2. (x_i) engendre F, donc est de cardinal au moins $\dim(F)$, avec égalité si, et seulement si, c'est une base, c'est-à-dire qu'elle est libre (comme elle est déjà génératrice).

□

II.2 Somme de sous-espaces vectoriels

Proposition II.7. *Soient F, G deux espaces supplémentaires dans un espace vectoriel E de dimension finie. Alors :* $\dim E = \dim F + \dim G$.

Démonstration. Considérons $(f_1, \dots, f_n)$ une base de F et $(g_1, \dots, g_m)$ une base de G, avec donc $n = \dim F$ et $m = \dim G$. Montrons que la famille $\mathcal{B} = (f_1, \dots, f_n, g_1, \dots, g_m)$ est une base de E.

— comme $E = F + G$, tout élément $x \in E$ s'écrit $x = x_F + x_G$ pour $x_F \in F$ et $x_G \in G$. Comme les familles (f_i) et (g_j) engendrent respectivement F et G, alors il existe des familles de scalaires (λ_i) et (μ_j) telles que : $x_F = \sum_i \lambda_i f_i$ et $x_G = \sum_j \mu_j g_j$. Et finalement : $x = \sum_i \lambda_i f_i + \sum_j \mu_j g_j$ est bien engendré par $\mathcal{B}$;
— comme $F \cap G = \{0\}$, soient $(\lambda_i), (\mu_j)$ tels que $\sum_i \lambda_i f_i + \sum_j \mu_j g_j = 0$. Alors :

$$\underbrace{\sum_i \lambda_i f_i}_{\in F} = \underbrace{-\sum_j \mu_j g_j}_{\in G} \in F \cap G$$

donc $\sum_i \lambda_i f_i = 0 = \sum_j \mu_j g_j$. Et comme les familles $(f_i), (g_j)$ sont libres on déduit que les scalaires (λ_i) et (μ_j) sont nuls : la famille $\mathcal{B}$ est libre.

Et donc $\dim E = \dim(F + G) = \text{card}\mathcal{B} = n + m = \dim F + \dim G$. □

Remarque II.8. *En fait on a un résultat plus fort : si F, G sont deux espaces de dimension finie, on a équivalence entre :*

1. *la somme $F + G$ est directe ;*
2. *la concaténation de deux bases de F et G est une base de $F + G$;*
3. $\dim(F + G) = \dim F + \dim G$.

Qui se démontre sensiblement de la même manière.
Dans ce cas, une base de $F+G$ obtenue par concaténation d'une base de F et d'une base de G sera appelée ***base adaptée*** *à la décomposition en somme directe $F \oplus G$. Le point important étant qu'il existe des bases non adaptées.*

Théorème II.9 (Formule de Grassmann)**.** *Soient F et G deux sous-espaces vectoriels de dimensions finies d'un espace vectoriel E (quelconque). Alors :*

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

Démonstration. Considérons $(e_1, \dots, e_p)$ une base de $F \cap G$ (ce qui a bien un sens comme $F \cap G$ est un sous-espace de F ou de G, donc est de dimension finie.
On complète la famille $(e_1, \dots, e_p)$ des deux manières suivantes :
— en $(e_1, \dots, e_p, f_1, \dots, f_n)$ pour avoir une base de F ;
— en $(e_1, \dots, e_p, g_1, \dots, g_m)$ pour avoir une base de G.
Et on a déjà que $p = \dim(F \cap G)$, $n + p = \dim F$ et $m + p = \dim G$.
Montrons que la famille $(e_1, \dots, e_p, f_1, \dots, f_n, g_1, \dots, g_m)$ est une base de $F + G$:
— elle est génératrice : si $x \in F + G$, on écrit $x = x_F + x_G$ pour $x_F \in F$ et $x_G \in G$. Comme $(e_1, \dots, e_p, f_1, \dots, f_n)$ et $(e_1, \dots, e_p, g_1, \dots, g_m)$ sont respectivement des bases (donc génératrices) de F et G, il existe de familles $(\alpha_i), (\beta_i), (\lambda_j), (\mu_k)$ telles que :

$$x_F = \sum_i \alpha_i e_i + \sum_j \lambda_j f_j \text{ et } x_G = \sum_i \beta_i e_i + \sum_k \mu_k g_k$$

et donc :

$$x = \sum_i (\alpha_i + \beta_i) e_i + \sum_j \lambda_j f_j + \sum_k \mu_k g_k$$

ce qui donne bien que la famille est génératrice ;
— elle est libre : si $(\alpha_i), (\lambda_j), (\mu_k)$ sont des familles de scalaires telles que :

$$0 = \sum_i \alpha_i e_i + \sum_j \lambda_j f_j + \sum_k \mu_k g_k$$

alors :

$$\underbrace{\sum_i \alpha_i e_i + \sum_j \lambda_j f_j}_{\in F} = \underbrace{-\sum_k \mu_k g_k}_{\in G} \in F \cap G$$

et donc on peut écrire :

$$\sum_k \mu_k g_k = \sum_i \beta_i e_i$$

Comme la famille $(e_1, \dots, e_p, g_1, \dots, g_m)$ est libre, cela donne que tous les μ_k sont nuls. Et il vient alors :

$$\sum_i \alpha_i e_i + \sum_j \lambda_j f_j = 0$$

et comme la famille $(e_1, \dots, e_p, f_1, \dots, f_n)$ est libre on trouve de même que les α_i et λ_j sont nuls, ce qui donne bien que la famille est libre.

On a donc une base de $F+G$, qui est de cardinal $n+m+p$, qui est donc la dimension de $F+G$. Et on a bien :

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

□

Corollaire II.10. *Soient F, G deux sev d'un espace vectoriel E de dimension finie. Alors F et G sont supplémentaires dans E si, et seulement si, deux des assertions suivantes sont vérifiées :*

1. $E = F + G$;
2. $F \cap G = \{0\}$;
3. $\dim F + \dim G = \dim E$.

et alors les trois assertions sont vérifiées.

Démonstration. Les deux premières assertions sont la définition d'être supplémentaire. Et la proposition précédente assure le résultat sur la dimension.

Il suffit donc de montrer que, si deux autres assertions que sont vérifiées, alors les deux premières sont vérifiées pour avoir le résultat :

- si $E = F + G$ et $\dim F + \dim G = \dim E$: alors par la formule de Grassmann, comme $E = F + G$, on a $\dim(F \cap G) = 0$, donc $F \cap G = \{0\}$ et F et G sont supplémentaires dans E ;
- si $F \cap G = \{0\}$ et $\dim F + \dim G = \dim E$: alors par la formule de Grassmann $\dim(F+G) = \dim F + \dim G = \dim E$, donc $(F+G)$ est un sev de E de même dimension **finie** que E, donc $F + G = E$ et F et G sont supplémentaires dans E.

□

Corollaire II.11. *Dans un espace E de dimension finie, tout sev F de E admet des supplémentaires. De plus, ils ont tous même dimension, à savoir* $\dim E - \dim F$.

Démonstration. Pour l'existence, on considère $(f_1, \dots, f_n)$ une base de F (de sorte que $n = \dim, F$), qu'on complète en une base de E : $(f_1, \dots, f_n, g_1, \dots, g_m)$ (avec donc $\dim E = n+m$).

On pose $G = \text{vect}(g_1, \dots, g_m)$. Comme $(g_1, \dots, g_m)$ est libre, alors c'est une base de G, donc $\dim G = m$.

Et ainsi on a : $E = \text{vect}(f_1, \dots, f_n, g_1, \dots, g_m) = F + G$ et $\dim E = \dim F + \dim G$, donc F et G sont bien supplémentaires dans E.

Le résultat sur la dimension découle de la formule de Grassmann.

□

Remarque II.12. *Ces résultats se généralisent à davantage de sous-espaces, ce que l'on pourrait prouver de manière analogue, ou en utilisant des résultats sur les applications linéaires en dimension finie (qu'on verra plus loin).*

Proposition II.13. *Si $F_1, \dots, F_n$ sont des sev d'un espace E de dimension finie, alors $\sum_{i=1}^n F_i$ est un sev de E de dimension finie tel que :*

$$\dim\left(\sum_{i=1}^n F_i\right) \leq \sum_{i=1}^n \dim F_i$$

avec égalité si, et seulement si, la somme est directe.
De plus, cette somme est directe si, et seulement si, la concaténation de bases des F_i est une base de $\sum_{i=1}^n F_i$.

III Applications linéaires en dimension finie

III.1 Dimension de $\mathcal{L}(E,F)$

Proposition III.1. *Si E, F sont deux espaces vectoriels de dimensions finies, alors $\mathcal{L}(E,F)$ est un espace vectoriel de dimension finie avec :* $\dim \mathcal{L}(E,F) = \dim E \times \dim F$.
En particulier, $\dim \mathcal{L}(E) = (\dim E)^2$ *et* $\dim E^* = \dim E$.

Démonstration. Soient $(e_1, \dots, e_p)$ et $(f_1, \dots, f_n)$ des bases respectivement de E et F. On considère, pour $(i,j) \in [\![1;n]\!] \times [\![1;p]\!]$ l'application linéaire $\varphi_{i,j} \in \mathcal{L}(E,F)$ définie par :

$$\varphi_{i,j} : \sum_{k=1}^p \lambda_k e_k \mapsto \lambda_j f_i$$

c'est-à-dire que $\varphi_{i,j}(e_k) = \delta_{k,j} f_i$.
Ces applications sont linéaires, et bien définies par le fait que (e_k) est une base de E.
Montrons que la famille $(\varphi_{i,j})$ est une base de $\mathcal{L}(E,F)$:

— si $\lambda_{i,j}$ sont des scalaires tels que $\sum_{i,j} \lambda_{i,j}\varphi_{i,j} = 0$: en évaluant en e_k pour $k \in [\![1;n]\!]$, il vient :

$$\sum_i \lambda_{i,k} f_i = 0$$

et par liberté de la famille (f_i) on déduit que tous les $\lambda_{i,k}$ sont nuls. Donc tous les $\lambda_{i,j}$ sont nuls, et la famille $(\varphi_{i,j})$ est libre ;

— soit $\varphi \in \mathcal{L}(E,F)$: pour tout $k \in [\![1;p]\!]$, on a $\varphi(e_k) \in F$, donc comme la famille (f_i) engendre F il existe des scalaires $\lambda_{i,k}$ tels que :

$$\varphi(e_k) = \sum_i \lambda_{i,k} f_i.$$

Montrons qu'alors : $\varphi = \sum_{i,j} \lambda_{i,j}\varphi_{i,j}$. Par détermination d'une application linéaire, il suffit de voir que les deux applications coïncident sur une base de E. Mais par construction, on a justement que pour tout $k \in [\![1;p]\!]$:

$$\left(\sum_{i,j} \lambda_{i,j}\varphi_{i,j}\right)(e_k) = \sum_{i,j} \lambda_{i,j}\varphi_{i,j}(e_k) = \sum_{i,j} \lambda_{i,j}\delta_{k,j} f_i = \sum_i \lambda_{i,k} f_i = \varphi(e_k)$$

ce qui prouve bien l'égalité.
Donc $(\varphi_{i,j})$ engendre bien $\mathcal{L}(E,F)$.

Et finalement $(\varphi_{i,j})$ est bien une base de $\mathcal{L}(E,F)$. Son cardinal est $n \times m = \dim E \times \dim F$, ce qui donne la dimension de $\mathcal{L}(E,F)$. □

III.2 Injectivité, surjectivité ou bijectivité d'une application linéaire

Proposition III.2. *Soient E, F deux espaces de même dimension finie, et $\varphi \in \mathcal{L}(E,F)$. On a équivalence entre :*

1. *φ est injective ;*
2. *φ est surjective ;*
3. *φ est bijective.*

Démonstration. On fixe $(e_1, \dots, e_n)$ une base de E. Alors la famille $(\varphi(e_1), \dots, \varphi(e_n))$ est une famille de F de cardinal $n = \dim F$. On a donc l'équivalence :

$$(\varphi(e_i)) \text{ libre } \Leftrightarrow (\varphi(e_i)) \text{ génératrice } \Leftrightarrow (\varphi(e_i)) \text{ base}$$

ce qui revient à dire que :

$$\varphi \text{ injective } \Leftrightarrow \varphi \text{ surjective } \Leftrightarrow \varphi \text{ bijective .}$$

□

Corollaire III.3. *Si E est un espace vectoriel de dimension finie, et $f \in \mathcal{L}(E)$, alors il y a équivalence entre :*

1. *f est inversible : il existe $g \in \mathcal{L}(E)$ telle que $g \circ f = \mathrm{id}_E = f \circ g$;*
2. *f est inversible à gauche : il existe $g \in \mathcal{L}(E)$ telle que $g \circ f = \mathrm{id}_E$;*
3. *f est inversible à droite : il existe $g \in \mathcal{L}(E)$ telle que $f \circ g = \mathrm{id}_E$.*

Et dans ce cas on a : $g = f^{-1}$.

Démonstration. L'inversibilité est en fait la bijectivité. Il suffit alors de constater que :
— si $g \circ f = \mathrm{id}_E$: alors $g \circ f$ est injective, donc f également, donc f est bijective ;
— si $f \circ g = \mathrm{id}_E$: alors $f \circ g$ est surjective, donc f également, donc f est bijective.
Et les réciproques découlent de la bijectivité.
Et en composant par f^{-1} (à gauche ou à droite) dans les égalités ci-dessus, on obtient bien que $g = f^{-1}$. □

Définition III.4. *Deux espaces vectoriels E, F sont dits **isomorphes** s'il existe une application linéaire bijective de E sur F.*

Théorème III.5. *Si E, F sont deux espaces vectoriels avec l'un des deux de dimension finie, ils sont isomorphes si, et seulement si, ils ont même dimension.*

Démonstration. Si E, F ont même dimension : notons n cette dimension (qui est finie par hypothèse), et posons $(e_1, \dots, e_n), (f_1, \dots, f_n)$ des bases de E et F respectivement. Alors l'application $\varphi \in \mathcal{L}(E,F)$ définie par $\varphi(e_i) = f_i$ pour tout $i \in [\![1; n]\!]$ envoie une base sur une base : elle est donc bijective. Donc E et F sont isomorphes.
Si E, F sont isomorphes : supposons par exemple que E est de dimension finie n, et notons $\varphi : E \to F$ application linéaire bijective. Soit $(e_1, \dots, e_n)$ une base de E. Alors par bijectivité de φ la famille $(\varphi(e_1), \dots, \varphi(e_n))$ est une base de F, qui est donc de dimension n également. □

Remarque III.6. *Comme $\dim \mathbb{K}^n = n$, un espace vectoriel E est de dimension n si, et seulement si, il est en bijection avec $\mathbb{K}^n$. Une telle bijection est donnée par l'application :*

$$(\lambda_1, \dots, \lambda_n) \mapsto \sum_{i=1}^{n} \lambda_i e_i$$

où (e_i) est une base de E (la bijectivité étant assurée par l'unicité et l'existence de l'écriture des éléments de E dans la base (e_i)).

Exemple III.7. *Si $F_1, \dots, F_n$ sont des espaces de dimension finie, ils sont en somme directe si, et seulement si, l'application :*

$$\varphi : \left\{ \begin{array}{ccc} F_1 \times \cdots \times F_n & \to & F_1 + \cdots + F_n \\ (x_1, \dots, x_n) & \mapsto & x_1 + \cdots + x_n \end{array} \right.$$

est bijective. Comme elle est surjective par définition, elle est injective si, et seulement si, les espaces $F_1 \times \cdots \times F_n$ et $F_1 + \cdots + F_n$ ont même dimension, c'est-à-dire si, et seulement si :

$$\dim \left(\sum_{i=1}^{n} F_i \right) = \sum_{i=1}^{n} \dim F_i.$$

III.3 Le théorème du rang

Définition III.8. *Soit f une application linéaire. Si $\mathrm{Im}f$ est un espace vectoriel de dimension finie, sa dimension est appelée **rang** de f est est notée $\mathrm{rg}(f)$.*

Remarque III.9. *Si E est muni d'une base ou d'une famille génératrice $(x_i)_{i\in I}$ (finie ou non), alors le rang de f est le rang de la famille $(f(x_i)_{i\in I})$ (comme cette famille engendre $\mathrm{Im}f$ par définition).*

Proposition III.10. *Si $f \in \mathcal{L}(E,F)$ avec E ou F de dimension finie, alors f est de rang fini avec $\mathrm{rg}(f) \leq \min(\dim E, \dim F)$.*

Démonstration. Si E est de dimension finie : notons $(e_1, \dots, e_n)$ une base de E. Alors la famille $(f(e_1), \dots, f(e_n))$ est une famille génératrice de $\mathrm{Im}f$ de cardinal $n = \dim E$, donc $\mathrm{rg}(f)$ est au plus $n = \dim E$.
Si F est de dimension finie : alors $\mathrm{Im}f$ est un sev de F, donc de dimension finie majorée par $\dim F$. □

Proposition III.11. *Si $f \in \mathcal{L}(E,F)$ et que S est un supplémentaire de $\mathrm{Ker}f$ dans E, alors $f_{|S}^{|\mathrm{Im}f}$ est un isomorphisme de S sur $\mathrm{Im}f$.*

Démonstration. Comme $S \subset E$, on a $f(S) \subset f(E) = \mathrm{Im}f$ donc $g = f_{|S}^{|\mathrm{Im}f}$ est bien définie, et est bijective :
- injectivité : soit $x \in \mathrm{Ker}\, g$: alors $x \in S$ vérifie $f(x) = 0$, donc $x \in \mathrm{Ker}f$. Et finalement : $x \in \mathrm{Ker}f \cap S = \{0\}$, d'où l'injectivité ;
- surjectivité : soit $y \in \mathrm{Im}f$: notons $x \in E$ tel que $y = f(x)$. Posons $x = x_1 + x_2$ avec $x_1 \in \mathrm{Ker}\, f$ et $x_2 \in S$. Alors :

$$y = f(x) = f(x_1 + x_2) = f(x_1) + f(x_2) = f(x_2) \in f(S) = \mathrm{Im}\, g$$

  donc g est surjective.

Et finalement g est bien bijective. □

Remarque III.12. *Ce résultat a un cadre d'application assez limité, dans la mesure où il n'existe pas toujours des supplémentaires.*

Théorème III.13 (Théorème du rang)**.** *Si E, F sont deux espaces vectoriels, avec E de dimension finie, et $f \in \mathcal{L}(E,F)$, alors :*

$$\dim E = \mathrm{rg}(f) + \dim \mathrm{Ker}f.$$

Démonstration. Comme E est de dimension finie, il existe S supplémentaire de $\mathrm{Ker}f$ dans E. On a donc :
- comme S est un supplémentaire de $\mathrm{Ker}f$: $\dim S = \dim E - \dim \mathrm{Ker}f$;
- par bijectivité de $f_{|S}^{|\mathrm{Im}f}$: $\dim S = \dim \mathrm{Im}f = \mathrm{rg}(f)$.

Et ainsi : $\dim E = \mathrm{rg}(f) + \dim \mathrm{Ker}f$. □

Remarque III.14. *La dimension de F n'a aucune incidence dans ce théorème. Ou du moins cette incidence est cachée dans la définition même de f. Par exemple, on pourrait considérer G espace vectoriel qui contient G, et voir un élément de $\mathcal{L}(E,F)$ comme un élément de $\mathcal{L}(E,G)$, sans en changer ni le rang ni le noyau. On obtient surtout que $\mathrm{rg}(f) \leq \dim E$: une application linéaire ne peut que diminuer la dimension.*

Proposition III.15. *Si $f \in \mathcal{L}(E,F)$, alors :*

1. *si E est de dimension finie : f est injective si, et seulement si,* $\mathrm{rg}(f) = \dim E$ *;*
2. *si F est de dimension finie, f est surjective si, et seulement si,* $\mathrm{rg}(f) = \dim F$.

Démonstration.

1. f est injective si, et seulement si, $\mathrm{Ker} f = \{0\}$, c'est-à-dire $\dim \mathrm{Ker} f = 0$; si E est de dimension finie, par théorème du rang, c'est équivalent au fait que : $\mathrm{rg}(f) = \dim E$;
2. f est surjective si, et seulement si, $\mathrm{Im} f = F$; si F est de dimension finie, comme $\mathrm{Im} f$ est un sev de F, c'est équivalent au fait que $\mathrm{rg}(f) = \dim F$.

□

Remarque III.16. *On retrouve ainsi d'une autre manière que, pour un endomorphisme f sur un espace de dimension finie :*

$$f \text{ injectif} \Leftrightarrow f \text{ surjectif} \Leftrightarrow f \text{ bijectif.}$$

Plus précisément, on a pour $f \in \mathcal{L}(E)$ et E de dimension $n \in \mathbb{N}^*$:

$$\mathrm{Ker}\, f = \{0\} \Leftrightarrow \mathrm{rg}(f) = n \Leftrightarrow f \text{ bijective.}$$

Corollaire III.17. *Si $f \in \mathcal{L}(E,F)$, avec E et F de dimensions finies, alors :*

1. *si* $\dim E < \dim F$*, alors f n'est pas surjective ;*
2. *si* $\dim E > \dim F$*, alors f n'est pas injective.*

Démonstration. Découle du résultat précédent et du fait que : $\mathrm{rg}(f) \leq \min(\dim E, \dim F)$. □

Remarque III.18. *En particulier, si f réalise un isomorphisme de E vers F, alors E et F ont même dimension.*

Proposition III.19. *Si E est un espace vectoriel (quelconque) et $f \in \mathrm{GL}(E)$, alors pour tout sous-espace F de E de dimension finie, l'espace $f(F)$ est de dimension finie, de même dimension que F.*

Démonstration. Il suffit de voir que, u étant injective, $f_{|F}$ l'est également, et induit donc un isomorphisme de F sur $f(F)$, qui ont donc même dimension. □

Remarque III.20. *En fait c'est seulement l'injectivité de f qui est importante ici.*

Corollaire III.21. *Si E, F sont deux espaces vectoriels quelconques et $f \in \mathcal{L}(E,F)$ de rang fini :*

1. *si $g \in \mathrm{GL}(E)$, alors* $\mathrm{rg}(f \circ g) = \mathrm{rg}(f)$ *;*
2. *si $h \in \mathrm{GL}(F)$, alors* $\mathrm{rg}(h \circ f) = \mathrm{rg}(f)$.

Démonstration.

1. Comme g est surjective alors $g(E) = E$, donc $\mathrm{Im}(f \circ g) = f \circ g(E) = f(E) = \mathrm{Im} f$, ce qui donne l'égalité en prenant la dimension.
2. Comme h est injective, alors $\mathrm{Im}(h \circ f) = h\,(\mathrm{Im} f)$, qui a donc même dimension que $\mathrm{Im} f$ par le résultat précédent.

□

Remarque III.22. *En fait c'est seulement la surjectivité de g et l'injectivité de h qu'on utilise ici.*

III.4 Formes linéaires et équations de sous-espaces

Proposition III.23. *Si E est un espace vectoriel de dimension finie $n \in \mathbb{N}^*$, et $(e_1, \dots, e_n)$ est une base de E, alors toute forme linéaire sur E est combinaison linéaire de applications φ_i (pour $i \in [\![1; n]\!]$) définies par :*

$$\forall i, j \in [\![1; n]\!],\ \varphi_i(x_j) = \delta_{i,j}.$$

Une telle écriture est unique. Plus précisément, si on note $\varphi = \sum_{i=1}^n \lambda_i \varphi_i$, alors :

$$\forall i \in [\![1; n]\!],\ \lambda_i = \varphi(e_i).$$

Démonstration. L'existence et unicité de l'écriture comme combinaison linéaire vient de la base de $\mathcal{L}(E, \mathbb{K}) = E^*$ donnée avant.
Le dernier point vient du fait que, si $\varphi = \sum_{i=1}^n \lambda_i \varphi_i$ et $i \in [\![1; n]\!]$, alors :

$$\varphi(e_i) = \sum_{j=1}^n \lambda_j \varphi_j(e_i) = \sum_{j=1}^n \lambda_j \delta_{i,j} = \lambda_i.$$

□

Remarque III.24. *Les φ_i et l'écriture $\varphi = \sum_i \lambda_i \varphi_i$ dépendent de la base choisie. Elles permettent d'exprimer l'image d'un vecteur par ses coordonnées.*

Exemple III.25. *On considère sur $\mathbb{R}^3$ la forme linéaire :*

$$\varphi : (x, y, z) \mapsto x + y + z$$

dont les coordonnées dans la base de E^* associée à la base canonique sont $(1, 1, 1)$.
On peut chercher à exprimer φ à partir de la base $(\underbrace{(1,0,0)}_{=e_1}, \underbrace{(1,1,0)}_{=e_2}, \underbrace{(1,1,1)}_{=e_3})$, dont on note $\varphi_1, \varphi_2, \varphi_3$ les formes linéaires correspondantes. Alors :

$$\varphi(e_1) = 1,\ \varphi(e_2) = 2 \text{ et } \varphi(e_3) = 3$$

donc : $\varphi = \varphi_1 + 2\varphi_2 + 3\varphi_3$.
On pourrait aussi chercher à déterminer $\varphi_1, \varphi_2, \varphi_3$. Pour cela, il faut exprimer les vecteurs de la base canonique en fonction de e_1, e_2, e_3. On trouve :

$$(1, 0, 0) = e_1,\ (0, 1, 0) = e_2 - e_1 \text{ et } (0, 0, 1) = e_3 - e_2$$

et donc :

$$\varphi_1(x, y, z) = x\varphi_1((1, 0, 0)) + y\varphi_1((0, 1, 0)) + z\varphi_1((0, 0, 1)) = x - y$$
$$\varphi_2(x, y, z) = x\varphi_2((1, 0, 0)) + y\varphi_2((0, 1, 0)) + z\varphi_2((0, 0, 1)) = y - z$$
$$\varphi_3(x, y, z) = x\varphi_3((1, 0, 0)) + y\varphi_3((0, 1, 0)) + z\varphi_3((0, 0, 1)) = z$$

et en combinant les deux formules on trouve bien que $\varphi : (x, y, z) \mapsto x + y + z$.

Corollaire III.26. *Si E est un espace vectoriel dimension finie $n \in \mathbb{N}^*$, les hyperplans de E sont exactement les sev de E de dimension $n - 1$.*
De plus, étant donnés $(e_1, \dots, e_n)$ une base de E et H un tel hyperplan, il existe $\lambda_1, \dots, \lambda_n$ non tous nuls tels que :

$$H = \left\{ \sum_{i=1}^n x_i e_i \mid \sum_{i=1}^n \lambda_i x_i = 0 \right\}.$$

Démonstration. Les hyperplans sont exactement les supplémentaires de droites (qui sont des espaces de dimension 1), donc ce sont les espaces de dimension $n-1$ (par la formule de Grassmann et l'existence de supplémentaires).
Soit $\varphi \in E^*$ non nulle telle que $H = \mathrm{Ker}\,\varphi$. Notons $\varphi = \sum_{i=1}^n \lambda_i \varphi_i$ (où les φ_i sont les formes linéaires associées à la base (e_i)). Alors les λ_i sont non tous nuls (comme $\varphi \neq 0$), et on trouve ainsi :

$$H = \mathrm{Ker}\varphi = \left\{ \sum_{i=1}^n x_i e_i \,|\, \sum_{j=1}^n \lambda_j \underbrace{\varphi_j\left(\sum_{i=1}^n x_i e_i\right)}_{=x_j} \right\}$$

ce qui donne bien le résultat. □

Remarque III.27. *On dit alors que l'équation $\sum_{i=1}^n \lambda_i x_i = 0$ est **une** équation de l'hyperplan H dans la base $(e_1, \ldots, e_n)$.*

Exemple III.28. *Considérons $E = \mathbb{R}_n[X]$ (pour $n \in \mathbb{N}$), qui est un espace vectoriel de dimension $n-1$. L'application $\varphi : P \mapsto P(1)$ est une forme linéaire (c'est clair) non nulle (car par exemple $\varphi(1) = 1 \neq 0$), donc son noyau $H = \mathrm{Ker}\varphi$ dans E est un hyperplan de E.*
Son équation dans la base canonique $(1, X, \ldots, X^n)$ est :

$$H \;:\; a_0 + a_1 + \cdots + a_n = 0$$

puisque l'on a : $\varphi\left(\sum_{i=0}^n a_i X^i\right) = \sum_{i=0}^n a_i$.

Corollaire III.29. *Deux hyperplans sont confondus si, et seulement si, leurs équations dans une même base sont proportionnelles.*

Démonstration. Si on note φ_1, φ_2 les formes linéaires associées aux deux hyperplans, alors les hyperplans sont confondus si, et seulement si, les forme sφ_1, φ_2 sont colinéaires, c'est-à-dire qu'elles sont proportionnelles. □

Corollaire III.30. *Si E est de dimension n et $m \in \mathbb{N}$ vérifie $m \leq n$, alors tout sev de E de dimension m est l'intersection de $(n-m)$ hyperplans de E.*

Démonstration. Soit F un sev de E de dimension m. On considère $(e_1, \ldots, e_m)$ un base de F, qu'on complète en $(e_1, \ldots, e_n)$ base de E.
Notons $(\varphi_1, \ldots, \varphi_n)$ les formes linéaires associées, et pour tout $i \in [\![1; n]\!]$ notons $H_i = \mathrm{Ker}\varphi_i$. Alors :

$$F = \cap_{i=m+1}^n H_i$$

est bien l'intersection de $n-m$ hyperplans. □

Remarque III.31. *En termes d'équations, cela veut dire que tout espace vectoriel de E de dimension m est donné par un système de $(n-m)$ équations (une par hyperplan). Ces équations sont en fait deux-à-deux linéairement indépendantes, et elles donnent le système d'équation associé à l'espace vectoriel.*
Pour une droite, on retrouve la situation déjà connue depuis longtemps :

- *dans le plan : il s'agit d'un hyperplan, qui est donc donné par une seule équation ;*
- *dans l'espace : c'est un espace de dimension 1, donc intersection de $(3-1) = 2$ (hyper)plans, donc un système de deux équations.*

Remarque III.32. *Plus généralement, on peut s'intéresser à l'intersection de p plans dans E, et on trouve que :*

$$\dim\left(\cap_{i=1}^p H_i\right) \geq \dim E - p.$$

On utilise l'application $\varphi : x \mapsto (\varphi_1(x), \ldots, \varphi_p(x))$, où les φ_i sont les formes linéaires associées aux hyperplans H_i. Le théorème du rang appliqué à φ donne le résultat (et montre qu'il y a égalité si, et seulement si, φ est bijective, ce qui est le cas si, et seulement si, les φ_i sont linéairement indépendantes).

Chapitre 22

Matrices et applications linéaires

I Matrice d'une application linéaire dans une base

I.1 Représentation matricielle

Définition I.1. *Soit E un espace vectoriel de dimension finie n, $\mathcal{B} = (e_1, \dots, e_n)$ une base de E, et $x \in E$. Si on note $\lambda_1, \dots, \lambda_n$ les coordonnées de x dans $\mathcal{B}$ (c'est-à-dire $x = \sum \lambda_i, e_i$), alors la* ***matrice de*** *x* ***dans la base*** *$\mathcal{B}$ est la matrice colonne :*

$$\mathrm{Mat}_{\mathcal{B}}(x) = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in \mathcal{M}_{n,1}(\mathbb{K}).$$

Plus généralement, si on note $x_1, \dots, x_p$ des vecteurs de E, et que les $\lambda_{i,j}$ sont les coordonnées de x_j (c'est-à-dire $x_j = \sum_i \lambda_{i,j} e_i$), alors la ***matrice de la famille*** *(x_j)* ***dans la base*** *$\mathcal{B}$ est la matrice :*

$$\mathrm{Mat}_{\mathcal{B}}((x_j)_{1\leq j\leq p} = \begin{pmatrix} \lambda_{1,1} & \lambda_{1,2} & \dots & \lambda_{1,p} \\ \lambda_{2,1} & \lambda_{2,2} & \dots & \lambda_{2,p} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{n,1} & \lambda_{n,2} & \dots & \lambda_{n,p} \end{pmatrix} = (\lambda_{i,j}) \in \mathcal{M}_{n,p}(\mathbb{K}).$$

Remarque I.2. *On prendra bien garde qu'un vecteur sera représenté par une matrice colonne.*

Exemple I.3. *Dans $\mathbb{R}^3$, la matrice de la famille (x_1, x_2, x_3) avec $x_1 = (3, 1, 4), x_2 = (1, 5, 9), x_3 = (2, 6, 5)$ dans la base canonique est :*

$$\begin{pmatrix} 3 & 1 & 2 \\ 1 & 5 & 6 \\ 4 & 9 & 5 \end{pmatrix}$$

Proposition I.4. *Étant donnée une base $\mathcal{B}$ de E, l'application $x \mapsto \mathrm{Mat}_{\mathcal{B}}(x)$ est une bijection de E sur $\mathcal{M}_{n,1}(\mathbb{K})$.*

Démonstration. Découle de l'unicité de l'écriture d'un vecteur comme combinaison linéaires d'éléments d'une base. □

Définition I.5. *Si E, F sont deux espaces vectoriels de dimension finie, $\mathcal{B} = (e_1, \dots, e_p)$ une base de E, et $\mathcal{C} = (f_1, \dots, f_n)$ une base de F et $f \in \mathcal{L}(E, F)$, on appelle* ***matrice de*** *f* ***dans bases*** *$\mathcal{B}$* ***et*** *$\mathcal{C}$ la matrice $\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f) = (\lambda_{i,j}) \in \mathcal{M}_{n,p}(\mathbb{K})$ où les $\lambda_{i,j}$ vérifient :*

$$\forall j \in [\![1; p]\!],\ f(e_j) = \sum_{i=1}^{n} \lambda_{i,j} f_i.$$

Dans, le cas particulier où $E = F$ (donc f est un endomorphisme de E) et $\mathcal{B} = \mathcal{C}$, on notera plus simplement $\mathrm{Mat}_{\mathcal{B}}(f)$ au lieu de $\mathrm{Mat}_{\mathcal{B},\mathcal{B}}(f)$.

Remarques I.6.

1. *La matrice de f est la matrice de la famille $(f(e_j))$ dans la base $\mathcal{C}$.*
2. *Si on reprend la base de $\mathcal{L}(E,F)$ des fonctions $\varphi_{i,j} : e_k \mapsto \delta_{k,j} f_i$, alors les $\lambda_{i,j}$ sont les coordonnées de f dans la base des $\varphi_{i,j}$.*

Exemples I.7.

1. *Peu importe le choix de $\mathcal{B}$, on a :* $\mathrm{Mat}_{\mathcal{B}}(\mathrm{id}_E) = I_n$.
2. *La dérivation de $\mathbb{K}_3[X]$ dans $\mathbb{K}_2[X]$, munis de leurs bases canoniques, a pour matrice :*

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

   et l'évaluation en a de $\mathbb{K}_n[X]$ sur $\mathbb{K}$ a pour matrice :

$$\begin{pmatrix} 1 & a & a^2 & \dots & a^n \end{pmatrix}.$$

3. *Si on voit $\mathbb{C}$ comme un $\mathbb{R}$-espace vectoriel de dimension 2, muni de la base $(1,i)$, alors la similitude $z \mapsto (a+ib)z$ est un endomorphisme de $\mathbb{C}$, dont la matrice est :*

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

   comme $f(1) = a + ib$ et $f(i) = -b + ia$.

Proposition I.8. *Étant données une base $\mathcal{B}$ de E et une base $\mathcal{C}$ de F, l'application $f \mapsto \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f)$ est une bijection de $\mathcal{L}(E,F)$ sur $\mathcal{M}_{n,p}(\mathbb{K})$.*

Démonstration. Soit $M = (\lambda_{i,j}) \in \mathcal{M}_{n,p}(\mathbb{K})$. Il existe une unique application $f \in \mathcal{L}(E,F)$ telle que :

$$\forall j \in [\![1;p]\!],\ f(e_j) = \sum_{i=1}^{n} \lambda_{i,j} f_i$$

c'est-à-dire que M a un unique antécédent dans $\mathcal{L}(E,F)$, ce qui donne la bijectivité. □

Remarque I.9. *Il faut bien prendre garde au fait que cette bijection nécessite en amont de fixer des bases de E et F.*

Corollaire I.10. *Étant donnée une base $\mathcal{B}$ de E, l'application $f \mapsto \mathrm{Mat}_{\mathcal{B}}(f)$ est une bijection de $\mathcal{L}(E)$ sur $\mathcal{M}_n(\mathbb{K})$.*

I.2 Compatibilité des opérations

Proposition I.11. *Étant données une base $\mathcal{B}$ de E et une base $\mathcal{C}$ de F, $f, g \in \mathcal{L}(E,F)$ et $\lambda, \mu \in \mathbb{K}$, alors :*

$$\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(\lambda f + \mu g) = \lambda \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f) + \mu \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(g)$$

et donc l'application $f \mapsto \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f)$ est un isomorphisme d'espaces vectoriels de $\mathcal{L}(E,F)$ sur $\mathcal{M}_{n,p}(\mathbb{K})$.

Démonstration. On note $\mathcal{B} = (e_1, \dots, e_p)$ et $\mathcal{C} = (f_1, \dots f_n)$. Alors :

$$(\lambda f + \mu g)(e_j) = \lambda f(e_j) + \mu g(e_j)$$

d'où l'égalité coordonnée par coordonnée de ces vecteurs sur la base (f_i), ce qui donne l'égalité coefficient par coefficient des matrices associées. □

Remarque I.12. *On retrouve au passage la dimension de $\mathcal{L}(E, F)$.*

Proposition I.13. *Si $\mathcal{B}$ et $\mathcal{C}$ sont des bases de E et F, $f \in \mathcal{L}(E, F)$ et $x \in E$, alors :*

$$\mathrm{Mat}_{\mathcal{C}}(f(x)) = \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f) \times \mathrm{Mat}_{\mathcal{B}}(x).$$

Démonstration. Notons $\mathcal{B} = (e_1, \dots, e_p)$ et $\mathcal{C} = (f_1, \dots, f_n)$. Si on note $\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f) = (a_{i,j})$ et $\mathrm{Mat}_{\mathcal{B}}(x) = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_p \end{pmatrix}$ alors :

$$f(x) = f\left(\sum_{j=1}^{p} \lambda_j e_j\right) = \sum_{j=1}^{p} \lambda_j f(e_j) = \sum_{j=1}^{p}\sum_{i=1}^{n} \lambda_j a_{i,j} f_i = \sum_{i=1}^{n}\left(\sum_{j=1}^{p} a_{i,j}\lambda_j\right) f_i$$

ce qui donne bien le résultat □

Proposition I.14. *Si $\mathcal{B}$, $\mathcal{C}$ et $\mathcal{D}$ sont des bases de E, F et G, $f \in \mathcal{L}(E, F)$ et $g \in \mathcal{L}(F, G)$, alors :*

$$\mathrm{Mat}_{\mathcal{B},\mathcal{D}}(g \circ f) = \mathrm{Mat}_{\mathcal{C},\mathcal{D}}(g) \times \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f).$$

Démonstration. Si on note $\mathcal{B} = (e_1, \dots, e_p), \mathcal{C} = (f_1, \dots, f_n)$ et $\mathcal{D} = (g_1, \dots, g_m)$, alors pour tout $j \in [\![1; p]\!]$:

$$\mathrm{Mat}_{\mathcal{D}}(g \circ f(e_j)) = \mathrm{Mat}_{\mathcal{C},\mathcal{D}}(g) \times \mathrm{Mat}_{\mathcal{C}}(f(e_j))$$

et donc la j-ème colonne de $\mathrm{Mat}_{\mathcal{B},\mathcal{D}}(g \circ f)$ est le produit de $\mathrm{Mat}_{\mathcal{C},\mathcal{D}}(g)$ par la j-ème colonne de $\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f)$, ce qui donne bien l'égalité voulue. □

Remarque I.15. *Il faut bien faire attention que l'on prend la même base pour F pour écrire la matrice de f et celle de g (sinon le résultat est faux).*

Exemple I.16. *On se place sur $\mathbb{K}_3[X]$. L'application $P \mapsto XP'$ est un endomorphisme de $\mathbb{K}_3[X]$, qu'on peut voir comme la composée des applications :*

$$f : \left\{ \begin{array}{ccc} \mathbb{K}_3[X] & \to & \mathbb{K}_2[X] \\ P & \mapsto & P' \end{array} \right. \quad \text{et } g : \left\{ \begin{array}{ccc} \mathbb{K}_2[X] & \to & K_3[X] \\ P & \mapsto & XP \end{array} \right.$$

et on trouve ainsi en notant $\mathcal{B}, \mathcal{C}$ les bases canoniques de $\mathbb{K}_3[X]$ et $\mathbb{K}_2[X]$:

$$\underbrace{\begin{pmatrix} 0 & & & \\ & 1 & & \\ & & 2 & \\ & & & 3 \end{pmatrix}}_{\mathrm{Mat}_{\mathcal{B}}(g\circ f)} = \underbrace{\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{\mathrm{Mat}_{\mathcal{B}}(g)} \times \underbrace{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}}_{\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f)}.$$

Corollaire I.17. *Étant donnée une base $\mathcal{B}$ de E, l'application $f \mapsto \mathrm{Mat}_{\mathcal{B}}(f)$ est un isomorphisme d'anneaux de $\mathcal{L}(E)$ sur $\mathcal{M}_n(\mathbb{K})$.*

Exemple I.18. *On fixe E un espace vectoriel, $\mathcal{B}(e_1, e_2, e_3)$ une base de E, et $s \in \mathcal{L}(E)$ dont la matrice dans la base $\mathcal{B}$ est :*

$$S = \begin{pmatrix} 0 & -2 & 1 \\ 0 & 1 & 0 \\ 1 & 2 & 0 \end{pmatrix}.$$

Alors on a :

$$S^2 = I_3 = \mathrm{Mat}_{\mathcal{B}}(\mathrm{id})$$

donc s est une symétrie.
Pour $x = a_e 1 + be_2 + ce_3 \in E$, on a :

$$s(x) = x \Leftrightarrow A \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \end{pmatrix} \Leftrightarrow \left\{ \begin{array}{rcl} -2b + c & = & a \\ b & = & b \\ a + 2b & = & c \end{array} \right. \Leftrightarrow a + 2b - c = 0$$

$$s(x) = -x \Leftrightarrow \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \end{pmatrix} \Leftrightarrow \left\{ \begin{array}{rcl} -2b + c & = & -a \\ b & = & -b \\ a + 2b & = & -c \end{array} \right. \Leftrightarrow\Leftrightarrow \left\{ \begin{array}{rcl} b & = & 0 \\ a + c & = & 0 \end{array} \right.$$

et donc s est la symétrie sur P parallèlement à D, où :

$$P = \mathrm{Vect}((2e_1 - e_2), (e_2 + 2e_3)) \text{ et } D = \mathrm{Vect}(e_1 - e_3).$$

Et ce peu importe l'espace E et la base $\mathcal{B}$ choisie. Par exemple, sur $\mathbb{K}_2[X]$ muni de la base canonique, on déduit que l'application linéaire : $a + bX + cX^2 \mapsto (-2b + c) + bX + (a + 2b)X^2$ est une symétrie sur $\{P \in \mathbb{K}_2[X] \,|\, 2P(0) + 4P'(0) - P''(0) = 0\}$ parallèlement à $\{\lambda(X^2 - 1) \,|\, \lambda \in \mathbb{K}\}$.

Corollaire I.19. *Si $\mathcal{B}$ et $\mathcal{C}$ sont des bases de E et F, avec E, F de même dimension finie, et $f \in \mathcal{L}(E, F)$, alors f est un isomorphisme si, et seulement si, $\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f)$ est inversible, et dans ce cas :*

$$\mathrm{Mat}_{\mathcal{C},\mathcal{B}}\left(f^{-1}\right) = \left(\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f)\right)^{-1}.$$

Démonstration. On note pour simplifier $A = \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f)$. Alors :

$$\begin{array}{rcl} f \text{ bijective} & \Leftrightarrow & \exists g \in \mathcal{L}(F, E),\ g \circ f = \mathrm{id}_E \text{ et } f \circ g = \mathrm{id}_F \\ & \Leftrightarrow & \exists B \in \mathcal{M}_n(\mathbb{K}),\ BA = AB = I_n \\ & & (\text{avec } M = \mathrm{Mat}_{\mathcal{C},\mathcal{B}}(g)) \\ & \Leftrightarrow & A \text{ est inversible} \end{array}$$

et alors on a :

$$I_n = \mathrm{Mat}_{\mathcal{B}}(\mathrm{id}_E) = \mathrm{Mat}_{\mathcal{B}}(f^{-1} \circ f) = \mathrm{Mat}_{\mathcal{C},\mathcal{B}}(f^{-1})\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f)$$

ce qui donne bien l'inverse à gauche, qui coïncide avec l'inverse à droite (par propriété des inverses matriciels), mais qu'on pourrait montrer indépendamment. □

Remarque I.20. *On retrouve même un résultat plus fort : l'inversibilité à gauche d'une application linéaire est équivalente à l'inversibilité à gauche de la matrice associée (et pareil à droite). Et ainsi on retrouve que, pour les matrices carrées comme pour les applications linéaires entre deux espaces vectoriels de même dimension finie, les inversibilités à gauche ou à droite sont équivalentes à l'inversibilité.*

Exemple I.21. *Sur $\mathbb{K}_2[X]$, on considère l'endomorphisme $f : P \mapsto P + P' + P''$. Alors la matrice de f dans la base canonique est la matrice :*

$$A = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

donc, comme A est triangulaire supérieure de coefficients diagonaux non nuls, alors A est inversible, donc f est bijective.
On inverse A par pivot, ce qui donne :

$$A^{-1} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}$$

et donc f est inversible, d'inverse $f^{-1} : P \mapsto P - P'$.
On aurait pu aussi déduire l'inversibilité (et surtout l'inverse) de A de celui de f, en constatant que : $f = \mathrm{id} + g + g^2$ où $g : P \mapsto P'$ est nilpotente d'ordre 3 (sur $\mathbb{K}_2[X]$), donc f est inversible d'inverse $\mathrm{id} - g$.

II Application linéaire canoniquement associée à une matrice

Définition II.1. *Si $A \in \mathcal{M}_{n,p}(\mathbb{K})$, on lui associe l'application :*

$$f : \left\{ \begin{array}{ccc} \mathcal{M}_{p,1}(\mathbb{K}) & \to & \mathcal{M}_{n,1}(\mathbb{K}) \\ X & \mapsto & AX \end{array} \right.$$

qu'on appellera l'application linéaire canoniquement associée à A.
En assimilant $\mathbb{K}^p$ et $\mathbb{K}^n$ à $\mathcal{M}_{p,1}(\mathbb{K})$ et $\mathcal{M}_{n,1}(\mathbb{K})$, l'application f est l'élément de $\mathcal{L}(\mathbb{K}^p, \mathbb{K}^n)$ dont la matrice dans les bases canoniques est A.

II.1 Rang d'une matrice

Définition II.2. *Si $A \in \mathcal{M}_{n,p}(\mathbb{K})$, on appelle **rang** de A, noté $\mathrm{rg}(A)$, le rang de la famille de ses colonnes (qui sont des éléments de $\mathcal{M}_{n,1}(\mathbb{K})$, assimilé à $\mathbb{K}^n$).*
*Plus généralement, on dira que l'**image** de A, notée $\mathrm{Im}\, A$, est l'espace vectoriel engendré par ses colonnes (vu indifféremment comme un sous-espace de $\mathcal{M}_{n,1}(\mathbb{K})$ ou $\mathbb{K}^n$).*
Et on a ainsi : $\dim \mathrm{Im}\, A = \mathrm{rg}(A)$.

Remarque II.3. *Du fait des multiplications matricielles avec des vecteurs colonnes, on a : $\mathrm{Im}\, A = \{AX \mid X \in \mathcal{M}_{p,1}(\mathbb{K})\}$.*

Proposition II.4. *Si $\mathcal{B}$ est une base d'un espace vectoriel E, et $(x_1, \dots, x_p)$ est une famille de E, alors :*

$$\mathrm{rg}\,(x_1, \dots, x_p) = \mathrm{rg}\,(\mathrm{Mat}_{\mathcal{B}}(x_1, \dots, x_p))\,.$$

Démonstration. Notons $\mathcal{B} = (e_1, \dots, e_n)$ base de E. Alors l'application :

$$\varphi_{\mathcal{B}} : \left\{ \begin{array}{ccc} \mathcal{M}_{n,1}(\mathbb{K}) & \to & E \\ \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} & \mapsto & \sum_{i=1}^n \lambda_i e_i \end{array} \right.$$

est un isomorphisme (il s'agit de la bijection réciproque de $x \mapsto \mathrm{Mat}_{\mathcal{B}}(x)$).
Mais cette application envoie $\mathrm{Im}\,(\mathrm{Mat}_{\mathcal{B}}(x_1, \dots, x_p))$ sur $\mathrm{Vect}\,(x_1, \dots, x_p)$ (elle envoie chaque colonne sur le vecteur correspondant).
Et comme un isomorphisme préserve les dimensions, on a donc bien l'égalité voulue. □

Corollaire II.5. *Si $f \in \mathcal{L}(E, F)$ et $\mathcal{B}$, $\mathcal{C}$ des bases de E et F respectivement, alors : $\mathrm{rg}(f) = \mathrm{rg}\,(\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f))$.*

Démonstration. On applique le résultat précédent à la famille $(f(e_1), \dots, f(e_p))$, où $\mathcal{B} = (e_1, \dots, e_p)$. □

Corollaire II.6. *Si $A \in \mathcal{M}_{n,p}(\mathbb{K})$, alors :*

1. $\mathrm{rg}(A) \leq \min(n,p)$;
2. *si $n = p$, alors A est inversible si, et seulement si,* $\mathrm{rg}(A) = n$;
3. *pour toutes matrices $P \in \mathrm{GL}_n(\mathbb{K})$ et $Q \in \mathrm{GL}_p(\mathbb{K})$, on a :* $\mathrm{rg}(A) = \mathrm{rg}(PAQ)$.

Démonstration. 1. découle du rang de f canoniquement associé à A ;

2. un endomorphisme en dimension finie est surjectif si, et seulement si, il est bijectif, et la surjectivité est donnée par le rang ;
3. découle de $\mathrm{rg}(g \circ f) = \mathrm{rg}(f) = \mathrm{rg}(f \circ h)$ pour g, h inversibles.

□

Remarques II.7.

1. *Pour le point 2, on peut aussi dire que cela revient à ce que les colonnes de A engendrent $\mathbb{K}^n$ (comme elles engendrent un sev de $\mathbb{K}^n$ de dimension* $\mathrm{rg}(A)$*).*
2. *On a même un résultat plus fort pour le 3 : si $Q \in \mathrm{GL}_p(\mathbb{K})$, alors* $\mathrm{Im}\, A = \mathrm{Im}\, AQ$

Corollaire II.8. *Si $\mathcal{B} = (e_1, \ldots, e_n)$ est une base de E et $(x_1, \ldots, x_n)$ est une famille de vecteurs de E, alors $(x_1, \ldots, x_n)$ est une base si, et seulement si,* $\mathrm{Mat}_{\mathcal{B}}(x_1, \ldots, x_n)$ *est inversible.*

Démonstration. Les deux assertions sont équivalentes au fait que $\mathrm{rg}(x_1, \ldots, x_n) = n$. □

II.2 Lien avec les systèmes linéaires

Définition II.9. *Si $A \in \mathcal{M}_{n,p}(\mathbb{K})$, on appellera* ***noyau*** *de A, noté* $\mathrm{Ker}\, A$*, l'ensemble des $X \in \mathcal{M}_{n,1}(\mathbb{K})$ tels que : $AX = 0$.*

Remarque II.10. *Le noyau d'une matrice est donc l'ensemble des solutions du système homogène $AX = 0$.*

Proposition II.11. *Le noyau d'une matrice est égal au noyau de son application linéaire canoniquement associée.*

Démonstration. Découle de l'égalité :

$$\mathrm{Mat}_{\mathcal{C}}\left(f(x)\right) = \mathrm{Mat}_{\mathcal{B},\mathcal{C}}\left(f\right) \times \mathrm{Mat}_{\mathcal{B}}\left(x\right).$$

□

Corollaire II.12 (Théorème du rang matriciel)**.** *Si $A \in \mathcal{M}_{n,p}(\mathbb{K})$, alors :*

$$p = \dim \mathrm{Ker}\, A + \mathrm{rg}(A).$$

Démonstration. Découle du théorème du rang pour $f \in \mathcal{L}(\mathbb{K}^p, \mathbb{K}^n)$ associée à A. □

Corollaire II.13. *Si $A \in \mathcal{M}_n(\mathbb{K})$, alors A est inversible si, et seulement si,* $\mathrm{Ker}\, A = \{0\}$.

Démonstration. Découle du résultat analogue pour les endomorphismes en dimension finie. □

Proposition II.14. *Si $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et $B \in \mathcal{M}_{n,1}(\mathbb{K})$, alors le système $AX = B$ (d'inconnue $X \in \mathcal{M}_{p,1}(\mathbb{K})$) admet une solution si, et seulement si,* $B \in \mathrm{Im}\, A$.
Dans ce cas, l'ensemble des solutions est un espace affine de $\mathcal{M}_{p,1}(\mathbb{K})$ dirigé par $\mathrm{Ker}\, A$*, qui est donc de dimension* $p - \mathrm{rg}(A)$.
Si $n = p$ et que A est inversible, le système $AX = B$ admet toujours une unique solution, et on dit qu'il s'agit d'un système de Cramer.

Démonstration. L'existence de solution découle de la définition de $\operatorname{Im} A$.
Pour la structure de l'ensemble solution, on l'a déjà vu lors de la présentation des espaces affines. La dimension des solutions découlent du théorème du rang qu'on applique à l'application linéaire canoniquement associée à A.
Le dernier résultat a déjà été montré. □

Remarque II.15. *La dimension de l'ensemble solution se lit bien sur la méthode du pivot : multiplier par une matrice inversible (à gauche ou à droite) ne change pas le rang, donc échelonner une matrice ne change pas son rang. Et il est clair (à la manière des familles de polynômes de degrés échelonnées) que le rang d'une matrice échelonnée est égal au nombre de ses pivots.*

Proposition II.16. *Si $A \in \mathcal{M}_{n,p}(\mathbb{K})$, alors :*

1. *si $P \in \mathrm{GL}_n(\mathbb{K})$, on a :* $\operatorname{Ker} A = \operatorname{Ker} PA$;
2. *si $Q \in \mathrm{GL}_p(\mathbb{K})$, on a :* $\operatorname{Im} A = \operatorname{Im} AQ$.

En particulier, les opérations élémentaires sur les lignes de A préservent le noyau, et celles sur les colonnes préservent l'image. Plus généralement, ces deux opérations préservent le rang.

Démonstration. On a pour tout $X \in \mathcal{M}_{p,1}(\mathbb{K})$ et $P \in \mathrm{GL}_n(\mathbb{K})$:

$$X \in \operatorname{Ker} A \Leftrightarrow AX = 0 \Leftrightarrow PAX = 0 \Leftrightarrow X \in \operatorname{Ker} PA$$

ce qui donne la première égalité.
La seconde a déjà été montrée.
Le reste découle de l'écriture matricielle des opérations élémentaires : une opération élémentaire sur une ligne (resp. une colonne) revient à multiplier à gauche (resp. à droite) par une matrice inversible, ce qui préserve donc le noyau (resp. l'image). La préservation du rang découle alors du théorème du rang matriciel. □

III Changements de bases, équivalence et similitude

III.1 Changements de bases

Définition III.1. *Soient $\mathcal{B}$ et $\mathcal{C}$ deux bases d'un espace vectoriel E de dimension finie. On appelle* ***matrice de passage de $\mathcal{B}$ à $\mathcal{C}$*** *la matrice :*

$$P_{\mathcal{B}}^{\mathcal{C}} = \mathcal{P}_{\mathcal{B}\to\mathcal{C}} = \operatorname{Mat}_{\mathcal{B}}(\mathcal{C}).$$

Proposition III.2. *Avec les mêmes notations, on a :*

$$P_{\mathcal{B}}^{\mathcal{C}} = \operatorname{Mat}_{\mathcal{C},\mathcal{B}}(\mathrm{id}_E).$$

Et on a ainsi que :

1. *$P_{\mathcal{B}}^{\mathcal{C}}$ est inversible, d'inverse : $P_{\mathcal{C}}^{\mathcal{B}}$;*
2. *si $\mathcal{D}$ est une autre base de E, alors : $P_{\mathcal{B}}^{\mathcal{D}} = P_{\mathcal{B}}^{\mathcal{C}} \cdot P_{\mathcal{C}}^{\mathcal{D}}$.*

Démonstration. Le premier point vient du fait que les éléments de $\mathcal{C}$ sont envoyés sur eux-même par id_E.
On déduit ainsi que :

1. comme $\mathrm{id}_E = \mathrm{id}_E^{-1}$, alors :

$$(\operatorname{Mat}_{\mathcal{B},\mathcal{C}}(\mathrm{id}_E))^{-1} = \operatorname{Mat}_{\mathcal{C},\mathcal{B}}(\mathrm{id}_E^{-1}) = \operatorname{Mat}_{\mathcal{C},\mathcal{B}}(\mathrm{id}_E)$$

ce qui donne bien l'égalité voulue ;

2. comme $\mathrm{id}_E \circ \mathrm{id}_E = \mathrm{id}_E$, alors :

$$\mathrm{Mat}_{\mathcal{D},\mathcal{B}}(\mathrm{id}_E) = \mathrm{Mat}_{\mathcal{C},\mathcal{B}}(\mathrm{id}_E) \times \mathrm{Mat}_{\mathcal{D},\mathcal{C}}(\mathrm{id}_E)$$

ce qui donne l'égalité sur les matrices de passage.

□

Exemple III.3. *On se place sur $\mathbb{K}_2[X]$. On considère $\mathcal{B}$ la base canonique, et on pose $\mathcal{C}$ la famille de polynômes d'interpolation de Lagrange associée à la famille $(0,1,2)$, c'est-à-dire :*

$$\mathcal{C} = \left(\underbrace{\frac{X^2-3X+2}{2}}_{L_0}, \underbrace{-X^2+2X}_{L_1}, \underbrace{\frac{X^2-X}{2}}_{L_2} \right).$$

Et donc :

$$P_{\mathcal{B}}^{\mathcal{C}} = A = \begin{pmatrix} 1 & 0 & 0 \\ -\frac{3}{2} & 2 & -\frac{1}{2} \\ \frac{1}{2} & -1 & \frac{1}{2} \end{pmatrix}$$

Mais on sait très bien exprimer un polynôme de $\mathbb{K}_2[X]$ dans la base (L_0, L_1, L_2), à savoir :

$$\forall P \in \mathbb{K}_2[X],\ P = P(0) \cdot L_0 + P(1) \cdot L_1 + P(2) \cdot L_2$$

et donc pour la base canonique, on trouve :

$$1 = L_0 + L_1 + L_2,\ X = L_1 + 2 \cdot L_2 \text{ et } X^2 = L_1 + 4 \cdot L_2$$

donc finalement on trouve :

$$A^{-1} = P_{\mathcal{C},\mathcal{B}} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 4 \end{pmatrix}.$$

Proposition III.4. *Si $\mathcal{B}$ et $\mathcal{C}$ sont deux bases de E, alors pour tout $x \in E$ on a :*

$$\mathrm{Mat}_{\mathcal{B}}(x) = P_{\mathcal{B},\mathcal{C}} \mathrm{Mat}_{\mathcal{C}}(x)$$

c'est-à-dire que la matrice de passage de $\mathcal{B}$ à $\mathcal{C}$ permet de passer des coordonnées de x dans $\mathcal{C}$ à celles dans $\mathcal{B}$.

Remarque III.5. *La terminologie semble donc assez mal choisie. On verra qu'elle s'adapte en fait très bien aux endomorphismes.*

Exemple III.6. *On reprend les polynômes L_0, L_1, L_2 d'interpolation associés à la famille $(0,1,2)$. Et on veut calculer rapidement dans la base canonique le polynôme $P = 4L_0 + L_1 - 2L_2$. On a :*

$$\mathrm{Mat}_{\mathcal{B}}(P) = P_{\mathcal{B},\mathcal{C}} \cdot \mathrm{Mat}_{\mathcal{C}}(P) = \begin{pmatrix} 1 & 0 & 0 \\ -\frac{1}{2} & 2 & -\frac{1}{2} \\ \frac{1}{2} & -1 & \frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 1 \\ -2 \end{pmatrix} = \begin{pmatrix} 4 \\ -3 \\ 0 \end{pmatrix}$$

donc $P = 4 - 3X$.

Théorème III.7 (Formule de changement de base)**.** *Soient E, F deux espaces vectoriels de dimension finie, $\mathcal{B}, \mathcal{B}'$ deux bases de E et $\mathcal{C}, \mathcal{C}'$ deux bases de F, alors pour tout $f \in \mathcal{L}(E,F)$ on a :*

$$\mathrm{Mat}_{\mathcal{B}',\mathcal{C}'}(f) = P_{\mathcal{C}'}^{\mathcal{C}} \mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f) P_{\mathcal{B}}^{\mathcal{B}'}.$$

Démonstration. Découle du fait que : $f = \mathrm{id}_F \circ f \circ \mathrm{id}_E$ et de la représentation matricielle d'une composée. □

Remarque III.8. *Il faut bien faire attention à l'ordre et au sens dans lequel on prend les matrices de passage. L'écriture se retient bien par le graphique suivant :*

$$\begin{array}{ccc} (E,\mathcal{B}) & \xrightarrow{\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f)} & (F,\mathcal{C}) \\ \Big\uparrow{\scriptstyle P_{\mathcal{B}}^{\mathcal{B}'}} & & \Big\downarrow{\scriptstyle P_{\mathcal{C}'}^{\mathcal{C}}} \\ (E,\mathcal{B}') & \xrightarrow[\mathrm{Mat}_{\mathcal{B}',\mathcal{C}'}(f)]{} & (F,\mathcal{C}') \end{array}$$

Corollaire III.9. *Si E est un espace vectoriel de dimension finie, et $\mathcal{B}, \mathcal{B}'$ deux bases de E, alors pour tout $f \in \mathcal{L}(E)$ on a :*

$$\mathrm{Mat}_{\mathcal{B}'}(f) = P_{\mathcal{B}'}^{\mathcal{B}} \mathrm{Mat}_{\mathcal{B}}(f) P_{\mathcal{B}}^{\mathcal{B}'} = \left(P_{\mathcal{B}}^{\mathcal{B}'}\right)^{-1} \mathrm{Mat}_{\mathcal{B}}(f) P_{\mathcal{B}}^{\mathcal{B}'}.$$

Remarque III.10. *L'intérêt d'une telle formule est de trouver une base dans laquelle la matrice de f est plus simple, et permet de faire des calculs, et d'en déduire ensuite des propriétés de f.*

Exemple III.11. *Considérons sur $\mathbb{K}_2[X]$ l'endomorphisme f tel que :*

$$A = \mathrm{Mat}_{\mathcal{B}}(f) = \begin{pmatrix} 2 & 0 & 0 \\ -3 & -2 & -6 \\ 2 & 3 & 7 \end{pmatrix}.$$

Alors en notant $P = P_{\mathcal{B}}^{\mathcal{C}}$, la matrice dans la base $\mathcal{C} = (L_0, L_1, L_2)$ de f est :

$$\mathrm{Mat}_{\mathcal{C}}(f) = P^{-1} \cdot A \cdot P = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 & 0 \\ -3 & -2 & -6 \\ 2 & 3 & 7 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ -3/2 & 2 & -1/2 \\ 1/2 & -1 & 1/2 \end{pmatrix} = \begin{pmatrix} 2 & & \\ & 1 & \\ & & 4 \end{pmatrix}$$

et on peut ainsi plus facilement calculer les puissances de f (ou d'autres propriétés de f).

III.2 Matrices équivalentes

Définition III.12. *Soient $A, B \in \mathcal{M}_{n,p}(\mathbb{K})$. On dit que A et B sont **équivalentes** s'il existe $P \in \mathrm{GL}_n(\mathbb{K})$ et $Q \in \mathrm{GL}_p(\mathbb{K})$ telles que : $A = P^{-1}BQ$.*

Remarque III.13. *Du fait de la formule de changement de base, cela revient à dire que A et B représentent une même application linéaire, mais dans des couples de bases différentes.*

Proposition III.14. *La relation précédente définit une relation d'équivalence sur $\mathcal{M}_{n,p}(\mathbb{K})$.*

Démonstration. On a les propriétés suivantes :
- réflexivité : si $A \in \mathcal{M}_{n,p}(\mathbb{K})$, avec $P = I_n \in \mathrm{GL}_n(\mathbb{K})$ et $Q = I_p \in \mathrm{GL}_p(\mathbb{K})$ on a : $A = P^{-1}AQ$;
- symétrie : si $A, B \in \mathcal{M}_{n,p}(\mathbb{K})$ et $P \in \mathrm{GL}_n(\mathbb{K})$, $Q \in \mathrm{GL}_p(\mathbb{K})$ telles que : $A = P^{-1}BQ$. Alors $B = PAQ^{-1} = (P^{-1})^{-1} A (Q^{-1})$ avec $P^{-1} \in \mathrm{GL}_n(\mathbb{K})$ et $Q^{-1} \in \mathrm{GL}_p(\mathbb{K})$;
- transitivité : si $A, B, C \in \mathcal{M}_{n,p}(\mathbb{K})$ et $P_1, P_2 \in \mathrm{GL}_n(\mathbb{K})$, $Q_1, Q_2 \in \mathrm{GL}_p(\mathbb{K})$ telles que : $A = P_1^{-1}BQ_1$ et $B = P_2^{-1}CQ_2$, alors : $A = P_1^{-1}P_2^{-1}CQ_2Q_1 = P^{-1}CQ$ avec $P = P_2P_1 \in \mathrm{GL}_n(\mathbb{K})$ et $Q = Q_2Q_1 \in \mathrm{GL}_p(\mathbb{K})$.

□

Proposition III.15. *Pour $n, p \in \mathbb{N}^*$ et $r \in [\![0; \min(n,p)]\!]$, on définit la matrice $J_{n,p,r} \in \mathcal{M}_{n,p}(\mathbb{K})$ comme la matrice en blocs :*

$$J_{n,p,r} = \begin{pmatrix} I_r & 0_{r,p-r} \\ 0_{n-r,r} & 0_{n-r,p-r} \end{pmatrix}.$$

Alors, si $A \in \mathcal{M}_{n,p}(\mathbb{K})$ est de rang r, la matrice A est équivalente à $J_{n,p,r}$.

Démonstration. Notons $f : \mathbb{K}^p \to \mathbb{K}^n$ l'application linéaire canoniquement associée à A.
On a $\mathrm{rg}(A) = \mathrm{rg}(f) = r$. Si on considère S un supplémentaire de $\mathrm{Ker}\, f$ dans $\mathbb{K}^p$, avec $(e_1, \dots, e_r, e_{r+1}, \dots, e_p)$ une base de $\mathbb{K}^p$ adaptée à la décomposition $\mathbb{K}^p = S \oplus \mathrm{Ker}\, f$, alors la famille $(f(e_1), \dots, f(e_r)) = (f_1, \dots, f_r)$ est une base de $\mathrm{Im} f$. Si on la complète en $(f_1, \dots, f_r, f_{r+1}, \dots, f_n)$ base de F, alors on a :

$$\forall j \in [\![1; p]\!],\ f(e_j) = \begin{cases} f_j & \text{si} \quad j \leq r \\ 0 & \text{si} \quad j > r \end{cases}$$

ce qui donne bien que :

$$J_{n,p,r} = \mathrm{Mat}_{(e_j),(f_i)}(f).$$

En posant P la matrice de passage de (f_i) à la base canonique de $\mathbb{K}^n$, et Q celle de (e_j) à la base canonique de $\mathbb{K}^p$, on a bien :

$$A = \mathrm{Mat}_{\mathcal{B}_p,\mathcal{B}_n}(f) = P^{-1} J_{n,p,r} Q$$

donc A est bien équivalente à $J_{n,r,p}$. □

Remarque III.16. *Le calcul effectif du rang se fait alors par méthode du pivot : on cherche à échelonner la matrice A par opérations sur les lignes ou les colonnes, ce qui donne finalement son rang (qui correspond au nombre de pivots après échelonnage) : la matrice P^{-1} correspond aux opérations sur les lignes effectuées, et Q celles sur les colonnes.*

Corollaire III.17. *Deux matrice sont équivalentes si, et seulement si, elles ont même rang.*

Démonstration. Soient $A, B \in \mathcal{M}_{n,p}(\mathbb{K})$. Notons $r = \mathrm{rg}(A)$ et $r' = \mathrm{rg}(B)$, de sorte que A et B sont respectivement équivalentes à $J_{n,p,r}$ et à $J_{n,p,r'}$:

- si $r = r'$: alors A et B sont équivalentes à une même matrice, donc équivalentes ;
- si A et B sont équivalentes : on note $P \in \mathrm{GL}_n(\mathbb{K})$ et $Q \in \mathrm{GL}_p(\mathbb{K})$ tels que $A = P^{-1}BQ$ et alors : $r = \mathrm{rg}(A) = \mathrm{rg}(P^{-1}BQ) = \mathrm{rg}(B) = r'$ (comme multiplier par des matrices inversibles à gauche ou à droite ne change pas le rang).

□

Corollaire III.18. *Si $A \in \mathcal{M}_{n,p}(\mathbb{K})$, alors* $\mathrm{rg}(A) = \mathrm{rg}(A^T)$.

Démonstration. Notons $r = \mathrm{rg}(A)$, et $P \in \mathrm{Gl}_n(\mathbb{K})$, $Q \in \mathrm{GL}_p(\mathbb{K})$ telles que $A = P^{-1} J_{n,p,r} Q$.
Alors :

$$A^T = \left(P^{-1} J_{n,p,r} Q\right)^T = \underbrace{Q^T}_{\in \mathrm{GL}_p(\mathbb{K})} \underbrace{J_{n,p,r}^T}_{= J_{p,n,r}} \underbrace{P^{-1\,T}}_{\in \mathrm{GL}_n(\mathbb{K})}$$

dont A^T est équivalente à $J_{p,n,r}$, donc est de rang r. □

Remarque III.19. *Comme le rang d'une matrice est le rang de la famille de ses colonnes, le résultat dit ainsi qu'il s'agit aussi du rang de la famille de ses lignes (qui sont les colonnes de sa transposée).*

Définition III.20. *Soit $A = (a_{i,j}) \in \mathcal{M}_{n,p}(\mathbb{K})$. Une* ***matrice extraite*** *de A est une matrice de la forme $(a_{i,j})_{\substack{i \in I \\ j \in J}} \in \mathcal{M}_{|I|,|J|}(\mathbb{K})$, pour $I \subset [\![1; p]\!]$ et $J \subset [\![1; n]\!]$.*

Proposition III.21. *Si $A \in \mathcal{M}_{n,p}(\mathbb{K})$:*

1. *toute matrice extraite de A a pour rang au plus* $\mathrm{rg}(A)$ *;*

2. *il existe une matrice extraite de A inversible de taille* $\mathrm{rg}(A)$.

Remarque III.22. *Et ainsi le rang de A est la plus grande taille possible d'une matrice inversible extraite de A.*

Démonstration.

1. Soit B une matrice extraite de A. Notons $A = (a_{i,j})$ et $B = (a_{i,j})_{\substack{i \in I \\ j \in J}}$.
   Notons $C = (a_{i,j})_{\substack{1 \leq i \leq n \\ j \in J}}$, c'est-à-dire que C est la matrice construite à partir de A, en retirant les mêmes colonnes à A que pour obtenir B, mais en gardant toutes les lignes.
   Comme les colonnes de C sont des colonnes de A, alors $\mathrm{rg}(C) \leq \mathrm{rg}(A)$.
   Et comme les lignes de B sont des lignes de C, alors $\mathrm{rg}(B) \leq \mathrm{rg}(C)$.
   Et finalement $\mathrm{rg}(B) \leq \mathrm{rg}(A)$.
2. Notons $r = \mathrm{rg}(A)$: comme le rang de A est la dimension de l'espace engendré par les colonnes de A, alors il existe une base de cet espace construit à partir de colonnes de A (par théorème de la base extraite). Notons C la matrice obtenue en ne gardant que ces colonnes, qui est donc de rang r et possédant r colonnes.
   Comme le rang de C est aussi le rang de ses lignes, on peut à nouveau utiliser le théorème de la base extraite pour ne garder que r lignes qui forment une base, ce qui forme la matrice B.
   La matrice B est carrée de taille r, et elle est de rang r, donc est bien inversible.

□

III.3 Matrices semblables

Définition III.23. *Soient $A, B \in \mathcal{M}_n(\mathbb{K})$. On dit que A et B sont **semblables** s'il existe $P \in \mathrm{GL}_n(\mathbb{K})$ telle que : $A = P^{-1}BP$.*

Remarques III.24.

1. *À nouveau par formule de changement de base, selon revient à dire que A et B représentent un même endomorphisme, mais dans des bases différentes.*
2. *L'intérêt, comme avant, est de trouver une matrice semblable qui facilite les manipulations. Par exemple, on dira que A est **diagonalisable** si elle est semblable à une matrice diagonale, ou **trigonalisable** si elle est semblable à une matrice triangulaire.*

Proposition III.25. *Le fait d'être semblable définit une relation d'équivalence sur $\mathcal{M}_n(\mathbb{K})$.*

Démonstration. Comme pour les matrices équivalentes. □

Proposition III.26. *Si $A \in \mathcal{M}_n(\mathbb{R})$, alors :*

1. *A est la matrice d'un projecteur si, et seulement si, elle est semblable à une matrice diagonale de comportant que des 0 et des 1 sur la diagonale ; c'est le cas si, et seulement si, on a $A^2 = A$.*
2. *A est la matrice d'une symétrie si, et seulement si, elle est semblable à une matrice diagonale ne comportant que des 1 et des -1 sur la diagonale ; c'est le cas si, et seulement si, on a $A^2 = I_n$.*

Démonstration. On pose f l'application linéaire canoniquement associée à f. Alors A^2 est la matrice de f^2 dans la base canonique, ce qui donne déjà que f est un projecteur (resp. une symétrie) si, et seulement si, $A^2 = A$ (resp. $A^2 = I_n$).
Montrons le résultat de similitude pour un projecteur :

— si A est semblable à une matrice diagonale D ne comportant que des 0 et des 1 sur la diagonale : alors $D^2 = D$ (comme $0^2 = 0$ et $1^2 = 1$), et $A = P^{-1}DP$ pour $P \in \mathrm{GL}_n(\mathbb{K})$. Donc $A^2 = P^{-1}DPP^{-1}DP = P^{-1}D^2P = P^{-1}DP = A$, donc A est bien la matrice d'un projecteur ;

— si A est la matrice d'un projecteur : comme $\mathrm{Im}\, f \oplus \mathrm{Ker}\, f = \mathbb{K}^n$, en posant $\mathcal{B}$ une base de $\mathbb{K}^n$ adaptée à cette décomposition, on a :

$$\mathrm{Mat}_{\mathcal{B}}(f) = D = \begin{pmatrix} I_m & 0 \\ 0 & 0 \end{pmatrix}$$

où $m = \mathrm{rg}(f) \leq n$. Et par formule de changement de base, en notant P la matrice de passage de $\mathcal{B}$ dans la base canonique, on a : $A = P^{-1}DP$, où D est bien de la forme voulue.

Le résultat de symétrie se montre de manière similaire. □

Définition III.27. *Si $A = (a_{i,j}) \in \mathcal{M}_n(\mathbb{K})$, on appelle **trace** de A la quantité notée $\mathrm{tr}(A)$ définie par :*

$$\mathrm{tr}(A) = \sum_{i=1}^{n} a_{i,i}.$$

Exemples III.28.
1. $\mathrm{tr}(I_n) = n$ *et* $\mathrm{tr}(0_n) = 0$;
2. *si A est antisymétrique :* $\mathrm{tr}(A) = 0$ *(car tous les coefficients diagonaux de A sont nuls) ;*
3. $\mathrm{tr}(\mathrm{diag}(\lambda_1, \ldots, \lambda_n)) = \lambda_1 + \cdots + \lambda_n$;
4. *si $A \in \mathcal{M}_{n,p}(\mathbb{K})$, alors $A^TA \in \mathcal{M}_p(\mathbb{K})$ et $AA^T \in \mathcal{M}_n(\mathbb{K})$ vérifient :* $\mathrm{tr}(AA^T) = \mathrm{tr}(A^TA) = \sum_{i,j} a_{i,j}^2$.

Proposition III.29. *L'application $A \mapsto \mathrm{tr}(A)$ définit une forme linéaire de $\mathcal{M}_n(\mathbb{K})$ sur $\mathbb{K}$.*
De plus, pour tous $A, B \in \mathcal{M}_n(\mathbb{K})$ on a :

$$\mathrm{tr}(A^T) = \mathrm{tr}(A) \text{ et } \mathrm{tr}(AB) = \mathrm{tr}(BA).$$

Démonstration. Si $A, B \in \mathcal{M}_n(\mathbb{K})$ et $\lambda, \mu \in \mathbb{K}$, alors :

$$\mathrm{tr}(\lambda A + \mu B) = \sum_{i=1}^{n} [\lambda A + \mu B]_{i,i} = \sum_{i=1}^{n} \lambda [A]_{i,i} + \mu [B]_{i,i} = \lambda \mathrm{tr}(A) + \mu \mathrm{tr}(B)$$

ce qui donne la linéarité.
Pour la transposée : A et A^T ont mêmes coefficients diagonaux, donc en les sommant on trouve que $\mathrm{tr}(A) = \mathrm{tr}(A^T)$.
Et enfin :

$$\mathrm{tr}(AB) = \sum_{i=1}^{n} [AB]_{i,i} = \sum_{i=1}^{n} \sum_{k=1}^{n} [A]_{i,k}[B]_{k,i} = \sum_{k=1}^{n} \sum_{i=1}^{n} [B]_{k,i}[A]_{i,k} = \sum_{k=1}^{n} [BA]_{k,k} = \mathrm{tr}(BA).$$

□

Remarque III.30. *Le dernier résultat se généralise : si $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et $B \in \mathcal{M}_{p,n}(\mathbb{K})$, alors les quantités $\mathrm{tr}(AB)$ et $\mathrm{tr}(BA)$ sont bien définies et sont égales.*
Il faut cependant bien faire attention : on peut inverser deux matrices dans un produit de deux facteurs, mais on ne peut pas échanger tous les ordres des matrices dans un produit et espérer la trace. Par exemple avec :

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \text{ et } C = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

on a :

$$ABC = \begin{pmatrix} 2 & 0 \\ 1 & 0 \end{pmatrix} \text{ et } ACB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

et donc $\mathrm{tr}(ABC) \neq \mathrm{tr}(ACB)$.
On peut en revanche les échanger de manière circulaire :

$$\mathrm{tr}(A_1A_2, \ldots A_{n-1}A_n) = \mathrm{tr}(A_2A_3 \ldots A_{n-1}A_nA_1) = \mathrm{tr}(A_3A_4 \ldots A_{n-1}A_nA_1A_2) = \ldots$$

et par exemple avec trois matrices on trouve :

$$\mathrm{tr}(ABC) = \mathrm{tr}(BCA) = \mathrm{tr}(CAB).$$

Corollaire III.31. *Deux matrices semblables ont même trace.*

Démonstration. Soient $A, B \in \mathcal{M}_n(\mathbb{K})$, et $P \in \mathrm{GL}_n(\mathbb{K})$ tels que : $A = P^{-1}BP$. Alors :

$$\mathrm{tr}(A) = \mathrm{tr}(P^{-1}BP) = \mathrm{tr}\left((P^{-1}B)P\right) = \mathrm{tr}\left(P(P^{-1}B)\right) = \mathrm{tr}\left((PP^{-1})B\right) = \mathrm{tr}(B).$$

□

Remarque III.32. *La notion de matrices semblables étant plus restrictive que celle de matrices équivalentes, on avait déjà que deux matrices semblables ont même rang.*
Mais cette condition n'est pas suffisante, car deux matrices peuvent avoir même rang et même trace sans être semblable : par exemple les matrices :

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

sont toutes les deux de rang et de trace valant 2*, mais ne sont pas semblable (comme la seule matrice semblable à I_2 est elle-même).*
En particulier, il est en général difficile de montrer que deux matrices sont semblables.

Proposition-Définition III.33. *Si $f \in \mathcal{L}(E)$, pour E de dimension finie, alors la trace de $\mathrm{Mat}_{\mathcal{B}}(f)$ ne dépend pas de la base $\mathcal{B}$ de E considérée.*
On définit cette quantité comme étant la trace de f, notée $\mathrm{tr}(f)$, et l'application $f \mapsto \mathrm{tr}(f)$ définit ainsi une forme linéaire sur $\mathcal{L}(E)$.

Démonstration. Toutes les représentations matricielles de f sont semblables, donc ont la même trace, ce qui montre qu'elle est bien définie.
La linéarité découle du résultat sur les matrices. □

Proposition III.34. *Si $f, g \in \mathcal{L}(E)$, alors $\mathrm{tr}(fg) = \mathrm{tr}(gf)$.*

Démonstration. Découle du résultat sur les matrices. □

Proposition III.35. *Soient F, G deux espaces supplémentaires d'un espace vectoriel E de dimension finie $n \in \mathbb{N}^*$, p le projecteur sur F parallèlement à G et s la symétrie sur F parallèlement à G. Alors :*

$$\dim F = \mathrm{tr}(p) = \frac{n + \mathrm{tr}(s)}{2} \text{ et } \dim G = n - \mathrm{tr}(p) = \frac{n - \mathrm{tr}(s)}{2}.$$

Démonstration. Comme la trace ne dépend pas du choix de la base, il suffit de représenter p et s dans une base $\mathcal{B}$ adaptée à la décomposition $F \oplus G = E$. Si on note $m = \dim F$ (de sorte que $\dim G = n - m$), alors on a :

$$\mathrm{Mat}_{\mathcal{B}}(p) = \begin{pmatrix} I_m & 0 \\ 0 & 0_{n-m} \end{pmatrix} \text{ et } \mathrm{Mat}_{\mathcal{B}}(s) = \begin{pmatrix} I_m & 0 \\ 0 & -I_{n-m} \end{pmatrix}$$

et donc : $\mathrm{tr}(p) = m$ et $\mathrm{tr}(s) = 2m - n$. □

Remarque III.36. *Pour un projecteur, on a même que : $\mathrm{tr}(p) = \mathrm{rg}(p)$, ce qui permet facilement de calculer le rang.*

Chapitre 23

Intégration

Dans tout le chapitre on désignera par $\mathbb{K}$ le corps $\mathbb{R}$ ou $\mathbb{C}$.

I Les fonctions uniformément continues

Définition I.1. *Soit $f : I \to \mathbb{K}$ pour $I \subset \mathbb{R}$. On dit que f est **uniformément continue** sur I si :*

$$\forall \varepsilon > 0,\ \exists \eta > 0,\ \forall x, y \in I,\ |x - y| \leq \eta \Rightarrow |f(x) - f(y)| \leq \varepsilon.$$

Remarque I.2. *La définition ressemble beaucoup à la continuité :*

$$\forall x \in I,\ \forall \varepsilon > 0,\ \exists \eta > 0,\ \forall y \in I,\ |x - y| \leq \eta \Rightarrow |f(x) - f(y)| \leq \varepsilon$$

et la différence est qu'on a inversé les quantificateurs : le "$\forall x \in I$" (qui permettait de donner la continuité en $x \in I$) est passé après le "$\forall \varepsilon > 0$", et surtout devant le "$\exists \eta$". Ainsi, à ε fixé, le η adapté ne dépend pas de x. La notion de fonction uniformément continue est donc plus contraignante que la notion de fonction continue.

Proposition I.3. *Toute fonction uniformément continue est continue.*

Remarque I.4. *La réciproque est fausse. Par exemple la fonction $x \mapsto x^2$ sur $\mathbb{R}$ n'est pas uniformément continue.*
Par l'absurde, si elle l'était, on aurait pour $\varepsilon = 1 > 0$ l'existence de $\eta > 0$ tel que : $\forall x, y \in \mathbb{R},\ |x - y| \leq \eta \Rightarrow |x^2 - y^2| \leq 1$.
Mais on a pour tout $x \in \mathbb{R}_+$: $(x + \eta)^2 = x^2 + 2x\eta + \eta^2$ et donc pour tout $x \in \mathbb{R}_+$ on aurait : $2x\eta \leq 1$, ce qui est impossible comme $\lim\limits_{x \to +\infty} 2x\eta = +\infty$ (comme $\eta > 0$).

Proposition I.5. *Toute fonction lipschitzienne est uniformément continue.*

Démonstration. Soit $f : I \to \mathbb{K}$ une fonction k-lipschitzienne pour $k \geq 0$.
Soit $\varepsilon > 0$. Alors $\eta = \dfrac{\varepsilon}{k+1}$ convient car :

$$\forall x, y \in I,\ |x - y| \leq \eta \Rightarrow |f(x) - f(y)| \leq k|x - y| \leq k\eta = k\frac{\varepsilon}{k+1} \leq \varepsilon.$$

□

Théorème I.6 (de Heine)**.** *Une fonction continue sur un segment est uniformément continue.*

Démonstration. On considère f continue sur $[a,b]$, et on suppose par l'absurde que f n'est pas uniformément continue, et donc :

$$\exists \varepsilon > 0,\ \forall \eta > 0,\ \exists x, y \in [a,b],\ |x-y| \leq \eta \text{ et } |f(x)-f(y)| > \varepsilon.$$

Prenons un tel $\varepsilon > 0$, et appliquons pour $n \in \mathbb{N}^*$ le résultat à $\eta = \frac{1}{n}$, cela veut dire qu'il existe deux suites $(x_n), (y_n)$ telles que pour tout $n \in \mathbb{N}^*$:

$$|x_n - y_n| \leq \frac{1}{n} \text{ et } |f(x_n) - f(y_n)| > \varepsilon.$$

Mais (x_n) est bornée (car un segment est borné) et donc par théorème de Bolzano–Weierstrass il existe une suite extraite $(x_{\varphi(n)})$ qui converge vers un réel x, qui est nécessairement dans $[a,b]$ comme un segment est fermé.
Par encadrement, comme $\lim\limits_{n\to+\infty} \varphi(n) = +\infty$, alors : $|x_{\varphi(n)} - y_{\varphi(n)}| \underset{n\to+\infty}{\to} 0$, et donc la suite $(y_{\varphi(n)})$ converge également vers x.
Comme f est continue en x, alors les suites $(f(x_{\varphi(n)}))$ et $(f(y_{\varphi(n)}))$ convergent vers $f(x)$. Et donc :

$$\lim_{n\to+\infty} |f(x_{\varphi(n)}) - f(y_{\varphi(n)})| = 0$$

mais on a aussi : $\forall n \in \mathbb{N}^*,\ |f(x_{\varphi(n)}) - f(y_{\varphi(n)})| > \varepsilon$, donc par passage à la limite : $0 \geq \varepsilon$.
D'où la contradiction.
Donc f est uniformément continue. □

Exemple I.7. *On a vu que la fonction $x \mapsto \sqrt{x}$ est continue mais non lipschitzienne sur $[0,1]$ (à cause de son comportement en 0). Mais par théorème de Heine, comme $[0,1]$ est un segment, elle est uniformément continue sur $[0,1]$ (et elle l'est même sur $\mathbb{R}_+$).*

II Intégrales des fonctions en escalier

II.1 Les fonctions en escalier

Définition II.1. *Étant donné $[a,b]$ un segment, on appelle **subdivision** de $[a,b]$ une partie finie $\sigma = \{x_0, \dots, x_n\}$ pour $n \in \mathbb{N}^*$ et $a = x_0 < x_1 < \cdots < x_n = b$.*
*On appelle alors le **pas** de σ la quantité : $\delta(\sigma) = \max\limits_{i \in [\![0;n-1]\!]} (x_{i+1} - x_i)$.*

Remarque II.2. *Pour mettre en évidence l'ordre dans lequel les x_i sont rangés, on pourra voir σ plutôt comme une famille que comme un ensemble.*

Exemple II.3. *Si $n \in \mathbb{N}^*$, on dispose de la subdivision à **pas régulier** donnée par :*

$$\forall k \in [\![0;n]\!],\ x_k = a + k\frac{b-a}{n}.$$

Définition II.4. *On dit qu'une fonction $f : [a,b] \to \mathbb{R}$ est une **fonction en escalier** s'il existe une subdivision $\sigma = (x_i)_{i \in [\![0;n]\!]}$ telle que : pour tout $i \in [\![0; n-1]\!]$, la fonction $f|_{]x_i;x_{i+1}[}$ est constante.*
*On dira alors que σ est une subdivision **adaptée** à f.*
Et on notera $\mathcal{E}([a,b])$ l'ensemble des fonctions en escalier sur $[a,b]$.

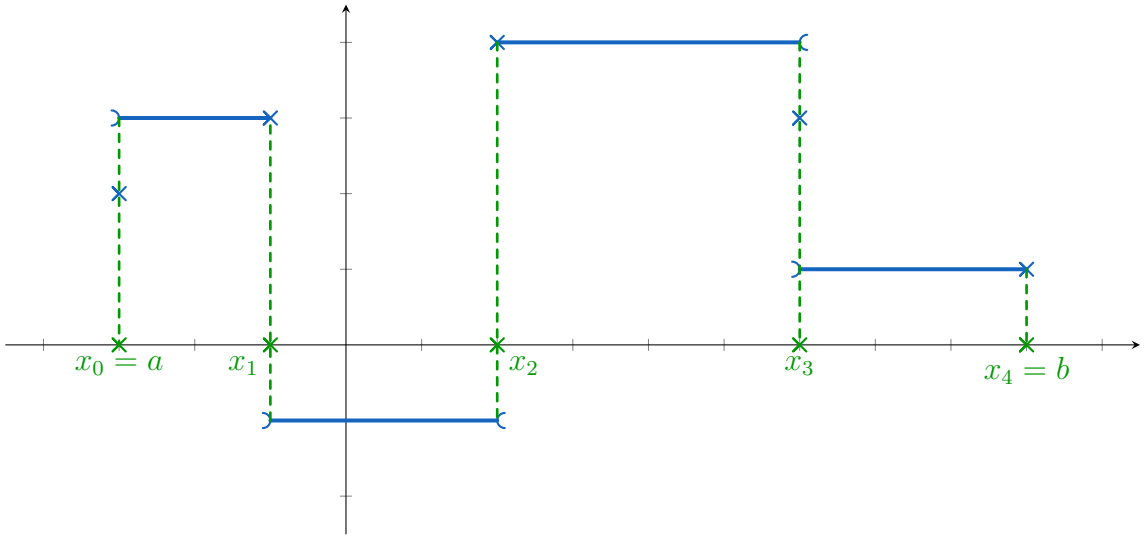
Remarques II.5.

1. *Il faut bien regarder f sur les intervalles **ouverts** $]x_i; x_{i+1}[$. Les valeurs de f en les x_i n'a pas d'importance.*

2. *Il n'y a pas unicité d'une subdivision. Plus précisément, si σ est une subdivision adaptée à f, tout subdivision τ de $[a,b]$ plus fine que σ (c'est-à-dire qui contient σ en tant qu'ensemble) est également adaptée à f.*

Exemples II.6.

1. *La restriction de la fonction $x \mapsto \lfloor x \rfloor$ à n'importe quel segment est une fonction en escalier.*
2. *La fonction définie sur $[a;b]$ dont le graphe est le suivant est en escalier :*



Proposition II.7. *L'ensemble $\mathcal{E}([a,b])$ est à la fois un sous-anneau et un sev de $\mathcal{F}([a,b],\mathbb{R})$.*

Démonstration. Pour le sous-anneau : la fonction constante de valeur 1 est constante, donc toutes ses restrictions aussi, donc elle est en escalier (toute subdivision convient).
De plus la différence et le produit de deux fonctions constantes est une fonction constante, donc en prenant deux fonctions en escalier et une subdivision adaptée simultanément aux deux (par union de subdivisions adaptées à chacune) on a le résultat.
Pour le sev : on procède comme pour le produit : une combinaison linéaire de fonctions constantes est constante, et il suffit juste de travailler à nouveau avec une subdivision adaptée aux deux fonctions en escalier considérées. □

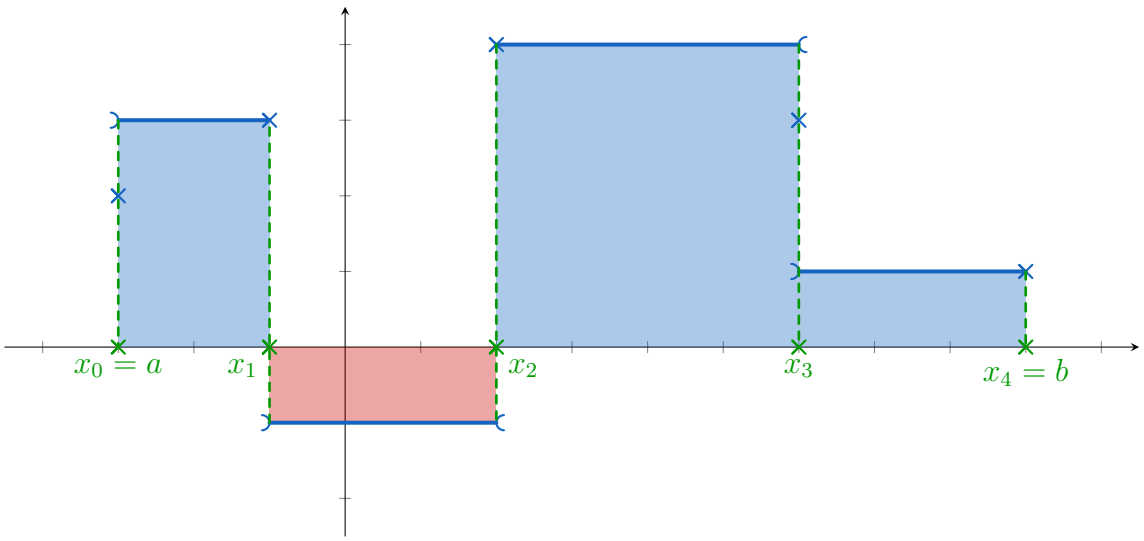
II.2 Intégrale d'une fonction en escalier

Théorème-Définition II.8. *Soit f une fonction en escalier sur $[a,b]$, et $\sigma = (x_i)_{i\in[\![0;n]\!]}$ une subdivision adaptée. Pour tout $i \in [\![0;n-1]\!]$, on note λ_i l'unique valeur prise par f sur $]x_i;x_{i+1}[$.*
Alors la quantité :

$$\sum_{i=0}^{n-1}(x_{i+1}-x_i)\lambda_i$$

*ne dépend pas du choix de σ adaptée à f. On l'appelle **l'intégrale de f entre a et b**, et on la notera indifféremment :*

$$\int_{[a,b]} f,\ \int_a^b f \text{ ou } \int_a^b f(t)\mathrm{d}t.$$



Remarque II.9. *On retrouve l'aire algébrisée sous la courbe (avec un signe "+" quand la fonction prend des valeurs positives, et avec un signe "−" sinon).*

Démonstration. La seule chose à prouver est que la quantité donnée ne dépend pas du choix de la subdivision adaptée.
On va déjà montrer que, si σ est une subdivision adaptée, alors ajouter un point à σ ne change pas la valeur de l'intégrale définie à l'aide de σ.
Soit $\sigma = (x_i)$ une subdivision adaptée à f. On note $k \in [\![0; n-1]\!]$ et $x \in]x_k; x_{k+1}[$ qu'on rajoute à σ. Comme σ est adaptée à f, alors f est constante sur $]x_k; x_{k+1}[$, de valeur λ_k (avec les notations précédentes), donc la valeur de f sur $]x_k; x[$ et $]x; x_{k+1}[$ est également λ_k. Ainsi l'intégrale associée à $\sigma \cup \{x\}$ est :

$$\left(\sum_{i=1}^{k-1}(x_{i+1}-x_i)\lambda_i\right) + \underbrace{(x-x_k)\lambda_k + (x_{k+1}-x)\lambda_k}_{=(x_{k+1}-x_k)\lambda_k} + \left(\sum_{i=k+1}^{n-1}(x_{i+1}-x_i)\lambda_i\right) = \sum_{i=1}^{n-1}(x_{i+1}-x_i)\lambda_i$$

et donc on retrouve la valeur associée à σ.
Une récurrence immédiate montre que l'on peut ainsi rajouter un nombre fini de points à une subdivision adaptée sans changer la valeur de l'intégrale associée.
Enfin, si σ_1, σ_2 sont deux subdivisions adaptées, alors l'intégrale associée à $\sigma = \sigma_1 \cup \sigma_2$ est obtenue indifféremment en rajoutant un nombre fini de points à σ_1 ou σ_2, donc l'intégrale associée est la même que celle associées à σ_1 ou σ_2, qui sont donc égales.
D'où le résultat. □

Remarque II.10. *La valeur de f en les x_i n'a aucune incidence sur son intégrale. Mieux : comme rajouter des points à une subdivision préserve le fait qu'elle soit adaptée, on peut changer la valeur de f en un nombre fini de points sans changer la valeur de l'intégrale.*

Proposition II.11. *Si $f, g \in \mathcal{E}([a,b])$ et $\lambda \in \mathbb{R}$, alors :*

1. $\displaystyle\int_a^b (\lambda f(t) + g(t))\,\mathrm{d}t = \lambda \int_a^b f(t)\mathrm{d}t + \int_a^b g(t)\mathrm{d}t$ *(linéarité de l'intégrale) ;*
2. *si $f \geq 0$, alors :* $\displaystyle\int_a^b f(t)\mathrm{d}t \geq 0$ *(positivité de l'intégrale) ;*
3. *si $f \leq g$, alors :* $\displaystyle\int_a^b f(t)\mathrm{d}t \leq \int_a^b g(t)\mathrm{d}t$ *(croissance de l'intégrale) ;*
4. *si $c \in [a,b]$:* $\displaystyle\int_a^b f(t)\mathrm{d}t = \int_a^c f(t)\mathrm{d}t + \int_b^c f(t)\mathrm{d}t$ *(relation de Chasles).*

Démonstration. Découle à chaque fois des propriétés analogues pour la somme, en prenant une subdivision adaptée à f et g. □

Remarque II.12. *On retrouve ainsi les mêmes propriétés que pour l'intégrale qu'on avait définie pour les fonctions continues à l'aide de primitives. La différence étant qu'on peut changer les fonctions en un nombre fini de points sans changer la valeur de l'intégrale, donc par exemple pour la croissance il suffit d'avoir $f(t) \leq g(t)$ pour tout $t \in [a,b]$ sauf en un nombre fini de points.*

Corollaire II.13. *Si $f \in \mathcal{E}([a,b])$ alors :*

$$\left|\int_a^b f(t)\mathrm{d}t\right| \leq \int_a^b |f(t)|\mathrm{d}t.$$

Démonstration. Découle de la croissance et de la linéarité, on notant que : $-|f| \leq f \leq |f|$, et donc :

$$-\int_a^b |f(t)|\mathrm{d}t \leq \int_a^b f(t)\mathrm{d}t \leq \int_a^b |f(t)|\mathrm{d}t$$

□

III Intégrales des fonctions continues par morceaux

III.1 Les fonctions continues par morceaux

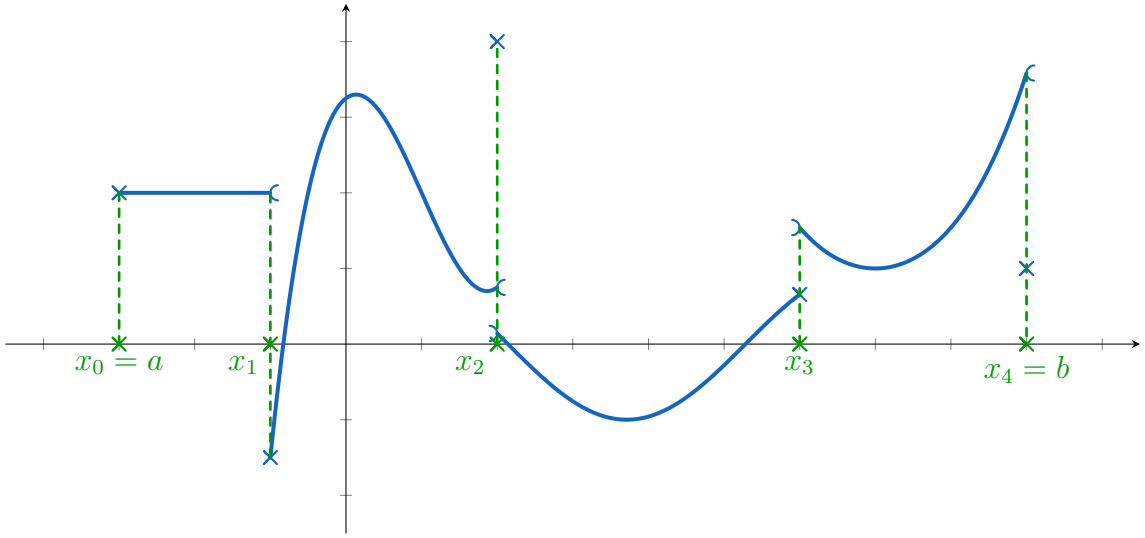
Définition III.1. *On dit qu'une fonction $f : [a,b] \to \mathbb{R}$ est une **fonction continue par morceaux** s'il existe une subdivision $\sigma = (x_i)_{i\in[\![0;n]\!]}$ telle que pour tout $i \in [\![0; n-1]\!]$ la fonction $f|_{]x_i;x_{i+1}[}$ est continue et prolongeable par continuité en x_i et x_{i+1}.*
*On dira alors que σ est une subdivision **adaptée** à f.*
Et on notera $\mathcal{C}_{pm}([a,b])$ l'ensemble des fonctions continues par morceaux sur $[a;b]$.

Remarques III.2.

1. *Une fonction constante est prolongeable par continuité (il suffit de fixer comme image l'unique valeur qu'elle prend). Donc toute fonction en escalier est continue par morceaux : $\mathcal{E}([a,b]) \subset \mathcal{C}([a,b])$.*
2. *Une fonction continue est continue par morceaux (toute subdivision convient).*
3. *Comme pour les fonctions en escalier, les valeurs en les x_i n'ont aucune incidence. Et une subdivision restera adaptée si on lui rajoute des points.*
4. *Le prolongement par continuité impose que f a des limites **finies** à gauche et à droite en les x_i. En revanche, ces limites n'ont pas de raison d'être égales (ce qui reviendrait à avoir une fonction continue).*
5. *Une fonction continue par morceaux sur $[a,b]$ a un nombre fini de points de discontinuité, puisqu'ils sont inclus dans les points d'une subdivision adaptée.*

Exemples III.3.

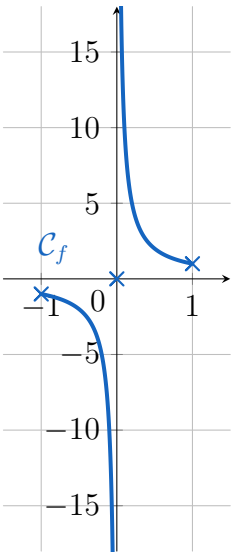
1. *La fonction définie sur $[a,b]$ dont le graphe est le suivant est continue par morceaux.*



2. *En revanche, la fonction f définie sur $[-1,1]$ par :*

$$f(x) = \begin{cases} \frac{1}{x} & si \quad x \neq 0 \\ 0 & si \quad x = 0 \end{cases}$$

n'est pas continue par morceaux. Elle est certes continue sur $[-1;0[$ et sur $]0;1]$, mais ses limites à gauche et à droite en 0 ne sont pas finies donc ses restrictions à $]-1;0[$ et $]0;1[$ ne sont pas prolongeables par continuité en 0.



Proposition III.4. *L'ensemble $\mathcal{C}_{pm}([a,b])$ est à la fois un sous-anneau et un sev de $\mathcal{F}([a,b],\mathbb{R})$.*

Démonstration. On procède comme pour les fonctions en escalier.
Pour le sous-anneau : la fonction constante de valeur 1 est continue donc continue par morceaux.
En prenant une subdivision adaptée à deux fonctions continues par morceaux, on constate facilement que :
- leur différence est continue par morceau : la continuité découle du fait que la différence de deux fonctions continues est continue ; le prolongement par continuité se fait par opération sur les limites ;
- et idem pour le produit.

Pour le sev : il suffit de voir qu'une combinaison linéaire de fonctions continues est continue, et le prolongement par continuité se déduit des opérations sur les limites. □

Proposition III.5. *Une fonction continue par morceaux sur un segment est bornée.*

Démonstration. Soit $f \in \mathcal{C}_{pm}([a,b])$, et $(x_i)_{i\in[\![0;n]\!]}$ adaptée à f.
Alors pour tout $i \in [\![0; n-1]\!]$, si on note f_i le prolongement par continuité de $f|_{]x_i,x_{i+1}[}$ à $[x_i, x_{i+1}]$, alors f_i est une fonction continue sur un segment, dont par théorème des bornes atteintes elle est bornée (et atteint ses bornes, mais ce n'est pas important ici), donc en notant M_i un majorant de $|f_i|$ on a :

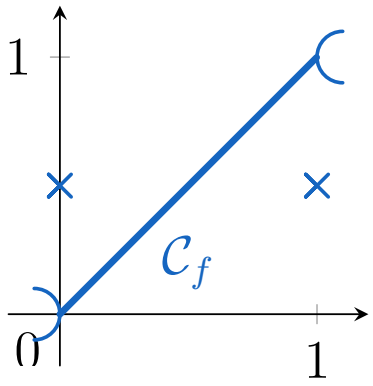
$$\forall x \in]x_i, x_{i+1}[,\ |f(x)| = |f_i(x)| \leq M_i$$

En notant $M = \max(M_0, \dots, M_{n-1}, |f(x_0)|, \dots, |f(x_n)|)$ on trouve bien un majorant de $|f|$ sur $[a,b]$, donc f est bornée. □

Remarque III.6. *Rien n'indique en revanche que les bornes sont atteintes. Par exemple, on peut considérer la fonction :*

$$\left\{\begin{array}{ccc} [0;1] & \to & [0;1] \\ x & \mapsto & \left\{\begin{array}{lll} \frac{1}{2} & si & x \in \{0;1\} \\ x & si & x \in]0;1[\end{array}\right. \end{array}\right.$$

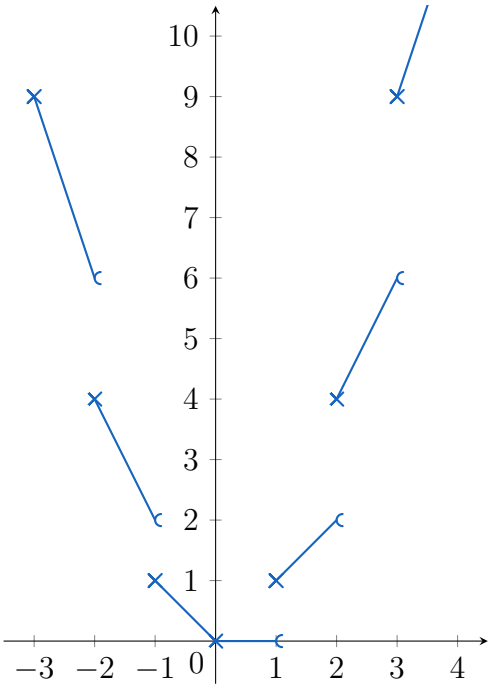
qui admet 0 *et* 1 *comme bornes inférieure et supérieure respectivement, mais qui ne sont pas atteintes.*



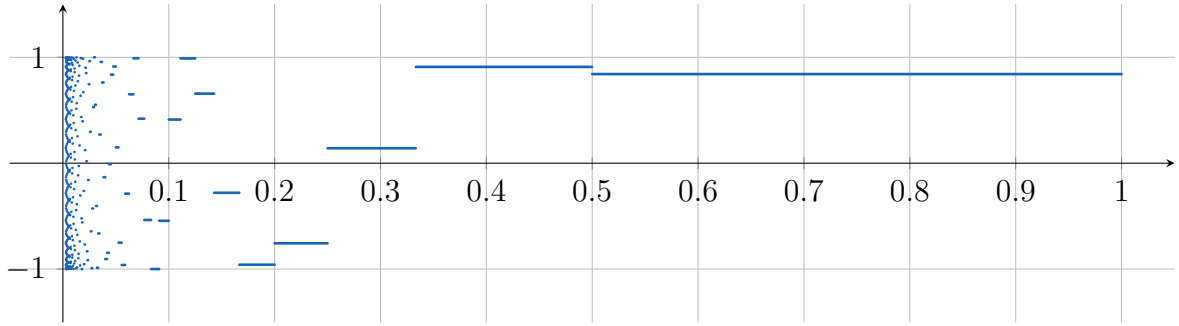
Définition III.7. *Si I est un intervalle quelconque de $\mathbb{R}$, une fonction f définie sur I sera dite continue par morceaux si la restriction de f à tout segment de I est continue par morceaux (au sens précédent).*

Exemples III.8.

1. *La fonction partie entière est continue par morceaux sur $\mathbb{R}$.*
2. *La fonction $x \mapsto x \cdot \lfloor x \rfloor$ est continue par morceaux sur $\mathbb{R}$:*



3. *La fonction* $x \mapsto \begin{cases} \sin\left(\lfloor \frac{1}{x} \rfloor\right) & si \quad x \neq 0 \\ 0 & si \quad x = 0 \end{cases}$ *est continue par morceau sur* $]0;1]$*, mais pas sur* $[0;1]$ *(on aurait besoin d'une subdivision "infinie" dans le second cas).*



III.2 Densité des fonctions en escalier

Définition III.9. *Étant donnée f une fonction bornée sur $[a;b]$, on appelle* ***norme infinie*** *(ou norme sup) la quantité :* $\|f\|_\infty = \sup_{x\in[a,b]} |f(x)|$.

Remarques III.10.

1. *Cette définition a bien un sens, car si f est bornée, alors* $\{|f(x)| \,|\, x \in [a,b]\}$ *est une partie non vide majorée de* $\mathbb{R}$*. Et comme il s'agit même d'une partie de* $\mathbb{R}_+$*, on a toujours* $\|f\|_\infty \geq 0$.
2. *Comme une fonction continue par morceaux sur un segment est bornée, on peut bien définir* $\|f\|_\infty$ *pour de telles fonctions. C'est également le cas pour le fonctions continues, et par théorème des bornes atteintes on a même un maximum (au lieu d'une borne supérieure).*
3. *Géométriquement, cela veut dire que le graphe de f est compris entre les droites horizontales d'équation* $y = \pm\|f\|_\infty$.

Proposition III.11. *Si f, g sont deux fonctions bornées sur $[a,b]$ et $\lambda \in \mathbb{R}$, alors :*

1. $\|\lambda f\|_\infty = |\lambda| \cdot \|f\|_\infty$ *(positive homogénéité de degré 1, ou juste homogénéité) ;*
2. $\|f+g\|_\infty \leq \|f\|_\infty + \|g\|_\infty$ *(inégalité triangulaire) ;*
3. $\|f\|_\infty = 0 \Leftrightarrow f = 0$ *(séparation).*

Démonstration.

1. Si $x \in [a,b]$, alors $|\lambda f(x)| = |\lambda| \cdot \|f(x)|$, et on a le résultat en passant au sup.
2. Si $x \in [a,b]$, alors : $|f(x)+g(x)| \leq |f(x)| + |g(x)| \leq \|f\|_\infty + \|g\|_\infty$.
3. Si $f = 0$, alors il est clair que $\|f\|_\infty = 0$ (par calcul direct ou par le premier point avec $\lambda = 0$). Réciproquement, si $\|f\|_\infty = 0$ alors pour tout $x \in [a,b]$ on a : $|f(x)| \leq 0$, donc $f(x) = 0$, et donc $f = 0$.

□

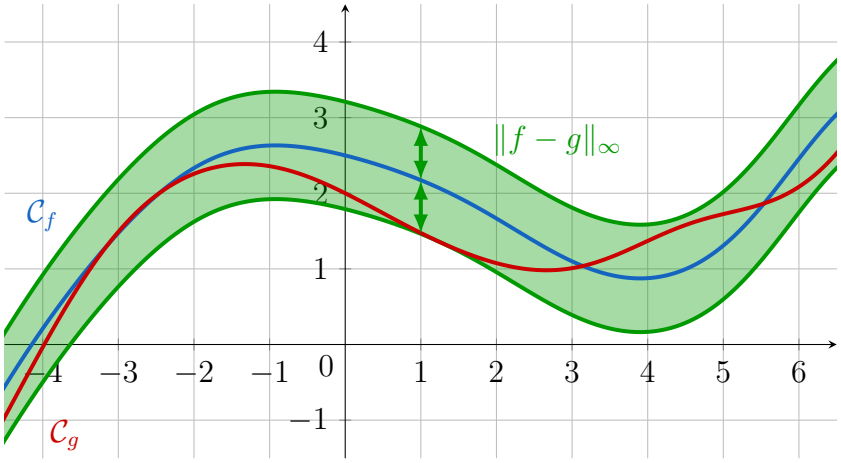
Remarque III.12. *On voit qu'en fait toutes les propriétés de la norme infinie découlent des propriétés analogues pour la valeur absolue : ces deux notions s'inscrivent plus généralement dans la notion de "normes", qui sont des applications à valeurs réelles (en fait nécessairement positives), qui vérifient les trois propriétés ci-dessus : homogénéité, inégalité triangulaire et séparation. Et on en verra d'autres que cette norme infinie ou la valeur absolue.*

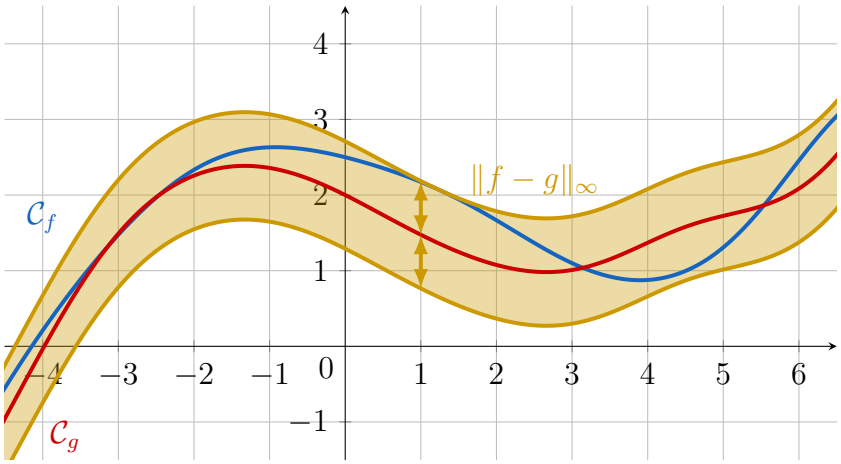
Définition III.13. *Si f et g sont deux fonctions bornées sur $[a,b]$, on définit la* ***distance uniforme entre f et g*** *comme la quantité* $\|f-g\|_\infty$.

Remarques III.14.

1. *Cette définition a bien un sens car, par inégalité triangulaire, si f et g sont bornées, alors $f-g$ aussi. Mais on pourrait aussi définir une distance entre deux fonctions non bornées, mais dont la différence serait bornée.*

2. *Graphiquement, cela veut dire que les courbes de f et g restent assez proches. On peut même voir cela de manière asymétrique : le graphe de g reste dans le "cylindre" de rayon $\|f-g\|_\infty$ autour du graphe de f, ou de manière équivalente le graphe de f reste dans le "cylindre" de rayon $\|f-g\|_\infty$ autour du graphe de g.*

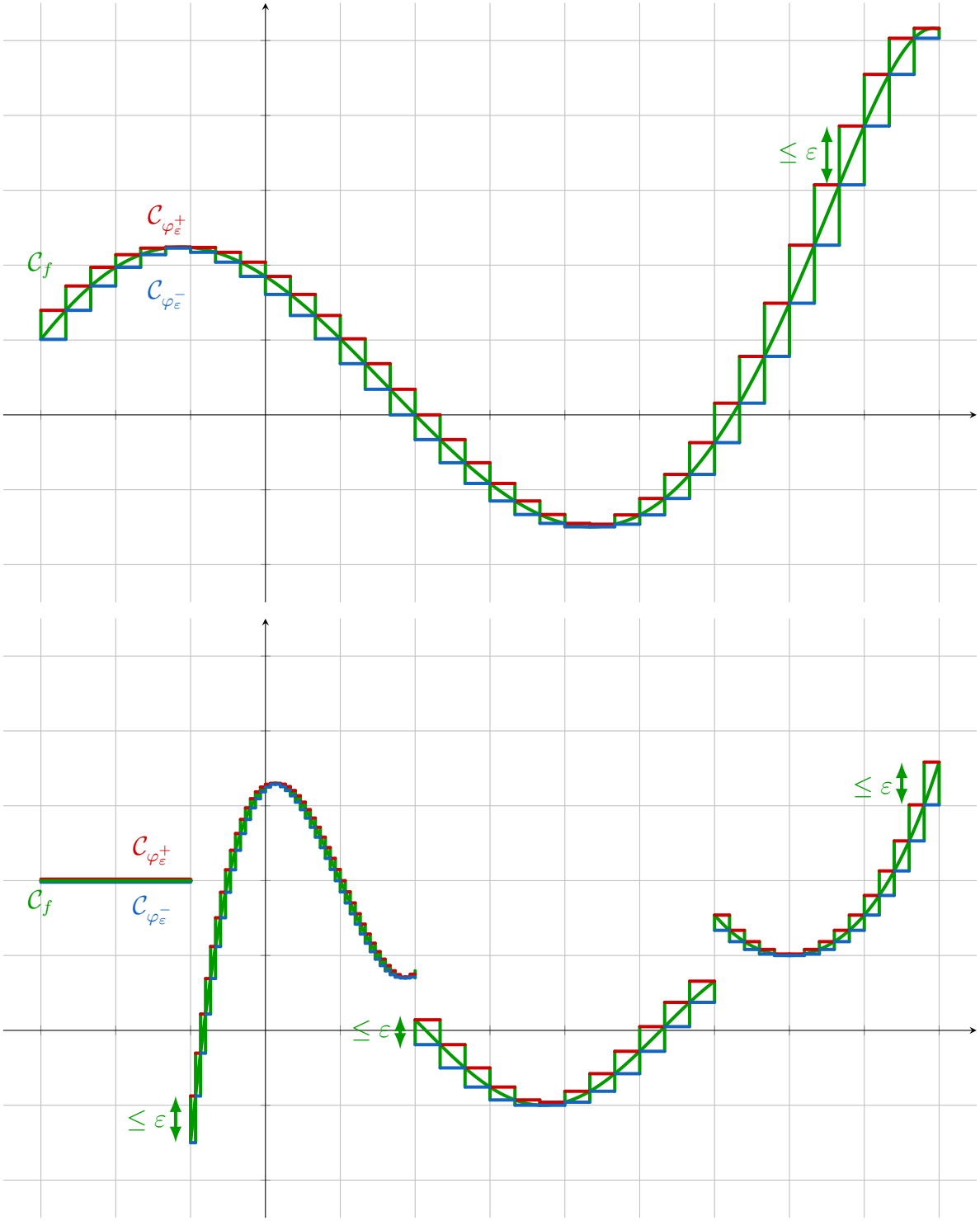




Théorème III.15. *Si f est une fonction continue par morceaux sur $[a,b]$ et $\varepsilon>0$, alors il existe deux fonctions en escalier φ_ε^- et φ_ε^+ telles que :*

1. $\varphi_\varepsilon^- \leq f \leq \varphi_\varepsilon^+$;

2. $\|\varphi_\varepsilon^+ - \varphi_\varepsilon^-\|_\infty \leq \varepsilon$.



Démonstration. Montrons d'abord le résultat si f est continue.
Comme f est continue sur $[a,b]$, par théorème de Heine elle y est uniformément continue. Il existe donc $\eta > 0$ tel que :

$$\forall x, y \in [a,b],\ |x-y| \leq \eta \Rightarrow |f(x)-f(y)| \leq \varepsilon.$$

Considérons $n \in \mathbb{N}^*$ tel que $\dfrac{b-a}{n} \leq \eta$, et prenons $(x_i)_{i\in[\![0;n]\!]}$ la subdivision à pas régulier associée, c'est-à-dire que :

$$\forall i \in [\![0;n]\!],\ x_i = a + i\frac{b-a}{n}.$$

Pour tout $i \in [\![0;n-1]\!]$, par théorème des bornes atteintes appliquée à f sur le segment $[x_i, x_{i+1}]$, on a : $f([x_i,x_{i+1}]) = [m_i, M_i]$. Par définition de m_i, M_i, il existe $y_i, z_i \in [x_i, x_{i+1}]$ tels que $f(y_i) = m_i$ et $f(z_i) = M_i$. Et donc, par définition des x_i on a :$|y_i - z_i| \leq |x_{i+1} - x_i| \leq \eta$, donc $|M_i - m_i| = M_i - m_i \leq \varepsilon$.

Et il est alors clair que les fonctions $\varphi_\varepsilon^+, \varphi_\varepsilon^-$ suivantes conviennent :

$$\varphi_\varepsilon^+ : \left\{ \begin{array}{ccc} [a,b] & \to & \mathbb{R} \\ x & \mapsto & \left\{ \begin{array}{lll} M_i & \text{si} & x \in [x_i; x_{i+1}[\\ f(b) & \text{si} & x = b \end{array} \right. \end{array} \right. \quad \text{et } \varphi_\varepsilon^- : \left\{ \begin{array}{ccc} [a,b] & \to & \mathbb{R} \\ x & \mapsto & \left\{ \begin{array}{lll} m_i & \text{si} & x \in [x_i; x_{i+1}[\\ f(b) & \text{si} & x = b \end{array} \right. \end{array} \right.$$

Pour le cas général, on considère $(x_i)_{i\in[\![0;n]\!]}$ une subdivision adaptée à f. Pour tout $i \in [\![0; n-1]\!]$, notons f_i le prolongement par continuité de $f|_{]x_i;x_{i+1}[}$ à $[x_i; x_{i+1}]$. Comme f_i est continue, il existe deux fonctions en escalier $\varphi_{\varepsilon,i}^+$ et $\varphi_{\varepsilon,i}^-$ telles que pour tout $x \in]x_i; x_{i+1}[$:

$$\varphi_{\varepsilon,i}^-(x) \leq \underbrace{f_i(x)}_{=f(x)} \leq \varphi_{\varepsilon,i}^+(x) \text{ et } \varphi_{\varepsilon,i}^+(x) - \varphi_{\varepsilon,i}^-(x) \leq \varepsilon.$$

Et ainsi les fonctions en escalier suivantes conviennent :

$$\varphi_\varepsilon^+ : \left\{ \begin{array}{ccc} [a,b] & \to & \mathbb{R} \\ x & \mapsto & \left\{ \begin{array}{lll} \varphi_{\varepsilon,i}^+(x) & \text{si} & x \in]x_i; x_{i+1}[\\ f(x_i) & \text{si} & x = x_i \end{array} \right. \end{array} \right. \quad \text{et } \varphi_\varepsilon^- : \left\{ \begin{array}{ccc} [a,b] & \to & \mathbb{R} \\ x & \mapsto & \left\{ \begin{array}{lll} \varphi_{\varepsilon,i}^-(x) & \text{si} & x \in]x_i; x_{i+1}[\\ f(x_i) & \text{si} & x = x_i \end{array} \right. \end{array} \right.$$

□

Remarque III.16. *L'idée est que l'on peut encadrer aussi proche que l'on veut (au sens de la distance définie avant) toute fonction continue par morceaux par des fonctions en escalier. Et on peut regarder aussi ces approximations de manière séparée puisque, par inégalité triangulaire, on a :*

$$\|\varphi_\varepsilon^+ - f\|_\infty \leq \varepsilon \text{ et } \|\varphi_\varepsilon^- - f\|_\infty \leq \varepsilon.$$

En ce sens, cette notion de densité est très proche de celle qu'on avait vue avec les réels (par exemple la densité de $\mathbb{Q}$ ou $\mathbb{R} \setminus \mathbb{Q}$ dans $\mathbb{R}$) : on dit que A est dense dans B si tout élément de B peut être approché arbitrairement près par un élément de A.

III.3 Intégrale des fonctions continues par morceaux

Théorème-Définition III.17. *Si $f \in \mathcal{C}_{pm}([a,b])$ on lui associe les ensembles :*

$$I^+(f) = \left\{ \int_a^b \varphi(t)\mathrm{d}t \,|\, \varphi \in \mathcal{E}([a,b]),\ \varphi \geq f \right\} \text{ et } I^-(f) = \left\{ \int_a^b \varphi(t)\mathrm{d}t \,|\, \varphi \in \mathcal{E}([a,b]),\ \varphi \leq f \right\}.$$

Les quantités $\sup(I^-(f))$ et $\inf(I_+(f))$ sont bien définies, et sont égales.
On appelle leur valeur commune ***l'intégrale de*** *f* ***entre*** *a* ***et*** *b, et on la notera indifféremment :*

$$\int_{[a,b]} f,\ \int_a^b f \text{ ou } \int_a^b f(t)\mathrm{d}t.$$

De plus, l'intégrale ainsi définie coïncide avec l'intégrale définie précédemment, dans le sens où les deux définitions donnent la même valeur pour $f \in \mathcal{E}([a,b])$.

Démonstration. Constatons déjà que les ensemble $I^+(f)$ et $I^-(f)$ sont non vides : f est bornée, et encadrée par les fonctions constantes (donc en escalier) de valeurs $\pm\|f\|_\infty$.
De plus, si on considère g, h en escalier sur $[a,b]$ telles que $g \leq f \leq h$, alors par croissance de l'intégrale (pour les fonctions en escalier), on a : $\int_a^b g \leq \int_a^b h$. Et donc, par définition des ensembles $I^+(f)$ et $I^-(f)$, on a que tout élément de $I^+(f)$ est plus grand que tout élément de $I^-(f)$.
Les ensembles $I^+(f)$ et $I^-(f)$ sont donc non vides, respectivement minoré (par tout élément de $I^-(f)$) et majoré (par tout élément de $I^+(f)$). Ce qui justifie que les bornes considérées sont bien définies, et vérifient même : $\sup(I^-(f)) \leq \inf(I_+(f))$.

Soit $\varepsilon > 0$. Considérons $\varphi_\varepsilon^+, \varphi_\varepsilon^-$ en escalier telles que $\varphi_\varepsilon^- \leq f \leq \varphi_\varepsilon^+$ et $\|\varphi_\varepsilon^+ - \varphi_\varepsilon^-\|_\infty \leq \varepsilon$. Alors par croissance de l'intégrale (montrée pour les intégrales de fonctions en escalier), on a :

$$\int_a^b \varphi_\varepsilon^+(t)\mathrm{d}t - \int_a^b \varphi_\varepsilon^-(t)\mathrm{d}t = \int_a^b \left(\varphi_\varepsilon^+(t) - \varphi_\varepsilon^-(t)\right)\mathrm{d}t \leq \int_a^b \varepsilon \mathrm{d}t = (b-a)\varepsilon$$

et comme par définition des bornes précédentes on a :

$$\int_a^b \varphi_\varepsilon^-(t)\mathrm{d}t \leq \sup I^-(f) \leq \inf I^+(f) \leq \int_a^b \varphi_\varepsilon^+(t)\mathrm{d}t$$

on déduit finalement que :

$$\inf I^+(f) - \sup I^-(f) \leq (b-a)\varepsilon$$

et comme ceci est vrai pour tout $\varepsilon > 0$, en faisant tendre ε vers 0, on déduit que : $\inf I^+(f) - \sup I^-(f) \leq 0$. D'où l'égalité cherchée : $\inf I^+(f) = \sup I^-(f)$.
Si f est en escalier, alors $f \leq f \leq f$ et par définition on a donc :

$$\underbrace{\int_a^b f(t)\mathrm{d}t}_{\text{au sens des fonctions en escalier}} \leq \underbrace{\int_a^b f(t)\mathrm{d}t}_{\text{au sens des fonctions continues par morceaux}} \leq \underbrace{\int_a^b f(t)\mathrm{d}t}_{\text{au sens des fonctions en escalier}}$$

ce qui donne le résultat. □

Remarques III.18. *L'intégrale ainsi définie s'interprète aussi comme une aire (algébrisée) sous la courbe d'une fonction, mais cela se voit moins directement.*
De plus, comme on peut changer une fonction en escalier en un nombre fini de points sans changer la valeur de son intégrale, on peut voir par encadrement que cela reste valable pour une fonction continue par morceaux.

Proposition III.19. *Si $f, g \in \mathcal{C}_{pm}([a,b])$ et $\lambda \in \mathbb{R}$, alors :*

1. $\int_a^b (\lambda f(t) + g(t))\,\mathrm{d}t = \lambda \int_a^b f(t)\mathrm{d}t + \int_a^b g(t)\mathrm{d}t$ *(linéarité de l'intégrale) ;*
2. *si $f \geq 0$, alors :* $\int_a^b f(t)\mathrm{d}t \geq 0$ *(positivité de l'intégrale) ;*
3. *si $f \leq g$, alors :* $\int_a^b f(t)\mathrm{d}t \leq \int_a^b g(t)\mathrm{d}t$ *(croissance de l'intégrale) ;*
4. *si $c \in [a,b]$:* $\int_a^b f(t)\mathrm{d}t = \int_a^c f(t)\mathrm{d}t + \int_b^c f(t)\mathrm{d}t$ *(relation de Chasles) ;*
5. $\left|\int_a^b f(t)\mathrm{d}t\right| \leq \int_a^b |f(t)|\mathrm{d}t$ *(inégalité triangulaire).*

Démonstration. Découle à chaque fois des propriétés de l'intégrale définie sur les fonctions en escalier. Tous les résultats se montrent par encadrement, par des encadrements arbitrairement proches par des fonctions en escaliers. □

Remarque III.20. *On retrouve par linéarité qu'on peut changer une fonction continue par morceaux en un nombre fini de points sans changer la valeur de son intégrale. L'idée est que les fonctions diffèrent d'une fonction nulle sauf en un nombre fini de points, dont l'intégrale vaut 0 (par formule de l'intégrale d'une fonction en escalier).*

Proposition III.21. *Si $f \in \mathcal{C}^0([a,b],\mathbb{R})$ de signe constant, alors :*

$$\int_a^b f(t)\mathrm{d}t = 0 \Leftrightarrow f = 0.$$

Démonstration. Si $f = 0$, on a directement que $\int_a^b f(t)\mathrm{d}t = 0$.
Réciproquement, supposons que f est continue positive non nulle. Notons $x_0 \in [a,b]$ tel que $f(x_0) > 0$. Par continuité, on peut même choisir un tel $x_0 \in]a;b[$. Et par définition de la continuité, il existe $\eta > 0$ tel que :

$$\forall x \in [a,b] \cap [x_0 - \eta; x_0 + \eta],\ |f(x) - f(x_0)| \leq \frac{f(x_0)}{2}$$

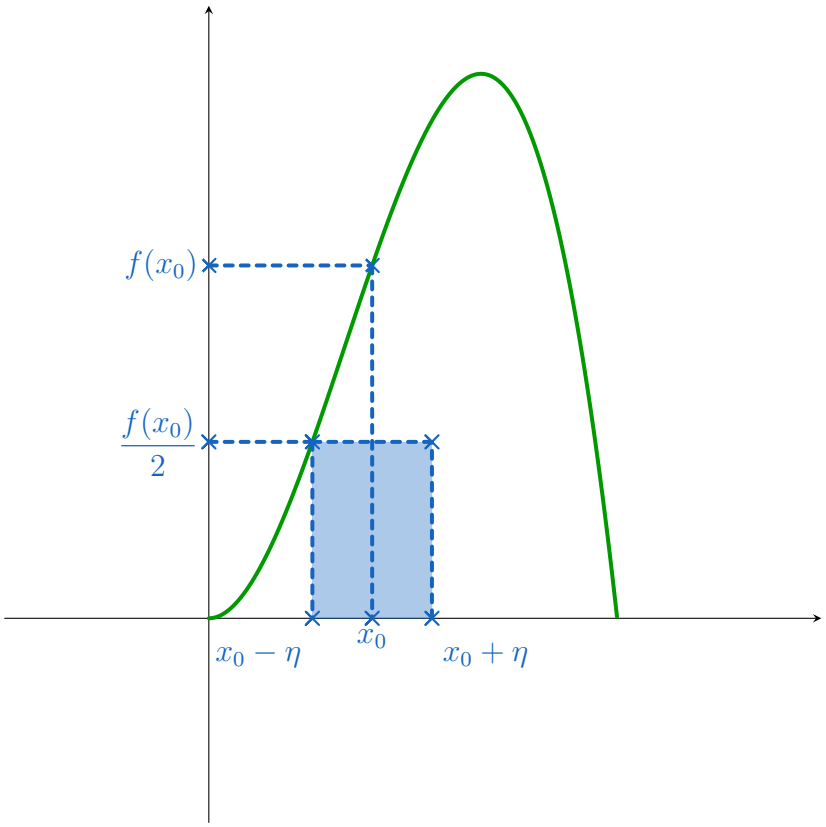
et quitte à réduire η on peut même supposer que $[x_0 - \eta; x_0 + \eta] \subset [a,b]$.
Par inégalité triangulaire, on a donc :

$$\forall x \in [x_0 - \eta; x_0 + \eta],\ f(x) \geq f(x_0) - \frac{f(x_0)}{2} = \frac{f(x_0)}{2}.$$

Et donc la fonction en escalier φ définie sur $[a,b]$ par :

$$\varphi : x \mapsto \begin{cases} \frac{f(x_0)}{2} & \text{si} \quad x \in [x_0 - \eta; x_0 + \eta] \\ 0 & \text{si} \quad x \notin [x_0 - \eta; x_0 + \eta] \end{cases}$$

vérifie $f \geq \varphi$ et $\int_a^b \varphi(t)\mathrm{d}t = (2\eta) \cdot \frac{f(x_0)}{2} = \eta f(x_0) > 0$.
Et par croissance de l'intégrale, on a bien : $\int_a^b f(t)\mathrm{d}t > 0$.



□

Remarque III.22. *On peut adapter le résultat à des fonctions continues par morceaux : une fonction continue par morceau de signe constant (sauf en un nombre fini de points) est d'intégrale nulle si, et seulement si, elle est nulle en tous les points en lesquels elle est continue.*

Définition III.23. *Si $f \in \mathcal{C}_{pm}([a,b])$, on définit* ***l'intégrale de*** f ***entre*** b ***et*** a*, notée* $\int_b^a f(t)\mathrm{d}t$*, comme :*

$$\int_b^a f(t)\mathrm{d}t = -\int_a^b f(t)\mathrm{d}t.$$

Remarque III.24. *La généralisation ci-dessus préserve la linéarité et la relation de Chasles.*
En revanche, la positivité, la croissance et l'inégalité triangulaire ne sont plus vérifiées, et il faudra se ramener à une intégrale entre deux bornes dans le "bon ordre" pour pouvoir les appliquer.

IV Propriétés des fonctions et de leurs intégrales

IV.1 Le théorème fondamental de l'analyse

Définition IV.1. *Si $f \in \mathcal{C}_{pm}([a,b])$, on appelle* ***valeur moyenne de*** f ***entre*** a ***et*** b *la quantité :*

$$\frac{1}{b-a}\int_a^b f(t)\mathrm{d}t.$$

Proposition IV.2. *Si f est continue sur le segment $[a,b]$, alors il existe $c \in [a,b]$ tel que* $f(c) = \dfrac{1}{b-a}\displaystyle\int_a^b f(t)\mathrm{d}t$.

Démonstration. Pour simplifier notons μ la valeur moyenne de f entre a et b.
Comme f est continue sur le segment $[a,b]$, alors par théorème des bornes atteintes il existe $\alpha, \beta \in [a,b]$ et $m, M \in \mathbb{R}$ tels que : $f([a,b]) = [m,M]$ et $f(\alpha) = m$, $f(\beta) = M$.
Pour tout $x \in [a,b]$, on a :

$$m \leq f(x) \leq M$$

donc par croissance de l'intégrale (en divisant par $(b-a)$) :

$$m \leq \mu \leq M$$

et donc $\mu \in [f(\alpha), f(\beta)]$. Par théorème des valeurs intermédiaires, comme f est continue sur $[a,b]$ donc entre α et β, on déduit qu'il existe c entre α et β (donc dans $[a,b]$) tel que $f(c) = \mu$. □

Remarques IV.3.

1. *On peut modifier la démonstration pour voir que c peut même être choisi dans $]a,b[$: c'est clair si μ est différent de m et M (car alors c est strictement entre α et β) ; et sinon cela veut dire que f est constante donc tout c convient.*
2. *Le résultat est faux si f n'est pas continue. Par exemple, si on prend f la fonction partie entière sur $[0;2]$, on trouve $\mu = \dfrac{1}{2} \notin \mathbb{Z}$ donc qui n'est pas dans l'image de f.*

Théorème IV.4 (Théorème fondamental de l'analyse)**.** *Si f est continue sur un intervalle I, alors f admet une primitive.*
Plus précisément, pour tout $x_0 \in I$ et $y_0 \in \mathbb{R}$, l'application :

$$x \mapsto \int_{x_0}^x f(t)\mathrm{d}t + y_0$$

est l'unique primitive de f sur I qui vaut y_0 en x_0.

Démonstration. Comme les primitives de f (si elles existent) diffèrent toutes d'une constante, il suffit de montrer que, pour $a \in I$ fixé, l'application $F : x \mapsto \int_a^x f(t)\mathrm{d}t$ est une primitive de f.
Fixons $x_0 \in I$ et considérons $x \in I$ distinct de x_0. Alors :

$$\frac{F(x)-F(x_0)}{x-x_0} = \frac{1}{x-x_0}\left(\int_a^x f(t)\mathrm{d}t - \int_a^{x_0} f(t)\mathrm{d}t\right) = \frac{1}{x-x_0}\left(\int_a^x f(t)\mathrm{d}t + \int_{x_0}^a f(t)\mathrm{d}t\right) = \frac{1}{x-x_0}\int_{x_0}^x f(t)\mathrm{d}t$$

en utilisant la relation de Chasles.
On reconnait ainsi la valeur moyenne de f entre x et x_0. Il existe donc c_x (qui dépend de x), entre x et x_0, tel que :

$$\frac{F(x)-F(x_0)}{x-x_0} = f(c_x).$$

En faisant tendre x vers x_0, on a que c_x tend vers x_0 (par encadrement). Et donc, comme f est continue, on déduit que :

$$\lim_{x\to x_0} f(c_x) = f(x_0)$$

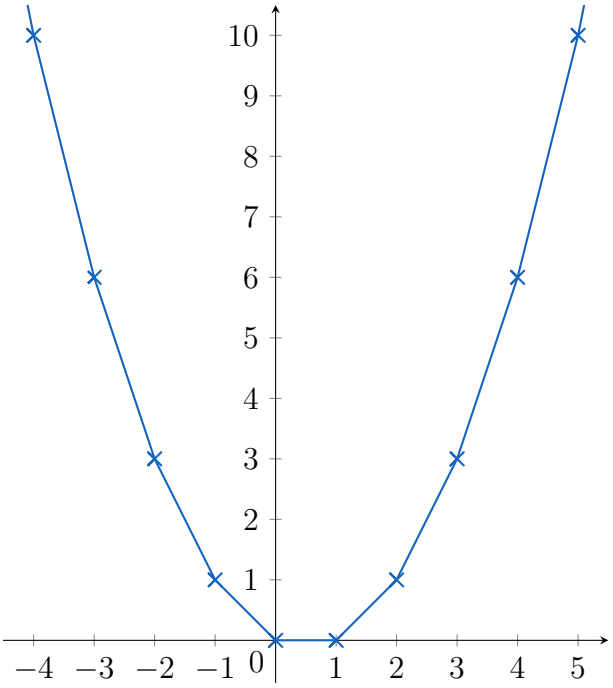
et finalement :

$$\lim_{x\to x_0} \frac{F(x)-F(x_0)}{x-x_0} = f(x_0)$$

ce qui montre bien que F est dérivable, et que sa dérivée est f. □

Remarques IV.5.

1. *La définition qu'on avait donné initialement (dans le chapitre sur les primitives) coïncide donc avec celle qu'on donne ici.*
2. *Il faut cependant bien prendre garde au fait que f est continue : pour f seulement continue par morceaux, la fonction $F : x \mapsto \int_a^x f(t)\mathrm{d}t$ n'est pas dérivable partout. Par exemple, si on pose $F : x \mapsto \int_0^x \lfloor t \rfloor \mathrm{d}t$, on obtient une fonction qui est dérivable en tout point sauf en les entiers, car alors ses dérivées à gauche et à droite sont différentes.*



Et on pouvait anticiper un tel résultat : on avait vu qu'une fonction dérivée doit vérifier le théorème des valeurs intermédiaires, ce qui n'est pas le cas de la fonction partie entière, qui ne peut donc pas être une dérivée.

3. *Il faut bien que f soit continue pour que F soit dérivable. Mais si f est seulement continue par morceaux, on a tout de même que F est continue. L'idée étant que f est bornée au voisinage de tout point (une fonction continue par morceaux sur un segment étant bornée), et si on considère M une telle borne, alors sur le même voisinage on voit facilement que F est même M-lipschitzienne (par croissance de l'intégrale).*

Corollaire IV.6. *Si f est continue par morceaux sur un intervalle I, et $a \in I$, alors la fonction $F : x \mapsto \int_a^x f(t)\mathrm{d}t$ est dérivable en tout point où f est continue, et sa dérivée coïncide alors avec f.*

Démonstration. Il suffit de restreindre f (et donc F) à un intervalle sur lequel f est continue, ce qui ramène au résultat précédent. □

Corollaire IV.7. *Si f est continue sur un intervalle I et $a, b \in I$, alors en notant F une primitive quelconque de f sur I on a :*

$$\int_a^b f(t)\mathrm{d}t = F(b) - F(a).$$

Démonstration. Prenons F une primitive de f sur I, qui existe bien comme f est continue, et dont on a vu qu'elle est de la forme $F : x \mapsto \int_{x_0}^x f(t)\mathrm{d}t + y_0$. Alors :

$$F(b) - F(a) = \int_{x_0}^b f(t)\mathrm{d}t + y_0 - \int_{x_0}^a f(t)\mathrm{d}t - y_0 = \int_{x_0}^b f(t)\mathrm{d}t + \int_a^{x_0} f(t)\mathrm{d}t = \int_a^b f(t)\mathrm{d}t.$$

□

Remarque IV.8. *On retrouve ainsi toutes les propriétés déjà énoncées pour l'intégrale d'une fonction continue sur un segment, et notamment l'intégration par parties, le changement de variable, ou les propriétés d'intégrales dépendant de leurs bornes. Ces résultats demandent les mêmes hypothèses que précédemment (notamment le fait d'être $\mathcal{C}^1$ pour faire des intégrations par parties).*
Les résultats s'adaptent alors à des fonctions continues par morceaux en découpant l'intégrale sur les différents segments sur lesquels f est continue, à l'aide de la relation de Chasles.

Proposition IV.9. *Soit f une fonction continue par morceaux sur $\mathbb{R}$, alors :*

1. *si f est paire : pour tout $a \in \mathbb{R}$, on a :*

$$\int_{-a}^a f(t)\mathrm{d}t = 2\int_0^a f(t)\mathrm{d}t.$$

2. *si f est impaire : pour tout $a \in \mathbb{R}$, on a :*

$$\int_{-a}^a f(t)\mathrm{d}t = 0.$$

3. *si f est T-périodique : pour tout $a \in \mathbb{R}$, on a :*

$$\int_a^{a+T} f(t)\mathrm{d}t = \int_0^T f(t)\mathrm{d}t.$$

Démonstration. Se montre par changement de variable ou par dérivée d'une intégrale dépendant de ses bornes (comme montré en début d'année) si la fonction f est continue.
Le cas général s'en déduit en découpant et en utilisant la relation de Chasles. □

Remarque IV.10. *Pour une fonction périodique, cela permet de donner un sens intuitif à la valeur moyenne. En effet, si f est T-périodique, on en déduit que :*

$$\frac{1}{T}\int_0^T f(t)\mathrm{d}t = \lim_{x\to\infty}\frac{1}{x}\int_0^x f(t)\mathrm{d}t = \lim_{x\to\infty}\frac{1}{2x}\int_{-x}^x f(t)\mathrm{d}t$$

qui se montre en encadrant x entre deux réels de la forme nT, $(n+1)T$ et en prenant la limite.

Exemple IV.11. *Étudions la fonction f définie sur $\mathbb{R}_+^*$ par :*

$$\forall x\in\mathbb{R}_+^*,\ f(x)=\int_0^1\sqrt{1+x^2e^{2t}}\mathrm{d}t.$$

Le problème est que la variable apparaît dans l'intégrande (et non dans les bornes). On procède alors à un changement de variable pour la faire passer de l'un à l'autre, en posant $u=xe^t$. On a alors $\mathrm{d}u = xe^t\mathrm{d}t = u\mathrm{d}t$, et donc pour tout $x>0$:

$$f(x)=\int_0^1\sqrt{1+x^2e^{2t}}\mathrm{d}t=\int_x^{ex}\frac{\sqrt{1+u^2}}{u}\mathrm{d}t$$

qui peut être manipulée à la manière du théorème fondamental de l'analyse.
En notant $g:u\mapsto\dfrac{\sqrt{1+u^2}}{u}$ (qui est continue sur $\mathbb{R}_+^*$) et G une primitive de g sur $\mathbb{R}_+^*$, on a alors :

$$\forall x>0,\ f(x)=G(ex)-G(x)$$

et donc, par composition, la fonction f est de classe $\mathcal{C}^1$ et vérifie :

$$\forall x>0,\ f'(x)=eG'(ex)-G'(x)=eg(ex)-g(x)=\frac{\sqrt{1+e^2x^2}-\sqrt{1+x^2}}{x}.$$

et on peut ensuite obtenir une expression explicite de f en fonction de x en intégrant chaque terme séparément, avec les changements de variables $u=\mathrm{Argsh}(ex)$ et $u=\mathrm{Argsh}(x)$

IV.2 Formules de Taylor globales

Théorème IV.12 (Formule de Taylor avec reste intégral)**.** *Si f est une fonction de classe $\mathcal{C}^{n+1}$ sur un intervalle I, et $a\in I$, alors pour tout $x\in I$ on a :*

$$\begin{aligned} f(x) &= f(a)+f'(a)(x-a)+\frac{f''(a)}{2}(x-a)^2+\cdots+\frac{f^{(n)}(a)}{n!}(x-a)^n+\int_a^x f^{(n+1)}(t)\frac{(x-t)^n}{n!}\mathrm{d}t \\ &= \sum_{k=0}^n\frac{f^{(k)}(a)}{k!}(x-a)^k+\int_a^x f^{(n+1)}(t)\frac{(x-t)^n}{n!}\mathrm{d}t \end{aligned}.$$

Démonstration. On procède par récurrence sur $n\in\mathbb{N}$.
Si $n=0$: soit f une fonction de classe $\mathcal{C}^1$. Alors f est une primitive de f', qui est continue, donc pour tous $a,x\in I$:

$$\int_a^x f'(t)\mathrm{d}t=f(x)-f(a)$$

ce qui donne bien la formule voulue, à savoir : $f(x)=f(a)+\int_a^x f'(t)\mathrm{d}t$ (avec la convention que $0!=1$).
Soit $n\in\mathbb{N}$ tel que la formule soit vraie pour tout fonction f de classe C^{n+1}, et considérons f de classe $\mathcal{C}^{n+2}$.

Alors en particulier f est de classe $\mathcal{C}^{n+1}$, donc on peut lui appliquer l'hypothèse de récurrence, donc :

$$f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k + \int_a^x f^{(n+1)}(t)\frac{(x-t)^n}{n!}\mathrm{d}t.$$

On procède alors par intégration par parties : les fonctions $f^{(n+1)}$ et $t \mapsto -\dfrac{(x-t)^{n+1}}{(n+1)!}$ sont de classe $\mathcal{C}^1$, et de dérivées respectives $f^{(n+2)}$ et $t \mapsto \dfrac{(x-t)^n}{n!}$, et donc :

$$\begin{aligned}\int_a^x f^{(n+1)}(t)\frac{(x-t)^n}{n!}\mathrm{d}t &= \left[-f^{(n+1)}(t)\frac{(x-t)^{n+1}}{(n+1)!}\right]_a^x + \int_a^x f^{(n+2)}(t)\frac{(x-t)^{n+1}}{(n+1)!}\mathrm{d}t \\ &= \frac{f^{(n+1)}(a)}{(n+1)!}(x-a)^{n+1} + \int_a^x f^{(n+2)}(t)\frac{(x-t)^{n+1}}{(n+1)!}\mathrm{d}t\end{aligned}.$$

Ce qui donne bien la formule voulue en réinjectant dans l'égalité précédente. □

Remarque IV.13. *On retrouve (et c'est normal) la partie régulière de la formule de Taylor–Young. La différence entre ces deux formules de Taylor est l'estimation de l'écart entre la fonction et sa partie régulière : la formule de Taylor–Young dit seulement que l'écart est "petit" si on se place au voisinage de a (et a donc une nature locale), tandis que celle avec reste intégral donne l'écart de manière exacte, et en n'importe quel point (d'où sa nature globale).*

Corollaire IV.14 (Inégalité de Taylor–Lagrange)**.** *Si f est de classe $\mathcal{C}^{(n+1)}$ sur un intervalle I, et $a, b \in I$ tels que $|f^{(n+1)}|$ est majorée par $M \in \mathbb{R}_+$ entre a et b, alors :*

$$\left| f(b) - \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(b-a)^k \right| \leq M\frac{|b-a|^{n+1}}{(n+1)!}.$$

Démonstration. Par formule de Taylor avec reste intégral, on a déjà :

$$f(b) - \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(b-a)^k = \int_a^b f^{(n+1)}(t)\frac{(b-t)^n}{n!}\mathrm{d}t.$$

Si $a \leq b$, alors par inégalité triangulaire on a :

$$\left|\int_a^b f^{(n+1)}(t)\frac{(b-t)^n}{n!}\mathrm{d}t\right| \leq \int_a^b \left|f^{(n+1)}(t)\frac{(b-t)^n}{n!}\right|\mathrm{d}t \leq \int_a^b M\frac{(b-t)^n}{n!}\mathrm{d}t = M\frac{(b-a)^{n+1}}{(n+1)!} = M\frac{|b-a|^{n+1}}{(n+1)!}.$$

Si $a > b$, on utilise à nouveau l'inégalité triangulaire, en échangeant les bornes des intégrales pour qu'elles soient dans le bon sens. On trouve le même résultat, ce qui prouve l'inégalité de Taylor–Lagrange. □

V Extension aux fonctions à valeurs complexes

Définition V.1. *On dit qu'une fonction $f : [a,b] \to \mathbb{C}$ est **continue par morceaux** si les fonctions $\mathrm{Re}(f)$ et $\mathrm{Im}(f)$ le sont.*

Définition V.2. *Étant donnée $f : [a,b] \to \mathbb{C}$ continue par morceaux, on définit **l'intégrale de f entre a et b** comme :*

$$\int_a^b f(t)\mathrm{d}t = \int_a^b \mathrm{Re}(f)(t)\mathrm{d}t + i\int_a^b \mathrm{Im}(f)(t)\mathrm{d}t.$$

Remarque V.3. *On peut aussi revenir aux intégrales de* $\mathrm{Re}(f)$ *et* $\mathrm{Im}(f)$ *à partir de celle de* f*, en constatant que :*

$$\mathrm{Re}\left(\int_a^b f(t)\mathrm{d}t\right) = \int_a^b \mathrm{Re}(f)(t)\mathrm{d}t \text{ et } \mathrm{Im}\left(\int_a^b f(t)\mathrm{d}t\right) = \int_a^b \mathrm{Im}(f)(t)\mathrm{d}t.$$

Proposition V.4. *L'intégrale ainsi étendue aux fonctions à valeurs complexes vérifie la propriété de linéarité, la relation de Chasles ainsi que l'inégalité triangulaire.*

Démonstration. La linéarité et la relation de Chasles se montrent facilement par les propriétés analogues pour les fonctions à valeurs réelles (en les appliquant à $\mathrm{Re}(f)$ et $\mathrm{Im}(f)$.
Pour l'inégalité triangulaire, considérons f continue par morceaux sur $[a,b]$ à valeurs dans $\mathbb{C}$. Notons $\theta \in \mathbb{R}$ u argument de $\int_a^b f(t)\mathrm{d}t$. Alors :

$$\int_a^b f(t)\mathrm{d}t = e^{i\theta}\left|\int_a^b f(t)\mathrm{d}t\right|.$$

Et on peut alors se ramener au cas réel, et utiliser l'inégalité triangulaire pour l'intégrale de fonctions à valeurs réelles, comme :

$$\begin{array}{rcl}\left|\int_a^b f(t)\mathrm{d}t\right| &=& e^{-i\theta}\int_a^b f(t)\mathrm{d}t \\ &=& \int_a^b f(t)e^{-i\theta}\mathrm{d}t \\ &=& \mathrm{Re}\left(\int_a^b f(t)e^{-i\theta}\mathrm{d}t\right) \\ &=& \int_a^b \mathrm{Re}(f(t)e^{-i\theta})\mathrm{d}t \\ &\leq& \int_a^b |f(t)e^{-i\theta}|\mathrm{d}t = \int_a^b |f(t)|\mathrm{d}t\end{array}$$

ce qui donne bien l'inégalité voulue. □

Remarque V.5. *On perd certains résultats propres à* $\mathbb{R}$*, notamment ceux liés à la relation d'ordre sur* $\mathbb{R}$ *(comme la positivité ou la croissance de l'intégrale).*
Le théorème fondamental de l'analyse, même si sa preuve reposait sur le théorème des valeurs intermédiaires, reste vrai pour une fonction à valeur complexe, en regardant séparément ses parties réelle et imaginaire.
Et les formules de Taylor (avec reste intégral on l'inégalité de Taylor–Lagrange) restent vraies, comme elles reposent sur des intégrations par parties (qui restent valables par linéarité) et l'inégalité triangulaire (dont on vient de voir qu'elle reste vraie).
En revanche, l'égalité de Taylor–Lagrange deviendrait fausse, à la manière du théorème de Rolle (dont il s'agit d'une généralisation).

VI Sommes de Riemann

Définition VI.1. *Étant donné* $[a,b]$ *un segment, on appelle* ***subdivision pointée*** *de* $[a,b]$ *la donnée d'un couple* $(\sigma,(t_i)_{i\in[\![0;n-1]\!]})$ *où* $\sigma = (x_i)_{i\in[\![0;n]\!]}$ *est une subdivision de* $[a,b]$*, et* $(t_i)_{i\in[\![0;n-1]\!]}$ *est une famille d'éléments de* $[a,b]$ *satisfaisant :* $\forall i \in [\![0;n-1]\!],\ t_i \in [x_i;x_{i+1}]$.
On définira alors le pas de s*, noté* $\delta(s)$*, comme le pas de* σ*.*

Définition VI.2 (Somme de Riemann)**.** *Si* $f \in \mathcal{C}_{pm}([a,b])$ *et si* $(\sigma,(t_i)_{i\in[\![0;n-1]\!]})$ *est une subdivision pointée de* $[a,b]$*, on lui associe la* ***somme de Riemann*** *notée* $R(f,s)$ *comme la quantité :*

$$R(f,s) = \sum_{i=0}^{n-1}(x_{i+1}-x_i)f(t_i).$$

Remarque VI.3. *En pratique, on travaillera souvent avec les subdivisions régulières, et avec les subdivisions pointées associées en prenant $t_i = x_i$ ou $t_i = x_{i+1}$, c'est-à-dire qu'on considèrera les deux sommes de Riemann suivantes :*

$$\frac{b-a}{n}\sum_{k=0}^{n-1} f\left(a+k\frac{b-a}{n}\right) \text{ et } \frac{b-a}{n}\sum_{k=1}^{n} f\left(a+k\frac{b-a}{n}\right).$$

Proposition VI.4. *Si f est une fonction continue sur $[a,b]$, et $\varepsilon > 0$, il existe $\eta > 0$ tel que, pour toute subdivision pointée s de $[a,b]$, si $\delta(s) \leq \eta$ alors :*

$$\left|\int_a^b f(t)\mathrm{d}t - R(f,s)\right| \leq \varepsilon.$$

Démonstration. Comme f est continue, par théorème de Heine elle est uniformément continue. Notons $\eta > 0$ qui correspond à la définition de l'uniforme continuité pour f avec $\dfrac{\varepsilon}{b-a} > 0$, et montrons qu'un tel η convient.
Soit $i \in [\![0; n-1]\!]$ et $t \in [x_i; x_{i+1}]$. Alors on a : $|t - t_i| \leq x_{i+1} - x_i \leq \eta$, et donc $|f(t) - f(t_i)| \leq \dfrac{\varepsilon}{b-a}$. Et ainsi :

$$\begin{aligned}
\left|\int_a^b f(t)\mathrm{d}t - \sum_{i=0}^{n-1}(x_{i+1}-x_i)f(t_i)\right| &= \left|\sum_{i=0}^{n-1}\int_{x_{i+1}}^{x_i} f(t)\mathrm{d}t - \sum_{i=0}^{n-1}(x_{i+1}-x_i)f(t_i)\right| \\
&= \left|\sum_{i=0}^{n-1}\int_{x_{i+1}}^{x_i} (f(t)-f(t_i))\,\mathrm{d}t\right| \\
&\leq \sum_{i=0}^{n-1}\int_{x_{i+1}}^{x_i} |f(t)-f(t_i)|\mathrm{d}t \\
&\leq \sum_{i=0}^{n-1}\int_{x_{i+1}}^{x_i} \frac{\varepsilon}{b-a}\mathrm{d}t \\
&\leq \int_a^b \frac{\varepsilon}{b-a}\mathrm{d}t = \varepsilon
\end{aligned}$$

ce qui donne bien le résultat. □

Remarque VI.5. *Ce résultat veut dire que l'on peut approcher de manière arbitrairement proche une intégrale (d'une fonction continue) par une somme de Riemann quelconque, à condition que le pas soit suffisamment petit.*
On peut aussi interpréter ce résultat en termes de limites :

$$R(s,f) \underset{\delta(s)\to 0}{\to} \int_a^b f(t)\mathrm{d}t.$$

Théorème VI.6. *Si f est une fonction continue par morceaux sur le segment $[a,b]$, alors :*

$$\int_a^b f(t)\mathrm{d}t = \lim_{n\to+\infty}\frac{b-a}{n}\sum_{k=0}^{n-1} f\left(a+k\frac{b-a}{n}\right) = \lim_{n\to+\infty}\frac{b-a}{n}\sum_{k=1}^{n} f\left(a+k\frac{b-a}{n}\right).$$

Démonstration. Notons déjà que, par relation de Chasles, en découpant l'intégrale en des intervalles sur lesquels f est continue, on peut se ramener au cas où f est continue.
Et si f est continue, on applique le résultat précédent, en notant que les deux sommes dont on cherches les limites sont des sommes de Riemann associées aux subdivision régulières : elles sont un pas de $\dfrac{b-a}{n}$, qui tend vers 0 quand n tend vers $+\infty$, ce qui donne le résultat par la proposition précédente. □

Remarque VI.7. *On aura parfois des sommes légèrement différentes, comme par exemple :*

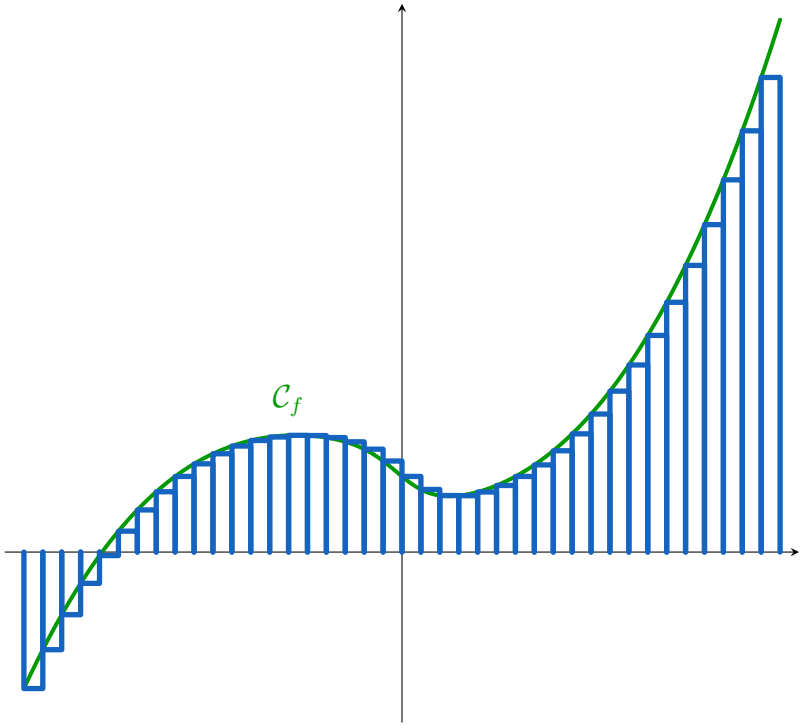
$$\frac{b-a}{n}\sum_{k=0}^{n} f\left(a+k\frac{b-a}{n}\right).$$

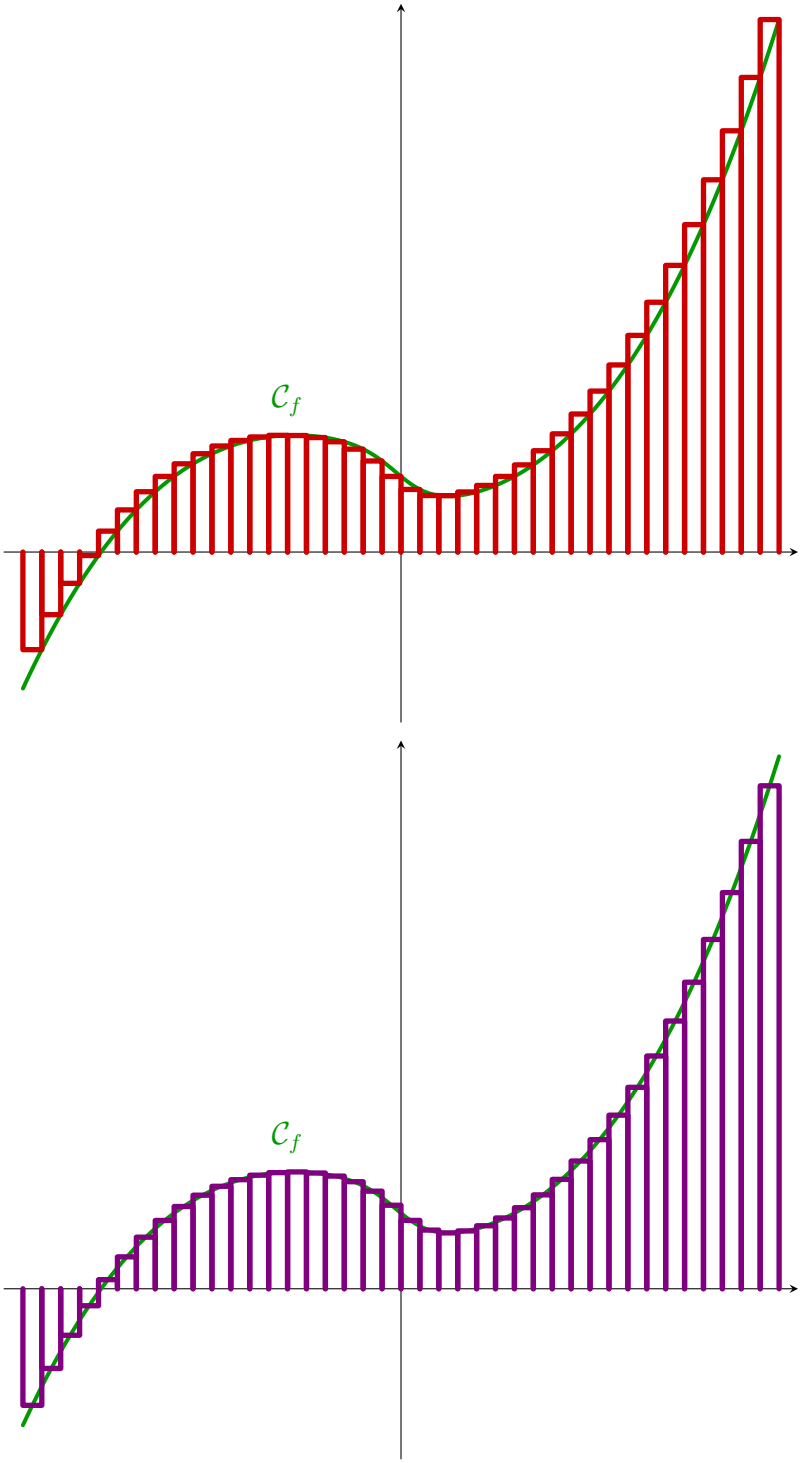
On essaie alors de se ramener aux sommes de Riemann, en calculant explicitement l'écart entre la somme considérée et une somme de Riemann.
Ici, l'écart est de $f(a)\cdot\dfrac{b-a}{n}$*, qui tend vers* 0*, donc on trouve :*

$$\int_a^b f(t)\mathrm{d}t = \lim_{n\to+\infty}\frac{b-a}{n}\sum_{k=0}^{n} f\left(a+k\frac{b-a}{n}\right).$$

Et le résultat se généralise bien sûr à toute somme de Riemann dont le pas tend vers 0*.*

Remarque VI.8. *Les deux sommes considérées ici et dont on prend les limites se comprennent bien graphiquement : on découpe* $[a,b]$ *en* n *parts égales, et on prend la fonction en escalier qui prend les mêmes valeurs que* f *à gauche dans le premier cas, ou à droite dans le second.*
On parle alors de ***méthode des rectangles à gauche*** *dans le premier cas, et de* ***méthode des rectangles à droite*** *dans le second. Il existe d'autres méthodes plus générales : l'idée est que l'on approxime ici sur chaque tronçon la fonction* f *par une fonction constante. On pourrait l'approximer par la constante prose au point milieu du rectangle (on parle de* ***méthode du point milieu****) ou par des polynômes de degrés arbitrairement grands, et de coefficients bien choisis (qui s'inscrivent dans le cadre général des méthode de Newton–Coates). Ces méthodes sont compliquées à gérer dans le cas général, mais se comprennent très bien avec des fonctions suffisamment régulières (par exemple des polynômes de degré suffisamment petit, sur lesquelles elles donnent des résultats exacts).*





Exemples VI.9.

1. *Étudions la limite de la suite* $(u_n)_{n\geq 1}$ *définie par :* $u_n = n \cdot \sum_{k=1}^{n} \frac{1}{(n+k)^2}$.

   On a :

$$u_n = \frac{1}{n}\sum_{k=1}^{n} \frac{1}{(1+\frac{k}{n})^2} = \frac{1-0}{n}\sum_{k=1}^{n} f\left(\frac{k}{n}\right)$$

   où $f : x \mapsto \dfrac{1}{(1+x)^2}$, *qui est continue sur* $[0;1]$. *Et en reconnaissant une somme de Riemann, on a donc que* (u_n) *tend vers :*

$$\int_0^1 f(t)\mathrm{d}t = \int_0^1 \frac{1}{(1+t)^2}\mathrm{d}t = \left[\frac{-1}{1+x}\right]_0^1 = \frac{1}{2}.$$

2. *Étudions la suite* $(u_n)_{n\geq 1}$ *définie par :* $u_n = \sum_{k=1}^{n} \frac{n}{n^2+k^2}$.

On a :

$$u_n = \frac{1}{n}\sum_{k=1}^{n} \frac{1}{1+\frac{k^2}{n^2}} = \frac{1-0}{n}\sum_{k=1}^{n} f\left(\frac{k}{n}\right)$$

où $f : x \mapsto \dfrac{1}{1+x^2}$, *qui est continue sur* $[0;1]$. *En en reconnaissant une somme de Riemann, on a donc que* (u_n) *tend vers :*

$$\int_0^1 f(t)\mathrm{d}t = \int_0^1 \frac{1}{1+t^2}\mathrm{d}t = \frac{\pi}{4}.$$

On peut aller plus loin et déterminer la vitesse de convergence de (u_n) *en étudiant la suite de terme général* $u_n - \dfrac{\pi}{4}$. *Pour tout* $n \in \mathbb{N}^*$, *on a :*

$$\begin{aligned} u_n - \frac{\pi}{4} &= \sum_{k=1}^{n} \frac{1/n}{1+\left(\frac{k}{n}\right)^2} - \int_0^1 \frac{1}{1+x^2}\mathrm{d}x \\ &= \sum_{k=1}^{n} \left(\frac{1/n}{1+\left(\frac{k}{n}\right)^2} - \int_{(k-1)/n}^{k/n} \frac{1}{1+x^2}\mathrm{d}x \right) \\ &= \sum_{k=1}^{n} \int_{(k-1)/n}^{k/n} (f(k/n) - f(x))\mathrm{d}x \end{aligned}$$

où on reprend $f : x \mapsto \dfrac{1}{1+x^2}$.

Mais par inégalité des accroissements finis (ou inégalité de Taylor–Lagrange à l'ordre 1, ce qui revient au même) la fonction f *étant de classe* $\mathcal{C}^1$ *sur* $[0;1]$ *de dérivée* $f' : x \mapsto \dfrac{-2x}{(1+x^2)^2}$, *et donc* $|f'| \leq 2$ *(par majoration un peu brutale du numérateur, et minoration aussi brutale du dénominateur, en valeur absolue) ce qui donne :*

$$\forall k \in [\![1;n]\!],\ \forall x \in \left[\frac{(k-1)}{n}; \frac{k}{n}\right],\ |f(k/n) - f(x)| \leq 2|k/n - x| = 2(k/n - x)$$

et en réinjectant on trouve finalement que :

$$|u_n - \frac{\pi}{4}| \leq \sum_{k=1}^{n} \int_{(k-1)/n}^{k/n} |f(k/n) - f(x)|\mathrm{d}x \leq \sum_{k=1}^{n} \int_{(k-1)/n}^{k/n} 2|k/n - x|\mathrm{d}x = \sum_{k=1}^{n} \frac{1}{n^2} = \frac{1}{n}$$

et donc u_n *converge vers* $\dfrac{\pi}{4}$ *avec* $u_n - \dfrac{\pi}{4} = \mathrm{O}\left(\dfrac{1}{n}\right)$.

Chapitre 24

Déterminants et groupe symétrique

I Le(s) groupe(s) symétrique(s)

I.1 Les permutations

Définition I.1. *Pour $n \in \mathbb{N}^*$, on appelle **groupe symétrique**, noté S_n (ou parfois $\mathfrak{S}_n$), l'ensemble des bijections de $[\![1;n]\!]$ dans lui-même.*

Proposition I.2. *Muni de la composition, S_n est un groupe de cardinal $n!$.*

Démonstration. L'aspect groupe a déjà été montré.
Le cardinal sera montré plus tard (dans le chapitre sur les dénombrements). □

Définition I.3. *Un élément $\sigma \in S_n$ sera appelé **permutation**. On la représentera alors de la manière suivante :*

$$\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n-1) & \sigma(n) \end{pmatrix}.$$

*et on appellera **support** de σ, noté $\mathrm{Supp}(\sigma)$, comme l'ensemble des éléments de qui ne sont pas fixés par σ :*

$$\mathrm{Supp}(\sigma) = \{k \in [\![1;n]\!] \,|\, \sigma(k) \neq k\}.$$

Remarque I.4. *Pour simplifier les notations, dans la notation précédente pour σ, on pourra ne faire apparaître que les éléments du support de σ (mais il y a alors une ambiguïté sur la valeur de n).*

Exemples I.5.

1. *Si $n = 1$, le seul élément de S_n est* id.
2. *Si $n = 2$, il y a deux éléments dans S_2, à savoir* id *et $\tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} : i \mapsto 3 - i$. Et $S_2 \simeq \mathbb{U}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ est un groupe abélien.*
3. *Si $n \geq 3$, alors S_n est non abélien, et devient rapidement compliqué. On peut noter que S_3 est l'unique groupe non abélien (à isomorphisme de groupe près) de cardinal 6.*

Proposition I.6. *Deux éléments de S_n de supports disjoints commutent si leurs supports sont disjoints.*

Démonstration. On considère $\sigma, \tau \in S_n$ de supports disjoints et $i \in S_n$:
— si $i \in \mathrm{Supp}(\sigma)$: alors $i \neq \sigma(i)$, puis par injectivité de σ on a : $\sigma(i) \neq \sigma(\sigma(i))$, donc $\sigma(i) \in \mathrm{Supp}(\sigma)$. Et ainsi $i, \sigma(i) \notin \mathrm{Supp}(\tau)$ donc : $\tau(i) = i$ et $\tau \circ \sigma(i) = \sigma(i)$. En composant avec σ on trouve donc : $\tau \circ \sigma(i) = \sigma \circ \tau(i)$.
— si $i \in \mathrm{Supp}(\tau)$: on procède de même en échangeant les rôles de τ et de σ.
— si $i \notin \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\tau)$: alors $i = \sigma(i) = \tau(i)$ et donc $\tau \circ \sigma(i) = \sigma \circ \tau(i)$.

Et ainsi on a bien que σ et τ commutent. □

Remarque I.7. *La réciproque est fausse : on peut prendre n'importe quel élément non trivial qui commute avec lui-même et avec ses puissances. Ou on peut aussi faire des exemples moins triviaux en considérant par exemple dans S_5 les permutations :*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} \text{ et } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$$

dont il n'est pas compliqué de voir qu'elles commutent, et qui ne sont pas puissance l'une de l'autre.

I.2 Cycles et transpositions

Proposition-Définition I.8. *Si $p \in [\![2; n]\!]$ et $a_1, \dots, a_p$ des éléments deux-à-deux distincts de $[\![1; n]\!]$, on lui associe l'application :*

$$\sigma : \begin{cases} [\![1;n]\!] & \to & [\![1;n]\!] \\ k & \mapsto & \begin{cases} k & si \quad k \notin \{a_1, \dots, a_p\} \\ a_{i+1} & si \quad k = a_i \text{ pour } i \in [\![1; p-1]\!] \\ a_1 & si \quad k = a_p \end{cases} \end{cases}$$

Alors σ ainsi définie est un élément de S_n qu'on notera $\begin{pmatrix} a_1 & a_2 & \dots & a_p \end{pmatrix}$.
*Les permutations de la forme précédentes sont appelées **cycles** (ou p-cycles, ou cycles de longueur p).*

Démonstration. Il faut seulement montrer la bijectivité de σ. Comme σ est définie entre deux ensembles finis de même cardinal (à savoir $[\![1; n]\!]$).
Et la surjectivité est claire. □

Exemple I.9. *Considérons $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 1 & 5 & 4 \end{pmatrix}$ correspond au 4-cycle : $\begin{pmatrix} 1 & 3 & 6 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 6 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 6 & 4 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 1 & 3 & 6 \end{pmatrix} =$.*
Et plus généralement, tout p-cycle s'écrit de p manières différentes.

Remarque I.10. *Un p-cycle a un support de cardinal p (constitué de tous les a_i en reprenant les notations précédentes), donc laisse $n - p$ points fixes. Mais la réciproque est fausse.*

Proposition I.11. *L'inverse d'un p-cycle est un p-cycle.*

Démonstration. Considérons $\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_p \end{pmatrix}$. Alors on a : $\sigma^{-1} = \begin{pmatrix} a_p & a_{p-1} & \dots & a_2 & a_1 \end{pmatrix}$ qui est donc bien un p-cycle. □

Remarque I.12. *Les puissances quelconques d'un p-cycle ne sont pas toujours des cycles. Par exemple, si on prend $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}$ alors :*

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

qui n'est pas un cycle.

Définition I.13. *Une **transposition** est un 2-cycle.*

Proposition I.14. *Les transpositions sont exactement les éléments de S_n dont le support est de cardinal 2. De plus elles sont involutives.*

Démonstration. Si on considère $\tau = \begin{pmatrix} i & j \end{pmatrix}$ une transposition, alors $\text{Supp}(\tau) = \{i, j\}$ est de cardinal 2, et on a directement que $\tau^2 = \text{id}$.
Inversement, si $\tau \in S_n$ a un support de cardinal 2 : notons $\text{Supp}(\tau) = \{i, j\}$. Comme $\tau(i) \neq i$, alors nécessairement $\tau(i) = j$, et de même $\tau(j) = i$, ce qui donne $\tau = \begin{pmatrix} i & j \end{pmatrix}$. □

I.3 Orbites et décomposition en cycles

Définition I.15. *Si $\sigma \in S_n$ et $i \in [\![1;n]\!]$, on appelle* ***orbite*** *de i sous (l'action de) σ l'ensemble :*

$$\mathcal{O}_\sigma(i) = \{\sigma^k(i) \,|\, k \in \mathbb{Z}\}.$$

Exemple I.16. *Prenons* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix}$. *Alors les orbites sont* $\{1,6\}$, $\{2,4,5\}$ *et* $\{3\}$.

Proposition I.17. *On fixe $\sigma \in S_n$ et on définit sur $[\![1;n]\!]$ la relation $\mathcal{R}_\sigma$ définie par :*

$$i\mathcal{R}_\sigma j \Leftrightarrow \exists k \in \mathbb{Z},\ \sigma^k(i) = j.$$

Alors $\mathcal{R}_\sigma$ est une relation d'équivalence. De plus, les classes d'équivalences sont les orbites sous σ.

Démonstration. Le fait qu'on a une relation d'équivalence est immédiat :
- réflexivité : $i = \sigma^0(i)$;
- symétrie : si $j = \sigma^k(i)$, alors $i = \sigma^{-k}(j)$;
- transitivité : si $j = \sigma^k(i)$ et $l = \sigma^{k'}(j)$, alors $l = \sigma^{k+k'}i$.

Et on a par définition :

$$\mathrm{cl}(i) = \{j \in [\![1,n]\!] \,|\, \exists k \in \mathbb{Z},\ j = \sigma^k(i)\} = \{\sigma^k(i) \,|\, k \in \mathbb{Z}\} = \mathcal{O}_\sigma(i).$$

□

Théorème I.18. *Tout permutation s'écrit comme produit de cycles à supports disjoints. De plus, une telle écriture est unique à l'ordre près des cycles.*

Démonstration. La preuve repose sur le lemme suivant :

Lemme I.19. *Si $\sigma \in S_n$ et $\mathcal{O}$ est une orbite sous σ non réduite à un singleton. Alors $\sigma|_\mathcal{O}$ est un cycle de support $\mathcal{O}$.*

Preuve du lemme : Notons $i \in [\![1;n]\!]$ tel que $\mathcal{O} = \mathcal{O}_\sigma(i) = \{\sigma^k(i) \,|\, k \in \mathbb{Z}\}$. On considère $p \in \mathbb{N}^*$ le plus petit possible tel que $\sigma^p(i) = i$, qui existe bien car $\mathcal{O}$ est un sous-ensemble de $[\![1;n]\!]$, donc est fini, donc il existe $k, l \in \mathbb{Z}$ distincts avec $\sigma^k(i) = \sigma^l(i)$.
Donc l'ensemble $\{k \in \mathbb{N}^* \,|\, \sigma^k(i) = i\}$ est une partie non vide (qui contient $|k-l|$) de $\mathbb{N}$, donc possède un plus petit élément.
Par division euclidienne, on trouve alors que :

$$\mathcal{O} = \{\sigma^k(i) \,|\, k \in [\![0; p-1]\!]\}$$

et tous les éléments dans la description ci-dessus sont deux-à-deux distincts (sinon cela contredirait la minimalité de p).
Et on a ainsi que :

$$\sigma|_\mathcal{O} = \begin{pmatrix} i & \sigma(i) & \sigma^2(i) & \dots & \sigma^{p-1}(i) \end{pmatrix}$$

qui est bien un cycle de support $\mathcal{O}$. □

On va construire grâce au lemme une décomposition, et montrer qu'elle est unique (à l'ordre près) :
- existence : comme $\mathcal{R}_\sigma$ est une relation d'équivalence, ses classes (qui sont les orbites) forment une partition de $[\![1;n]\!]$. Plus précisément, les orbites non réduites à un singleton forment une partition du support de σ. On écrit alors :

$$\mathrm{Supp}(\sigma) = \cup_{i=1}^p \mathcal{O}_i$$

et pour tout $i \in [\![1;p]\!]$, on note σ_i la permutation définie par :

$$\sigma : x \mapsto \begin{cases} \sigma(x) & \text{si } x \in \mathcal{O}_i \\ x & \text{sinon} \end{cases}$$

qui est un cycle de support $\mathcal{O}_i$ (d'après le lemme).
Comme les orbites de σ sont deux-à-deux disjointes, les supports des σ_i aussi (et donc ils commutent).
Montrons que $\sigma = \sigma_1 \circ \cdots \circ \sigma_p$. Pour cela, soit $x \in [\![1;n]\!]$:

— si $x \notin \text{Supp}(\sigma)$: alors on a déjà que $\sigma(x) = x$. Mais x n'est dans aucun des supports des σ_i, donc pour tout i on a également $\sigma_i(x) = x$, et par composition $\sigma(x) = \sigma_1 \circ \cdots \circ \sigma_p(x)$;

— si $x \in \text{Supp}(\sigma)$: notons $i \in [\![1;p]\!]$ (unique) tel que $x \in \mathcal{O}_i$. Et alors par commutativité des σ_i :

$$\sigma_1 \circ \ldots \sigma_p(x) = \sigma_i \left(\underbrace{\sigma_1 \circ \cdots \circ \sigma_p}_{\text{avec tous les indices sauf} i} \quad (x) \right) = \sigma_i(x) = \sigma(x)$$

ce qui donne bien la décomposition voulue, et assure l'existence.

— unicité : si $\sigma = \sigma_1 \circ \cdots \circ \sigma_p$ est un produit de cycles à supports disjoints, alors on a déjà que $\text{Supp}(\sigma) = \cup_{i=1}^{p} \text{Supp}(\sigma_i)$ et cette écriture correspond exactement à la décomposition de $\text{Supp}(\sigma)$ en orbites.
Donc les supports de σ_i sont entièrement déterminés par σ, et leur nombre aussi (il y en a autant que d'orbites non déduites à un singleton).
Enfin on a pour tout i que :

$$\sigma_i|_{\text{Supp}(\sigma_i)} = \sigma|_{\text{Supp}(\sigma_i)}$$

comme les autres cycles ont une action triviale sur $\text{Supp}(\sigma_i)$, ce qui détermine entièrement σ_i.
D'où l'unicité.

□

Remarque I.20. *Le point important dans cette démonstration est qu'elle donne une méthode pour déterminer explicitement l'écriture d'une permutation en produit de cycles.*

Exemple I.21. *Reprenons* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix}$. *Alors on a :*

$$\sigma = \begin{pmatrix} 1 & 6 \end{pmatrix} \begin{pmatrix} 2 & 4 & 5 \end{pmatrix} \begin{pmatrix} 3 \end{pmatrix} = \begin{pmatrix} 1 & 6 \end{pmatrix} \begin{pmatrix} 2 & 4 & 5 \end{pmatrix}$$

Et on peut ensuite calculer les ordres des permutations. Pour la permutation σ *on a pour tout* $k \in \mathbb{Z}$ *que :*

$$\sigma^k = \begin{pmatrix} 1 & 6 \end{pmatrix}^k \begin{pmatrix} 2 & 4 & 5 \end{pmatrix}^k$$

et donc $\sigma^k = \text{id} \Leftrightarrow k \in 6\mathbb{Z}$.

Remarque I.22. *Plus généralement, si* σ *est le produit de cycles de longueurs* $p_1, \ldots, p_r$, *alors* σ *est d'ordre* $\text{ppcm}(p_1, \ldots, p_r)$.

Corollaire I.23. *Toute permutation s'écrit comme produit de transpositions.*

Démonstration. Du fait du théorème précédente, il suffit de montrer que tout cycle s'écrit comme produit de transpositions.
Considérons le cycle $\sigma = \begin{pmatrix} a_1 & a_2 & \ldots & a_p \end{pmatrix}$.
Un calcul directe montre que :

$$\sigma = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \begin{pmatrix} a_2 & a_3 \end{pmatrix} \ldots \begin{pmatrix} a_{p-2} & a_{p-1} \end{pmatrix} \begin{pmatrix} a_{p-1} & a_p \end{pmatrix}$$

□

Remarques I.24.

1. *Une telle écriture n'est évidemment pas unique. Prenons par exemple* id *qu'on peut toujours écrire* $\tau \circ \tau$ *avec* τ *une transposition quelconque.*
   Du fait de l'unicité dans l'écriture précédente, il ne faut pas non plus espérer que les transpositions aient des supports disjoints, ou qu'elles commutent.
2. *Le résultat se comprend bien : on peut réarranger comme on veut un ensemble fini en échangeant les éléments deux par deux. On a même mieux : on pourrait n'échanger que des éléments consécutifs (à la manière du tri à bulles), ce qui revient à ne considérer que les transpositions de la forme* $\begin{pmatrix} i & i+1 \end{pmatrix}$ *(pour* $i \in [\![1; n-1]\!]$*). Et il y a de nombreux autres systèmes de générateurs.*

I.4 Signature d'une permutation

Définition I.25. *Étant donnée* $\sigma \in S_n$*, on définit sa* ***signature****, notée* $\varepsilon(\sigma)$*, comme la quantité :*

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Théorème I.26. *La signature est l'unique morphisme de groupe non trivial de* S_n *dans* $\{-1; 1\}$*.*

Démonstration. Montrons déjà que la signature est un morphisme de groupe non trivial de S_n dans $\{-1; 1\}$:

— elle est à valeurs dans $\{-1; 1\}$: posons $I = \{(i, j) \,|\, 1 \leq i < j \leq n\}$; par bijectivité de σ, on a que l'application :

$$\varphi_\sigma : \left\{ \begin{array}{ccc} I & \to & I \\ (i,j) & \mapsto & \left\{ \begin{array}{lll} (\sigma(i), \sigma(j)) & \text{si} & \sigma(i) < \sigma(j) \\ (\sigma(j), \sigma(i)) & \text{si} & \sigma(j) < \sigma(i) \end{array} \right. \end{array} \right.$$

est injective, donc bijective (en tant qu'application entre deux ensembles finis de même cardinal). Et alors :

$$\prod_{(i,j) \in I} |\sigma(i) - \sigma(j)| = \prod_{(i,j) \in I} |i - j|$$

ce qui donne par quotient : $|\varepsilon(\sigma)| = 1$, donc $\varepsilon(\sigma) \in \{-1; 1\}$.

— c'est un morphisme de groupe : si $\sigma, \tau \in S_n$, alors :

$$\frac{\varepsilon(\sigma\tau)}{\varepsilon(\tau)} = \prod_{i<j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{i - j} \cdot \prod_{i<j} \frac{i - j}{\tau(i) - \tau(j)} = \prod_{i<j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} = \prod_{(i,j) \in \varphi_\tau(I)} \frac{\sigma(i) - \sigma(j)}{i - j} = \varepsilon(\sigma)$$

ce qui montre bien que $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$, et on a bien un morphisme.

— elle est non triviale : on a directement que :

$$\begin{aligned} \varepsilon(\begin{pmatrix} 1 & 2 \end{pmatrix}) &= \prod_{i<j} \frac{\tau(i) - \tau(j)}{i - j} \\ &= \prod_{3 \leq i < j} \frac{\tau(i) - \tau(j)}{i - j} \cdot \prod_{2<j} \frac{\tau(2) - \tau(j)}{2 - j} \cdot \prod_{1<j} \frac{\tau(1) - \tau(j)}{1 - j} \cdot \frac{\tau(1) - \tau(2)}{1 - 2} \\ &= \underbrace{\prod_{3 \leq i < j} \frac{i - j}{i - j}}_{=1} \cdot \underbrace{\prod_{2<j} \frac{1 - j}{2 - j} \cdot \prod_{2<j} \frac{2 - j}{1 - j}}_{=1} \cdot \frac{2 - 1}{1 - 2} = -1 \end{aligned}$$

Pour l'unicité, considérons φ un tel morphisme non trivial. Comme S_n est engendré par les transpositions, il suffit de montrer que toute transposition a pour image -1, l'image des autres permutations découlera par morphisme.

Montrons déjà que toutes les transpositions ont même image. Pour cela, considérons $\begin{pmatrix} i & j \end{pmatrix}$ et $\begin{pmatrix} k & l \end{pmatrix}$ deux transpositions. Comme $i \neq j$ et $k \neq l$, on peut trouver une permutation qui envoie i sur k et j sur l. En notant σ une telle transposition, on a :

$$\sigma^{-1} \begin{pmatrix} i & j \end{pmatrix} \sigma = \begin{pmatrix} k & l \end{pmatrix}$$

et donc :

$$\varphi(\begin{pmatrix} k & l \end{pmatrix}) = \varphi(\sigma^{-1} \begin{pmatrix} i & j \end{pmatrix} \sigma) = \underbrace{\varphi(\sigma^{-1})}_{=(\varphi(\sigma))^{-1}} \varphi(\begin{pmatrix} i & j \end{pmatrix})\varphi(\sigma) = \underbrace{\varphi(\sigma^{-1})\varphi(\sigma)}_{=1} \varphi(\begin{pmatrix} i & j \end{pmatrix}) = \varphi(\begin{pmatrix} i & j \end{pmatrix})$$

et ainsi toutes les transpositions ont même image. Soit elles ont pour image 1, et dans ce cas φ est trivial, soit elles ont pour image -1 et alors $\varphi = \varepsilon$.
Ce qui montre bien l'unicité. □

Remarque I.27. *Le résultat sur les transpositions se généralise à des permutations quelconques : étant données deux permutations σ_1, σ_2, elles sont conjuguées (c'est-à-dire que l'on peut trouver $\sigma \in S_n$ telle que $\sigma_1 = \sigma^{-1}\sigma_2\sigma$) si, et seulement si, leurs décompositions en cycles à supports disjoints font intervenir autant de cycles de chaque longueur.*

Corollaire I.28. *Si $\sigma \in S_n$ s'écrit comme le produit de transpositions $\sigma = \tau_1 \circ \ldots \tau_p$, alors la parité de p est donnée par : $(-1)^p = \varepsilon(\sigma)$.*

Remarque I.29. *On avait montré qu'une telle écriture n'était pas unique. Le résultat précédent montre qu'elle a tout de même une certaine rigidité.*

Corollaire I.30. *Un p-cycle a pour signature $(-1)^{p-1}$.*

Démonstration. On avait écrit un p-cycle en produit de $(p-1)$ transpositions. Comme les transpositions sont de signature (-1), le résultat découle par morphisme. □

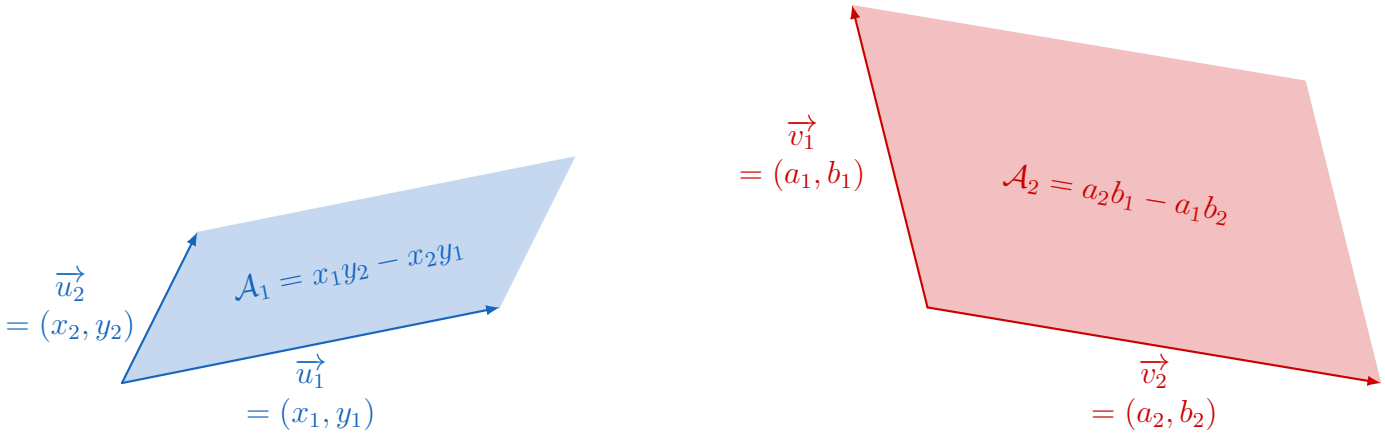
Remarque I.31. *Ce résultat permet en pratique de calculer facilement une signature, en décomposant une permutation en produit de cycles (ce qui est plus pratique qu'une décomposition en produit de transpositions).*

Exemple I.32. *Reprenons* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 6 \end{pmatrix}\begin{pmatrix} 2 & 4 & 5 \end{pmatrix}$. *Alors :*

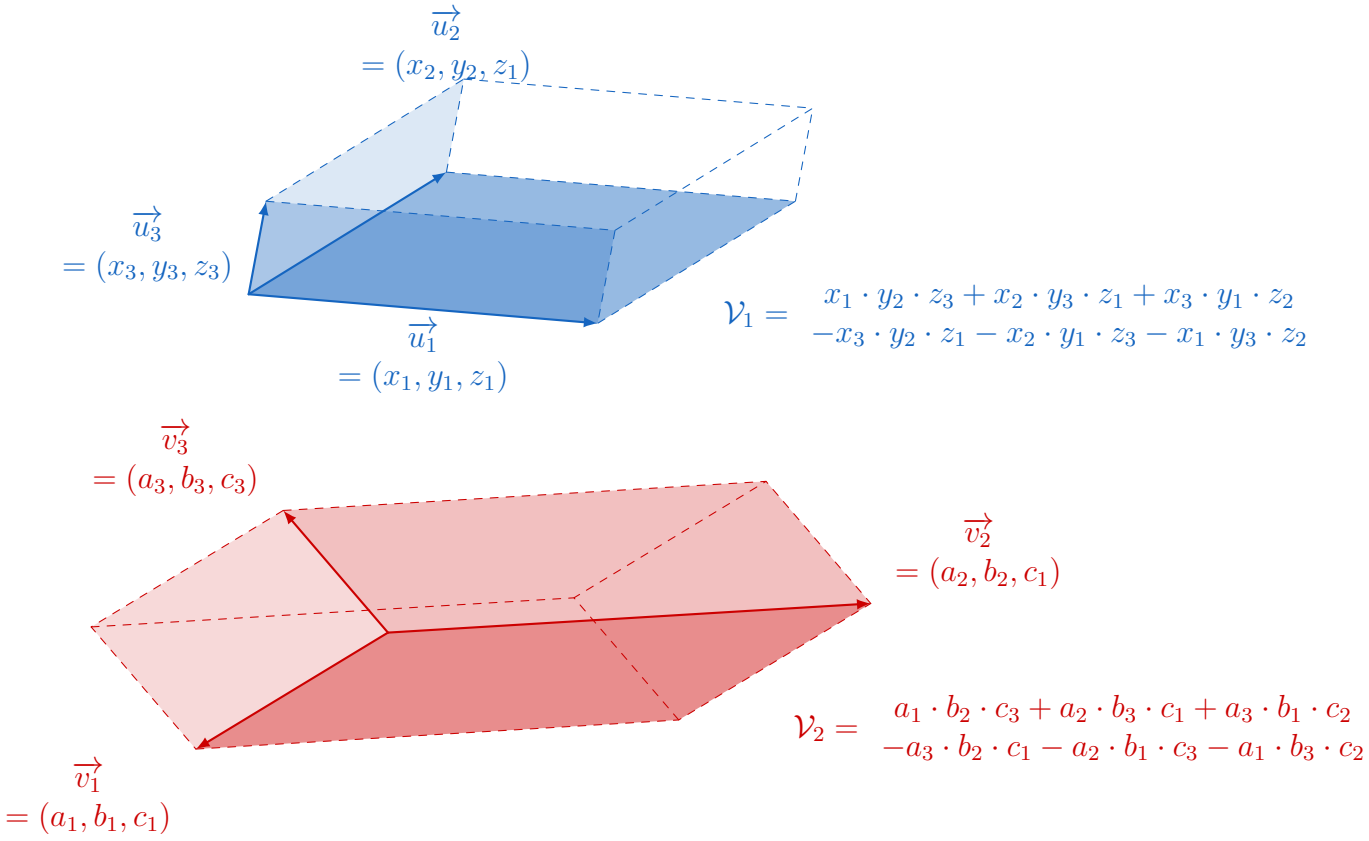
$$\varepsilon(\sigma) = \varepsilon\begin{pmatrix} 1 & 6 \end{pmatrix} \cdot \begin{pmatrix} 2 & 4 & 5 \end{pmatrix} = (-1)^1 \cdot (-1)^2 = -1$$

II Formes multilinéaires alternées

Remarque II.1. *Les déterminants permettent de généraliser les notions d'aires et de volumes. C'est ce qu'on a en dimension 2 :*



ou en dimension 3 :



On est donc à la recherche d'une fonction définie sur les familles de vecteurs qui généraliserait tout cela : on veut qu'elle vérifie certaines propriétés qui se comprennent intuitivement (et qu'on expliquera quand elles apparaîtront).

II.1 Formes multilinéaires

Définition II.2. *Étant donnés $E_1, \dots, E_n$ et F des espaces vectoriels, une application $f : E_1 \times \cdots \times E_n \to F$ sera dite* ***multilinéaire*** *(ou n-linéaire si on veut mettre en évidence le nombre d'espaces) si elle est linéaire par rapport à chacune de ses variables, c'est-à-dire que pour tout $i \in [\![1; n]\!]$ et tout $(x_1, \dots, x_{i-1}, x_{i+1}, \dots x_n) \in E_1 \times \cdots \times E_{i-1} \times E_{i+1} \cdots \times \dots E_n$ l'application :*

$$f_i : x \mapsto f(x_1, \dots x_{i-1}, x, x_{i+1}, \dots, x_n)$$

est une application linéaire de E_i dans F.

Remarques II.3.

1. *Une application multilinéaire n'est en général pas linéaire : si $\lambda \in \mathbb{K}$ et $(x_1, \dots, x_n) \in E_1 \times \cdots \times E_n$, alors :*
$$f(\lambda(x_1, \dots, x_n)) = f(\lambda x_1, \dots, \lambda x_n) = \lambda^n f(x_1, \dots, x_n).$$
2. *Dans le cas particulier où $n = 2$, on parle d'application* ***bilinéaire****. On parle alors de* ***linéarité à gauche*** *pour désigner la linéarité par rapport aux éléments de E_1, et* ***linéarité à droite*** *par rapport à ceux de E_2.*

Exemples II.4.

1. *L'application qui à deux matrices associe leur produit est bilinéaire (on l'avait montré quand on avait défini les produits matriciels). Plus généralement, si $m_0, m_1, \dots, m_n \in \mathbb{N}^*$, alors l'application :*

$$\left\{ \begin{array}{rcl} \mathcal{M}_{m_0,m_1}(\mathbb{K}) \times \cdots \times \mathcal{M}_{m_{n-1},m_n}(\mathbb{K}) & \to & \mathcal{M}_{m_0,m_n}(\mathbb{K}) \\ (A_1, \dots, A_n) & \mapsto & A_1 \times \cdots \times A_n \end{array} \right.$$

est une forme n-linéaire.

2. *Et on a des résultats analogues avec toutes les algèbres qu'on a rencontrées : il s'agit en fait d'une conséquence de la distributivité du produit sur l'addition.*

3. *Le déterminant en dimension 2 défini par :*

$$\det \begin{pmatrix} a & c \\ b & d \end{pmatrix} = ad - bc$$

est bilinéaire, vu comme l'application :

$$\det : \left\{ \begin{array}{rcl} \mathbb{R}^2 & \mapsto & \mathbb{R} \\ ((a,b),(c,d)) & \mapsto & ad - bc \end{array} \right.$$

On peut par exemple vérifier la linéarité à gauche. Si $a, a', b, b', c, d \in \mathbb{R}$ et $\lambda, \mu \in \mathbb{R}$, alors :

$$\begin{array}{rcl} \det\left(\lambda(a,b) + \mu(a',b'),(c,d)\right) & = & \det\left((\lambda a + \mu a', \lambda b + \mu b'),(c,d)\right) = (\lambda a + \mu a')d - (\lambda b + \mu b')c \\ & = & \lambda\left(ad - bc\right) + \mu\left(a'd - b'c\right) = \lambda \det((a,b),(c,d)) + \mu \det((a',b'),(c,d)) \end{array}.$$

4. *De même, le produit scalaire en dimension 2 défini par :*

$$(a,b) \cdot (c,d) = ac + bd$$

est bilinéaire.

Définition II.5. *Si E est un $\mathbb{K}$-espace vectoriel, et $n \in \mathbb{N}^*$, une application n-linéaire de E^n dans $\mathbb{K}$ est appelée* ***forme n-linéaire sur E****.*

Exemple II.6. *Dans les exemples précédents, le déterminant et le produit scalaire sont des applications 2-linéaires de $\mathbb{R}^2 \times \mathbb{R}^2$ sur $\mathbb{R}$: ce sont des formes 2-linéaires sur $\mathbb{R}^2$.*

II.2 Formes alternées

Définition II.7. *Pour E un $\mathbb{K}$-ev et $n \in \mathbb{N}^*$, une forme n-linéaire φ sur E est dite* ***alternée*** *si :*

$$\forall (x_1, \dots, x_n) \in E^n,\ \forall i, j \in [\![1; n]\!],\ \left\{ \begin{array}{c} i \neq j \\ x_i = x_j \end{array} \right. \Rightarrow \varphi(x_1, \dots, x_n) = 0$$

c'est-à-dire que tout n-uplet dont deux éléments sont égaux ont une image nulle par φ.

Exemples II.8.

1. *Le déterminant est une forme 2-linéaire alternée :*

$$\det((a,b),(a,b)) = ab - ab = 0$$

2. *Le produit scalaire n'est pas alternée :*

$$(a,b) \cdot (a,b) = a^2 + b^2$$

donc par exemple avec $a = 1$ et $b = 0$ on a : $(1,0) \cdot (1,0) = 1 \neq 0$.

Proposition II.9. *Si φ est une forme n-linéaire alternée , alors l'image par φ d'un n-uplet ne change pas si on ajoute à l'un se ses éléments une combinaison linéaire de ses autres éléments.*

Démonstration. On considère $(x_1, \dots, x_n) \in E^n$, alors pour tous $i, j \in [\![1; n]\!]$ distincts et tout $\lambda \in \mathbb{K}$, on peut changer la valeur de x_i en $x_i + \lambda x_j$ sans changer la valeur de φ. Comme modifier x_i par une combinaison linéaire des x_j (pour $j \neq i$) revient à faire un nombre fini d'opérations de ce type, le résultat voulu en découlera.
Par n-linéarité, on a déjà :

$$\varphi(\dots, x_i + \lambda x_j, \dots) = \varphi(\dots x_i, \dots) + \lambda\varphi(\dots, x_j, \dots)$$

Mais comme φ est alternée, on déduit que le second terme ci-dessus est nul. Ce qui prouve le résultat. □

Corollaire II.10. *L'image d'une famille liée par une forme n-linéaire alternée est nulle.*

Démonstration. Considérons $(x_1, \dots, x_n)$ famille liée. Alors l'un des vecteurs s'exprime comme combinaison linéaire des autres. Il existe donc $i \in [\![1; n]\!]$ et des scalaires $(\lambda_j)_{j\neq i}$ tels que : $x_i = \sum_{j\neq i} \lambda_j x_j = 0$.
Et ainsi :

$$\varphi(\dots, x_i, \dots) = \varphi(\dots, x_i - \sum_{j\neq i} \lambda_j x_j, \dots) = \varphi(\dots, 0, \dots) = 0$$

par linéarité par rapport à la i-ème coordonnée. □

II.3 Antisymétrie et permutation

Proposition-Définition II.11. *Une forme n-linéaire φ est dite **antisymétrique** si :*

$$\forall (x_1, \dots, x_n) \in E^n,\ \forall i, j \in [\![1; n]\!],\ i < j \Rightarrow \varphi(x_1, \dots, x_i, \dots, x_j, \dots, x_n) = -\varphi(x_1, \dots, x_j, \dots, x_i, \dots, x_n)$$

c'est-à-dire que le fait d'inverser deux éléments dans un n-uplet change son image par φ en son opposé. Les formes n-linéaires alternées sont exactement les formes n-linéaires antisymétriques.

Démonstration. On procède par double implication :

— si φ est alternée : considérons $(x_1, \dots, x_n) \in E^n$ et fixons $i, j \in [\![1; n]\!]$ tels que $i < j$. Alors comme φ est alternée :

$$\varphi(\dots, x_i + x_j, \dots, x_i + x_j, \dots) = 0$$

mais par n-linéarité, on a également :

$$\begin{aligned} & \varphi(\dots, x_i + x_j, \dots, x_i + x_j, \dots) = \varphi(\dots, x_i, \dots, x_i + x_j, \dots) + \varphi(\dots, x_j, \dots, x_i + x_j, \dots) \\ = & \underbrace{\varphi(\dots, x_i, \dots, x_i, \dots)}_{=0} + \varphi(\dots, x_i, \dots, x_j, \dots) + \varphi(\dots, x_j, \dots, x_i, \dots) + \underbrace{\varphi(\dots, x_j, \dots, x_j, \dots)}_{=0} \\ = & \varphi(\dots, x_i, \dots, x_j, \dots) + \varphi(\dots, x_j, \dots, x_i, \dots) \end{aligned}$$

ce qui donne finalement :

$$\varphi(\dots, x_j, \dots, x_i, \dots) = -\varphi(\dots, x_i, \dots, x_j, \dots)$$

donc φ est antisymétrique.

— si φ est antisymétrique : considérons $(x_1, \dots, x_n) \in E_n$ et $i, j \in [\![1; n]\!]$ distincts tels que $x_i = x_j$. Quitte à échanger i et j, on peut supposer que $i < j$, et ainsi en échangeant x_i et x_j dans le n-uplet $(x_1, \dots, x_n)$ (ce qui ne changer rien à la valeur du n-uplet), on trouve que :

$$\varphi(x_1, \dots, x_n) = -\varphi(x_1, \dots x_n)$$

et donc $\varphi(x_1, \dots, x_n) = 0$, donc φ est alternée.

□

Corollaire II.12. *Si φ est une forme n-linéaire alternée et $\sigma \in S_n$, alors :*

$$\forall (x_1, \dots, x_n) \in E^n,\ \varphi(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \varepsilon(\sigma)\varphi(x_1, \dots, x_n)$$

c'est-à-dire que le fait d'échanger les éléments d'un n-uplet suivant une permutation modifie la valeur de φ en la multipliant par la signature de la permutation.

Démonstration. On sait qu'inverser deux éléments dans un n-uplet multiplie par -1 son image par φ. Le résultat est donc vrai pour tout transposition.
On en déduit alors le résultat général : on considère une permutation σ, qu'on écrit comme produit des transpositions $\tau_1 \circ \cdots \circ \tau_p$. Le fait le permuter les éléments suivant σ revient à appliquer p transpositions, donc à multiplier φ par $(-1)^p = \varepsilon(\sigma)$. □

II.4 Formes multilinéaires alternées en dimension finie

Proposition II.13. *Étant donnés E un espace vectoriel de dimension $n \in \mathbb{N}^*$, $(e_1, \dots, e_n)$ une base de E, et $n \in \mathbb{N}*$, une forme p-linéaire alternée φ sur E est entièrement déterminée par les quantités :*

$$\varphi(e_{i_1}, \dots, e_{i_p}) \text{ pour } 1 \leq i_1 < i_2 < \cdots < i_p \leq n$$

Démonstration. Considérons $(x_1, \dots, x_p) \in E^p$, et notons $(a_{i,j}) = \mathrm{Mat}_{(e_i)}(x_j)$, de sorte que :

$$\forall j \in [\![1; p]\!],\ x_j = \sum_{i=1}^{n} a_{i,j} e_i$$

Alors par n-linéarité de φ, on déduit déjà que :

$$\varphi(x_1, \dots, x_n) = \sum_{i_1, \dots, i_p \in [\![1;n]\!]} a_{i_1,1} a_{i_2,1}, \dots a_{i_p,1} \varphi\left(e_{i_1}, e_{i_2}, \dots, e_{i_p}\right)$$

Mais par le caractère alterné de φ, on a que :
- si deux indices $i_j, i_{j'}$ sont égaux : $\varphi\left(e_{i_1}, e_{i_2}, \dots, e_{i_p}\right) = 0$;
- si tous les indices sont distincts : en permutant les indices, on peut se ramener à les ranger dans l'ordre (strictement) croissant, en multipliant par la signature de la permutation correspondante.

Et donc dans la somme ne resteront que des termes de la forme de l'énoncé, ce qui prouve le résultat. □

Théorème II.14. *Si E est un espace vectoriel de dimension n, alors une forme n-linéaire alternée est entièrement déterminée par l'image d'une base.*
Plus précisément, si $(x_1, \dots, x_n)$ est une famille de vecteur de E dont la matrice dans la base $(e_1, \dots, e_n)$ est $(a_{i,j})$, alors :

$$\varphi(x_1, \dots, x_n) = \varphi(e_1, \dots, e_n) \cdot \left(\sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma(1),1} \dots a_{\sigma(n),n} \right).$$

C'est donc une droite vectorielle engendrée par la forme n-linéaire alternée :

$$\left(x_1 = \sum_{i=1}^{n} a_{i,1} e_i, \dots, x_n = \sum_{i=1}^{n} a_{i,n} e_i \right) \mapsto \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma(1),1} \dots a_{\sigma(n),n}$$

Démonstration. Le lemme précédent donne déjà l'écriture de $\varphi(x_1, \dots, n)$: dans la somme du lemme, il ne restera que les termes où les i_k sont deux-à-deux distincts (et forment donc l'ensemble $[\![1; n]\!]$), où on fait à chaque fois ressortir la signature de la permutation qui permet de ranger les i_k dans l'ordre croissant.
Pour montrer qu'il s'agit d'une droite vectorielle, on constate déjà que :

— c'est un espace vectoriel : c'est un sev de $\mathcal{F}(E^n, \mathbb{K})$ en tant que sous-ensemble non vide (la fonction nulle est n-linéaire alternée) stable par combinaison linéaire (immédiat par le calcul) ;
— il est engendré par un vecteur : par l'écriture précédente, il suffit de voir que l'application ψ donnée dans le théorème est une forme n-linéaire alternée. La n-linéarité vient du fait que chaque application : $(x_1, \dots, x_n) \mapsto a_{\sigma(1),1} \dots a_{\sigma(n),n}$ est n-linéaire (par n-linéarité du produit de n facteurs, comme chaque facteur correspond à un unique x_i). Le caractère alterné est plus calculatoire, mais se montre en faisant agir une transposition, et en utilisant que pour tout transposition τ on a : $\{\tau \circ \sigma \,|\, \sigma \in S_n\} = S_n$ et que $\varepsilon(\tau \circ \sigma) = -\varepsilon(\sigma)$ (ce qui fera bien apparaître le "$-$" des formes antisymétriques, donc alternées).
— et ce vecteur est non nul : il suffit de voir que ψ est non nulle, mais comme $\mathrm{Mat}_{(e_i)}(e_i) = I_n = (\delta_{i,j})$, alors :

$$\psi(e_1, \dots, e_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \delta_{\sigma(1),1} \dots \delta_{\sigma(n),n} = \varepsilon(\mathrm{id}) = 1$$

□

Remarque II.15. *On a en fait un résultat plus général, mais plus compliqué à montrer, qui est que l'ensemble des formes p-linéaires alternées sur un espace de dimension n est un espace vectoriel de dimension* $\binom{n}{k}$.
La structure d'espace vectoriel se montre comme dans le cas où $p = n$.
Pour la dimension :
— *le cas général se comprend bien : on a vu qu'il suffisait de regarder les* $\varphi(e_{i_1}, \dots, e_{i_p})$ *(avec* $1 \leq i_1 < \dots < i_p \leq n$*) pour déterminer* φ*, ce qui donne une majoration de la dimension par* $\binom{n}{p}$ *(car d'un côté la dimension constitue le nombre de degré de libertés, et de l'autre on a* $\binom{n}{p}$ *choix pour les* i_j*) ;*
— *on retrouve le cas particulier où* $n = p$ *comme* $\binom{n}{p} = 1$ *;*
— *on retrouve le cas où* $p = 1$*, puisqu'une forme* 1*-linéaire alternée est en fait un forme linéaire, et* $\dim E^* = \dim E = n = \binom{n}{1}$ *;*
— *le cas où* $p = 0$ *est un peu plus subtile, mais se comprend bien : une application* 0*-linéaire alternée est en fait une application de* E^0 *dans* $\mathbb{K}$*, donc une fonction de* $\{0\}$ *dans* $\mathbb{K}$*, et* $\mathcal{F}(\Omega, F)$ *est un espace vectoriel de dimension* $\mathrm{card}(\Omega) \cdot \dim(F)$*, ce qui donne bien une dimension* 1 *dans notre cas ;*
— *et on retrouve le cas où* $n < p$ *: toute famille à p éléments étant liée, une forme p-linéaire alternée sur un espace de dimension plus petit est nulle ;*

III Déterminants

III.1 Déterminant d'une famille de vecteurs dans une base

Théorème-Définition III.1. *Étant donné E un espace vectoriel de dimension n et* $\mathcal{B} = (e_1, \dots, e_n)$ *une base de E, il existe une unique forme n-linéaire alternée sur E telle que l'image de* $(e_1, \dots, e_n)$ *soit égale à* 1.
On l'appelle ***le déterminant dans la base*** (e_i)*, et on le note* $\det_{(ei)}$ *ou* $\det_{\mathcal{B}}$.
Si $(x_1, \dots, x_n) \in E^n$ *vérifie :* $\mathrm{Mat}_{\mathcal{B}}(x_j) = (a_{i,j})$*, alors :*

$$\det_{\mathcal{B}}(x_1, \dots, x_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma(1),1} \dots a_{\sigma(n),n} = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i}.$$

De plus, toute forme n-linéaire alternée est un multiple de $\det_{\mathcal{B}}$*. Plus précisément, si* φ *est une telle forme, alors :*

$$\varphi = \varphi(e_1, \dots, e_n) \cdot \det_{\mathcal{B}}.$$

Démonstration. L'unicité vient du fait que l'ensemble des formes n-linéaires forme une droite vectorielle : si une autre forme existait, elle serait de la forme $\varphi = \lambda \det_{\mathcal{B}}$. Et on trouve alors $\lambda = 1$ en évaluant en $(e_1, \dots, e_n)$ ce qui donne bien l'unicité.
L'existence vient de l'application ψ construite au théorème précédent (on avait bien que $\psi(e_1, \dots, e_n) = 1$), et donne la formule du théorème par son caractère n-linéaire alterné.
Enfin, comme $\det_{\mathcal{B}}$ est une forme n-linéaire alternée non nulle, alors elle engendre l'ensemble des formes n-linéaires alternées (comme il s'agit d'une droite vectorielle). Donc toute forme n-linéaire alternée φ s'écrit sous la forme $\varphi = \lambda \det_{\mathcal{B}}$, et l'évaluation en $(e_1, \dots, e_n)$ donne $\lambda = \varphi(e_1, \dots, e_n)$. □

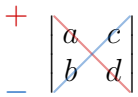
Exemples III.2.

1. *Donnons l'expression du déterminant dans $\mathbb{K}^2$ muni de sa base canonique $\mathcal{B}$. Considérons les vecteurs $x = (a, b)$ et $y = (c, d)$. Alors on a déjà que :*

$$\mathrm{Mat}_{\mathcal{B}}(x, y) = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

On a $S_2 = \{\mathrm{id}, \tau_{1,2}\}$, avec $\varepsilon(\mathrm{id}) = 1$ et $\varepsilon(\tau_{1,2}) = -1$. Donc :

$$\det_{\mathcal{B}}(x, y) = \varepsilon(\mathrm{id}) \underbrace{a_{1,1}a_{2,2}}_{\sigma=\mathrm{id}} + \varepsilon(\tau_{1,2}) \underbrace{a_{2,1}a_{1,2}}_{\sigma=\tau_{1,2}} = ad - bc$$



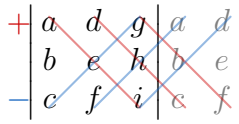
2. *Pour $\mathbb{K}^3$ muni de sa base canonique $\mathcal{B}$, on procède de même. On considère les vecteurs $x = (a, b, c), y = (d, e, f), z = (g, h, i)$, ce qui donne pour matrice :*

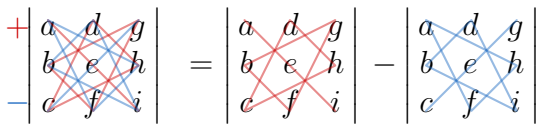
$$A = (a_{i,j}) = \mathrm{Mat}_{\mathcal{B}}(x, y, z) = \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & i \end{pmatrix}.$$

On a : $S_3 = \{\mathrm{id}, (1\ \ 2), (1\ \ 3), (2\ \ 3), (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\}$, avec comme signature 1 pour id *et les 3-cycles, et -1 pour les transpositions.*
Et par la formule explicite du déterminant on trouve :

$$\det_{\mathcal{B}}(x, y, z) = \underbrace{aei}_{\mathrm{id}} - \underbrace{bdi}_{(1\ \ 2)} - \underbrace{cge}_{(1\ \ 3)} - \underbrace{afh}_{(2\ \ 3)} + \underbrace{bfg}_{(1\ \ 2\ \ 3)} + \underbrace{cdh}_{(1\ \ 3\ \ 2)}$$

Qu'on ne retiendra pas par cœur, mais qu'on retrouve avec la règle de Sarrus :





Remarque III.3. *En dimensions 2 et 3, on retrouve les formules pour l'aire d'un parallélogramme ou pour le volume d'un parallélépipède. Cette conformité du déterminant avec l'aire ou le volume se comprennent bien par les propriétés du déterminant :*

— *le caractère n-linéaire se décompose en sa compatibilité vis-à-vis de la somme, et de la multiplication par un scalaire, ce qui est cohérent avec le fait que l'aire de de surface est la somme des aires, et qu'une surface dilatée d'un facteur suivant une direction a son aire multipliée par le même facteur.*
— *le caractère alterné permet de donner un signe à l'aire, un peu à la manière de l'aire sous la courbe d'une fonction pour comprendre son intégrale : on parle d'aire algébrisée.*

Et on comprend bien qu'une forme n-linéaire n'est en général pas linéaire : doubler la taille d'un carré (respectivement d'un cube) c'est multiplier son aire par 4 *(respectivement son volume par* 8*).*

Corollaire III.4 (Formule de changement de base)**.** *Si $\mathcal{B}$ et $\mathcal{C}$ sont deux bases de E de dimension n, alors :*

$$\det_{\mathcal{C}} = \det_{\mathcal{C}}(\mathcal{B}) \cdot \det_{\mathcal{B}}$$

et donc pour tout $(x_1, \dots, x_n) \in E^n$ on a :

$$\det_{\mathcal{C}}(x_1, \dots, x_n) = \det_{\mathcal{C}}(\mathcal{B}) \cdot \det_{\mathcal{B}}(x_1, \dots, x_n).$$

Démonstration. C'est le résultat précédent, appliqué à $\varphi = \det_{\mathcal{C}}$. □

Corollaire III.5. *Si $(x_1, \dots, x_n)$ est une famille de vecteur de E, alors c'est une base si, et seulement si, pour n'importe quelle base $\mathcal{B}$ de E on a :* $\det_{\mathcal{B}}(x_1, \dots, x_n) \neq 0$.

Démonstration. Si $(x_1, \dots, x_n)$ n'est pas une base, alors elle elle liée et donc son image par toute forme n-linéaire alternée est nulle.
Si $(x_1, \dots, x_n)$ est une base, alors par formule de changement de base :

$$1 = \det_{(x_1,\dots,x_n)}(x_1, \dots, x_n) = \det_{x_1,\dots,x_n}(\mathcal{B})\det_{\mathcal{B}}(x_1, \dots, x_n)$$

et on a donc bien que : $\det_{\mathcal{B}}(x_1, \dots, x_n) \neq 0$. □

Remarque III.6. *On a en fait un résultat plus fort, à savoir que :* $\det_{\mathcal{B}}(\mathcal{C}) \cdot \det_{\mathcal{C}}(\mathcal{B}) = 1$.

III.2 Déterminant d'un endomorphisme

Proposition-Définition III.7. *Si E est un espace vectoriel de dimension finie, $\mathcal{B} = (e_1, \dots, e_n)$ une base et $f \in \mathcal{L}(E)$, on appelle* ***déterminant de*** *f la quantité* $\det_{\mathcal{B}}(f(e_1), \dots, f(e_n))$.
Celle-ci ne dépend pas de la base de E considérée, et sera notée $\det(f)$.
De plus, pour tous $x_1, \dots, x_n \in E$ on a :

$$\det_{\mathcal{B}}(f(x_1), \dots, f(x_n)) = \det(f) \cdot \det_{\mathcal{B}}(x_1, \dots, x_n).$$

Démonstration. La seule chose à prouver est que cette quantité ne dépend pas de la base choisie. Considérons donc $\mathcal{B} = (e_1, \dots, e_n), \mathcal{C} = (f_1, \dots, f_n)$ deux bases de E.
On considère l'application :

$$\varphi : \left\{ \begin{array}{rcl} E^n & \to & \mathbb{K} \\ (x_1, \dots, x_n) & \mapsto & \det_{\mathcal{B}}(f(x_1), \dots, f(x_n)) \end{array} \right.$$

qui est une forme n-linéaire alternée sur E (par caractère n-linéaire alterné de $\det_{\mathcal{B}}$ et linéarité de f). Et donc on peut écrire :

$$\varphi = \varphi(e_1, \dots, e_n) \cdot \det_{\mathcal{B}} = \varphi(f_1, \dots, f_n) \cdot \det_{\mathcal{C}}$$

En évaluant la dernière égalité en $(e_1, \dots, e_n)$, on a donc en remplaçant φ par son expression :

$$\det_{\mathcal{B}}(f(e_1), \dots, f(e_n)) \underbrace{\det_{\mathcal{B}}(e_1, \dots, e_n)}_{=1} = \det_{\mathcal{B}}(f(f_1), \dots, f(f_n)) \cdot \det_{\mathcal{C}}(e_1, \dots, e_n)) = \det_{\mathcal{C}}(f(f_1), \dots, f(f_n))$$

par formule du changement de base. Ce qui donne bien que le déterminant de f est bien défini et le dépend pas de la base choisie.
Et le fait que $\varphi = \varphi(e_1, \dots, e_n)\det_{\mathcal{B}}$ donne le dernier résultat. □

Proposition III.8 (Déterminant d'une composée)**.** *Si $f, g \in \mathcal{L}(E)$ alors :*

$$\det(g \circ f) = \det(g) \cdot \det(f) = \det(f \circ g).$$

Démonstration. On considère $\mathcal{B} = (e_1, \dots, e_n)$ une base de E, et alors :

$$\det(g \circ f) = \det_{\mathcal{B}}(g \circ f(e_1), \dots, g \circ f(e_n)) = \det(g)\det_{\mathcal{B}}(f(e_1), \dots, f(e_n)) = \det(g)\det(f)$$

ce qui donne la première égalité.
Comme $\det(g)\det(f) = \det(f)\det(f)$, on déduit la seconde en échangeant les rôles de f et g. □

Exemple III.9. *Si E est de dimension n et $\lambda \in \mathbb{K}$, alors par n-linéarité du déterminant on a :* $\det(\lambda \mathrm{id}_E) = \lambda^n$.
Plus généralement, si $f \in \mathcal{L}(E)$, alors : $\det(\lambda f) = \lambda^n \det(f)$.

Corollaire III.10. *Un endomorphisme f de E est un automorphisme si, et seulement si, son déterminant est non nul, et on a alors :*

$$\det(f^{-1}) = \frac{1}{\det(f)}.$$

L'application det *réalise ainsi un morphisme de groupes de* $\mathrm{GL}(E)$ *dans* $\mathbb{K}^*$.

Remarque III.11. *Le premier résultat se comprend bien en terme de familles de vecteurs, dans la mesure où :*

- *un endomorphisme est bijectif si, et seulement si, l'image d'une base est une base ;*
- *une famille est une base si, et seulement si, son déterminant est non nul.*

III.3 Déterminant d'une matrice carrée

Définition III.12. *Soit $A = (a_{i,j}) \in \mathcal{M}_n(\mathbb{K})$. On appelle* ***déterminant de*** *A la quantité :*

$$\det(A) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i}.$$

On notera alors :

$$\det(A) = \begin{vmatrix} a_{1,1} & \dots & a_{1,j} & \dots & a_{1,n} \\ \vdots & & \vdots & & \vdots \\ a_{i,1} & \dots & a_{i,j} & \dots & a_{i,n} \\ \vdots & & \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,j} & \dots & a_{n,n} \end{vmatrix}.$$

Remarque III.13.
Le déterminant d'une matrice est le déterminant dans la base canonique de $\mathcal{M}_{n,1}(\mathbb{K})$ de la famille de ses vecteurs colonnes. C'est donc le déterminant de l'endomorphisme canoniquement associé.

Proposition III.14. *Si E est un espace de dimension n, et $\mathcal{B}$ une base de E, alors :*

1. *si $(x_1, \dots, x_n)$ est une famille de vecteurs de E :* $\det_{\mathcal{B}}(x_1, \dots, x_n) = \mathrm{detMat}_{\mathcal{B}}(x_1, \dots, x_n)$;
2. *si $f \in \mathcal{L}(E)$, alors :* $\det(f) = \mathrm{detMat}_{\mathcal{B}}(f)$.

Démonstration. Découle directement de la formule. □

Proposition III.15. *Étant données $A, B \in \mathcal{M}_n(\mathbb{K})$ et $\lambda \in \mathbb{K}$, on a :*

1. $\det(\lambda A) = \lambda^n \det(A)$;

2. $\det(AB) = \det(A)\det(B) = \det(BA)$.

Démonstration. Découle des résultats pour les endomorphismes, appliqués aux endomorphismes canoniquement associés à A et à B. □

Remarque III.16. *Le second résultat se généralise à davantage de matrices, du fait de la commutativité de la multiplication sur* $\mathbb{K}$. *En effet, si* $A_1, \dots, A_r \in \mathcal{M}_n(\mathbb{K})$, *alors on :*

$$\det(A_1 \dots A_n) = \det(A_1)\det(A_2 \dots A_n) = \dots = \det(A_1) \dots \det(A_n)$$

et en échangeant les déterminants à droite, on déduit que pour toute permutation $\sigma \in S_n$ *on a :*

$$\det(A_1 \dots A_n) = \det(A_{\sigma(1)} \dots A_{\sigma(n)}) = \det(A_1) \dots \det(A_n).$$

Corollaire III.17. *Deux matrices semblables ont même déterminant.*

Démonstration. Considérons $A, B \in \mathcal{M}_n(\mathbb{K})$ et $P \in \mathrm{GL}_n(\mathbb{K})$ telles que : $A = P^{-1}BP$. Alors :

$$\det(A) = \det(P^{-1}BP) = \det(PP^{-1}B) = \det(B).$$

□

Remarque III.18. *On peut aussi interpréter ce résultat en terme d'endomorphismes, comme on a montré que le déterminant d'un endomorphisme ne dépend pas de la base choisie.*

Corollaire III.19. *Une matrice* $A \in \mathcal{M}_n(\mathbb{K})$ *est inversible si, et seulement si, son déterminant est non nul, et on a alors :*

$$\det(A^{-1}) = \frac{1}{\det(A)}.$$

L'application det *réalise ainsi un morphisme de groupes de* $\mathrm{GL}_n(\mathbb{K})$ *dans* $\mathbb{K}^*$.

Remarque III.20. *On retrouve d'une autre manière que deux matrices semblables ont même déterminant, comme :*

$$\det(P^{-1}BP) = \det(P^{-1})\det(B)\det(P) = \det(P)^{-1}\det(B)\det(P) = \det(B).$$

Proposition III.21. *Si* $A \in \mathcal{M}_n(\mathbb{K})$, *alors :* $\det(A) = \det(A^T)$.
Ainsi, le déterminant d'une matrice est également le déterminant de la famille de ses vecteurs lignes dans la base canonique.

Démonstration. Par formule qui définit le déterminant, on a :

$$\begin{aligned}
\det(A) &= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i} \\
&= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{j=1}^{n} a_{j,\sigma^{-1}(j)} \text{ (en posant } j = \sigma(i)) \\
&= \sum_{\tau \in S_n} \varepsilon(\tau^{-1}) \prod_{j=1}^{n} a_{j,\tau(j)} \text{ (en posant } \tau = \sigma^{-1}) \\
&= \sum_{\tau \in S_n} \varepsilon(\tau) \prod_{j=1}^{n} \left[A^T\right]_{\tau(j),j} \text{ (comme } \varepsilon(\tau) = \varepsilon(\tau^{-1})) \\
&= \det(A^T)
\end{aligned}$$

□

Exemple III.22. *Si $A \in \mathrm{GL}_n(\mathbb{K})$ et $B \in \mathcal{M}_{n,1}(\mathbb{K})$, alors l'unique solution $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ de l'équation $AX = B$ est donnée par :*

$$\forall i \in [\![1; n]\!],\ x_i = \frac{\det(A_i)}{\det(A)}$$

où A_i désigne la matrice obtenue à partir de A en changeant la i-ème colonne par B.
On a déjà montré l'existence. Considérons donc une telle solution. Alors, en notant $C_1, \dots, C_n$ les colonnes de A, on a :

$$x_1 C_1 + \cdots + x_n C_n = B$$

de sorte que :

$$\begin{aligned} \det(A_i) &= \det(C_1, \dots, B, \dots, C_n) \\ &= \det(C_1, \dots, (x_1 C_1 + \cdots + x_n C_n), C_n) \\ &= \det(C_1, \dots, x_i C_i, \dots, C_n) \ \textit{comme le déterminant est } n\textit{-linéaire alterné} \\ &= x_i \cdot \underbrace{\det(C_1, \dots, C_i, \dots, C_n)}_{=\det(A)} \end{aligned}$$

ce qui donne bien la formule voulue.

IV Calculs de et avec des déterminants

IV.1 Opérations élémentaires

Proposition IV.1. *Étant donnée $A \in \mathcal{M}_n(\mathbb{K})$:*

1. *La permutation de deux lignes ou deux colonnes de A multiplie son déterminant par -1.*
2. *La dilatation de coefficient λ d'une ligne ou d'une colonne de A multiplie le déterminant par λ.*
3. *La transvection d'une ligne d'une ligne ou d'une colonne de A ne change pas son déterminant.*

Démonstration. On utilise que le déterminant d'une matrice est une forme n-linéaire alternée, vue comme une application sur les colonnes ou les lignes.
Une permutation revient à faire agir une transposition sur les lignes ou les colonnes, et donc multiplie le déterminant par -1 (car le déterminant est antisymétrique).
Une dilatation revient à multiplier une ligne ou une colonne par λ, donc à multiplier le déterminant par λ (car le déterminant est n-linéaire).
Une transvection revient à ajouter à une ligne ou une colonne une combinaison linéaire des autres lignes ou colonnes, et ne change pas le déterminant (car le déterminant est alterné). □

Remarque IV.2. *Un point important est que toutes ces opérations préservent le rang (et l'inversibilité), donc il est rassurant de voir que ces opérations préservent la nullité ou non du déterminant.*

Remarque IV.3. *On peut ainsi effectuer la méthode du pivot pour calculer le déterminant d'une matrice :*
- *soit on se ramène par opérations élémentaires à la matrice I_n, dont le déterminant est 1 ;*
- *soit on se ramène à une matrice non inversible, donc le déterminant est 0.*

Et les opérations élémentaires utilisées permettent d'en déduire le déterminant de la matrice de départ.

Proposition IV.4. *Le déterminant d'une matrice triangulaire est égal au produit de ses coefficients diagonaux.*

Démonstration. Montrons le pour une matrice triangulaire supérieure (le cas des matrices triangulaires inférieures se déduit par passage à la transposée).
Soit $A = (a_{i,j}) \in \mathcal{M}_n(\mathbb{K})$ triangulaire supérieure, c'est-à-dire que : $\forall i, j \in [\![1; n]\!],\ i > j \Rightarrow a_{i,j} = 0$.
On utilise le lemme suivant :

Lemme IV.5. *Soit $\sigma \in S_n$ telle que : $\forall i \in [\![1; n]\!],\ \sigma(i) \leq i$. Alors $\sigma = \mathrm{id}$.*

Preuve du lemme : On montre par récurrence forte (finie) sur $i \in [\![1; n]\!]$ que $\sigma(i) = i$:
- si $i = 1$: $\sigma(1) \leq 1$, donc nécessairement $\sigma(1) = 1$.
- si $i \in [\![1; n-1]\!]$ tel que pour tout $j \in [\![1; i]\!]$, $\sigma(j) = j$. Alors $\sigma(i+1) \leq i+1$ donc $\sigma(i+1) \in [\![1; i+1]\!]$. Mais par injectivité de σ, on a que $\sigma(i+1) \notin \sigma([\![1; i]\!]) = [\![1; i]\!]$. Et donc $\sigma(i+1) = i+1$.

Ce qui prouve le lemme par récurrence. □

On a par définition :

$$\det(A) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i} = \sum_{\sigma = \mathrm{id}} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i} = \prod_{i=1}^{n} a_{i,i}.$$

car dans la somme tout élément $\sigma \in S_n \setminus \{\mathrm{id}\}$ vérifie $\sigma(i) > i$ pour un $i \in [\![1; n]\!]$ (d'après le lemme), et donc pour un tel σ on a : $\prod_{i=1}^{n} a_{\sigma(i),i} = 0$ (car l'un des facteurs est nul). □

Remarques IV.6.

1. *Ce résultat simplifie beaucoup les calculs, puisqu'il suffit d'échelonner une matrice (par opérations élémentaires) pour calculer son déterminant, au lieu de faire toute la méthode du pivot.*
2. *On retrouve au passage qu'une matrice triangulaire est inversible si, et seulement si, ses coefficients diagonaux sont non nuls.*

Exemple IV.7. *Calculons le déterminant de la matrice :* $A = \begin{pmatrix} 1 & -1 & 2 & -1 \\ 2 & -1 & 1 & -2 \\ -1 & 3 & 1 & -1 \\ 3 & 0 & -2 & 0 \end{pmatrix}$ *:*

$$\begin{aligned}
\det(A) &= \begin{vmatrix} 1 & -1 & 2 & -1 \\ 2 & -1 & 1 & -2 \\ -1 & 3 & 1 & -1 \\ 3 & 0 & -2 & 0 \end{vmatrix} \\
&= \begin{vmatrix} 1 & -1 & 2 & -1 \\ 0 & 1 & -3 & 0 \\ 0 & 2 & 3 & -2 \\ 0 & 3 & -8 & 3 \end{vmatrix} \\
&= \begin{vmatrix} 1 & -1 & 2 & -1 \\ 0 & 1 & -3 & 0 \\ 0 & 0 & 9 & -2 \\ 0 & 0 & 1 & 3 \end{vmatrix} \\
&= -\begin{vmatrix} 1 & -1 & 2 & -1 \\ 0 & 1 & -3 & 0 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 9 & -2 \end{vmatrix} \\
&= -\begin{vmatrix} 1 & -1 & 2 & -1 \\ 0 & 1 & -3 & 0 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & -29 \end{vmatrix} \\
&= 29
\end{aligned}$$

Proposition IV.8. *Le déterminant d'une matrice triangulaire en bloc est égal au produit des déterminants de ses blocs diagonaux.*

Preuve avec les décompositions de permutations : Montrons déjà le cas de deux blocs diagonaux.
Considérons la matrice en blocs : $A = (a_{i,j}) = \begin{pmatrix} A_{1,1} & A_{1,2} \\ 0 & A_{2,2} \end{pmatrix} \in \mathcal{M}_n(\mathbb{K})$ où $A_{1,1} \in \mathcal{M}_{n_1}(\mathbb{K})$ et $A_{2,2} \in \mathcal{M}_{n_2}(\mathbb{K})$. Alors on obtient :

$$\det(A) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i}.$$

Mais, du fait de la forme de A, les seuls termes non nuls de la sommes sont ceux pour lesquels $\sigma([\![1; n_1]\!]) \subset [\![1; n_1]\!]$, et donc $\sigma([\![1; n_1]\!]) = [\![1; n_1]\!]$ (en tant qu'application injective entre ensembles de même cardinal, la restriction de σ à $[\![1; n_1]\!]$ réalise une bijection sur $[\![1; n_1]\!]$).
Un tel $\sigma \in S_n$ vérifie également : $\sigma([\![n_1 + 1; n]\!]) \subset [\![n_1 + 1; n]\!]$, et donc $\sigma([\![n_1 + 1; n]\!]) = [\![n_1 + 1; n]\!]$ (par le même argument).
On note S'_n l'ensemble de tels éléments $\sigma \in S_n$, auxquels on associe les restrictions σ_1, σ_2 respectivement à $[\![1; n_1]\!]$ et à $[\![n_1 + 1; n]\!]$, on a :

$$\det(A) = \sum_{\sigma \in S'_n} \varepsilon(\sigma) \prod_{i=1}^{n_1} a_{\sigma_1(i),i} \prod_{j=n_1+1}^{n} a_{\sigma_2(j),j}$$

mais en assimilant σ_1 à un élément de S_{n_1} (par restriction) et σ_2 à un élément de S_{n_2} (à savoir l'élément : $j \mapsto \sigma_2(j + n_1) - n_1$), on trouve que :

$$\det(A) = \sum_{\sigma_1 \in S_{n_1}, \sigma_2 \in S_{n_2}} \varepsilon(\sigma_1) \cdot \varepsilon(\sigma_2) \prod_{i=1}^{n_1} [A_{1,1}]_{\sigma_1(i),i} \prod_{j=1}^{n_2} [A_{2,2}]_{\sigma_2(j),j} = \det(A_{1,1})\det(A_{2,2}).$$

Le résultat général se déduit alors par récurrence, en notant que toute matrice triangulaire en blocs peut se décomposer en matrice triangulaire en blocs de la forme ci-dessus. □

Preuve par les formes n-linéaire alternées : Montrons déjà le cas de deux blocs diagonaux.
Considérons la matrice en blocs : $A = (a_{i,j}) = \begin{pmatrix} A_{1,1} & A_{1,2} \\ 0 & A_{2,2} \end{pmatrix} \in \mathcal{M}_n(\mathbb{K})$ où $A_{1,1} \in \mathcal{M}_{n_1}(\mathbb{K})$ et $A_{2,2} \in \mathcal{M}_{n_2}(\mathbb{K})$.
On pose φ l'application :

$$\varphi : \left\{ \begin{array}{ccc} \mathcal{M}_{n_1,1}(\mathbb{K})^{n_1} & \to & \mathbb{K} \\ (X_1, \ldots, X_{n_1}) & \mapsto & \det \begin{pmatrix} X_1 & \ldots & X_{n_1} & A_{1,2} \\ & 0 & & A_{2,2} \end{pmatrix} \end{array} \right.$$

Par linéarité du déterminant par rapport aux n_1 premières colonnes et par son caractère alterné, on voit facilement que φ est une forme n_1-linéaire alternée sur $\mathcal{M}_{n_1,1}(\mathbb{K})$, et donc en notant $\mathcal{B}$ la base canonique de $\mathcal{M}_{n_1,1}(\mathbb{K})$ on obtient que pour tous $X_1, \ldots, X_{n_1} \in \mathcal{M}_{n_1,1}(\mathbb{K})$ on a :

$$\varphi(X_1, \ldots, X_{n_1}) = \det_{\mathcal{B}}(X_1, \ldots, X_{n_1})\varphi(\mathcal{B}) = \det_{\mathcal{B}}(X_1, \ldots, X_{n_1})\det \begin{pmatrix} I_{n_1} & A_{1,2} \\ 0 & A_{2,2} \end{pmatrix}.$$

On applique la même méthode que ci-dessus à l'application :

$$\psi : \left\{ \begin{array}{ccc} \mathcal{M}_{n_2,1}(\mathbb{K})^{n_2} & \to & \mathbb{K} \\ (Y_1, \ldots, Y_{n_2}) & \mapsto & \det \begin{pmatrix} I_{n_1} & & A_{1,2} & \\ 0 & Y_1 & \ldots & Y_{n_2} \end{pmatrix} \end{array} \right.$$

et on obtient de même, en notant $\mathcal{C}$ la base canonique de $\mathcal{M}_{n_2,1}(\mathbb{K})$, que pour tous $Y_1,\dots,Y_{n_2}\in\mathcal{M}_{n_2,1}(\mathbb{K})$:

$$\psi(Y_1,\dots Y_{n_2})=\det_{\mathcal{C}}(Y_1,\dots,Y_{n_2})\det\begin{pmatrix}I_{n_1}&A_{1,2}\\0&I_{n_2}\end{pmatrix}.$$

La dernière matrice est triangulaire avec des 1 sur la diagonale, donc de déterminant 1, ce qui donne finalement que pour tous $X_1,\dots,X_{n_1}\in\mathcal{M}_{n_1,1}(\mathbb{K})$ et $Y_1,\dots,Y_{n_2}\in\mathcal{M}_{n_2,1}(\mathbb{K})$:

$$\det\begin{pmatrix}X_1&\dots&X_{n_1}&&A_{1,2}&\\&0&&Y_1&\dots&Y_{n_2}\end{pmatrix}=\det_{\mathcal{B}}(X_1,\dots,X_{n_1})\cdot\det_{\mathcal{C}}(Y_1,\dots,Y_{n_2})$$

En prenant pour $X_1,\dots,X_{n_1},Y_1,\dots,Y_{n_2}$ les colonnes respectivement de $A_{1,1}$ et $A_{2,2}$, on obtient donc :

$$\det(A)=\det(A_{1,1})\cdot\det(A_{2,2}).$$

Le résultat général se déduit par récurrence comme dans l'autre preuve. □

Exemple IV.9. *Calculons le déterminant de la matrice :*

$$A=\begin{pmatrix}-2&-1&-1&3&-1\\2&3&3&-3&2\\0&0&2&4&-2\\0&0&0&-2&0\\0&0&0&-1&1\end{pmatrix}$$

On reconnaît une matrice triangulaire en blocs, avec les trois blocs diagonaux : $\begin{pmatrix}-2&-1\\2&3\end{pmatrix}$, $\begin{pmatrix}2\end{pmatrix}$ *et* $\begin{pmatrix}-2&0\\-1&1\end{pmatrix}$.
Et donc :

$$\det(A)=\begin{vmatrix}-2&-1\\2&3\end{vmatrix}\cdot\begin{vmatrix}2\end{vmatrix}\cdot\begin{vmatrix}-2&0\\-1&1\end{vmatrix}=(-4)\cdot2\cdot(-2)=16$$

IV.2 Cofacteur et développement suivant une ligne ou colonne

Définition IV.10. *Soient $A\in\mathcal{M}_n(\mathbb{K})$ et $i,j\in[\![1;n]\!]$. On appelle alors :*

1. ***mineur d'ordre*** (i,j) *de A, noté $\Delta_{i,j}(A)$ (ou plus simplement $\Delta_{i,j}$ lorsqu'il n'y a pas d'ambiguïté) le déterminant de la matrice extraite de A, obtenue en supprimant la i-ème ligne et la j-ème colonne ;*
2. ***cofacteur d'ordre*** (i,j) *de A la quantité $(-1)^{i+j}\Delta_{i,j}(A)$.*

Théorème IV.11 (Développement du déterminant suivant une colonne)**.** *Si $A=(a_{i,j})\in\mathcal{M}_n(\mathbb{K})$ et $j\in[\![1;n]\!]$, alors :*

$$\det(A)=\sum_{i=1}^{n}(-1)^{i+j}a_{i,j}\Delta_{i,j}.$$

Démonstration. Notons $C_1,\dots,C_n$ les colonnes de A et $\mathcal{B}=(E_1,\dots,E_n)$ la base canonique de $\mathcal{M}_{n,1}(\mathbb{K})$, de sorte que :

$$\det(A)=\det_{\mathcal{B}}(C_1,\dots,C_n).$$

On a alors : $C_j=\sum_{i=1}^{n}a_{i,j}E_i$, et donc par n-linéarité :

$$\det(A)=\sum_{i=1}^{n}a_{i,j}\det_{\mathcal{B}}(C_1,\dots,C_{j-1},E_i,C_{j+1},\dots,C_n).$$

Fixons $i \in [\![1;n]\!]$, et calculons $\det_{\mathcal{B}}(C_1, \dots, C_{j-1}, E_i, C_{j+1}, \dots, C_n)$. On a :

$$\begin{aligned}
\det_{\mathcal{B}}(C_1, \dots, C_{j-1}, E_i, C_{j+1}, \dots, C_n) &= \begin{vmatrix} a_{1,1} & \dots & a_{1,j-1} & 0 & a_{1,j+1} & \dots & a_{1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{i-1,1} & \dots & a_{i-1,j-1} & 0 & a_{i-1,j+1} & \dots & a_{i-1,n} \\ a_{i,1} & \dots & a_{i,j-1} & 1 & a_{i,j+1} & \dots & a_{i-1,n} \\ a_{i+1,1} & \dots & a_{i+1,j-1} & 0 & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,j-1} & 0 & a_{n,j+1} & \dots & a_{n,n} \end{vmatrix} \\
&= (-1)^{i-1} \cdot (-1)^{j-1} \cdot \begin{vmatrix} 1 & a_{i,1} & \dots & a_{i,j-1} & a_{i,j+1} & \dots & a_{i-1,n} \\ 0 & a_{1,1} & \dots & a_{1,j-1} & a_{1,j+1} & \dots & a_{1,n} \\ & \vdots & & \vdots & \vdots & & \vdots \\ \vdots & a_{i-1,1} & \dots & a_{i-1,j-1} & a_{i-1,j+1} & \dots & a_{i-1,n} \\ & a_{i+1,1} & \dots & a_{i+1,j-1} & a_{i+1,j+1} & \dots & a_{i+1,n} \\ & & \vdots & \vdots & \vdots & & \vdots \\ 0 & a_{n,1} & \dots & a_{n,j-1} & a_{n,j+1} & \dots & a_{n,n} \end{vmatrix} \\
&= (-1)^{i+j} \cdot \begin{vmatrix} a_{1,1} & \dots & a_{1,j-1} & a_{1,j+1} & \dots & a_{1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{i-1,1} & \dots & a_{i-1,j-1} & a_{i-1,j+1} & \dots & a_{i-1,n} \\ a_{i+1,1} & \dots & a_{i+1,j-1} & a_{i+1,j+1} & \dots & a_{i+1,n} \\ & \vdots & \vdots & \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,j-1} & a_{n,j+1} & \dots & a_{n,n} \end{vmatrix} \\
&= (-1)^{i+j} \Delta_{i,j}
\end{aligned}$$

où on a permuté les i premières lignes par le cycle $\begin{pmatrix} 1 & 2 & \dots & i \end{pmatrix}$ qui est de signature $(-1)^{i-1}$, et les j premières colonnes par le cycle $\begin{pmatrix} 1 & 2 & \dots & j \end{pmatrix}$ qui est de signature $(-1)^{j-1}$, et où le dernier déterminant se calcule par blocs. □

Corollaire IV.12 (Développement du déterminant suivant une ligne)**.** *Si $A = (a_{i,j}) \in \mathcal{M}_n(\mathbb{K})$ et $i \in [\![1;n]\!]$, alors :*

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{i,j} \Delta_{i,j}.$$

Démonstration. Découle du théorème précédent appliqué à A^T. □

Remarques IV.13.

1. *On peut ainsi transformer le calcul du déterminant d'une matrice de taille n en celui de n matrices de taille $(n-1)$. Cette méthode n'est en général pas rentable (on peut voir que la complexité est de l'ordre de $n!$ si on effectue toutes les étapes, donc bien plus long qu'un pivot qui demande $\frac{n(n-1)}{2}$ opérations). Mais elle peut être utile lorsque la matrice considérée présente beaucoup de 0 sur une ligne ou une colonne (et on choisira alors cette ligne ou colonne pour développer le déterminant).*
2. *Il ne faut pas oublier les signes à rajouter du fait des $(-1)^{i+j}$. Du fait de la somme, cela revient à alterner les signes, qu'on peut visualiser en mettant en regard la matrice dont on veut calculer le*

déterminant et la matrice des signes :

$$\begin{vmatrix} + & - & + & - & + & \dots \\ - & + & - & + & - & \dots \\ + & - & + & - & + & \dots \\ \vdots & \vdots & & & & \end{vmatrix}.$$

Exemple IV.14. *Reprenons la matrice* $A = \begin{pmatrix} 1 & -1 & 2 & -1 \\ 2 & -1 & 1 & -2 \\ -1 & 3 & 1 & -1 \\ 3 & 0 & -2 & 0 \end{pmatrix}$.
La dernière ligne comporte deux 0*, et en développant suivant cette ligne on trouve :*

$$\det(A) = -3 \cdot \begin{vmatrix} -1 & 2 & -1 \\ -1 & 1 & -2 \\ 3 & 1 & -1 \end{vmatrix} + 2 \cdot \begin{vmatrix} 1 & -1 & -1 \\ 2 & -1 & -2 \\ -1 & 3 & -1 \end{vmatrix}$$

et les deux déterminants de taille 3 *que l'on fait apparaître se calculent rapidement par la règle de Sarrus, ou avec un pivot :*

$$\begin{vmatrix} -1 & 2 & -1 \\ -1 & 1 & -2 \\ 3 & 1 & -1 \end{vmatrix} = \begin{vmatrix} -1 & 2 & -1 \\ 0 & -1 & -1 \\ 0 & 7 & -4 \end{vmatrix} = -\begin{vmatrix} -1 & -1 \\ 7 & -4 \end{vmatrix} = -(4+7) = -11$$

$$\begin{vmatrix} 1 & -1 & -1 \\ 2 & -1 & -2 \\ -1 & 3 & -1 \end{vmatrix} = \begin{vmatrix} 1 & -1 & -1 \\ 0 & 1 & 0 \\ 0 & 2 & -2 \end{vmatrix} = \begin{vmatrix} 1 & 0 \\ 2 & -2 \end{vmatrix} = -2$$

et finalement :

$$\det(A) = -3 \cdots (-11) + 2 \cdot (-2) = 29.$$

IV.3 Le déterminant de Vandermonde

Définition IV.15. *Étant donnés* $n \in \mathbb{N}^*$ *et* $x_1, \dots, x_n \in \mathbb{K}$*, on appelle* ***déterminant de Vandermonde*** *la quantité :*

$$V(x_1, \dots, x_n) = \begin{vmatrix} 1 & 1 & \dots & 1 & 1 \\ x_1 & x_2 & \dots & x_{n-1} & x_n \\ x_1^2 & x_2^2 & \dots & x_{n-1}^2 & x_n^2 \\ \vdots & \vdots & & \vdots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_{n-1}^{n-1} & x_n^{n-1} \end{vmatrix}$$

Proposition IV.16. *Avec les mêmes notations, on a :*

$$V(x_1, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_j - x_i).$$

Démonstration. Montrons le résultat par récurrence sur $n \in \mathbb{N}^*$:
- si $n = 1$: alors $V(x_1) = \big|1\big| = 1$, qui vérifie bien la formule car on trouve le produit vide (qui vaut 1) ;
- si $n = 2$: alors :

$$V(x_1, x_2) = \begin{vmatrix} 1 & 1 \\ x_1 & x_2 \end{vmatrix} = x_2 - x_1$$

qui correspond bien à la formule ;

— supposons le résultat acquis jusqu'au rang n pour $n \in \mathbb{N}^*$, et considérons $x_1, \dots, x_{n+1}$. On souhaite calculer $V(x_1, \dots, x_{n+1})$.
Notons déjà que, si deux des x_i sont égaux, alors la matrice qui définit le déterminant de Vandermonde a deux colonnes égales, donc n'est pas inversible, et l'égalité à montrer est vraie (les deux membres sont nuls).
Si les x_i sont deux-à-deux distincts, posons l'application P définie sur $\mathbb{K}$ par :

$$P : x \mapsto V(x_1, \dots, x_n, x)$$

de sorte que l'on veut calculer $P(x_{n+1})$.
En développant suivant la dernière colonne, on a pour tout $x \in \mathbb{K}$:

$$\begin{aligned} P(x) &= \begin{vmatrix} 1 & 1 & \dots & 1 & 1 \\ x_1 & x_2 & \dots & x_n & x \\ x_1^2 & x_2^2 & \dots & x_n^2 & x^2 \\ \vdots & \vdots & & \vdots & \vdots \\ x_1^n & x_2^n & \dots & x_n^n & x^n \end{vmatrix} = (-1)^{n+2} \cdot 1 \cdot \begin{vmatrix} x_1 & x_2 & \dots & x_n \\ x_1^2 & x_2^2 & \dots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^n & x_2^n & \dots & x_n^n \end{vmatrix} \\ &+ (-1)^{n+3} \cdot x \cdot \begin{vmatrix} 1 & 1 & \dots & 1 \\ x_1^2 & x_2^2 & \dots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^n & x_2^n & \dots & x_n^n \end{vmatrix} + \dots + (-1)^{2n+2} \cdot x^n \cdot \underbrace{\begin{vmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ x_1^2 & x_2^2 & \dots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{vmatrix}}_{V(x_1,\dots,x_n)x^n} \end{aligned}$$

Et ainsi la fonction P est une fonction polynomiale. Plus précisément :
— son monôme dominant est $V(x_1, \dots, x_n) \cdot x^n$;
— $x_1, \dots, x_n$ sont des racines de P.
Et ainsi, on déduit que P est scindé, car, comme tous les x_i sont distincts, P a au moins autant de racines que son degré.
Et finalement on déduit que :

$$\forall x \in \mathbb{K},\ P(x) = V(x_1, \dots, x_n, x) = V(x_1, \dots, x_n) \cdot \prod_{i=1}^{n} (x - x_i)$$

et ainsi, par hypothèse de récurrence, en évaluant en $x = x_{n+1}$ on trouve bien :

$$V(x_1, \dots, x_{n+1}) = V(x_1, \dots, x_n) \prod_{i=1}^{n} (x_{n+1} - x_i) = \prod_{1 \leq i < j \leq n} (x_j - x_i) \cdot \prod_{1 \leq i < j = n+1} (x_j - x_i) = \prod_{1 \leq i < j \leq n+1} (x_j - x_i)$$

ce qui conclut la récurrence.

□

Remarque IV.17. *Le déterminant d'une matrice étant égal à celui de sa transposée, on a également que :*

$$V(x_1, \dots, x_n) = \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix}$$

et on reconnaît la matrice, dans les bases canoniques de $\mathbb{K}_{n-1}[X]$ et $\mathbb{K}^n$, de l'application :

$$\varphi : P \mapsto (P(x_1), \dots, P(x_n)).$$

Il est clair d'une telle application n'est pas inversible si deux des x_i sont égaux. On peut voir indifféremment que, si $x_i = x_j$ pour $i \neq j$ fixés, alors :

— $\varphi(\prod_{k\neq i}(X-x_k)) = 0 = \varphi(0)$, *donc* φ *n'est pas injective ;*
— $(0,\dots,1,\dots 0)$ *(un* 1 *en position* i *et des* 0 *partout ailleurs) n'a pas d'antécédent, car un élément de* $\mathrm{Im}\varphi$ *a mêmes coordonnées en places* i *et* j *; donc* φ *n'est pas surjective.*

Inversement, si les x_i *sont deux-à-deux distincts, en notant* $L_1,\dots,L_n$ *les polynômes interpolateurs de Lagrange associés à la famille* (x_i)*, l'application* φ *est inversible d'inverse :*

$$\varphi^{-1} : (y_1,\dots,x_n) \mapsto \sum_{i=1}^{n} y_i L_i.$$

IV.4 Comatrices

Définition IV.18. *Étant donnée* $A \in \mathcal{M}_n(\mathbb{K})$*, on appelle* ***comatrice de*** A*, notée* $\mathrm{Com}(A)$*, comme la matrice de* $\mathcal{M}_n(\mathbb{K})$ *dont les coefficients sont les cofacteurs de* A*, c'est-à-dire que :*

$$\forall i,j \in [\![1;n]\!],\ [\mathrm{Com}(A)]_{i,j} = (-1)^{i+j}\Delta_{i,j}.$$

Exemple IV.19. *Si* $A = \begin{pmatrix} 2 & -1 & 3 \\ 1 & 1 & 2 \\ 0 & 0 & -3 \end{pmatrix}$*, alors :*

$$\mathrm{Com}(A) = \begin{pmatrix} +\begin{vmatrix} 1 & 2 \\ 0 & -3 \end{vmatrix} & -\begin{vmatrix} 1 & 2 \\ 0 & -3 \end{vmatrix} & +\begin{vmatrix} 1 & 1 \\ 0 & 0 \end{vmatrix} \\ -\begin{vmatrix} -1 & 3 \\ 0 & -3 \end{vmatrix} & +\begin{vmatrix} 2 & 3 \\ 0 & -3 \end{vmatrix} & -\begin{vmatrix} 2 & -1 \\ 0 & 0 \end{vmatrix} \\ +\begin{vmatrix} -1 & 3 \\ 1 & 2 \end{vmatrix} & -\begin{vmatrix} 2 & 3 \\ 1 & 2 \end{vmatrix} & +\begin{vmatrix} 2 & -1 \\ 1 & 1 \end{vmatrix} \end{pmatrix} = \begin{pmatrix} -3 & 3 & 0 \\ -3 & -6 & 0 \\ -5 & -1 & 3 \end{pmatrix}$$

Théorème IV.20. *Si* $A \in \mathcal{M}_n(\mathbb{K})$*, alors :*

$$(\mathrm{Com}(A))^T \cdot A = \det(A)\cdot I_n = A \cdot (\mathrm{Com}(A))^T.$$

Démonstration. Pour $i,j \in [\![1;n]\!]$, on a :

$$\left[A\,(\mathrm{Com}(A))^T\right]_{i,j} = \sum_{k=1}^{n} a_{i,k}(-1)^{j+k}\Delta_{j,k}$$

en notant $\Delta_{j,k}$ les mineurs de A.
On a alors deux situations :
— si $i = j$: on reconnaît directement le développement du déterminant de A suivant la i-ème ligne, et on a ainsi : $\left[A\,(\mathrm{Com}(A))^T\right]_{i,i} = \det(A)$.
— si $i \neq j$: on reconnaît alors le développement suivant la j-ème ligne de la matrice construite à partir de A en remplaçant la j-ème ligne par la i-ème. C'est donc le déterminant d'une matrice ayant deux lignes égales, donc : $\left[A\,(\mathrm{Com}(A))^T\right]_{i,j} = 0$.

Et ainsi : $\left[A\,(\mathrm{Com}(A))^T\right]_{i,j} = \det(A)\cdot\delta_{i,j} = [\det(A)I_n]_{i,j}$ donc $A\,(\mathrm{Com}(A))^T = \det(A)I_n$.
La seconde égalité se montre de même (en reconnaissant des développements de déterminants suivant des colonnes). □

Remarque IV.21. *En prenant la transposée dans les égalités précédentes, on trouve également que*

$$A^T \cdot \mathrm{Com}(A) = \det(A)\cdot I_n = \mathrm{Com}(A)\cdot A^T$$

Corollaire IV.22. *Si $A \in \mathrm{GL}_n(\mathbb{K})$, on a :* $A^{-1} = \dfrac{1}{\det(A)}\mathrm{Com}(A)^T$.

Remarque IV.23. *Cette méthode permet d'exprimer implicitement des inverses de matrices, mais est en général peu efficace car assez longue en calculs. Elle reste raisonnable pour les matrices de taille 2 ou 3, à plus forte raison quand elles présentent de nombreux coefficients nuls (car alors les cofacteurs sont plus facile à calculer).*

Exemples IV.24.

1. *Pour une matrice de taille 2 :* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, *la comatrice est :* $\mathrm{Com}(A) = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$.

   Et donc, si A est inversible, son inverse est : $A^{-1} = \dfrac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

   Si de plus $c = 0$, on obtient que : $A^{-1} = \begin{pmatrix} 1/a & -b/ad \\ 0 & 1/d \end{pmatrix}$, *et on retrouve qu'une matrice triangulaire inversible est triangulaire, avec comme coefficients diagonaux les inverses des coefficients diagonaux de la matrice de départ. Il n'est d'ailleurs pas difficile d'étendre ce résultat à des matrices triangulaires de taille quelconques par un calcul analogue.*

   Si A n'est pas inversible, avec $A \neq 0$, on déduit que les colonnes de $\mathrm{Com}(A)^T$ *sont des éléments de* $\mathrm{Ker}A$ *(qui est de dimension 1), et comme* $\mathrm{Com}(A)^T$ *est non nulle, on déduit que ses colonnes engendrent* $\mathrm{Ker}A$ *(et sont proportionnelles).*

2. *Pour une matrice de taille 3, considérons :* $A = \begin{pmatrix} 4 & 3 & -2 \\ -5 & -1 & 2 \\ -2 & 6 & 3 \end{pmatrix}$.

   On calcule le déterminant de A par règle de Sarrus, ce qui donne :

   $$\det(A) = -12 + 60 - 12 + 4 - 48 + 45 = 37$$

   Et de plus :

   $$\mathrm{Com}(A) = \begin{pmatrix} -15 & 11 & -32 \\ -21 & 8 & -30 \\ 4 & 2 & 11 \end{pmatrix}$$

   Et donc :

   $$A^{-1} = \frac{1}{37} \cdot \begin{pmatrix} -15 & -21 & 4 \\ 11 & 8 & 2 \\ -32 & -30 & 11 \end{pmatrix}$$

Chapitre 25

Séries numériques

I Convergence et divergence d'une série

I.1 Notion de série

Définition I.1. *Étant donnée $(u_n)_{n\in\mathbb{N}}$ une suite à valeurs réelles on complexes, on lui associe la* ***série de terme général*** *u_n, notée $\sum u_n$ (ou $\sum_n u_n$, ou $\sum_{n\geq 0} u_n$), qui est la suite $(S_n)_{n\in\mathbb{N}}$ définie par :*

$$\forall n \in \mathbb{N},\ S_n = \sum_{k=0}^{n} u_k$$

Pour $n \in \mathbb{N}$, on dira que S_n est la ***somme partielle d'ordre*** *n de la série $\sum u_n$.*

Remarques I.2.

1. *Ces notions se généralisent à des suites définies à partir d'un rang n_0. On notera également $\sum_n u_n$ la série associée (s'il n'y a pas d'ambiguïté) ou $\sum_{n\geq n_0} u_n$ si on veut être plus précis). Les sommes partielles sont alors définies seulement pour $n \geq n_0$ par : $S_n = \sum_{k=n_0}^{n} u_k$.*
2. *Une série peut s'analyse comme une suite, en regardant les sommes partielles. Et inversement, on peut analyser n'importe quelle suite (u_n) comme la série de terme général $(u_{n+1} - u_n)$. L'idée sera d'exploiter des résultats de suite pour analyser une série, ou inversement, selon le contexte.*

Exemples I.3.
On a vu différentes situations où les sommes partielles (donc les termes de la série) s'expriment facilement :

1. *si (u_n) est une suite arithmétique : par exemple si $u_n = 3 + 2 \cdot n$ (suite arithmétique de raison 2 et de premier terme 3) alors :*

$$S_n = \sum_{k=0}^{n} 3 + 2 \cdot k = \frac{(n+1)(3+3+2n)}{2} = (n+1)(n+3).$$

2. *si (u_n) est une suite géométrique : par exemple si $u_n = 3 \cdot 2^n$ (suite géométrique de raison 2 et de premier terme 3) alors :*

$$S_n = \sum_{k=0}^{n} 3 \cdot 2^n = 3 \cdot \frac{2^{n+1} - 1}{2 - 1} = 3 \cdot \left(2^{n+1} - 1\right).$$

3. *si on a un télescopage : par exemple si $u_n = \dfrac{1}{n(n+1)} = \dfrac{1}{n} - \dfrac{1}{n+1}$ alors :*

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

Et la linéarité de la somme permet aussi d'utiliser plus généralement ces situations connues.

Définition I.4. *Si (u_n) est une suite numérique, on dira que la série $\sum u_n$* ***converge*** *(ou* ***est convergente****) si la suite (S_n) des sommes partielles converge.*
On notera alors $\sum_{n=0}^{+\infty} u_n$ sa limite, qu'on appellera ***somme*** *de la série.*
Une série qui ne converge pas sera dite divergente.
Plus généralement, on parlera de ***nature*** *d'une série selon qu'elle converge ou non.*

Remarque I.5. *On prendra bien garde à ne pas confondre :*
- *la série $\sum u_n$: qui est une suite ;*
- *la somme partielle $\sum_{k=0}^{n} u_k$: qui est un réel ou un complexe, construit en tant que somme finie ;*
- *la somme de la série $\sum_{n=0}^{+\infty} u_n$: qui n'a même pas toujours un sens.*

Exemples I.6.

1. *Dans les exemples précédents, seule la série associée au téléscopage convergeait.*
2. *La série de terme général $(-1)^n$ diverge. On a en effet que pour tout $n \in \mathbb{N}$:*
$$\sum_{k=0}^{n} (-1)^k = \begin{cases} 0 & si \quad n \text{ est impair} \\ 1 & si \quad n \text{ est pair} \end{cases}$$
3. *La série de terme général $\dfrac{1}{n}$ diverge, tandis que la série de terme général $\dfrac{1}{n^2}$ converge. On avait montré ces deux résultats en montrant que :*
   - *si on note $(S_n)_{n\geq 1}$ la suite des sommes partielles de la série $\sum \dfrac{1}{n}$, alors pour tout $n \in \mathbb{N}^*$ on a :*
   $$S_{2n} - S_n = \sum_{k=n+1}^{2n} \frac{1}{k} \geq \sum_{k=n+1}^{2n} \frac{1}{2n} = \frac{1}{2}$$
   donc la suite (S_n) ne peut converger, car sinon la suite extraite (S_{2n}) convergerait vers la même limite, donc on aurait que $(S_{2n} - S_n)$ tend vers 0 ;
   - *si on note $(T_n)_{n\geq 1}$ la suite des sommes partielles de la série $\sum \dfrac{1}{n^2}$, alors la suite (T_n) est croissante : elle converge si, et seulement si, elle est majorée. Mais pour tout $n \in \mathbb{N}^*$ on a :*
   $$T_n = \sum_{k=1}^{n} \frac{1}{k^2} = 1 + \sum_{k=2}^{n} \frac{1}{k^2} \leq 1 + \underbrace{\sum_{k=2}^{n} \frac{1}{k(k-1)}}_{=1-\frac{1}{n} \text{ par téléscopage}} \leq 2$$
   et donc (T_n) converge, donc la série $\sum \dfrac{1}{n^2}$ converge.

Proposition I.7. *Étant donnée $(u_n)_{n\geq n_0}$ une suite complexe et $n_1 \geq n_0$, les séries $\sum_{n\geq n_0} u_n$ et $\sum_{n\geq n_1} u_n$ ont même nature.*

Démonstration. On revient à la définition de la convergence, avec les sommes partielles. On a pour tout $n \geq n_1$:
$$\sum_{k=n_0}^{n} u_k = \sum_{k=n_0}^{n_1-1} u_k + \sum_{k=n_1}^{n} u_k$$
et donc les sommes partielles associées aux suites $(u_n)_{n\geq n_0}$ et $(u_n)_{n\geq n_1}$ diffèrent d'une constante : l'une converge si, et seulement si, l'autre converge. C'est-à-dire que les séries associées ont même nature. □

Remarque I.8. *On s'intéressera ainsi plus particulièrement au comportement en l'infini d'une suite pour déterminer la nature de la série associée, et retirer éventuellement les premiers termes si ceux-ci posent problème.*
En revanche, pour déterminer la somme d'une série, il faudra bien prendre garde à conserver tous les termes, puisque ceux-ci ont une incidence sur la somme.

Proposition I.9. *La suite (u_n) et la série télescopique $\sum (u_{n+1} - u_n)$ ont même nature.*

Démonstration. Pour tout $n \in \mathbb{N}$, on a :

$$\sum_{k=0}^{n} u_{k+1} - u_k = u_{n+1} - u_0$$

et donc la série $\sum(u_{n+1} - u_n)$ a même nature que la suite (u_{n+1}), donc que la suite (u_n) par extraction. □

I.2 Sommes et restes d'une série convergente

Proposition I.10 (Linéarité de la somme)**.** *Si $\sum u_n, \sum v_n$ sont deux séries convergentes et $\lambda, \mu \in \mathbb{C}$, alors la série $\sum (\lambda u_n + \mu v_n)$ converge et :*

$$\sum_{n=0}^{+\infty} (\lambda u_n + \mu v_n) = \lambda \sum_{n=0}^{+\infty} u_n + \mu \sum_{n=0}^{+\infty} v_n.$$

Démonstration. Cela découle directement de la linéarité de la somme. Plus précisément, si $n \in \mathbb{N}$ on a :

$$\sum_{k=0}^{n} (\lambda u_k + \mu v_k) = \lambda \sum_{k=0}^{n} u_k + \mu \sum_{k=0}^{n} v_k$$

et en passant à la limite dans le membre de droite, on déduit que :

$$\lim_{n \to +\infty} \sum_{k=0}^{n} (\lambda u_k + \mu v_k) = \lambda \sum_{n=0}^{+\infty} u_n + \mu \sum_{n=0}^{+\infty} v_n$$

□

Remarques I.11.

1. *On obtient notamment que multiplier une suite par un scalaire (non nul) ne change pas la nature de sa série.*
2. *La réciproque est fausse : prenons $\lambda = \mu = 1$ et $(v_n) = (-u_n)$ avec $\sum u_n$ divergente, ce qui donne une combinaison linéaire de série qui converge, alors qu'aucune des séries ne converge.*
3. *Ce résultat peut aussi s'utiliser pour déterminer la nature d'une série : si $\sum u_n$ converge, alors les deux séries $\sum v_n$ et $\sum(u_n + v_n)$ ont même nature. La réciproque se déduit de la proposition appliquée à $\sum u_n$ et $\sum v_n$, et la réciproque avec $\sum(-u_n)$ et $\sum(u_n + v_n)$.*

Proposition-Définition I.12. *Si la série $\sum u_n$ converge, alors la suite (u_n) tend vers 0.*
Ainsi, si la suite (u_n) ne tend pas vers 0, la série $\sum u_n$ sera divergente, et on dira qu'elle ***diverge grossièrement****.*

Démonstration. Si la série $\sum u_n$ converge, alors les suites $(\sum_{k=0}^{n} u_k)$ et $\left(\sum_{k=0}^{n-1} u_k\right)$ convergent vers une même limite, donc leur différence, à savoir (u_n) tend vers 0.
Le reste découle par contraposée. □

Remarque I.13. *La réciproque est fausse. Une suite peut tendre vers* 0 *sans que sa série ne converge, ou même ne soit bornée. On a vu par exemple que* $\sum \frac{1}{n}$ *diverge alors que* $\left(\frac{1}{n}\right)$ *tend vers* 0.
En revanche, cela dit plus rapidement que $\sum(-1)^n$ *diverge, sans avoir à calculer les sommes partielles. La première chose à faire pour déterminer si une série converge est donc de vérifier si son terme général tend vers* 0.

Exemple I.14. *La série de terme général* $\left(1-\frac{\pi}{n}\right)^{\sqrt{n}}$ *est divergente car :*

$$\left(1-\frac{\pi}{n}\right)^{\sqrt{n}} = \exp\left(\sqrt{n}\ln\left(1-\frac{\pi}{n}\right)\right) = \exp\left(\sqrt{n}\left(\frac{-\pi}{n}+\mathrm{o}\left(\frac{1}{n}\right)\right)\right) = \exp\left(-\frac{\pi}{\sqrt{n}}+\mathrm{o}\left(\frac{1}{\sqrt{n}}\right)\right) \underset{n\to+\infty}{\to} 1 \neq 0$$

Remarque I.15. *Cette analyse asymptotique est d'autant plus intéressante qu'on verra d'autres critères, en fonction de la vitesse à laquelle la suite* (u_n) *tend vers* 0*, pour en déduire la nature de la série* $\sum u_n$*. L'idée derrière est que non seulement le terme général doit tendre vers* 0*, mais il doit tendre suffisamment vite pour avoir la convergence de la série (à une considération près sur le signe dont on parlera plus tard).*

Définition I.16. *Si* $\sum u_n$ *est une série convergente, on définit son* ***reste de rang*** n*, pour* $n \in \mathbb{N}$*, comme la quantité :*

$$R_n = \sum_{k=0}^{+\infty} u_k - \sum_{k=0}^{n} u_k = \sum_{k=n+1}^{+\infty} u_k.$$

Remarque I.17. *Le reste donne la vitesse de convergence d'une série vers sa limite.*

Proposition I.18. *Avec les mêmes notations, la suite* (R_n) *tend vers* 0.

Démonstration. On a pour tout $n \in \mathbb{N}$ que :

$$R_n = \sum_{k=0}^{+\infty} u_k - \sum_{k=0}^{n} u_k$$

et par convergence de la série $\sum u_n$, on a : $\lim\limits_{n\to+\infty} \sum_{k=0}^{n} u_k = \sum_{k=0}^{+\infty} u_k$. Ce qui donne bien que R_n tend vers 0 par opérations sur les limites. □

I.3 Séries usuelles

Remarque I.19. *Comme la seule suite arithmétique qui tend vers* 0 *est la suite constante nulle, on ne s'intéresse pas à l'étude de "séries arithmétiques".*

Proposition I.20 (Série géométrique)**.** *Pour* $q \in \mathbb{C}$*, la série de terme général* q^n *est convergente si, et seulement si,* $|q| < 1$*, et on a alors :*

$$\sum_{n=0}^{+\infty} q^n = \frac{1}{1-q}.$$

Démonstration. Notons déjà que, si $|q| \geq 1$, alors pour tout $n \in \mathbb{N}$ on a : $|q^n| = |q|^n \geq 1$, donc la série $\sum q^n$ diverge grossièrement.
Si $|q| < 1$, alors on a explicitement les sommes partielles, avec :

$$\forall n \in \mathbb{N},\ \sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q} \underset{n\to+\infty}{\to} \frac{1}{1-q}$$

en notant que $\lim\limits_{n\to+\infty} q^n = 0$ (par limite classique). Et ainsi $\sum q^n$ converge, et sa somme vaut $\frac{1}{1-q}$. □

Corollaire I.21. *Si (u_n) est une suite géométrique (non nulle) de raison $q \in \mathbb{C}$, la série $\sum u_n$ converge si, et seulement si, $|q| < 1$, et dans ce cas sa somme est : $\dfrac{u_0}{1-q}$.*

Démonstration. Par linéarité. □

Exemple I.22. *Soit $u_n = \dfrac{5^{2n+3}}{3^{3n-2}}$. Alors (u_n) est une suite géométrique de raison $q = \dfrac{5^2}{3^3} = \dfrac{25}{27}$, et donc la série $\sum u_n$ converge, et sa somme vaut :*

$$\sum_{n=0}^{+\infty} u_n = \frac{5^3}{3^{-2}} \frac{1}{1-\dfrac{5^2}{3^3}} = \frac{5^3 \cdot 3^5}{3^3 - 5^2} = \frac{3^5 \cdot 5^3}{2} = \frac{30375}{2}.$$

Proposition I.23 (Série exponentielle)**.** *Si $z \in \mathbb{C}$, la série de terme général $\dfrac{z^n}{n!}$ est convergente, avec :*

$$\sum_{n=0}^{+\infty} \frac{z^n}{n!} = e^z.$$

Démonstration. Fixons $z \in \mathbb{C}$, et considérons la fonction $f : \left\{ \begin{array}{ccc} [0;1] & \to & \mathbb{C} \\ t & \mapsto & e^{tz} \end{array} \right.$.
Alors on avait vu (au Chapitre 8) que, comme la fonction $t \mapsto tz$ est dérivable sur $[0;1]$, alors f est dérivable sur $[0;1]$ avec : $f' : t \mapsto ze^{tz}$.
Une récurrence immédiate montre alors que f est infiniment dérivable avec :

$$\forall k \in \mathbb{N},\ \forall t \in [0;1],\ f^{(k)}(t) = z^k e^{tz}.$$

On déduit ainsi que :

$$\forall k \in \mathbb{N},\ \forall t \in [0;1],\ |f^{(k)}(t)| = |z|^k |e^{tz}| = |z| e^{t\mathrm{Re}(z)} \leq |z|^k \cdot e^{|z|}.$$

Par inégalité de Taylor–Lagrange appliquée à f à l'ordre n, on a donc :

$$\left| e^z - \sum_{k=0}^{n} \frac{z^k}{k!} \right| = \left| f(1) - \sum_{k=0}^{n} \frac{f^{(k)}(0)}{k!}(1-0)^k \right| \leq e^{|z|} \frac{|z|^{n+1} \cdot 1^n}{(n+1)!}$$

où le membre de droite tend vers 0 par croissances comparées.
Et on a donc bien : que la série $\sum \dfrac{z^n}{n!}$ converge, et que sa somme vaut e^z. □

Remarque I.24. *Beaucoup considèrent cette série comme la **définition** de la fonction exponentielle : grâce aux différents résultats sur les séries qu'on verra dans ce chapitre, on peut ainsi retrouver toutes les propriétés de l'exponentielle (exponentielle d'une somme, dérivée, etc.).*
On peut ainsi définir les fonctions cos *et* sin *à partir de l'exponentielle ainsi définie, grâce aux formules d'Euler, et retrouver leurs propriétés.*
Et surtout, cela donne une autre définition au nombre π : c'est le double du premier point d'annulation sur $\mathbb{R}_+$ de la fonction cos.

Exemple I.25. *Si l'on considère $z \in \mathbb{C}$, alors les séries $\sum \dfrac{z^n}{n!}$ et $\sum \dfrac{(-z)^n}{n}!$ sont convergentes, de sommes respectives : e^z et e^{-z}.*
Et donc pour tout $n \in \mathbb{N}$ on que la série de terme général $\dfrac{1}{2}\dfrac{z^n}{n!} + \dfrac{1}{2}\dfrac{(-z)^n}{n!}$ converge. Sa somme vaut :

— *par définition :*

$$\sum_{n=0}^{+\infty} \frac{z^n + (-z)^n}{2 \cdot n!} = \sum_{n=0,\ n\ pair}^{+\infty} \frac{z^n}{n!} = \sum_{n=0}^{+\infty} \frac{z^{2n}}{(2n)!}$$

— *par linéarité :*

$$\frac{e^z + e^{-z}}{2} = \mathrm{ch}(z).$$

et donc on trouve que : $\mathrm{ch}(z) = \sum_{n=0}^{+\infty} \frac{z^{2n}}{(2n)!}$*, ce qui coïncide (pour* $z \in \mathbb{R}$*) avec la formule et le développement limité (poussé à l'infini par inégalité de Taylor–Lagrange) du cosinus hyperbolique.*
Et on pourrait faire de même avec le sinus hyperbolique. Et tout cela reste très proche des considérations énoncées précédemment autour de cos *et de* sin*.*

II Séries à termes positifs

II.1 Inégalité et séries à termes positifs

Remarque II.1. *Du fait de la linéarité, l'étude des séries à termes positifs permet de comprendre les séries à termes de signe (ou argument) constant.*
Et comme changer les premiers termes d'une suite ne change pas la nature de sa série, on peut étendre les résultats à des séries à termes positifs à partir d'un certain rang.
Le problème reste quand la suite change une infinité de fois de signe.

Proposition II.2. *Si* $\sum u_n$ *est une série à termes positifs, alors elle converge si, et seulement si, la suite de ses sommes partielles est majorée.*

Démonstration. Si $\sum u_n$ est à termes positifs, alors la suite (S_n) de ses sommes partielles est une suite croissante : elle converge si, et seulement si, elle est majorée. □

Remarque II.3. *On a en fait un peu mieux : la série* $\sum u_n$ *a toujours une limite, et dans le cas où elle diverge cette limite est* $+\infty$*.*
Dans le cas où elle converge, on a :

$$\sum_{n=0}^{+\infty} u_n = \sup\{\sum_{k=0}^{n} u_k \,|\, n \in \mathbb{N}\}.$$

Proposition II.4. *Soient* $(u_n), (v_n)$ *deux suites à valeurs positives telles que :* $\forall n \in \mathbb{N},\ 0 \leq u_n \leq v_n$*. Alors :*

1. *si* $\sum v_n$ *converge, alors* $\sum u_n$ *converge ;*
2. *si* $\sum u_n$ *diverge, alors* $\sum v_n$ *diverge.*

De plus, s'il y a convergence, alors : $0 \leq \sum_{n=0}^{+\infty} u_n \leq \sum_{n=0}^{+\infty} v_n$*.*

Démonstration.

1. si $\sum v_n$ converge : alors pour tout $n \in \mathbb{N}$, on a :

$$0 \leq \sum_{k=0}^{n} u_k \leq \sum_{k=0}^{n} v_k \leq \sum_{k=0}^{+\infty} v_k$$

et donc les sommes partielles de la série $\sum u_n$ sont majorées, donc la série $\sum u_n$ converge.
En passant à la limite dans l'inégalité précédente, on trouve bien que $0 \leq \sum_{n=0}^{+\infty} u_n \leq \sum_{n=0}^{+\infty} v_n$.

2. si $\sum u_n$ diverge : alors $\sum u_n$ tend vers $+\infty$, et en utilisant à nouveau que $0 \leq \sum_{k=0}^{n} u_k \leq \sum_{k=0}^{n} v_k$ on déduit que la série $\sum v_n$ tend vers $+\infty$ par encadrement.

□

Remarque II.5. *Les résultats de convergence restent valables si l'inégalité $0 \leq u_n \leq v_n$ n'est valable qu'à partir d'un certain rang. En revanche, l'inégalité sur les sommes n'est alors plus vérifiée.*
Et ils s'étendent également par linéarité à des suites de même argument constant à partir d'un certain rang.

Exemples II.6.

1. *Pour tout $n \in \mathbb{N}$, on a : $1 \leq 2 + \cos(n) \leq 3$ et donc la série $\sum \dfrac{2+\cos(n)}{3^n}$ converge (étant majorée par $\sum \dfrac{3}{3^n}$ qui converge) mais la série $\sum \dfrac{2+\cos(n)}{n}$ diverge (étant minorée par $\sum \dfrac{1}{n}$ qui diverge).*
2. *Si $P \in \mathbb{R}[X]$, la série $\sum P(n)e^{-n}$ converge car :*
   — *si P est unitaire, on a alors $\lim\limits_{n\to+\infty} P(n) = +\infty$, et donc à partir d'un certain rang la suite $(P(n)e^{-n})$ est positive.*
   — *sinon on se ramène par linéarité au cas où P est unitaire ;*
   Et alors, par croissance comparée on a : $\lim\limits_{n\to+\infty} P(n)e^{-n/2} = 0$. Et donc, à partir d'un certain rang on a $0 \leq P(n)e^{-n} \leq e^{-n/2} = \left(e^{-1/2}\right)^n$, qui est le terme général d'une série convergente (comme on a une série géométrique de raison $e^{-1/2}$ avec $|e^{-1/2}| < 1$).
   Et le résultat se généralise sans trop de mal au cas où $P \in \mathbb{C}[X]$ par linéarité (en traitant séparément la convergence des monômes). On verra qu'on peut même les étendre à une série de la forme $\sum P(n)q^n$ pour $P \in \mathbb{C}[X]$ et $q \in \mathbb{C}$ avec $|q| < 1$.
3. *Comme on a vu que $\sum \dfrac{1}{n}$ diverge, alors pour tout $\alpha \leq 1$ on a que $\sum \dfrac{1}{n^\alpha}$ diverge également comme on a pour un tel α : $\dfrac{1}{n} \leq \dfrac{1}{n^\alpha}$.*

II.2 Relations de comparaisons et séries à termes positifs

Proposition II.7. *Si $(u_n), (v_n)$ sont telles que :*

1. *les suites (u_n) et (v_n) sont à termes positifs ;*
2. *$u_n = \mathrm{O}(v_n)$;*
3. *$\sum v_n$ converge ;*

alors $\sum u_n$ converge.

Démonstration. Comme $(u_n), (v_n)$ sont à termes positifs et que $u_n = \mathrm{O}(v_n)$, il existe $M \in \mathbb{R}_+$ telle que : $\forall n \in \mathbb{N},\ 0 \leq u_n \leq M \cdot v_n$.
La série $\sum v_n$ converge, donc la série $\sum Mv_n$ également, et on conclut par la proposition précédente que $\sum u_n$ converge. □

Théorème II.8. *Si $(u_n), (v_n)$ sont deux suites **à termes positifs** telles que $u_n \sim v_n$, alors les séries $\sum u_n$ et $\sum v_n$ ont même nature.*

Démonstration. On utilise la proposition précédente, en notant que, comme $u_n \sim v_n$, alors :
— $u_n = \mathrm{O}(v_n)$: si $\sum v_n$ converge, alors $\sum u_n$ aussi ;
— $v_n = \mathrm{O}(u_n)$: si $\sum u_n$ converge, alors $\sum v_n$ aussi.
Ce qui donne bien l'équivalence. □

Remarque II.9. *Le résultat est faux si les suites considérées ne sont pas à termes positifs (ou au moins de signe constant). Et il faudra toujours le préciser. On verra par exemple que la série* $\sum \frac{(-1)^n}{\sqrt{n}}$ *converge, ce qui implique la divergence de la série* $\sum \left(\frac{(-1)^n}{\sqrt{n}} + \frac{1}{n}\right)$*, alors que les termes généraux sont équivalents.*

Du fait des propriétés des équivalences de suites, il suffira en fait de voir que l'une des deux suites est à termes positifs.

Exemples II.10.

1. *Si* $u_n = \cos\left(\frac{n}{2^n}\right) - 1$*, alors* $u_n \sim -\frac{n^2}{4^n}$*, qui est le terme général d'une série convergente de signe constant. La convergence vient du fait que, par croissances comparées :* $\frac{n^2}{4^n} = \mathrm{O}\left(\frac{1}{2^n}\right)$.

2. *Si* $u_n = 1 - e^{1/n}$*, alors* $\sum u_n$ *diverge comme* $u_n \sim \frac{1}{n}$ *qui est le terme général d'une série divergente* ***à termes positifs****.*

3. *Si* $n \in \mathbb{N}^*$*, on a :* $\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$*, et donc la série de terme général* $\frac{1}{n(n+1)}$ *converge.*

   Comme $\frac{1}{n^2} \sim \frac{1}{n(n+1)}$ *et que ces suites sont* ***à termes positifs****, on déduit que la série* $\sum \frac{1}{n^2}$ *converge.*

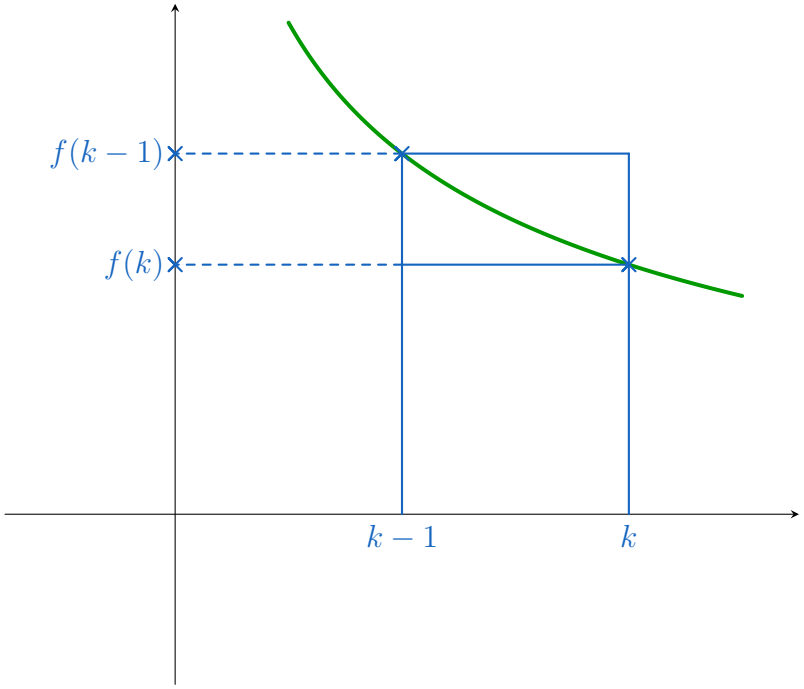
   On montrerait de même que, pour tout $\alpha > 1$*, la série* $\sum \frac{1}{n^\alpha}$ *converge, en notant que, par télescopage sur les sommes partielles, la série* $\sum \left(\frac{1}{n^{\alpha-1}} - \frac{1}{(n+1)^{\alpha-1}}\right)$ *converge et que :*

$$\frac{1}{n^{\alpha-1}} - \frac{1}{(n+1)^{\alpha-1}} = \frac{\left(1+\frac{1}{n}\right)^{\alpha-1} - 1}{(n+1)^{\alpha-1}} \sim \frac{\alpha-1}{n^\alpha}.$$

II.3 Comparaisons entre séries et intégrales

Théorème II.11 (Comparaison séries/intégrales)**.** *Soit* f *une fonction continue par morceaux positive décroissante sur* $[0;+\infty[$*. Alors la séries* $\sum_{n\geq a} f(n)$ *converge si, et seulement si, la suite* $\left(\int_0^n f(t)\mathrm{d}t\right)_{n\in\mathbb{N}}$ *converge.*

Démonstration.



Notons déjà que, comme f est positive, alors la série $\sum f(n)$ est convergente si, et seulement si, elle est majorée.
Et de même, par positivité de f, la suite $\left(\int_0^n f(t)\mathrm{d}t\right)_{n\in\mathbb{N}}$ est croissante, comme pour tout $n \in \mathbb{N}$ on a :

$$\int_0^{n+1} f(t)\mathrm{d}t - \int_0^n f(t)\mathrm{d}t = \int_n^{n+1} f(t)\mathrm{d}t \geq 0$$

en utilisant la relation de Chasles et la positivité de l'intégrale. Donc la suite $\left(\int_0^n f(t)\mathrm{d}t\right)_{n\in\mathbb{N}}$ converge si, et seulement si elle est bornée.
Considérons $k \in \mathbb{N}$. Alors par monotonie de f on a :

$$\forall t \in [k; k+1],\ f(k+1) \leq f(t) \leq f(k)$$

et donc en intégrant entre k et $k+1$ on trouve :

$$f(k+1) = \int_k^{k+1} f(k+1)\mathrm{d}t \leq \int_k^{k+1} f(t)\mathrm{d}t \leq \int_k^{k+1} f(k)\mathrm{d}t = f(k)$$

puis en sommant pour $k \in [\![0; n-1]\!]$ on trouve :

$$\sum_{k=1}^{n} f(k) \leq \int_0^n f(t)\mathrm{d}t \leq \sum_{k=0}^{n-1} f(k)$$

et finalement :

- si $\sum f(n)$ converge : alors elle est majorée, et tout majorant est un majorant de $\left(\int_0^n f(t)\mathrm{d}t\right)$, qui est donc convergente ;
- si $\sum f(n)$ diverge : alors elles tend vers $+\infty$, donc $\sum_{n\geq 1} f(n)$ aussi, et donc par encadrement $\left(\int_0^n f(t)\mathrm{d}t\right)$ diverge aussi.

ce qui donne bien l'équivalence. □

Remarques II.12.

1. *On peut tout aussi bien translater la série ou l'intégrale sans changer le résultat. Plus précisément, si $a \in \mathbb{R}$ et f continue par morceaux, positive, décroissante sur $[a; +\infty[$, alors la série $\sum_{n\geq a} f(n)$ a même nature que la suite $\left(\int_a^n f(t)\mathrm{d}t\right)_{n\geq a}$.*

2. *L'encadrement donné entre les sommes partielles et les intégrales se comprend bien en terme de croissance d'intégrale : il s'agit d'encadrer, à la manière des rectangles, la fonction f par les fonctions en escaliers qui prennent les mêmes valeurs que f en les entiers. Et on peut ainsi interpréter la série comme une intégrale, et on a un problème de comparaison d'intégrales.*
   Inversement, par télescopage, on peut interpréter la suite des intégrales comme la série de terme général $\int_n^{n+1} f(t)\mathrm{d}t$ (par télescopage), qui est une série à termes positifs. Et on peut alors traiter le problème comme une comparaison entre des séries à termes positifs (les mêmes encadrements donnant que les séries considérées ont même nature).
3. *On a mieux que la convergence ou la divergence des séries : l'encadrement entre sommes partielles et intégrales permet d'avoir des équivalents des restes (en cas de convergence de la série) ou des sommes partielles (en cas de divergence de la série).*

Théorème II.13 (Séries de Riemann)**.** *Pour $\alpha \in \mathbb{R}$, la série $\sum \dfrac{1}{n^\alpha}$ converge si, et seulement si, $\alpha > 1$.*

*De telles séries sont appelées **séries de Riemann**. Lorsque $\alpha = 1$, on retrouve la série $\sum_{n\geq 1} \dfrac{1}{n}$ qu'on appelle **série harmonique**.*

Démonstration. Notons déjà que, si $\alpha \leq 0$, alors la série $\sum \dfrac{1}{n^\alpha}$ diverge grossièrement.

Si $\alpha > 0$, considérons la fonction $f : t \mapsto \dfrac{1}{t^\alpha}$ qui est continue, positive, décroissante sur $[1;+\infty[$. Et donc par le théorème précédent, la série $\sum \dfrac{1}{n^\alpha}$ converge si, et seulement si, la suite $\left(\int_1^n \dfrac{\mathrm{d}t}{t^\alpha}\right)$ converge. Mais on a pour tout $n \in \mathbb{N}^*$:

$$\int_1^n \frac{\mathrm{d}t}{t^\alpha} = \begin{cases} \ln(n) & \text{si} \quad \alpha = 1 \\ \dfrac{1}{\alpha-1}\left(1 - \dfrac{1}{n^{\alpha-1}}\right) & \text{si} \quad \alpha \neq 1 \end{cases} \underset{n\to+\infty}{\to} \begin{cases} +\infty & \text{si} \quad \alpha \leq 1 \\ \dfrac{1}{\alpha-1} & \text{si} \quad \alpha > 1 \end{cases}$$

ce qui donne bien que la série $\sum \dfrac{1}{n^\alpha}$ converge si, et seulement si, $\alpha > 1$. □

Remarques II.14.

1. *On peut se passer de la comparaison à des intégrales : le cas $\alpha = 1$ avait été fait en regardant les sommes partielles de rang n et $2n$, et permet de déduire les cas $\alpha \leq 1$. Et le cas $\alpha > 1$ avait été traité par télescopage. L'intérêt des intégrales est surtout qu'elle donne des encadrements, et donc des meilleures estimations des sommes partielles ou des restes.*
2. *Il ne faut pas les confondre avec les **sommes** de Riemann, qu'on a vu au chapitre d'intégration, qui ne sont pas du tout de la même forme (même si on a vu certains liens entre les deux notions).*
3. *On n'aura pas toujours des séries de Riemann, mais l'intérêt est que l'on pourra parfois comparer (par exemple grâce au théorème de croissances comparées) à des séries de Riemann, ce qui permettra d'estimer la convergence ou non d'une série.*
4. *Le théorème ci-dessus donne la convergence des séries, mais pas leurs sommes. Elles sont en générales très compliquées à expliciter, et constituent un objet fondamental en recherche mathématiques, à savoir la fonction zêta de Riemann, définie par : $\zeta : \alpha \mapsto \sum_{n=1}^{+\infty} \dfrac{1}{n^\alpha}$. On peut donner explicitement les valeurs de ζ aux entiers positifs pairs (par exemple $\zeta(2) = \sum_{n=1}^{+\infty} \dfrac{1}{n^2} = \dfrac{\pi^2}{6}$), mais on connaît très peu d'informations sur les valeurs en les entiers impairs. On sait depuis 2000 qu'une infinité est irrationnels, et depuis 2001 que l'un des quatre nombres $\zeta(5), \zeta(7), \zeta(9), \zeta(11)$ est irrationnel. Mais c'est à peu près tout.*

Exemples II.15.

1. *La série de terme général* $\frac{1}{n}$ *diverge. Et on a pour tout* $n \in \mathbb{N}^*$ *l'encadrement :*

$$\sum_{k=2}^{n+1} \frac{1}{k} \leq \int_1^{n+1} \frac{1}{t}\mathrm{d}t \leq \sum_{k=1}^{n} \frac{1}{k}$$

ce qui donne donc :

$$\int_1^{n+1} \frac{1}{t}\mathrm{d}t \leq \sum_{k=1}^{n} \frac{1}{k} \leq 1 + \int_1^{n} \frac{1}{t}\mathrm{d}t$$

et comme $\int_1^{n+1} \frac{1}{t}\mathrm{d}t = \ln(n+1) \sim \ln(n)$ *et* $1 + \int_1^n \frac{1}{t}\mathrm{d}t = 1 + \ln(n) \sim \ln(n)$*, on trouve que :*

$$S_n = \sum_{k=1}^{n} \frac{1}{k} \sim \ln(n).$$

2. *La série de terme général* $\frac{1}{n^2}$ *converge, et pour tout* $n \in \mathbb{N}^*$ *et* $N \geq n+1$ *on a :*

$$\sum_{k=n+1}^{N+1} \frac{1}{k^2} \leq \int_n^{N+1} \frac{1}{t^2}\mathrm{d}t \leq \sum_{k=n}^{N} \frac{1}{k^2}$$

ce qui donne donc :

$$\int_{n+1}^{N+1} \frac{1}{t^2}\mathrm{d}t \leq \sum_{k=n+1}^{N} \frac{1}{k^2} \leq \frac{1}{(n+1)^2} + \int_{n+1}^{N} \frac{1}{t^2}\mathrm{d}t$$

Et on a :

$$\int_{n+1}^{N+1} \frac{1}{t^2}\mathrm{d}t = \frac{1}{n+1} - \frac{1}{N+1} \underset{N\to+\infty}{\to} \frac{1}{n+1} \sim \frac{1}{n}$$

$$\frac{1}{(n+1)^2} + \int_{n+1}^{N} \frac{1}{t^2}\mathrm{d}t = \frac{1}{(n+1)^2} + \frac{1}{n+1} - \frac{1}{N} \underset{N\to+\infty}{\to} \frac{1}{n+1} + \frac{1}{(n+1)^2} \sim \frac{1}{n}$$

ce qui donne, en passant à la limite dans l'inégalité précédente et par encadrement d'équivalents que :

$$R_n = \sum_{k=n+1}^{+\infty} \frac{1}{k^2} \sim \frac{1}{n}.$$

Exemple II.16. *On considère* $\alpha, \beta \in \mathbb{R}$*, et on s'intéresse à la série de terme général* $\frac{1}{n^\alpha \ln(n)^\beta}$*. Alors :*

— *si* $\alpha < 1$ *: alors par croissances comparées, on a que :*

$$\frac{1}{n^{(1+\alpha)/2}} = \mathrm{o}\left(\frac{1}{n^\alpha \ln(n)^\beta}\right)$$

comme :

$$\frac{1}{n^\alpha \ln(n)^\beta} = \frac{1}{n^{(1+\alpha)/2}} \cdot \underbrace{\frac{n^{(1-\alpha)/2}}{\ln(n)^\beta}}_{\underset{n\to+\infty}{\to} +\infty}$$

et donc, comme la série de terme général $\frac{1}{n^{(1+\alpha)/2}}$ *diverge (comme* $\frac{1+\alpha}{2} < 1$*), alors la série de terme général* $\frac{1}{n^\alpha \ln(n)^\beta}$ *diverge également ;*

— *si $\alpha > 1$: on procède à nouveau par croissances comparées, et on trouve que :*

$$\frac{1}{n^\alpha \ln(n)^\beta} = \mathrm{o}\left(\frac{1}{n^{(1+\alpha)/2}}\right)$$

comme on a cette fois-ci :

$$\frac{1}{n^\alpha \ln(n)^\beta} = \frac{1}{n^{(1+\alpha)/2}} \cdot \underbrace{\frac{n^{(1-\alpha)/2}}{\ln(n)^\beta}}_{\underset{n\to+\infty}{\to} 0}$$

et comme la série de terme général $\dfrac{1}{n^{(1+\alpha)/2}}$ converge (comme $\frac{1+\alpha}{2} > 1$), alors la série de terme général $\dfrac{1}{n^\alpha \ln(n)^\beta}$ converge également ;

— *reste le cas où $\alpha = 1$: si $\beta \leq 0$, alors $\dfrac{1}{n\ln(n)^\beta} \geq \dfrac{1}{n}$ et on a donc divergence de la série. Si $\beta > 0$, on procède par comparaison à une intégrale, comme la fonction $t \mapsto \dfrac{1}{t\ln(t)^\beta}$ est continue positive décroissante sur $[2;+\infty[$. Pour $n \geq 2$ on a par changement de variable $u = \ln(t)$:*

$$\int_2^n \frac{1}{t\ln(t)^\beta}\mathrm{d}t = \int_{\ln(2)}^{\ln(n)} \frac{\mathrm{d}u}{u^\beta}$$

qu'on avait déjà étudiée pour les séries de Riemann, et qui tend vers une limite finie si, et seulement si, $\beta > 1$.

Et finalement la série de terme général $\dfrac{1}{n^\alpha \ln(n)^\beta}$ converge si, et seulement si, $\alpha > 1$ ou $\alpha = 1$ et $\beta > 1$.

III Séries absolument convergentes

III.1 Convergence et absolue convergence

Définition III.1. *Si (u_n) est une suite à valeurs complexes, la série $\sum u_n$ est dite* ***absolument convergente*** *si la série $\sum |u_n|$ converge.*

Remarque III.2. *L'intérêt est de ramener l'étude d'une série à termes complexes à celle d'une série à termes positifs. Et comme changer une suite de signe constant en sa valeur absolue revient à la multiplier par une constant (1 ou -1 selon son signe), une série à termes de signe constant est convergente si, et seulement si, elle est absolument convergente.*

Exemples III.3.

1. *En tant que séries à termes positifs, les séries de Riemann de paramètre $\alpha > 1$ sont absolument convergentes.*
2. *Une série géométrique est absolument convergente si, et seulement si, elle est convergente : si (u_n) est géométrique de raison q, alors $|u_n|$ est géométrique de raison $|q|$. La convergence de l'une ou l'autre des séries est équivalente au fait que $|q| < 1$.*
3. *La série exponentielle est absolument convergente, puisque pour tout $z \in \mathbb{C}$ on a :*

$$\left|\frac{z^n}{n!}\right| = \frac{|z|^n}{n!}$$

qui est le terme général d'une série convergente, à savoir de la série qui définit $e^{|z|}$.

4. *La série* $\sum \dfrac{(-1)^n}{n^2}$ *est absolument convergente, car on retrouve la série de Riemann de paramètre* 2.
   En revanche la série $\sum \dfrac{(-1)^n}{n}$ *n'est pas absolument convergente (on retrouve la série harmonique).*

Théorème III.4. *Toute série absolument convergente est convergente.*
De plus, si $\sum u_n$ *est absolument convergente, alors :*

$$\left|\sum_{k=0}^{+\infty} u_n\right| \leq \sum_{k=0}^{+\infty} |u_n|.$$

Démonstration. Notons (u_n) suite numérique telle que $\sum u_n$ converge absolument.
Si (u_n) est à valeurs réelles : posons $v_n = \max(u_n, 0)$ et $w_n = \max(-u_n, 0)$, de sorte que les suites $(v_n), (w_n)$ sont à valeurs positives et que :

$$\forall n \in \mathbb{N},\ u_n = v_n - w_n \text{ et } 0 \leq v_n, w_n \leq |u_n|.$$

On a ainsi que les suites $(v_n), (w_n)$ sont à valeurs positives, et majorées par $|u_n|$, dont la série converge, donc les séries $\sum v_n$ et $\sum w_n$ convergent.
Et donc la série $\sum u_n = \sum(v_n - w_n)$ converge également par linéarité.
Si (u_n) est à valeurs complexes : on considère les suites $(v_n) = (\mathrm{Re}(u_n))$ et $(w_n) = (\mathrm{Im}(u_n))$, qui convergent absolument (comme elles sont majorées par $|u_n|$), donc qui convergent (en tant que suites réelles qui convergent absolument). Et donc $\sum u_n$ converge également.
Pour l'inégalité triangulaire, on utilise que pour tout $n \in \mathbb{N}$:

$$\left|\sum_{k=0}^{n} u_k\right| \leq \sum_{k=0}^{n} |u_k|$$

et donc en passant à la limite :

$$\left|\sum_{k=0}^{+\infty} u_k\right| \leq \sum_{k=0}^{+\infty} |u_k|$$

□

Remarque III.5. *La réciproque est fausse : par exemple la série* $\sum_{n\geq 1} \dfrac{(-1)^{n+1}}{n}$ *dont on a vu qu'elle est convergente (sa somme valant* $\ln(2)$*, mais non absolument convergente par comparaison avec la série harmonique).*
Une série qui converge, mais qui ne converge pas absolument sera dite ***semi-convergente****.*

III.2 Comparaison à des séries à termes positifs

Proposition III.6. *Si* $(u_n), (v_n)$ *sont des suites à valeurs complexes telles que* $\sum v_n$ *converge absolument et que* $u_n = \mathrm{O}(v_n)$*, alors* $\sum u_n$ *converge absolument.*

Démonstration. Comme $u_n = \mathrm{O}(v_n)$, alors $|u_n| = \mathrm{O}(|v_n|)$, et donc, comme la série $\sum |v_n|$ converge, alors la série $\sum |u_n|$ converge également, donc $\sum u_n$ converge absolument. □

Corollaire III.7. *Si* (u_n) *est une suite complexe, et* (v_n) *est une suite* ***de réels positifs*** *telle que* $\sum v_n$ *converge et que* $u_n = \mathrm{O}(v_n)$*, alors* $\sum u_n$ *converge.*

Démonstration. Comme $\sum v_n$ est convergente et à termes positifs, alors elle converge absolument.
Donc $\sum u_n$ converge absolument, donc converge. □

Remarques III.8.

1. *Comme la notion de* O *englobe celle de* o *ou d'équivalent, on peut utiliser ce résultat lorsque* $u_n \sim v_n$ *ou* $u_n = \mathrm{o}(v_n)$.
2. *En pratique, on essaie de travailler avec des séries absolument convergentes bien connues : par exemple les séries de Riemann, les séries géométriques, ou la série exponentielle. Par exemple, s'il existe* $\alpha > 1$ *tel que* $u_n = \mathrm{O}\left(\dfrac{1}{n^\alpha}\right)$, *alors* $\sum u_n$ *est (absolument) convergente. En pratique, on cherchera* $\alpha > 1$ *tel que la suite* $(n^\alpha u_n)$ *tend vers* 0.
3. *Ce résultat est très utile pour montrer la convergence d'une série. Mais il ne saurait montrer la divergence : on essaie alors de se ramener à une série à termes de signe constant et d'utiliser les résultats précédents (par exemple une comparaison à une série de Riemann).*

Exemple III.9.
Si on fixe $x > 0$, *on peut chercher à montrer que la suite* (u_n) *définie par :*

$$\forall n \in \mathbb{N},\ u_n = \frac{n^x n!}{(x+n)(x+n-1)\dots(x+1)x}$$

converge. Pour cela, on préfère travailler avec des sommes qu'avec des produits, et on pose donc la suite (v_n) *définie par :*

$$v_n = \ln(u_n) = x\ln(n) + \sum_{k=1}^{n} \ln(k) - \sum_{k=0}^{n} \ln(x+k)$$

et plutôt que d'étudier la convergence de (v_n) *(ce qui donnerait la convergence de* (u_n)*), on va plutôt étudier la convergence de la série de terme général* $v_{n+1} - v_n$, *ce qui est équivalent (pas télescopage). On a pour tout* $n \in \mathbb{N}$ *:*

$$\begin{aligned} v_{n+1} - v_n &= x\ln(n+1) + \ln(n+1) - \ln(x+n+1) - x\ln(n) \\ &= x\ln\left(1+\frac{1}{n}\right) - \ln\left(1+\frac{x}{n+1}\right) \\ &= \frac{x}{n} - \frac{x}{n+1} + \mathrm{O}\left(\frac{1}{n^2}\right) \\ &= \frac{x}{n(n+1)} + \mathrm{O}\left(\frac{1}{n^2}\right) = \mathrm{O}\left(\frac{1}{n^2}\right) \end{aligned}$$

et donc la série $\sum(v_{n+1} - v_n)$ *converge absolument, donc converge.*
Donc (v_n) *converge, donc* (u_n) *également.*

III.3 Le critère de d'Alembert

Proposition III.10. *On considère* (u_n) *une suite complexe qui ne s'annule pas. On suppose que la suite* $\left|\dfrac{u_{n+1}}{u_n}\right|$ *tend vers* $l \in \overline{\mathbb{R}}$. *Alors :*

1. *si* $l > 1$ *: la série* $\sum u_n$ *diverge grossièrement ;*
2. *si* $l < 1$ *: la série* $\sum u_n$ *converge absolument.*

Démonstration. Traitons séparément les deux cas :

1. si $l > 1$: alors par définition de la limite avec $\varepsilon = \dfrac{l-1}{2} > 0$, il existe $n_0 \in \mathbb{N}$ tel que :

$$\forall n \geq n_0,\ |u_{n+1}| \geq \frac{(l+1)}{2}|u_n|$$

et donc, en itérant :

$$\forall n \geq n_0,\ |u_n| \geq \left(\frac{1+l}{2}\right)^{n-n_0} |u_{n_0}|$$

donc $|u_n|$ tend vers $+\infty$ (comme $\left|\frac{1+l}{2}\right| > 1$), et la série $\sum u_n$ diverge grossièrement.

2. si $l < 1$: alors par définition de la limite avec $\varepsilon = \frac{1-l}{2} > 0$, il existe $n_0 \in \mathbb{N}$ tel que :

$$\forall n \geq n_0,\ |u_{n+1}| \leq \frac{1+l}{2}|u_n|$$

et donc, en itérant :

$$\forall n \geq n_0,\ |u_n| \leq \left(\frac{1+l}{2}\right)^{n-n_0} |u_{n_0}|$$

c'est-à-dire que $u_n = \mathrm{O}\left(\left(\frac{1+l}{2}\right)^n\right)$. Et comme la série $\sum \left(\frac{1+l}{2}\right)^n$ converge (absolument) alors $\sum u_n$ converge absolument.

□

Remarques III.11.

1. *Ce critère est un peu comme une comparaison à des séries géométriques (comme on le voit dans la preuve), et permet d'avoir un panel plus large de comparaison que seulement les séries de Riemann.*
2. *On peut aussi l'appliquer à des séries dont certains termes sont nuls : il faut alors utiliser la suite extraite $(u_{\varphi(n)})$ construite à partir de (u_n) en ne gardant que les termes non nuls.*
3. *On a en fait un résultat plus fort : il suffit que la suite $\left|\frac{u_{n+1}}{u_n}\right|$ soit minorée par un $l > 1$ à partir d'un certain rang pour le premier cas, ou majorée par un $l < 1$ dans le second (et pas nécessairement qu'elle converge).*
4. *Dans le cas où $l = 1$, on ne peut rien dire, comme le montrent les séries $\sum 1$, $\sum \frac{1}{n}$, $\sum \frac{(-1)^n}{n}$ et $\sum \frac{1}{n^2}$ dont la première diverge grossièrement, la deuxième diverge, la troisième converge mais pas absolument, et la dernière converge absolument.*

Exemples III.12.

1. *On peut retrouver rapidement la convergence de la série exponentielle (mais pas sa limite). Considérons $z \in \mathbb{C}^*$ et posons $u_n = \frac{z^n}{n!}$. Alors pour tout $n \in \mathbb{N}$ on a :*

$$\frac{|u_{n+1}|}{|u_n|} = \frac{|z|}{n+1} \underset{n\to+\infty}{\to} 0$$

et donc la série $\sum \frac{z^n}{n!}$ converge absolument.

2. *Étudions la convergence de la série de terme général $u_n = \frac{n!}{n^n}$. On a pour tout $n \in \mathbb{N}$:*

$$\begin{aligned}
\frac{u_{n+1}}{u_n} &= \frac{(n+1)!}{n!} \cdot \frac{n^n}{(n+1)^{n+1}} = \left(1 - \frac{1}{n+1}\right)^n \\
&= \exp\left(n \ln\left(1 - \frac{1}{n+1}\right)\right) \\
&= \exp\left(n \cdot \left(-\frac{1}{n+1} + \mathrm{o}\left(\frac{1}{n+1}\right)\right)\right) \\
&= \exp\left(-1 + \mathrm{o}(1)\right) \underset{n\to+\infty}{\to} e^{-1} < 1
\end{aligned}$$

et donc la série $\sum \dfrac{n!}{n^n}$ *converge.*

III.4 Séries alternées

Théorème III.13. *Si* (u_n) *est une suite positive décroissante tendant vers* 0*, on dit que la série* $\sum(-1)^n u_n$ *est une* ***série alternée****.*
C'est une série convergente, dont la suite des reste est contrôlée par son premier terme, dans le sens où il est du signe de son premier terme et majoré en valeur absolue par celui-ci :

$$\forall n \in \mathbb{N},\ |R_n| = \left|\sum_{k=n+1}^{+\infty} (-1)^k u_k\right| = (-1)^{n+1} R_n \leq u_{n+1}.$$

Démonstration. Pour montrer la convergence, considérons la suite (S_n) des sommes partielles : $\forall n \in \mathbb{N},\ S_n = \sum_{k=0}^{n}(-1)^k u_k$;
Alors pour tout $n \in \mathbb{N}$ on a :

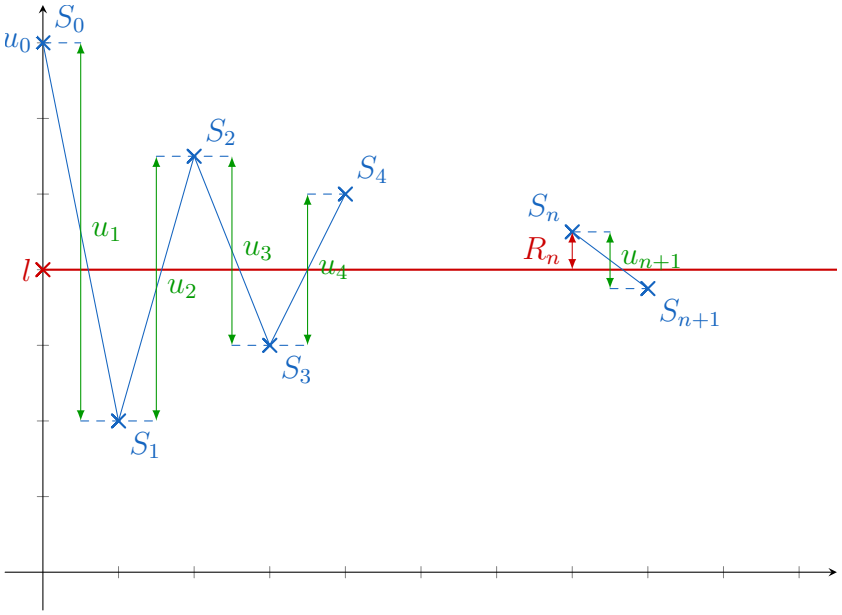
- $S_{2n+2} - S_{2n} = u_{2n+2} - u_{2n+1} \leq 0$ donc la suite (S_{2n}) est décroissante ;
- $S_{2n+3} - S_{2n+1} = -u_{2n+3} + u_{2n+2} \geq 0$ donc la suite (S_{2n+1}) est croissante ;
- $S_{2n} - S_{2n+1} = u_{2n+1} \underset{n\to+\infty}{\to} 0$.

Donc les suites (S_{2n}) et (S_{2n+1}) sont adjacentes : elles convergent vers une même limite l qui est donc la limite de (S_n). Donc la série $\sum(-1)^n u_n$ est convergente, de somme l. Et de plus, l vérifie :

$$\forall n, m \in \mathbb{N},\ S_{2m+1} \leq l \leq S_{2n}.$$

Pour la majoration de $|R_n|$, on procède par disjonction de cas :

- si n est pair : on a par propriétés des suites adjacentes que : $S_{n+1} \leq l \leq S_n$. Et donc $R_n = l - S_n \in [S_{n+1} - S_n; 0] = [-u_{n+1}; 0]$. Donc $|R_n| = -R_n \leq u_{n+1}$.
- si n est impair : on a de même que : $S_n \leq l \leq S_{n+1}$ et donc $R_n \in [0; u_{n+1}]$. Donc $|R_n| = R_n \leq u_{n+1}$.



□

Remarques III.14.

1. *Il suffit en fait que* (u_n) *soit décroissante à partir d'un certain rang. En revanche, il faut toujours que* (u_n) *tende vers* 0*.*

2. *En pratique, pour déterminer la convergence d'une série, on essaiera de se ramener à une combinaisons linéaires de séries dont on peut déterminer la nature (par critère des séries alternées ou par comparaison pour les séries à termes positifs) dont au plus une ne converge pas, comme modifier une série par une série convergente ne change pas sa nature.*

Exemples III.15.

1. *Avec* $(u_n) = \left(\dfrac{\ln(n)}{n}\right)$, *on trouve la série :* $\sum \dfrac{(-1)^n \ln(n)}{n}$.
   Par comparaison avec la série harmonique, on voit déjà qu'elle n'est pas absolument convergente. Et comme elle n'est pas de signe constant on ne peut pas non plus utiliser de comparaison (encadrements ou équivalents).
   On a déjà par croissance comparées que (u_n) *tend vers* 0.
   La fonction $f : x \mapsto \dfrac{\ln(x)}{x}$ *est dérivable sur* $\mathbb{R}_+^*$, *de dérivée définie par :*

$$\forall x \in \mathbb{R}_+^*,\ f'(x) = \frac{1 - \ln(x)}{x}$$

   et donc f *est strictement décroissante sur* $[e; +\infty[$. *On peut donc appliquer le théorème des séries alternées, en notant que la suite* $(u_n)_{n\geq 3}$ *est positive décroissante tendant vers* 0.
   On peut même estimer sa limite plus précisément : si on note $l = \sum_{n=1}^{+\infty} \dfrac{(-1)^n \ln(n)}{n}$ *et* $S_n = \sum_{k=1}^{n} \dfrac{(-1)^n \ln(n)}{n}$, *alors pour tout* $n \geq 3$ *on a :*

$$|l - S_n| \leq \frac{\ln(n+1)}{n+1}.$$

2. *Considérons* $(u_n) = \dfrac{1}{\sqrt{n} + (-1)^n}$ *et intéressons-nous à la série* $\sum (-1)^n u_n$.
   Notons déjà que $u_n \sim \dfrac{1}{\sqrt{n}}$ *donc la série* $\sum u_n$ *diverge (par équivalent avec une série à termes positifs), donc on n'a pas la convergence absolue.*
   Pour établir la nature de la série, on fait un développement asymptotique :

$$\begin{aligned}
(-1)^n u_n &= \frac{(-1)^n}{\sqrt{n} + (-1)^n} \\
&= \frac{(-1)^n}{\sqrt{n}} \cdot \frac{1}{1 + \dfrac{(-1)^n}{\sqrt{n}}} \\
&= \frac{(-1)^n}{\sqrt{n}} \left(1 - \frac{(-1)^n}{\sqrt{n}} + \frac{1}{n} + \mathrm{o}\left(\frac{1}{n}\right)\right) \\
&= \frac{(-1)^n}{\sqrt{n}} - \frac{1}{n} + \mathrm{o}\left(\frac{1}{n}\right)
\end{aligned}$$

   Et on peut étudier chacun des termes :
   — $\sum \dfrac{(-1)^n}{\sqrt{n}}$ *converge par théorème des séries alternées ;*
   — $\sum -\dfrac{1}{n} + \mathrm{o}\left(\dfrac{1}{n}\right)$ *diverge, comme* $-\dfrac{1}{n} + \mathrm{o}\left(\dfrac{1}{n}\right) \sim -\dfrac{1}{n}$, *et l'on peut utiliser les équivalents (comme* $-\dfrac{1}{n}$ *est de signe constant), et que* $\sum -\dfrac{1}{n}$ *diverge (par propriété des séries de Riemann.*
   Donc finalement $\sum (-1)^n u_n$ *diverge.*

Remarque III.16. *Dans le second exemple, on a ainsi que :*

$$\frac{(-1)^n}{\sqrt{n}+(-1)^n} \sim \frac{(-1)^n}{\sqrt{n}}$$

mais les séries $\sum \frac{(-1)^n}{\sqrt{n}+(-1)^n}$ *et* $\sum \frac{(-1)^n}{\sqrt{n}}$ *ne sont pas de même nature.*

Exemple III.17. *Montrons que* $\pi < 4$*, où on définit* π *comme le double du premier point d'annulation sur* $\mathbb{R}_+$ *de l'application* cos *définie par :* $\cos(x) = \frac{e^{ix}+e^{-ix}}{2}$.
Par linéarité de la somme, on a pour tout $x \in \mathbb{R}$ *(en fait la même formule serait valable pour* $x \in \mathbb{C}$*) que :*

$$\cos(x) = \sum_{n=0}^{+\infty} \frac{(ix)^n}{2 \cdot n!} + \frac{(-ix)^n}{2 \cdot n!} = \sum_{n=0}^{+\infty} \frac{(-1)^n x^{2n}}{(2n)!}.$$

Posons $(u_n) = \frac{2^{2n}}{(2n)!}$*. Alors* (u_n) *est positive, tend vers* 0*, et pour tout* $n \in \mathbb{N}$ *on a :*

$$u_{n+1} - u_n = \frac{2^{2n+2}}{(2n+2)!} - \frac{2^{2n}}{(2n)!} = \frac{2^{2n}}{(2n)!}\left(\frac{4}{(2n+2)(2n+1)} - 1\right)$$

donc (u_n) *est décroissante à partir de son deuxième terme.*
Donc $\cos(x)$ *est définie à l'aide d'une série alternée. Par contrôle du reste, on a :*

$$\cos(2) = \underbrace{1 - \frac{2^2}{2!} + \frac{2^4}{4!}}_{=-\frac{1}{3}} + \underbrace{\sum_{k=3}^{+\infty} (-1)^k u_k}_{\leq 0}$$

et donc $\cos(2) \leq -\frac{1}{3} < 0$.
En tant que premier point d'annulation de cos*, on déduit que* $\frac{\pi}{2} < 2$*, et donc* $\pi < 4$.

IV Familles sommables

IV.1 Ensembles dénombrables

Définition IV.1. *Un ensemble* I *est dit* ***dénombrable*** *s'il existe une bijection* $\sigma : \mathbb{N} \to I$.
Inversement, un ensemble infini qui n'est pas dénombrable sera dit ***indénombrable****.*

Remarques IV.2.

1. *Un ensemble fini ou dénombrable sera dit* ***au plus dénombrable*** *(dans le sens où il n'a pas plus d'éléments qu'un ensemble dénombrable).*
2. *Dans certaines terminologies, on considère que les ensembles finis sont aussi dénombrables. On parlera ainsi plutôt d'ensemble infinis dénombrables pour éviter les confusions sachant que, avec la définition précédente, un ensemble dénombrable est nécessairement infini.*
3. *Comme la composée et l'inverse d'une bijection sont bijectives, alors un ensemble est dénombrable si, et seulement si, il est en bijection avec n'importe quel ensemble dénombrable.*

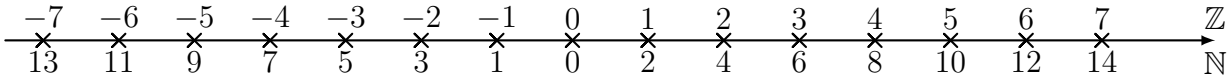
Exemples IV.3.

1. *L'ensemble $\mathbb{N}$ est dénombrable, de même que toute partie infinie de $\mathbb{N}$. Plus généralement, tout sous-ensemble infini d'un ensemble dénombrable est dénombrable, ce qui se montre à l'aide une composée à droite (à la manière des suites extraites). Et donc toute partie d'un ensemble (au plus) dénombrable est au plus dénombrable.*

2. *L'ensemble $\mathbb{Z}$ est dénombrable, comme l'application :*

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{Z} \\ n & \mapsto & \left\{ \begin{array}{ll} \frac{n}{2} & si \quad n \text{ est pair} \\ -\frac{n+1}{2} & si \quad n \text{ est impair} \end{array} \right. \end{array} \right.$$

est une bijection.



3. *En revanche, $\mathbb{R}$ n'est pas dénombrable, tout comme n'importe quel intervalle de $\mathbb{R}$ non réduit à un point. De manière plus subtile, les ensembles $\mathcal{P}(\mathbb{N})$ ou $E^{\mathbb{N}}$ (pour E un ensemble ayant au moins deux éléments) sont indénombrables.*

Proposition IV.4. *Si I est un ensemble dénombrable et J un ensemble quelconque, alors :*

1. *s'il existe $\sigma : I \to J$ surjective, alors J est au plus dénombrable ;*

2. *s'il existe $\sigma : J \to I$ injective, alors J est au plus dénombrable.*

Démonstration. Dans un cas comme dans l'autre, on peut mettre J en bijection avec une partie de I (par restriction et correstriction).
Une telle partie est :
— soit finie : dans ce cas J est fini ;
— soit infinie : alors cette partie est dénombrable et en bijection avec J, donc J est dénombrable.

□

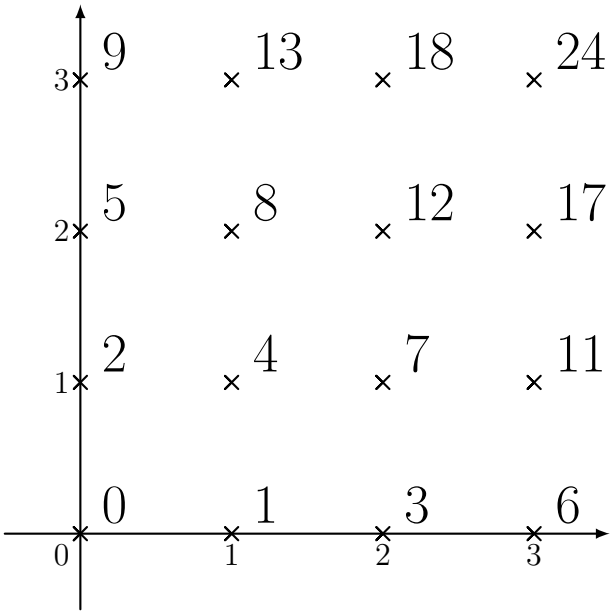
Remarque IV.5. *L'idée est qu'une application injective ne perd pas d'information, et qu'une application (peu importe ses propriétés) n'en crée pas, ce qui ressemble aux inégalités sur le rang qu'on avait vu pour les applications linéaires en dimension finie.*

Proposition IV.6. *L'ensemble $\mathbb{N} \times \mathbb{N}$ est dénombrable.*

Démonstration. On peut montrer facilement (avec des encadrements) que l'application :

$$f : \left\{ \begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \to & \mathbb{N} \\ (n,m) & \mapsto & \dfrac{(n+m)(n+m+1)}{2} + m \end{array} \right.$$

définit bien une bijection de $\mathbb{N} \times \mathbb{N}$ sur $\mathbb{N}$. Celle-ci revient à numéroter les éléments de $\mathbb{N} \times \mathbb{N}$ suivant les "diagonales" : $D_k = \{(n,m) \in \mathbb{N} \times \mathbb{N} \,|\, n+m = k\}$:



□

Corollaire IV.7.

1. *Un produit cartésien d'un nombre fini d'ensembles dénombrables est dénombrable.*
2. *Une union finie ou dénombrable d'ensembles finis ou dénombrables est finie ou dénombrable.*

Démonstration.

1. Comme tout ensemble dénombrable est en bijection avec $\mathbb{N}$, il suffit de montrer que $\mathbb{N}^p$ est dénombrable pour tout $p \in \mathbb{N}^*$, ce qui se fait par récursivement. Plus précisément, pour tout $p \in \mathbb{N}^*$ on définit l'application $\varphi_p : \mathbb{N}^p \to \mathbb{N}$ par :
   — si $p = 1$: alors $\varphi_p = \mathrm{id}_{\mathbb{N}}$;
   — si $p \geq 2$: $\varphi_p : (n_1, \ldots, n_p) \mapsto f\left(\varphi_{p-1}(n_1, \ldots, n_{p-1}), n_{p+1}\right)$
   où f est une bijection de $\mathbb{N}^2$ dans $\mathbb{N}$ (par exemple celle donnée dans la proposition précédente).
   Et la bijectivité des applications φ_p découle de celle de f.
2. Montrons déjà le résultat sur une union dénombrable d'ensembles dénombrables. Notons J un ensemble dénombrable, et pour tout $j \in J$ considérons I_j ensemble dénombrable. Montrons que $I = \cup_{j\in J} I_j$ est dénombrable :
   — comme J est dénombrable, il existe $\sigma : \mathbb{N} \to J$ bijective ;
   — pour tout $j \in J$ l'ensemble I_j est dénombrable, donc il existe $\tau_j : \mathbb{N} \to I_j$ bijective.
   Et donc l'application :
   $$\varphi : \left\{ \begin{array}{ccc} \mathbb{N}^2 & \to & I \\ (n,m) & \mapsto & \tau_{\sigma(n)}(m) \end{array} \right.$$
   est une surjection de $\mathbb{N}^2$ (qui est dénombrable) dans I, donc I est dénombrable.
   Et rajouter une infinité dénombrable de fois les ensembles considérés dans l'union, ou à rajouter à chaque ensemble une infinité dénombrable d'éléments, ne ferait qu'augmenter cette union. Donc une union finie ou dénombrable d'ensembles finis ou dénombrables est une partie d'une union dénombrable d'ensemble dénombrables : elle est au plus dénombrable.

□

Exemple IV.8.

L'ensemble $\mathbb{Q}$ est donc dénombrable, comme l'application :

$$\left\{ \begin{array}{ccc} \mathbb{Z}\times\mathbb{N} & \to & \mathbb{Q} \\ (n,m) & \mapsto & \dfrac{n}{m+1} \end{array} \right.$$

est surjective de $\mathbb{Z} \times \mathbb{N}$ (qui est dénombrable) dans $\mathbb{Q}$.

IV.2 Somme d'une famille de réels positifs

Définition IV.9. *On considère I un ensemble quelconque, et $(u_i)_{i\in I}$ une famille d'éléments de $\mathbb{R}_+\cup\{+\infty\} = [0;+\infty]$ indexée par I.*
On définit alors la ***somme de la famille*** *(u_i) comme la borne supérieure dans $\overline{\mathbb{R}}$ de l'ensemble :*

$$A = \{\sum_{i\in F} u_i \,|\, F \subset I,\ F \text{ fini}\}$$

et que l'on notera : $\sum_{i\in I} u_i$.

Remarque IV.10. *La somme d'une famille de réels a toujours un sens : selon que l'ensemble A est majoré ou non, la somme sera alors un réel positif ou $+\infty$.*

Proposition IV.11. *Si $(u_i)_{i\in I}$ est une famille d'éléments de $\mathbb{R}_+$, alors :*

1. *si I est fini : la somme $\sum_{i\in I} u_i$ (au sens précédent) coïncide avec la somme $\sum_{i\in I} u_i$ (au sens donné aux sommes finies) ;*
2. *si $I = \mathbb{N}$: alors la somme $\sum_{i\in I} u_i$ coïncide avec la limite de la série $\sum u_n$. En particulier, cette somme est finie si, et seulement si, la série de terme général u_n converge.*

Démonstration.

1. si I est fini : alors en reprenant les notations de la définition, on a que $\sum_{i\in I} u_i$ (au sens des sommes finies) est le maximum de A puisque :
   — si $F \subset I$: alors $\sum_{i\in F} u_i = \sum_{i\in I} u_i - \underbrace{\sum_{i\in I\setminus F} u_i}_{\leq 0} \leq \sum_{i\in I} u_i$; donc $\sum_{i\in I} u_i$ (au sens des sommes finies) est un majorant de A ;
   — avec $F = I$ (qui est bien fini) : alors $\sum_{i\in I} u_i$ (au sens des sommes finies) est un élément de A.
   Et donc $\sup A = \sum_{i\in I} u_i$ (au sens des sommes finies), puisque l'on a même que $\sum_{i\in I} u_i = \max A$.
2. si $I = \mathbb{N}$: montrons que $\sum_{n=0}^{+\infty} u_n = \sum_{n\in\mathbb{N}} u_n$. Pour cela, notons (S_n) la suite des sommes partielles (qui converge vers $\sum_{n=0}^{+\infty} u_n$) :
   — si $\sum u_n$ diverge : alors (S_n) tend vers $+\infty$ (par propriété des séries à termes positifs). Mais on a par définition que pour tout $n \in \mathbb{N}$:

   $$S_n = \sum_{k=0}^{n} u_k = \sum_{i\in[\![0;n]\!]} u_i \in A$$

   et donc (S_n) est une suite d'éléments de A qui tend vers $+\infty$, donc A n'est pas majorée, donc $\sum_{n\in\mathbb{N}} u_n = \sup A = +\infty$.
   — si $\sum u_n$ converge : alors (S_n) est majorée par $\sum_{n=0}^{+\infty} u_n$, qui est également sa limite. Si $F \subset \mathbb{N}$ est fini, alors en notant $n_0 = \max(F)$ on a : $F \subset [\![0; n_0]\!]$. Et donc comme les u_n sont positifs :

   $$\sum_{i\in F} u_i \leq \sum_{i\in[\![0;n_0]\!]} u_i = S_{n_0} \leq \sum_{n=0}^{+\infty} u_n$$

   et donc $\sum_{n=0}^{+\infty} u_n$ est un majorant de A. Et comme, par la même considération que ci-dessus, on trouve que (S_n) est une suite d'éléments de A, dont la limite est $\sum_{n=0}^{+\infty} u_n$, alors par caractérisation on trouve que : $\sup A = \sum_{n=0}^{+\infty} u_n$, et donc $\sum_{n\in\mathbb{N}} u_n = \sum_{n=0}^{+\infty} u_n$.

□

Théorème IV.12. *Si $(u_i)_{i\in I}$ est une famille de réels positifs indexé par I et σ est une permutation de I, alors :*

$$\sum_{i\in I} u_i = \sum_{i\in I} u_{\sigma(i)}.$$

Démonstration. Si $F \subset I$ est fini, alors $\sigma(F)$ et $\sigma^{-1}(F)$ sont des ensembles fini de I (de même cardinal que I). Ainsi, σ permet de définir une bijection sur l'ensemble E des parties finies de I, définie par : $F \mapsto \sigma(F)$, de bijection réciproque $F \mapsto \sigma^{-1}(F)$.
Et ainsi on a l'égalité ensembliste (par double inclusion) :

$$\{\sum_{i\in F} u_i \,|\, F \subset I,\ F \text{ fini}\} = \{\sum_{i\in F} u_{\sigma(i)} \,|\, F \subset I,\ F \text{ fini}\}$$

ce qui donne l'égalité voulue en considérant les bornes supérieures de ces ensembles. □

Remarque IV.13. *Lorsque tous les termes sont positifs, on peut réordonner les termes d'une série sans en changer la valeur (et donc sans en changer la nature).*
À l'inverse, changer l'ordre des termes dans une somme infinie peut en changer la valeur. On verra en exercice que la série harmonique alternée, si on renumérote ses termes, peut changer de valeur, et même ne plus converger.

Définition IV.14. *Une famille $(u_i)_{i\in I}$ de réels positifs est dite* ***sommable*** *si : $\sum_{i\in I} u_i < +\infty$, c'est-à-dire si l'ensemble :*

$$A = \{\sum_{i\in F} u_i \,|\, F \subset I,\ F \textit{ fini}\}$$

est borné.

Exemple IV.15.
Si $I = \mathbb{Z}$ et $x \in]0;1[$, alors la famille $\left(x^{|n|}\right)_{n\in\mathbb{Z}}$ est sommable.
On a en effet que, si $F \subset N$ est fini, alors F est borné, donc inclus dans un intervalle d'entiers de la forme $[\![-n;n]\!]$ (pour $n \in \mathbb{N}^*$). Et alors :

$$\sum_{i\in F} x^{|i|} \leq \sum_{k=-n}^{n} x^{|k|} = 2\sum_{k=0}^{n} x^k - 1 = 2\frac{1-x^{n+1}}{1-x} - 1 \leq \frac{2}{1-x} - 1 = \frac{1+x}{1-x}$$

donc l'ensemble des sommes finies est majoré par $\dfrac{1+x}{1-x}$.
Et de plus, en considérant $F_n = [\![-n;n]\!]$ (pour $n \in \mathbb{N}^*$) on a :

$$\sum_{i\in F_n} x^{|i|} = 2\frac{1-x^{n+1}}{1-x} - 1 \lim_{n\to+\infty} \frac{1+x}{1-x}$$

ce qui donne que $\dfrac{1+x}{1-x}$ est même la borne supérieure cherchée. Et donc $\sum_{n\in\mathbb{Z}} x^{|n|} = \dfrac{1+x}{1-x}$.

Proposition IV.16. *Une famille $(u_i)_{i\in I}$ de réels positifs sommable est* ***à support au plus dénombrable****, c'est-à-dire que l'ensemble :*

$$\text{supp}(u) = \{i \in I \,|\, u_i \neq 0\}$$

est au plus dénombrable.

Démonstration. Posons pour tout $n \in \mathbb{N}^*$: $I_n = \{i \in I \,|\, u_i \geq \dfrac{1}{n}\}$. Alors pour tout $n \in \mathbb{N}^*$ l'ensemble I_n est fini, comme par croissance :

$$\frac{|I_n|}{n} \leq \sum_{i\in I_n} u_i \leq \sum_{i\in I} u_i < +\infty$$

De plus, comme $\mathbb{R}$ est archimédien : si $i \in I$ vérifie $u_i \neq 0$, alors il existe $n \in \mathbb{N}^*$ tel que $u_i \geq \dfrac{1}{n}$, c'est-à-dire $i \in I_n$. Et donc :

$$\text{supp}(u) = \cup_{n\in\mathbb{N}^*} I_n$$

donc $\text{supp}(u)$ est une union dénombrable d'ensemble finis : il est au plus dénombrable. □

Remarque IV.17. *On a en fait un résultat plus fort : si $(u_i)_{i\in I}$ est une famille sommable, alors pour tout $\varepsilon > 0$ l'ensemble $\{i \in I \,|\, u_i > \varepsilon\}$ est fini, ce qui permet par contraposée de facilement montrer que certaines familles ne sont pas sommables.*

Exemple IV.18.
La famille $\left(\frac{1}{x^2}\right)_{x\in\mathbb{Q}\cap[\pi;+\infty[}$ n'est pas sommable car l'ensemble $[4,5]\cap\mathbb{Q}$ est infini, et pour tout $x \in [4,5]\cap\mathbb{Q}$ on a : $\frac{1}{x^2} \geq \frac{1}{25}$.

Proposition IV.19 (Linéarité de la somme)**.** *Si $(u_i)_{i\in I}$ et $(v_i)_{i\in I}$ sont des familles sommables et $\lambda, \mu \in \mathbb{R}_+$, alors la famille $(\lambda u_i + \mu v_i)_{i\in I}$ est sommable, et :*

$$\sum_{i\in I} (\lambda u_i + \mu v_i) = \lambda \sum_{i\in I} u_i + \mu \sum_{i\in I} v_i.$$

Démonstration. Découle de la linéarité de la somme (pour le sommes finies), qui assure que pour tout $F \subset I$ fini on a :

$$\sum_{i\in F} (\lambda u_i + \mu v_i) = \lambda \sum_{i\in F} u_i + \mu \sum_{i\in F} v_i$$

et l'égalité voulue découle en passage au sup. □

Proposition IV.20 (Croissance de la somme)**.** *Si $(u_i)_{i\in I}$ et $(v_i)_{i\in I}$ sont deux familles de réels positifs, alors :*

1. *si : $\forall i \in I,\ u_i \leq v_i$, alors $\sum_{i\in I} u_i \leq \sum_{i\in I} v_i$;*
2. *si $J \subset I$ (avec J fini ou non), alors $\sum_{i\in J} u_i \leq \sum_{i\in I} u_i$.*

Démonstration.

1. avec l'inégalité vérifiée par (u_i) et (v_i), on a pour tout $F \subset I$ fini :

$$\sum_{i\in F} u_i \leq \sum_{i\in F} v_i$$

   et donc en passant au sup on trouve l'égalité voulue.

2. par transitivité de l'inclusion, si $F \subset I'$, alors $F \subset I$. Et on a donc l'inclusion :

$$A' = \{\sum_{i\in F} u_i \,|\, F \subset I',\ F \text{ fini}\} \subset \{\sum_{i\in F} u_j \,|\, F \subset I,\ F \text{ fini}\} = A$$

   et donc tout majorant de A est un majorant de A', donc $\sup A' \leq \sup A$, ce qui donne l'inégalité voulue.

□

Remarque IV.21. *Les inégalités précédentes ont un sens que les famille soient sommable ou non. Dans le cas de familles non sommables, on travaille en fait avec la relation d'ordre $\leq$ définie sur $\overline{\mathbb{R}}$.*

Corollaire IV.22.

1. *Si $(u_i)_{i\in I}, (v_i)_{i\in I}$ sont des familles de réels positifs telles que $\forall i \in I,\ u_i \leq v_i$ et que la famille (v_i) est sommable, alors (u_i) est sommable.*
2. *Si $(u_i)_{i\in I}$ et sommable et si $J \subset I$, alors $(u_i)_{i\in J}$ est sommable.*

Démonstration. C'est le résultat précédent, dans le cas où les sommes sont finies. □

IV.3 Groupement dans les sommes à termes positifs

Théorème IV.23 (Sommation par paquets, cas positif)**.** *Soit $(u_i)_{i\in I}$ une famille de réels positifs. On suppose qu'il existe un ensemble J et une famille $(I_j)_{j\in J}$ tels que I est la réunion disjointe des I_j.*
Alors :

$$\sum_{i\in I} u_i = \sum_{j\in J}\left(\sum_{i\in I_j} u_i\right).$$

En particulier, la famille $(u_i)_{i\in I}$ est sommable si, et seulement si, les deux conditions suivantes sont réalisées :

1. *pour tout $j\in J$, la famille $(u_i)_{i\in I_j}$ est sommable ;*
2. *la famille $\left(\sum_{i\in I_j} u_i\right)_{j\in J}$ est sommable.*

Démonstration. Posons pour $j\in J$: $S_j = \sum_{i\in I_j} u_i$. Et notons $S = \sum_{j\in J} S_n$. Les S_j et S sont donc des éléments de $[0;+\infty]$.
Supposons que tous les S_j et S sont finis (ce qui correspond aux deux conditions de la fin du théorème). Notons $F\subset I$ fini. Alors comme F est fini et que les I_j sont deux-à-deux disjoints, l'ensemble $J_0 = \{j\in J \mid F\cap I_j\neq\emptyset\}$ est fini. Et on a :

$$\sum_{i\in F} u_i = \sum_{j\in J_0}\left(\sum_{i\in F\cap I_j} u_i\right) \leq \sum_{j\in J_0}\sum_{i\in I_j} u_i = \sum_{j\in J_0} S_j \leq S$$

ce qui donne que $(u_i)_{i\in I}$ est sommable, et que sa somme Σ vérifie $\sigma\leq S$.

Réciproquement, si (u_i) est sommable. Notons Σ sa somme.
Soit $j\in J$, et considérons F partie finie de I_j. Alors F est également une partie finie de I, donc $\sum_{i\in F} u_i\leq\Sigma$, ce qui assure que la famille $(u_i)_{i\in I_j}$ est sommable, donc S_j est finie.
De plus, si on note $J_0\subset J$ fini, et pour tout $j\in J_0$ on se donne $F_j\subset I_j$ fini, alors : $F = \cup_{j\in J_0} F_j$ est une partie finie de I, et comme les F_j sont deux-à-deux disjoints on déduit que :

$$\sum_{i\in F} u_i = \sum_{j\in J_0}\sum_{i\in F_j} u_i \leq \Sigma$$

et en passant au sup pour les $F_j\subset I_j$, on déduit que :

$$\sum_{j\in J_0} S_j \leq \Sigma$$

et en passant au sup pour $J_0\subset J$ on trouve que la famille $(S_j)_{j\in J}$ est sommable, de somme $S\leq\Sigma$.

Finalement, on trouve bien que la famille $(u_i)_{i\in I}$ est sommable si, et seulement si, toutes les familles $(u_i)_{i\in I_j}$ sont sommables et que la famille $\left(\sum_{i\in I_j} u_i\right)_{j\in J}$ également. Et en combinant les deux inégalités précédentes, on trouve alors que :

$$\sum_{i\in I} u_i = \sum_{j\in J}\left(\sum_{i\in I_j} u_i\right).$$

Enfin, si $(u_i)_{i\in I}$ n'est pas sommable, alors $\sum_{i\in I} u_i = +\infty$, et par contraposée du point précédent on a également que $\sum_{j\in J}\left(\sum_{i\in I_j} u_i\right) = +\infty$, car :

— ou bien l'une des familles $(u_i)_{i\in I_j}$ n'est pas sommable : et alors la somme comporte un terme égal à $+\infty$, donc vaut $+\infty$;
— ou bien la famille $\left(\sum_{i\in I_j} u_i\right)_{j\in J}$ n'est pas sommable, et sa somme vaut $+\infty$.

□

Corollaire IV.24 (Théorème de Fubini positif)**.** *On considère la famille $(u_{i,j})_{(i,j)\in I\times J}$ de réels positifs. Alors :*

$$\sum_{(i,j)\in I\times J} u_{i,j} = \sum_{i\in I}\left(\sum_{j\in J} u_{i,j}\right) = \sum_{j\in J}\left(\sum_{i\in I} u_{i,j}\right)$$

Remarque IV.25. *On peut voir cette somme sur une indexation par un produit comme une somme double. L'intérêt est que, comme on le voit dans la formule, on peut sommer dans l'ordre que l'on veut, comme pour les sommes finies : soit fixer un élément de I et sommer pour tous les éléments de J, soit l'inverse. Et le résultat est vrai que les famille soient sommables ou non, et permet donc de prouver la sommabilité d'une famille.*

Exemple IV.26.

On considère l'ensemble $I = \{(n,m)\in\mathbb{N}^2 \mid m\geq n\}$ et on considère la famille $\left(\frac{1}{m!}\right)_{(n,m)\in I}$. Montrons que la famille est sommable et calculons sa somme.
On a :

$$\sum_{(n,m)\in I}\frac{1}{m!} = \sum_{n=0}^{+\infty}\sum_{m=n}^{+\infty}\frac{1}{m!} = \sum_{m=0}^{+\infty}\sum_{n=0}^{m}\frac{1}{m!}$$

et on va utiliser la deuxième écriture, qui permet de calculer plus facilement puisque l'on a :

$$\sum_{m=0}^{+\infty}\sum_{n=0}^{m}\frac{1}{m!} = \sum_{m=0}^{+\infty}\frac{(m+1)}{m!} = \sum_{m=1}^{+\infty}\frac{1}{(m-1)!} + \sum_{m=0}^{+\infty}\frac{1}{m!} = 2\sum_{m=0}^{+\infty}\frac{1}{m!} = 2e$$

Ce qui prouve que la famille considérée est sommable, et que sa somme vaut $2e$.

Corollaire IV.27. *On considère les familles $(a_i)_{i\in I}$ et $(b_j)_{j\in J}$ de réels positifs. Alors :*

$$\sum_{(i,j)\in I\times J} a_i\cdot b_j = \left(\sum_{i\in I} a_i\right)\cdot\left(\sum_{j\in J} b_j\right).$$

Démonstration. Découle du résultat précédent, appliqué à $(u_{i,j}) = (a_i\cdot b_j)$ et par linéarité, comme :

$$\sum_{(i,j)\in I\times J} a_i\cdot b_j = \sum_{i\in I}\left(\sum_{j\in J} a_i\cdot b_j\right) = \sum_{i\in I}\left(a_i\left(\sum_{j\in J} b_j\right)\right) = \left(\sum_{i\in I} a_i\right)\cdot\left(\sum_{j\in J} b_j\right).$$

□

Remarque IV.28. *Là encore, comme le résultat est valable pour des familles sommables ou non, on peut l'utiliser pour montrer la sommabilité d'une famille.*

Exemple IV.29.

Montrons que la famille $\left(\frac{1}{n^2m^2}\right)_{(n,m)\in\mathbb{N}^*\times\mathbb{N}^*}$ est sommable.
Par théorème de Fubini, on a :

$$\sum_{(n,m)\in\mathbb{N}^*\times\mathbb{N}^*}\frac{1}{n^2m^2} = \sum_{n\in\mathbb{N}^*}\frac{1}{n^2}\sum_{m\in\mathbb{N}^*}\frac{1}{m^2}$$

et on reconnaît à droite deux sommes finies (par critère de Riemann), dont le produit est donc fini : la famille est sommable, et on a même :

$$\sum_{(n,m)\in\mathbb{N}^*\times\mathbb{N}^*} \frac{1}{n^2m^2} = \left(\sum_{n\in\mathbb{N}^*} \frac{1}{n^2}\right)^2 = \frac{\pi^4}{36}.$$

IV.4 Familles sommables de complexes

Définition IV.30. *Une famille $(u_i)_{i\in I}$ de complexe est dite **sommable** si la famille $(|u_i|)_{i\in I}$ est sommable, c'est-à-dire si $\sum_{i\in I} |u_i| < +\infty$.*
On note $l^1(I)$ l'ensemble des familles sommables indexées par I.

Remarques IV.31.

1. *Si $I = \mathbb{N}$, une famille sommable revient à la donnée d'une série absolument convergente. Et si I est fini on est ramené aux sommes finies, qu'on a déjà traitées.*
2. *Toute famille finie est sommable.*
3. *Si $J \subset I$ et que $(u_i)_{i\in I}$ est sommable, alors $(u_i)_{i\in I}$ est également sommable.*
4. *Du fait du résultat analogue sur les familles sommables de réels positifs, si $(u_i)_{i\in I}$ est sommable, l'ensemble $\{i \in I \,|\, u_i \neq 0\}$ est au plus dénombrable.*

Proposition-Définition IV.32. *On considère $(u_i)_{i\in I} \in l^1(I)$ pour I dénombrable, et on note $\sigma : \mathbb{N} \to I$ bijective. Alors la quantité :*

$$\sum_{n=0}^{+\infty} u_{\sigma(n)}$$

*est bien définie, et est un complexe dont la valeur ne dépend pas de σ. On l'appelle la **somme** de la famille $(u_i)_{i\in I}$, et on la note : $\sum_{i\in I} u_i$.*
De plus, pour tout $\varepsilon > 0$, il existe $F \subset I$ finie telle que :

$$\left|\sum_{i\in I} u_i - \sum_{i\in F} u_i\right| \leq \varepsilon.$$

Démonstration. Notons déjà que, comme $(u_i)_{i\in I}$ est sommable, alors $(u_{\sigma(n)})_{n\in\mathbb{N}}$ aussi, comme on a directement que :

$$\{\sum_{i\in F} |u_i| \,|\, F \subset I,\ F \text{ fini}\} = \{\sum_{n\in F} |u_{\sigma(n)}| \,|\, F \subset \mathbb{N},\ F \text{ fini}\}.$$

Et donc la série $\sum u_{\sigma(n)}$ est absolument convergente, donc convergente. Ce qui prouve déjà que $\sum_{n=0}^{+\infty} u_{\sigma(n)}$ a bien un sens, et est un complexe (fini).
Pour montrer que la quantité ne dépend pas de σ, il suffit de voir qu'on peut réordonner les termes dans la somme $\sum_{n=0}^{+\infty} u_{\sigma(n)}$ sans changer sa valeur :

— si les u_i sont des réels positifs : alors on a déjà montré le résultat ;
— si les u_i sont des réels : on écrit $u_i = \underbrace{u_i + |u_i|}_{\geq 0} - \underbrace{|u_i|}_{\geq 0}$ et donc :

$$\sum_{n=0}^{+\infty} u_{\sigma(n)} = \sum_{n=0}^{+\infty} \big(u_{\sigma(n)} + |u_{\sigma(n)}|\big) - \sum_{n=0}^{+\infty} \big(|u_{\sigma(n)}|\big)$$

où les deux sommes de droites ont bien un sens comme elles sont absolument convergentes, et on peut y réordonner les termes comme ce sont deux séries à termes positifs ;

— si les u_i sont des complexes : on se ramène au cas précédent en notant que $u_i = \underbrace{\mathrm{Re}(u_i)}_{\in\mathbb{R}} + i\underbrace{\mathrm{Im}(u_i)}_{\in\mathbb{R}}$.

Le dernier résultat vient du fait que, si on pose pour $n \in \mathbb{N}$ que $F_n = \sigma([\![0;n]\!])$ (qui est bien un sous-ensemble fini de I), alors on reconnaît le reste d'une série convergente :

$$\sum_{i\in I} u_i - \sum_{i\in F_n} u_i = \sum_{k=n+1}^{+\infty} u_{\sigma(n)}$$

qui tend vers 0 pour n tendant vers $+\infty$. Donc pour n suffisamment grand, on aura bien l'inégalité voulue pour ε (avec $F = F_n$ qui est bien fini). □

Remarques IV.33.

1. *Lorsque I n'est pas dénombrable, on a deux situations : ou bien I est fini, ou bien I est **indénombrable**. Dans le premier cas, la quantité $\sum_{i\in I} u_i$ a déjà été définie, et dans le second, comme $(u_i)_{i\in I}$ est sommable, alors $\{i \in I \,|\, u_i \neq 0\}$ est fini ou dénombrable, et on peut donc se ramener aux deux situations connues.*
2. *En modifiant un peu la démonstration, on peut mettre montrer que, pour tout $\varepsilon > 0$ il existe $F \subset I$ fini tel que :*
$$\forall J \subset I,\ F \subset J \Rightarrow \left|\sum_{i\in I} u_i - \sum_{i\in J} u_i\right| \leq \varepsilon$$
(en considérant des restes de séries absolument convergentes), et ce que les ensembles J ci-dessus soient fini ou non.
3. *Comme la série $u_{\sigma(n)}$ converge (même absolument) alors $u_{\sigma(n)}$ tend vers 0. Et donc dans une famille sommable, toute suite d'éléments de la famille tend vers 0.*

Proposition IV.34 (Inégalité triangulaire)**.** *Si $(u_i)_{i\in I}$ est une famille sommable de nombre complexes, alors :*

$$\left|\sum_{i\in I} u_i\right| \leq \sum_{i\in I} |u_i|.$$

Démonstration. Découle de l'inégalité triangulaire pour les séries, appliquée à la série de terme général $u_{\sigma(n)}$ où σ est une bijection de $\mathbb{N}$ dans I. □

Proposition IV.35. *Soient $(u_i)_{i\in I}$ une famille de complexes et $(v_i)_{i\in I}$ une famille de **réels positifs** telles que :*

1. *$\forall i \in I,\ |u_i| \leq v_i$;*
2. *la famille $(v_i)_{i\in I}$ est sommable.*

Alors la famille $(u_i)_{i\in I}$ est sommable, avec :

$$\left|\sum_{i\in I} u_i\right| \leq \sum_{i\in I} v_i.$$

Démonstration. Comme $(v_i)_{i\in I}$ est sommable, alors la somme $\sum_{i\in I} v_i$ est finie.
Par croissance des sommes (pour les sommes à termes positifs) on déduit que $\sum_{i\in I} |u_i|$ est finie, donc $(u_i)_{i\in I}$ est sommable.
La proposition précédente, et la croissance, assurent que :

$$\left|\sum_{i\in I} u_i\right| \leq \sum_{i\in I} |u_i| \leq \sum_{i\in I} v_i.$$

□

Proposition IV.36 (Linéarité de la somme)**.** *Si $(u_i)_{i\in I}, (v_i)_{i\in I}$ sont deux famille sommables, et $\lambda, \mu \in \mathbb{C}$, alors la famille $(\lambda u_i + \mu v_i)_{i\in I}$ est sommable, avec :*

$$\sum_{i\in I}(\lambda u_i + \mu v_i) = \lambda \sum_{i\in I} u_i + \mu \sum_{i\in I} v_i.$$

Démonstration. Par inégalité triangulaire, on a pour tout $i \in I$ que :

$$|\lambda u_i + \mu v_i| \leq |\lambda u_i| + |\mu v_i| = |\lambda| \cdot |u_i| + |\mu| \cdot |v_i|$$

Par linéarité de la somme (pour les sommes à termes positifs) on a que :

$$\sum_{i\in I} (|\lambda| \cdot |u_i| + |\mu| \cdot |v_i|) = |\lambda| \sum_{i\in I} |u_i| + |\mu| \sum_{i\in I} |v_i| < +\infty$$

donc la famille $(|\lambda| \cdot |u_i| + |\mu| \cdot |v_i|)_{i\in I}$ est une famille sommable de réels positifs.
Par le point précédent, on déduit que la famille $(\lambda u_i + \mu v_i)_{i\in I}$ est sommable.
La somme $\sum_{i\in I} \lambda u_i + \mu v_i$ est ainsi bien définie, et la linéarité pour les sommes de séries permet de conclure. □

IV.5 Groupement dans les sommes à termes complexes

Théorème IV.37 (Sommation par paquets, cas complexe)**.** *Soit $(u_i)_{i\in I}$ une famille sommable de complexes. On suppose qu'il existe un ensemble J et une famille $(I_j)_{j\in J}$ tels que I est la réunion disjointe des I_j. Alors :*

1. *pour tout $j \in J$, la famille $(u_i)_{i\in I_j}$ est sommable ;*
2. *la famille $\left(\sum_{i\in I_j} u_i\right)_{j\in J}$ est sommable ;*

Et on a de plus :

$$\sum_{i\in I} u_i = \sum_{j\in J} \left(\sum_{i\in I_j} u_i \right).$$

Démonstration. Par théorème de sommation par paquets (cas positif), comme la famille $(|u_i|)_{i\in I}$ est sommable, on a déjà que les familles $(|u_i|)_{i\in I_j}$ sont sommables, et que la famille $\left(\sum_{i\in I_j} |u_i|\right)_{j\in J}$ également. On déduit ainsi que :

— pour tout $j \in J$, la quantité $S_j = \sum_{i\in I_j} u_i$ est bien définie, et vérifie par inégalité triangulaire que : $S_j \leq \sum_{i\in I_j} |u_i|$;
— par majoration par une famille sommable, la famille $(S_j)_{j\in J}$ est donc sommable également.

Reste à montrer l'égalité sur les sommes, qu'on fait en se ramenant au cas de la sommation par paquets dans le cas positifs par linéarité :

— si les u_i sont des réels positifs : alors on a déjà montré le résultat ;
— si les u_i sont des réels : on écrit $u_i = u_i + |u_i| - |u_i|$ et donc par linéarité et par théorème :

$$\begin{array}{rcl} \sum_{i\in I} u_i & = & \sum_{i\in I}(|u_i| + u_i) - \sum_{i\in I} |u_i| \\ & = & \sum_{j\in J} \left(\sum_{i\in I_j} (|u_i| + u_i) \right) - \sum_{j\in J} \left(\sum_{i\in I_j} |u_i| \right) \\ & = & \sum_{j\in J} \left(\sum_{i\in I_j} (|u_i| + u_i) - |u_i| \right) \\ & = & \sum_{j\in J} \left(\sum_{i\in I_j} u_i \right) \end{array}.$$

— si les u_i sont des complexes : on se ramène au cas précédent en notant que $u_i = \underbrace{\mathrm{Re}(u_i)}_{\in\mathbb{R}} + i \underbrace{\mathrm{Im}(u_i)}_{\in\mathbb{R}}$.

□

Corollaire IV.38 (Théorème de Fubini)**.** *Si la famille $(u_{i,j})_{(i,j)\in I\times J}$ est sommable, alors :*

$$\sum_{(i,j)\in I\times J} u_{i,j} = \sum_{i\in I}\left(\sum_{j\in J} u_{i,j}\right) = \sum_{j\in J}\left(\sum_{i\in I} u_{i,j}\right)$$

Corollaire IV.39. *Si les familles $(a_i)_{i\in I}$ et $(b_j)_{j\in J}$ sont sommables, alors la famille $(a_i\cdot b_j)_{(i,j)\in I\times J}$ est sommable, et on a :*

$$\sum_{(i,j)\in I\times J} a_i\cdot b_j = \left(\sum_{i\in I} a_i\right)\cdot\left(\sum_{j\in J} b_j\right).$$

Démonstration. Comme pour les réels positifs. □

Remarque IV.40. *Ce résultat, comme le théorème de Fubini, se généralise à des sommes sur des produits finis d'ensembles.*

Proposition-Définition IV.41. *Étant données $\sum u_n$ et $\sum v_n$ deux séries absolument convergentes, on définit leur* ***produit de Cauchy*** *comme la série de terme général w_n défini par :*

$$\forall n\in\mathbb{N},\ w_n = \sum_{k=0}^{n} u_k v_{n-k} = \sum_{k=0}^{n} u_{n-k}v_k = \sum_{k+l=n} u_k v_l.$$

Alors la série $\sum w_n$ est absolument convergente, et vérifie :

$$\sum_{n=0}^{+\infty} w_n = \left(\sum_{n=0}^{+\infty} u_n\right)\cdot\left(\sum_{n=0}^{+\infty} v_n\right).$$

Démonstration. On applique successivement le théorème de Fubini et le théorème de sommation par paquets à la famille $(u_n v_m)_{(n,m)\in\mathbb{N}\times\mathbb{N}}$, en écrivant que $\mathbb{N}^2$ est l'union disjointe des éléments de la famille $(I_k)_{k\in\mathbb{N}}$ définie par :

$$\forall k\in\mathbb{N},\ I_k = \{(n,m)\in\mathbb{N}^2 \mid n+m=k\}$$

ce qui donne :

$$\left(\sum_{n=0}^{+\infty} u_n\right)\cdot\left(\sum_{m=0}^{+\infty} v_m\right) = \sum_{(n,m)\in\mathbb{N}^2} u_n v_m = \sum_{k=0}^{+\infty}\left(\sum_{(n,m)\in I_k} u_n v_m\right) = \sum_{k=0}^{+\infty} w_n$$

□

Proposition IV.42. *La fonction* exp*, définie sur $\mathbb{C}$ par :*

$$\forall z\in\mathbb{C},\ \exp(z) = \sum_{n=0}^{+\infty}\frac{z^n}{n!}$$

est un morphisme de groupes de $(\mathbb{C},+)$ dans $(\mathbb{C}^*,\times)$.

Démonstration. Considérons $z_1, z_2\in\mathbb{C}$. Les séries $\sum\frac{z_1^n}{n!}$ et $\sum\frac{z_2^n}{n!}$ sont absolument convergentes, et on a donc :

$$\exp(z_1)\exp(z_2) = \left(\sum_{n=0}^{+\infty}\frac{z_1^n}{n!}\right)\left(\sum_{n=0}^{+\infty}\frac{z_2^n}{n!}\right) = \sum_{n=0}^{+\infty}\left(\sum_{k=0}^{n}\frac{z_1^k z_2^{n-k}}{k!(n-k)!}\right)$$

mais on a également pour tout $n \in \mathbb{N}$ que :

$$\sum_{k=0}^{n} \frac{z_1^k z_2^{n-k}}{k!(n-k)!} = \frac{1}{n!} \cdot \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} z_1^k z_2^{n-k} = \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} z_1^k z_2^{n-k} = \frac{(z_1+z_2)^n}{n!}$$

en reconnaissant la formule du binôme. Et finalement on a :

$$\exp(z_1)\exp(z_2) = \sum_{n=0}^{+\infty} \frac{(z_1+z_2)^n}{n!} = \exp(z_1+z_2)$$

Comme $\exp(0) = \sum_{n=0}^{+\infty} \frac{0^n}{n!} = 1$, on déduit déjà que :

$$\forall z \in \mathbb{C},\ \exp(z)\exp(-z) = \exp(0) = 1$$

et donc $\exp : \mathbb{C} \to \mathbb{C}^*$.
Et d'après la formule précédente, exp réalise bien un morphisme de groupes. □

Chapitre 26

Probabilités et dénombrement

I Rappels et compléments de dénombrement

I.1 Rappels sur les applications entre ensembles finis

Théorème I.1. *Si $f : E \to F$ avec E, F ensembles finis de même cardinal, alors on a équivalence entre :*

1. *f injective ;*
2. *f surjective ;*
3. *f bijective.*

Proposition I.2. *Si $f : E \to F$ est bijective, avec E ou F fini, alors E et F sont finis de même cardinal.*

Corollaire I.3. *Si $f : E \to F$, alors :*

1. *si f est surjective et que E est fini, alors F est fini avec $|F| \leq |E|$;*
2. *si f est injective et que F est fini, alors E est fini avec $|E| \leq |F|$.*

Démonstration. Par restriction ou corestriction on met E ou F en bijection avec une partie de F ou E. □

Théorème I.4 (Principe des tiroirs)**.** *Si $f : E \to F$, avec F fini et E infini ou de cardinal strictement plus grand que F, alors f n'est pas injective.*

Démonstration. C'est la contraposée du second point. □

Remarque I.5. *L'idée derrière le nom de ce théorème est que, étant donnés $n, p \in \mathbb{N}$ avec $n > p$, si on a n tiroirs et p chaussettes, alors au moins deux chaussettes sont dans le même tiroir.*

Exemple I.6. *Prenons 10 entiers quelconques entre 10 et 99. Alors on peut trouver deux sous-ensembles disjoints dont les éléments ont même somme.*
Prenons I un tel ensemble de nombres, notons :

$$\varphi : \left\{ \begin{array}{ccc} \mathcal{P}(I) & \to & \mathbb{N} \\ J & \mapsto & \sum_{j \in J} j \end{array} \right.$$

Alors $\mathrm{Im}\varphi \subset [\![0; 945]\!]$, tandis que $|\mathcal{P}(I)| = 2^{|I|} = 2^{10} = 1024$.
Donc φ n'est pas injective : il existe deux ensembles $J_1, J_2 \subset I$ distincts avec $\varphi(J_1) = \varphi(J_2)$. Et donc les parties $J_1 \setminus J_2$ et $J_2 \setminus J_1$ sont disjointes de même somme.

Théorème I.7 (Principe des bergers)**.** *Si $f : E \to F$ est surjective, avec F fini, et que tout élément de F possède p antécédents, alors E est fini de cardinal : $|E| = p \cdot |F|$.*

Démonstration. Par surjectivité de f, on peut écrire E comme l'union disjointe : $E = \cup_{y \in F} f^{-1}(\{y\})$.
En passant au cardinal, on a : $|E| = \sum_{y \in F} |f^{-1}(\{y\})| = \sum_{y \in F} p = p \cdot |F|$. □

Remarque I.8. *L'idée derrière le nom est qu'un berger, pour compter le nombre de pattes de ses moutons, peut se contenter de compter ses moutons, comme chaque mouton a quatre pattes.*

I.2 Arrangements et permutations

Définition I.9. *Étant donnés E un ensemble quelconque et $p \in \mathbb{N}$, on appelle p-**arrangement** un p-uplet d'éléments distincts de E.*

Remarques I.10.

1. *Un p-arrangement est un p-uplet de la forme $(x_1, \dots, x_p) \in E^p$ tel que : $i \neq j \Rightarrow x_i \neq x_j$. Mais l'ordre compte dans la représentation d'un p-arrangement, de sorte que les p-uplets $(x_1, x_2, \dots, x_p)$ et $(x_2, x_1, \dots, x_p)$ sont distincts.*
2. *Un p-arrangement revient à choisir une application injective de $[\![1; p]\!]$ dans E. Et ainsi, d'après un résultat sur les ensembles finis, on a donc qu'un tel p-arrangement existe si, et seulement si,* $\mathrm{Card}(E) \geq p$.

Proposition I.11. *Si E est un ensemble fini de cardinal $n \in \mathbb{N}$ et $p \in [\![0; n]\!]$, alors le nombre A_n^p de p-arrangements d'éléments de E est :*

$$A_n^p = n(n-1)\dots(n-p+1) = \frac{n!}{(n-p)!}.$$

Démonstration. On procède par récurrence sur p. Plus précisément, montrons par récurrence sur $p \in \mathbb{N}$ que : $\forall n \geq p,\ A_n^p = \dfrac{n!}{(n-p)!}$:

— si $p = 0$: alors il y a bien un seul 0-arrangement (qui correspond à la liste vide) ; mais cela ne fait sûrement pas consensus donc montrons le cas suivant ;

— si $p = 1$: alors tout 1-uplet a ses éléments deux-à-deux distincts (il n'a qu'un seul élément), donc il y a autant de 1-arrangements que d'éléments de E, à savoir n ;

— supposons que la formule vérifiée pour un $p \in \mathbb{N}$, pour tout $n \geq p$, et considérons E de cardinal $n \geq p+1$: alors l'application :

$$\varphi : \left\{ \begin{array}{rcl} E^{p+1} & \to & E \\ (x_0, \dots, x_p) & \mapsto & x_0 \end{array} \right.$$

induit une bijection de l'ensemble des $(p+1)$-arrangements de E vers E.
Plus précisément, si on fixe $x_0 \in E$, alors l'ensemble des antécédents de x_0 par φ parmi les $(p+1)$-arrangements forme l'ensemble :

$$\{(x_0, x_1, \dots, x_p) \,|\, (x_1, \dots, x_p) \text{ } p\text{-arrangement de } E \setminus \{x_0\}$$

et il y a donc autant d'antécédents que de p-arrangements d'éléments de $E \setminus \{x_0\}$, à savoir $\dfrac{(n-1)!}{(n-1-p)!}$ par hypothèse de récurrence.
Comme il y a $(n+1)$-valeurs pour x_0, on a finalement par principe des bergers que :

$$A_n^{p+1} = n \cdot \frac{(n-1)!}{(n-1-p)!} = \frac{n!}{(n-(p+1))!}$$

ce qui conclut la récurrence.

□

Corollaire I.12. *Étant donnés E un ensemble à p éléments et F un ensemble à n éléments, alors l'ensemble des applications injectives de E dans F possède $\dfrac{n!}{(n-p)!}$ éléments si $p \leq n$, et est vide sinon.*

Corollaire I.13. *Si E est un ensemble fini à n éléments, alors le groupe $\mathfrak{S}_E$ des permutations de E possède $n!$ éléments.*

Démonstration. Comme E est fini, une application $f : E \to E$ est bijective si, et seulement si, elle est injective. Il suffit donc de compter les applications injectives, qui sont bien au nombre de $n!$ par le résultat précédent (avec $n = p$). □

I.3 Combinaisons et parties

Définition I.14. *Étant donnés E un ensemble quelconque et $p \in \mathbb{N}$, on appelle p-**combinaison** une partie de E à p éléments.*

Remarque I.15.
Comme pour un arrangement, une p-combinaison revient à choisir p éléments de E, à la différence près que l'ordre ne compte pas : $\{x_1, x_2, \dots, x_p\} = \{x_2, x_2, \dots, x_p\}$.
Il y a donc autant de p-combinaisons que d'ensembles images d'applications injectives de $[\![1; p]\!]$ dans E.

Proposition I.16. *Si E est un ensemble fini de cardinal $n \in \mathbb{N}$ et $p \in [\![0; n]\!]$, le nombre C_n^p de p-combinaisons d'éléments de E est :*

$$C_n^p = \frac{A_n^p}{p!} = \frac{n(n-1)\dots(n-p+1)}{p!} = \frac{n!}{p!(n-p)!} = \binom{n}{p}.$$

Démonstration. On va utiliser le résultat sur le nombre de p-arrangements.
Plus précisément, deux p-arrangements $(x_1, \dots, x_p)$ et $(y_1, \dots, y_p)$ donnent la même combinaison si, et seulement si, il existe une bijection $\sigma \in S_p$ telle que :

$$\forall i \in [\![1; p]\!],\ x_{\sigma(i)} = y_i.$$

Comme les x_i sont deux-à-deux distincts, deux bijections distinctes donnent des p-arrangements distincts. Et donc il y a autant de p-arrangements donnant la même p-combinaison qu'il y a d'éléments dans S_p, c'est-à-dire $p!$.
Et finalement : $C_n^p = \dfrac{A_n^p}{p!} = \binom{n}{p}$. □

Remarque I.17. *On peut ainsi donner une interprétation combinatoire aux coefficients binomiaux, et donc un démonstration combinatoire aux résultat associés.*

Exemples I.18.

1. *Si $n \in \mathbb{N}$ et E est un ensemble à n élément, toutes les parties de E on un cardinal dans $[\![0; n]\!]$. Pour $p \in [\![0; n]\!]$ fixé, il y a $\binom{n}{p}$ parties à p éléments, et comme il y a en tout 2^n parties dans E, on trouve :*

$$\sum_{p=0}^{n} \binom{n}{p} = 2^n.$$

Plus généralement, on peut retrouver la formule du binôme :

$$(a+b)^n = \underbrace{(a+b)\dots(a+b)}_{n\ fois}$$

et donc il y a autant de termes en $a^p b^{n-p}$ que de manières de choisir p-fois a dans les n-facteurs ci-dessus, donc $\binom{n}{p}$. Et on a bien :

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

2. *L'application :*

$$\varphi : \left\{ \begin{array}{ccc} \mathcal{P}(E) & \to & \mathcal{P}(E) \\ A & \mapsto & \overline{A} \end{array} \right.$$

qui à une partie de E associe son complémentaire réalise une bijection (elle est involutive), et envoie toute partie à p-élément sur une partie à $n-p$-élément, ce qui donne que :

$$\forall p \in [\![1; n]\!],\ \binom{n}{p} = \binom{n}{n-p}.$$

3. *Pour le triangle de Pascal, fixons $p \in [\![1;n]\!]$, et cherchons à compter les parties de $[\![1;n]\!]$ à p éléments :*
   — *soit la partie contient n : et il reste à fixer la partie à $(p-1)$ éléments de $[\![1;n-1]\!]$ pour avoir p éléments en tout ; cela représente $\binom{n-1}{p-1}$ choix ;*
   — *soit la partie ne contient pas n : et il faut fixer une partie à p éléments dans $[\![1;n-1]\!]$; cela représente $\binom{n-1}{p}$ choix.*

   et donc on a en sommant :
$$\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p}.$$

4. *Si on a à disposition n personnes et que l'on veut former une équipe de p personnes, avec un capitaine, alors on peut procéder de différentes manières :*
   — *on choisit le capitaine (on a n choix), puis le reste de l'équipe, ce qui donne $n \cdot \binom{n-1}{p-1}$ manières de faire ;*
   — *on choisit les membres de l'équipe, puis parmi les personnes choisies on décide du capitaine, ce qui donne $p \cdot \binom{n}{p}$ manières ;*
   — *on choisit les non-capitaines, puis parmi les personnes non choisies on décide du capitaine, ce qui donne $\binom{n}{p-1} \cdot (n-p+1)$.*

   Et on trouve donc la fameuse ***formule du capitaine*** *:*
$$n\binom{n-1}{p-1} = p\binom{n}{p} = (n-p+1)\binom{n}{p-1}$$

Remarque I.19. *On voit bien apparaître, surtout dans le dernier exemple, un des enjeux des problèmes de dénombrements : trouver la "bonne" manière de compter les éléments, ce qui peut donner des expressions différentes sur le résultat final.*

Proposition I.20. *On considère E un ensemble quelconque $x_1, \dots, x_n \in E$ non nécessairement deux-à-deux distincts, et on note $k_1, \dots, k_r$ les multiplicités d'occurrence dans la famille (x_i) (si les x_i sont deux-à-deux distincts, on aura $r = n$ et $k_1 = \cdots = k_n = 1$). Alors le nombre de n-uplets distincts que l'on peut former avec les x_i est de :*
$$\frac{n!}{k_1! \cdot \dots \cdot k_r!}$$
(qu'on appelle aussi coefficient binomial généralisé).

Démonstration. O peut procéder de deux manières :
— on peut adapter la preuve qui donne le nombre de combinaisons : on considère l'application :
$$\varphi : \left\{ \begin{array}{rcl} S_n & \mapsto & E^n \\ \sigma & \mapsto & (x_{\sigma(1)}, \dots, x_{\sigma(n)}) \end{array} \right.$$
dont l'image est justement l'ensemble dont on cherche le cardinal.
Considérons $Y = (y_1, \dots, y_n)$ un tel n-uplet : alors on peut échanger les coordonnées de même valeurs sans changer Y, et donc Y possède $k1! \cdot \dots \cdot k_r!$ antécédents (toutes les permutations entre coordonnées égales).
Mais on a de plus la partition :
$$S_n = \cup_{Y \in \mathrm{Im}\varphi} \varphi^{-1}(\{Y\})$$
et ainsi, comme on a une union disjointe :
$$|S_n| = n! = \sum_{Y \in \mathrm{Im}\varphi} |\varphi^{-1}(\{Y\})| = |\mathrm{Im}\varphi| k_1! \cdot \dots \cdot k_r!$$
ce qui donne bien la formule voulue.

— par une "vraie" méthode combinatoire : on compte les n-uplets possibles en raisonnant sur les positions de chaque valeur prise par les x_i. On a k_1 coordonnées qui prennent la première valeur, ce qui laisse $\binom{n}{k_1}$ choix pour les coordonnées associées. Pour la valeur suivante, il y a $\binom{n-k_1}{k_2}$ choix. Puis $\binom{n-k_1-k_2}{k_3}$ choix pour la suivante. Et ainsi de suite jusqu'à avoir $\binom{n-k_1-\cdots-k_{r-1}}{k_r}$ choix pour la dernière.
En utilisant les expressions factorielles des coefficients binomiaux, et en utilisant que $k_1+\cdots+k_r = n$, on déduit que l'ensemble des n-uplets a pour cardinal :

$$\frac{n!}{k_1!(n-k_1)!}\cdot\frac{(n-k_1)!}{k_2!(n-k_1-k_2)!}\cdot\frac{(n-k_1-k_2)!}{k_3!(n-k_1-k_2-k_3)!}\cdot\cdots\cdot\frac{(n-k_1-\cdots-k_{r-1})!}{k_r!(n-k_1-\cdots-k_r)!}$$

ce qui donne bien la formule voulue par télescopage.

□

Exemple I.21. *On peut se demander combien de mots on peut former à partir de DIPLODOCUS. On a parmi les lettres de DIPLODOCUS :*
— *deux D et deux O ;*
— *une fois les lettres I,P,L,C,U,S.*
avec donc un total de 10 *lettres, cela fait un nombre de mots de :*

$$\frac{10!}{2!\cdot 2!\cdot 1!\cdot\cdots\cdot 1!} = 907200.$$

II Espaces probabilisés

II.1 Univers et événements

Définition II.1. *Une* ***expérience aléatoire*** *est une expérience dont on ne peut prédire l'issue.*
L'ensemble des issues d'une expérience aléatoire est appelé ***l'univers****.*

Remarque II.2. *En général, on notera Ω l'univers d'une expérience aléatoire, et ω ses éléments. On ne travaillera cette année qu'avec des univers finis.*

Exemples II.3.
1. *Pour un lancer de pièce, l'univers est $\{Pile, Face\}$.*
2. *Pour un lancer de dé, l'univers est $\{1,\ldots,n\}$ (selon le nombre de faces du dé).*

Définition II.4. *Étant donnée une expérience aléatoire d'univers Ω, on appellera* ***événement*** *une partie de Ω. Plus précisément, on dira que :*
1. *Ω est l'événement certain ;*
2. *$\emptyset$ est l'événement impossible ;*
3. *les singletons sont les événements élémentaires.*

Exemple II.5. *Si on considère l'expérience "tirer une carte au hasard dans un jeu de tarot", alors $|\Omega| = 78$, et l'événement $A = \{R\clubsuit, R\diamondsuit, R\heartsuit, R\spadesuit\}$ revient à tirer un Roi.*

Définition II.6. *Étant donné $A \subset \Omega$ un événement, on définit le* ***contraire*** *de A, noté $\overline{A}$, comme le complémentaire de A dans Ω, c'est-à-dire : $\overline{A} = \Omega \setminus A$.*
Si de plus $B \subset \Omega$ est un autre événement, on associe à A et B :
— *la* ***disjonction*** *(appelée aussi "A ou B"), comme l'événement $A \cup B$;*
— *la* ***conjonction*** *(appelée aussi "A et B"), comme l'événement $A \cap B$.*
Et on dira que A et B sont ***incompatibles*** *si $A \cap B = \emptyset$.*

Exemple II.7. *On considère un lancer de dé à 6 faces, avec les événements A =“le numéro est pair”= $\{2,4,6\}$ et B =“le numéro est premier”= $\{2,3,5\}$. Alors :*
- $\overline{A} = \{1,3,5\}$ =“le numéro est impair”;
- $\overline{B} = \{1,4,6\}$ =“le numéro n'est pas premier”;
- $A \cup B = \{2,3,4,5,6\} = \overline{\{1\}}$;
- $A \cap B = \{2\}$.

Définition II.8. *Un **système complet d'événements** est une famille $(A_i)_{i\in[\![1;n]\!]}$ d'événements deux-à-deux incompatibles tels que : $\cup_{i=1}^n A_i = \Omega$.*

Remarque II.9. *C'est une partition, dans laquelle on autorise certains événements à être vide.*

Exemples II.10.
1. $(\{\omega\})_{\omega\in\Omega}$ *est un système complet d'événements ;*
2. *si $A \subset \Omega$, alors $(A, \overline{A})$ est un système complet d'événements.*

II.2 Probabilité sur un ensemble fini

Définition II.11 (Probabilité)**.** *Si Ω est un univers fini, une **probabilité** sur Ω est la donnée d'une application $\mathbb{P} : \Omega \to [0;1]$ telle que :*
1. $P(\Omega) = 1$;
2. $\forall A, B \in \mathcal{P}(\Omega),\ A \cap B = \emptyset \Rightarrow \mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B)$ *(additivité)*

*On dira alors que $(\Omega, \mathbb{P})$ est un **espace probabilisé**.*

Remarque II.12. *Le point important ici est que la probabilité est une donnée à rajouter à l'univers considérer. On peut avoir des expériences aléatoires qui ont même univers, mais pas la même probabilité. Par exemple, ce serait la différence entre un dé équilibré et un dé truqué.*

Proposition II.13. *Si $(\Omega, \mathbb{P})$ est un espace probabilité, alors :*
1. $\mathbb{P}(\emptyset) = 0$;
2. *si $A \in \mathcal{P}(\Omega)$, alors $\mathbb{P}(\overline{A}) = 1 - \mathbb{P}(A)$;*
3. *si $A, B \in \mathcal{P}(\Omega)$ avec $A \subset B$, alors $\mathbb{P}(A) \leq \mathbb{P}(B)$ (croissance d'une probabilité) ;*
4. *si $A, B \in \mathcal{P}(\Omega)$, alors $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$;*
5. *si $(A_i)_{i\in[\![1;n]\!]}$ est une famille finie d'événements, alors : $\mathbb{P}\left(\cup_{i=1}^n A_i\right) \leq \sum_{i=1}^n \mathbb{P}(A_i)$ (sous-additivité). De plus, on a égalité dès lors que les A_i sont deux-à-deux incompatibles.*

Démonstration.

1. Comme $\Omega \cap \emptyset = \emptyset$ et $\Omega \cup \emptyset = \Omega$, alors par additivité :
$$\mathbb{P}(\Omega) = \mathbb{P}(\Omega) + \mathbb{P}(\emptyset)$$
et donc $\mathbb{P}(\emptyset) = 0$.
2. Comme $A \cap \overline{A} = \emptyset$ et $A \cup \overline{A} = \Omega$, alors par additivité :
$$1 = \mathbb{P}(\Omega) = \mathbb{P}(A) + \mathbb{P}(\overline{A}).$$
3. Si $A \subset B$, alors on écrit $B = A \cup (B \setminus A)$ (qui est une union disjointe). Et ainsi :
$$\mathbb{P}(B) = \mathbb{P}(A) + \underbrace{\mathbb{P}(B \setminus A)}_{\geq 0} \geq \mathbb{P}(A).$$

4. On a l'union disjointe : $(A \cup B) = A \cup (B \setminus A)$ qui donne déjà que : $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B \setminus A)$. Et on a également l'union disjointe : $B = (A \cap B) \cup (B \setminus A)$, ce qui donne : $\mathbb{P}(B) = \mathbb{P}(A \cap B) + \mathbb{P}(B \setminus A)$. En réinjectant, on a bien :
$$\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B).$$

5. Procédons par récurrence sur $n \in \mathbb{N}^*$.
   — si $n = 1$: on a même une égalité ;
   — si $n = 2$: on a montré que $\mathbb{P}(A_1 \cup A_2) = \mathbb{P}(A_1) + \mathbb{P}(A_2) - \mathbb{P}(A_1 \cap A_2) \leq \mathbb{P}(A_1) + \mathbb{P}(A_2)$. Si A_1 et A_2 sont incompatibles, on a $\mathbb{P}(A_1 \cap A_2) = 0$ ce qui donne bien l'égalité.
   — supposons le résultat vérifié pour un $n \in \mathbb{N}^*$, et considérons $A_1, \ldots, A_{n+1} \in \mathcal{P}(\Omega)$. Alors :
   $$\mathbb{P}\left(\cup_{i=1}^{n+1} A_i\right) = \mathbb{P}\left((\cup_{i=1}^{n} A_i) \cup A_{n+1}\right) \leq \mathbb{P}\left(\cup_{i=1}^{n} A_i\right) + \mathbb{P}(A_{n+1}) \leq \sum_{i=1}^{n} \mathbb{P}(A_i) + \mathbb{P}(A_{n+1}) = \sum_{i=1}^{n+1} \mathbb{P}(A_i)$$
   ce qui montre bien la formule.
   Si les A_i sont deux-à-deux incompatibles, alors A_{n+1} et $(\cup_{i=1}^{n} A_i)$ le sont également, ce qui assure que la première inégalité est une égalité. Et pour la seconde on retrouve le cas d'égalité du résultat au rang n.

□

Remarques II.14.

1. *Ces résultats se comprennent bien d'un point de vue probabiliste. Par exemple, pour la croissance : si l'événement A est réalisé et que $A \subset B$, alors l'événement B est aussi réalisé. Et donc la probabilité de B est plus grande que celle de A, comme B est réalisé dès que A l'est.*
2. *La réciproque des points 3. et 5. est fausse, dans le sens où on pourrait avoir $\mathbb{P}(A) \leq \mathbb{P}(B)$ sans avoir $A \subset B$, et on peut avoir $\mathbb{P}(\cup A_i) = \sum \mathbb{P}(A_i)$ même avec des A_i non incompatibles.*

Corollaire II.15. *Si $(A_i)_{i \in [\![1;n]\!]}$ est un système complet d'événements, alors :*
$$\sum_{i=1}^{n} \mathbb{P}(A_i) = 1$$
et plus généralement, si $A \in \mathcal{P}(\Omega)$, on a :
$$\mathbb{P}(A) = \sum_{i=1}^{n} \mathbb{P}(A \cap A_i).$$
En particulier :
$$\sum_{\omega \in \Omega} \mathbb{P}(\{\omega\}) = 1$$
et plus généralement si $A \in \mathcal{P}(\Omega)$, on a :
$$\mathbb{P}(A) = \sum_{\omega \in A} \mathbb{P}(\{\omega\}).$$

Démonstration. C'est le cas d'égalité de la dernière assertion. □

Définition II.16. *On considère Ω un ensemble fini. On appelle **distribution de probabilité sur** Ω une famille $(p_\omega)_{\omega \in \Omega}$ de réels positifs telle que : $\sum_{\omega \in \Omega} p_\omega = 1$.*

Théorème II.17. *Si Ω est une ensemble fini muni d'une probabilité $\mathbb{P}$, alors la famille $(\mathbb{P}(\{\omega\}))_{\omega\in\Omega}$ est une distribution de probabilité qui détermine entièrement $\mathbb{P}$, dans le sens où l'application $\mathbb{P} \mapsto (\mathbb{P}(\{\omega\}))_{\omega\in\Omega}$ définit une bijection des probabilités sur Ω vers les distributions de probabilité sur Ω.*

Démonstration. Notons déjà que, comme la famille $(\{\omega\})_{\omega\in\Omega}$ forme un système complet d'événements, on a bien que $(\mathbb{P}(\{\omega\}))_{\omega\in\Omega}$ est une distribution de probabilité.
Reste à montrer la bijectivité de $\varphi : \mathbb{P} \mapsto (\mathbb{P}(\{\omega\}))_{\omega\in\Omega}$:

— injectivité : par probabilité d'une union disjointe, on a que :

$$\forall A \subset \Omega,\ \mathbb{P}(A) = \sum_{\omega\in A} \mathbb{P}(\{\omega\})$$

et donc $\mathbb{P}$ est entièrement déterminée par les probabilités des événements élémentaires, donc par $\varphi(\mathbb{P})$, ce qui donne bien l'injectivité.

— surjectivité : considérons $(p_\omega)_{\omega\in\Omega}$ une distribution de probabilité sur Ω. On considère sur $\mathcal{P}(\Omega)$ l'application $\mathbb{P} : A \mapsto \sum_{\omega\in A} p_\omega$. Montrons que $\mathbb{P}$ vérifie bien $\varphi(\mathbb{P}) = (p_\omega)$:
— $\mathbb{P}(\Omega) = \sum_{\omega\in\Omega} p_\omega = 1$ par définition d'une distribution de probabilités ;
— si A et B sont incompatibles, alors :

$$\mathbb{P}(A \cup B) = \sum_{\omega\in A\cup B} p_\omega = \sum_{\omega\in A} p_\omega + \sum_{\omega\in B} p_\omega = \mathbb{P}(A) + \mathbb{P}(B)$$

et on déduit également de ces deux résultats, comme φ est à valeurs dans $\mathbb{R}_+$ (somme de réels positifs) que :

$$\forall A \in \mathcal{P}(\Omega),\ 1 = \mathbb{P}(\Omega) = \mathbb{P}(A \cap \overline{A}) = \mathbb{P}(A) + \underbrace{\mathbb{P}(\overline{A})}_{\geq 0}$$

donc finalement $\mathbb{P}$ est une application de $\mathcal{P}(\Omega)$ dans $[0;1]$, avec $\mathbb{P}(\Omega) = 1$ et additive : c'est une probabilité.
De plus, si $\omega_0 \in \Omega$, alors :

$$\mathbb{P}(\{\omega_0\}) = \sum_{\omega\in\{\omega_0\}} p_\omega = p_{\omega_0}$$

et donc $(\mathbb{P}(\{\omega\})) = (p_\omega)$, donc $\varphi(\mathbb{P}) = (p_\omega)$, ce qui donne la surjectivité.

□

Remarques II.18.

1. *L'idée est qu'une probabilité se comprend bien en termes de probabilité des événements élémentaires. C'est d'autant plus légitime sur un univers fini, mais pourrait très bien s'étendre à des univers infinis (les termes sont toujours positifs donc les sommes ont toujours un sens, et comme toutes les sommes finies étant majorées par 1, on ne manipule que des familles sommables).*
2. *Ce résultat met en évidence le lien entre probabilités et dénombrement : on peut raisonner sur les événements élémentaires, qu'on peut dénombrer et évaluer individuellement leurs probabilités pour déduire la probabilité de tout événement.*

Proposition-Définition II.19. *Si Ω est un univers fini, il existe une unique probabilité $\mathbb{P}$ telle que tous les événements élémentaires ont même probabilité.*
On l'appelle la ***probabilité uniforme sur*** *Ω, et elle est donnée par :*

$$\forall A \in \Omega,\ \mathbb{P}(A) = \frac{|A|}{|\Omega|}.$$

Démonstration. Nécessairement, si les événements élémentaires ont tous la même probabilité, en notant α cette probabilité, on a par probabilité d'une union disjointe que :

$$1 = \mathbb{P}(\Omega) = \sum_{\omega\in\Omega} \mathbb{P}(\{\omega\}) = |\Omega| \cdot \alpha$$

et donc $\alpha = \dfrac{1}{|\Omega|}$.

La famille $(p_\omega) = \left(\dfrac{1}{|\Omega|}\right)$ forme alors une distribution de probabilités, et par union disjointe on trouve que :

$$\forall A \subset \Omega,\ \mathbb{P}(A) = \sum_{\omega\in A} \frac{1}{|\Omega|} = \frac{|A|}{|\Omega|}.$$

□

Remarques II.20.

1. *On parlera aussi d'**équiprobabilité**, comme tous les événements élémentaires ont même probabilité.*
2. *Pour mettre en évidence le caractère uniforme d'une probabilité, on emploiera le terme **équilibré** pour un lancer (d'un dé ou d'une pièce par exemple) ou **indiscernable** pour un tirage (de cartes ou de boules).*
3. *Dans le cas d'une probabilité uniforme, le fait de dénombrer les événements élémentaires (ce qui revient à calculer des cardinaux d'ensembles) permet directement de déduire les probabilités. C'est dans ce cadre que les technique de dénombrement sont les plus efficaces.*

Exemple II.21. *Les problèmes de dénombrements sont souvent présentés sous forme de tirages. Si on considère une urne contenant $n \in \mathbb{N}^*$ boules, et que l'on effectue p tirages successifs, on a deux paramètres à prendre en compte, selon que l'on fait des remises ou non et que l'ordre compte ou non.*
Le fait de ne pas compter l'ordre revient à faire des tirages simultanés, pour lesquels la notion de remise n'a pas vraiment de sens, si bien qu'on a généralement l'un des trois cas suivants :

- *sans remise et sans ordre : $\binom{n}{p}$ possibilités ;*
- *sans remise et avec ordre : A_n^p possibilités ;*
- *avec remise et avec ordre : n^p possibilités.*

Et le tirage avec remise sans tenir compte de l'ordre correspond à $\binom{n+p-1}{p}$ possibilités (ce que l'on montrera en exercice).

III Probabilité conditionnelle

III.1 Probabilités conditionnelles

Définition III.1 (Probabilité conditionnelle)**.** *On considère A, B deux événements d'un espace probabilisé $(\Omega, \mathbb{P})$ tels que $\mathbb{P}(B) \neq 0$.*
*On définit alors la **probabilité conditionnelle de** A **sachant** B est la quantité notée $\mathbb{P}_B(A)$ ou $\mathbb{P}(A \mid B)$ définie par :*

$$\mathbb{P}_B(A) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(A)}$$

Remarque III.2. *Le sens derrière est celui conforme à l'intuition : c'est la probabilité de réaliser l'événement A tout en sachant déjà que B est réalisé.*

Exemple III.3. *Considérons un jeu de tarot, duquel on tire une carte avec équiprobabilité.*
On considère les événements $A =$"tirer un roi" et $B =$"tirer une tête".
Un jeu de tarot contient 78 cartes, dont les têtes sont les valets, cavaliers, reines et rois (chaque valeur étant représentée par 4 cartes, ce qui fait 16 têtes). Comme on a une équiprobabilité, on déduit que :

$$\mathbb{P}(A) = \frac{4}{78} = \frac{2}{39},\ \mathbb{P}(B) = \frac{16}{78} = \frac{8}{39} \text{ et } \mathbb{P}(A \cap B) = \mathbb{P}(A) = \frac{2}{39}$$

Par définition, on a les probabilités conditionnelles :

$$\mathbb{P}_B(A) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)} = \frac{\frac{2}{39}}{\frac{8}{39}} = \frac{1}{4} \text{ et } \mathbb{P}_A(B) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(A)} = \frac{\frac{2}{39}}{\frac{2}{39}} = 1$$

ce que l'on comprend bien intuitivement :
- *pour $\mathbb{P}_B(A)$: si on a pioché une tête, comme toutes les têtes sont équiprobables, on a 1 chance sur 4 d'avoir pioché un roi ;*
- *pour $\mathbb{P}_A(B)$: si on a pioché un roi, on a nécessairement pioché une tête, d'où une probabilité de 1.*

Remarque III.4. *L'événement "A sachant B" n'existe pas : pour calculer une probabilité conditionnelle, il faudra systématiquement revenir aux calculs des probabilités de $A \cap B$ et de B.*

Proposition III.5. *Si B est un événement de l'espace probabilisé $(\Omega, \mathbb{P})$ tel que $\mathbb{P}(B) \neq 0$, alors l'application :*

$$\mathbb{P}_B : \left\{ \begin{array}{rcl} \mathcal{P}(\Omega) & \to & [0;1] \\ A & \mapsto & P_B(A) \end{array} \right.$$

est une probabilité sur Ω.

Démonstration. Notons déjà que, si $A \subset \Omega$ alors $A \cap B \subset B$, et donc par croissance de $\mathbb{P}$ on a : $P(A \cap B) \in [0; \mathbb{P}(B)]$.
Comme $\mathbb{P}(B) \neq 0$, alors $\mathbb{P}(B) > 0$ et donc : $\mathbb{P}_B(A) \in [0;1]$.
De plus, on a :
- $\Omega \cap B = B$, et donc $\mathbb{P}_B(\Omega) = \dfrac{\mathbb{P}(B)}{\mathbb{P}(B)} = 1$;
- si A_1, A_2 sont incompatibles : alors $A_1 \cap B$ et $A_2 \cap B$ sont également incompatibles, comme par associativité et commutativité de l'intersection on a : $(A_1 \cap B) \cap (A_2 \cap B) = (A_1 \cap A_2) \cap B = \emptyset$. Et ainsi :

$$\mathbb{P}_B(A_1) + \mathbb{P}_B(A_2) = \frac{\mathbb{P}(A_1 \cap B) + \mathbb{P}(A_2 \cap B)}{\mathbb{P}(B)} = \frac{\mathbb{P}((A_1 \cap B) \cup (A_2 \cap B))}{\mathbb{P}(B)} = \frac{\mathbb{P}\left((A_1 \cup A_2) \cap B\right)}{\mathbb{P}(B)} = \mathbb{P}_B(A_1 \cup A_2)$$

par distributivité de l'intersection par rapport à l'union.

Et on a donc bien une probabilité. □

Remarque III.6. *Les propriétés des probabilités (passage au complémentaire, croissance, sous-additivité, etc.) sont donc aussi vérifiées par les probabilités conditionnelles.*

III.2 Probabilités et probabilités conditionnelles

Théorème III.7 (Formule des probabilités composées)**.** *On considère $A_1, \ldots, A_n$ des événements d'un espace probabilisé $(\Omega, \mathbb{P})$ tels que $\mathbb{P}(A_1 \cap \cdots \cap A_{n-1}) \neq 0$. Alors :*

$$\begin{array}{rcl} P\left(A_1 \cap \cdots \cap A_n\right) & = & \mathbb{P}(A_1)\mathbb{P}_{A_1}(A_2)\mathbb{P}_{A_1 \cap A_2}(A_3) \ldots \mathbb{P}_{A_1 \cap \cdots \cap A_{n-1}}(A_n) \\ & = & \prod_{i=0}^{n-1} \mathbb{P}_{A_1 \cap \cdots \cap A_i}(A_{i+1}) \end{array}.$$

Démonstration. Notons déjà que, pour tout $i \in [\![1; n-1]\!]$ on a :

$$(A_1 \cap \cdots \cap A_{n-1}) \subset (A_1 \cap \cdots \cap A_i)$$

et donc par croissance des probabilités on déduit que : $\mathbb{P}(A_1 \cap \cdots \cap A_i) \geq \mathbb{P}(A_1 \cap \cdots \cap A_{n-1}) > 0$, ce qui assure que les probabilités conditionnelles ci-dessus sont bien définies.
Pour obtenir l'égalité, il suffit de constater qu'on a un télescopage, en écrivant en extension les probabilités conditionnelles :

$$\prod_{i=0}^{n-1} \mathbb{P}_{A_1 \cap \cdots \cap A_i}(A_{i+1}) = \mathbb{P}(A_1) \cdot \prod_{i=1}^{n-1} \frac{\mathbb{P}(A_1 \cap \cdots \cap A_{i+1})}{\mathbb{P}(A_1 \cap \cdots \cap A_i)} = \mathbb{P}(A_1 \cap \cdots \cap A_n)$$

□

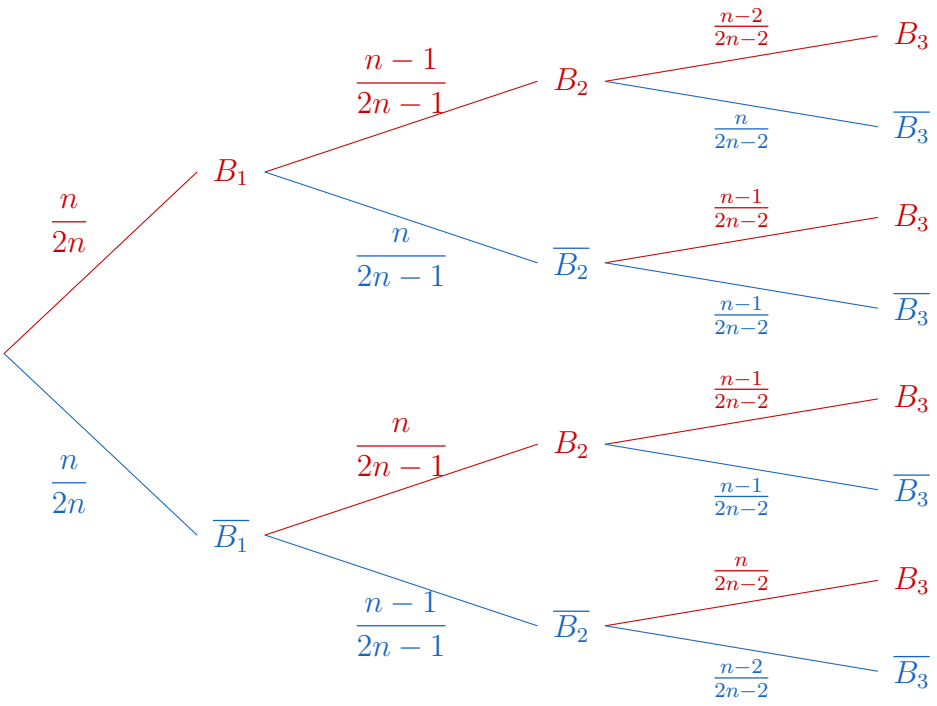
Remarques III.8.

1. *Cette formule est particulièrement utile lors de tirages successifs sans remise : chaque tirage modifie les probabilités des tirages suivants, ce qui fait apparaître les produits de probabilités conditionnelles du théorème.*
   Et elles se comprennent bien en terme d'arbres de probabilité : le produit correspond au produit des probabilités associées à chaque branche.
   Et le même raisonnement se transpose à un tirage simultané, en ordonnant les éléments tirés.
2. *La formule s'étend au cas où $\mathbb{P}(A_1 \cap \cdots \cap A_{n-1}) = 0$, en posant par convention que $P_B(A) \cdot P(B) = 0$ dès que $\mathbb{P}(B) = 0$.*

Exemple III.9.
On considère une urne contenant $2n$ boules (n noires et n blanches), et on y tire successivement sans remise 3 boules. On se demande la probabilité de tirer dans cet ordre des boules noire/blanche/noire.
Pour $i \in \{1, 2, 3\}$ notons B_i l'événement "tirer une boule blanche au tirage i". On veut donc calculer la probabilité de $\overline{B_1} \cap B_2 \cap \overline{B_3}$, ce qui se fait par les probabilités composées :

$$\mathbb{P}\left(\overline{B_1} \cap B_2 \cap \overline{B_3}\right) = \mathbb{P}\left(\overline{B_1}\right) \mathbb{P}_{\overline{B_1}}(B_2) \cdot \mathbb{P}_{\overline{B_1} \cap B_2}\left(\overline{B_3}\right) = \frac{n}{2n} \cdot \frac{n}{2n-1} \cdot \frac{n-1}{2n-2} = \frac{n}{4(2n-1)}$$

ce qui se comprend bien avec l'arbre suivant :



Théorème III.10 (Formule des probabilités totales)**.** *Si on considère $\{A_1, \dots, A_n\}$ un système complet d'événements, et $B \in \mathcal{P}(\Omega)$, alors :*

$$\mathbb{P}(B) = \sum_{i=1}^{n} \mathbb{P}(B \cap A_i) = \sum_{i=1}^{n} \mathbb{P}(A_i)\mathbb{P}_{A_i}(B)$$

(en reprenant à nouveau la convention selon laquelle $P_A(B) \cdot P(A) = 0$ dès que $\mathbb{P}(A) = 0$).

Démonstration. Comme on a un système complet d'événements, alors $\Omega = \cup_{i=1}^{n} A_i$ (comme union disjointe) et donc pour tout événement B on a : $B = \cup_{i=1}^{n}(B \cap A_i)$ (l'union étant également disjointe). Par additivité, il vient donc :

$$\mathbb{P}(B) = \sum_{i=1}^{n} \mathbb{P}(B \cap A_i)$$

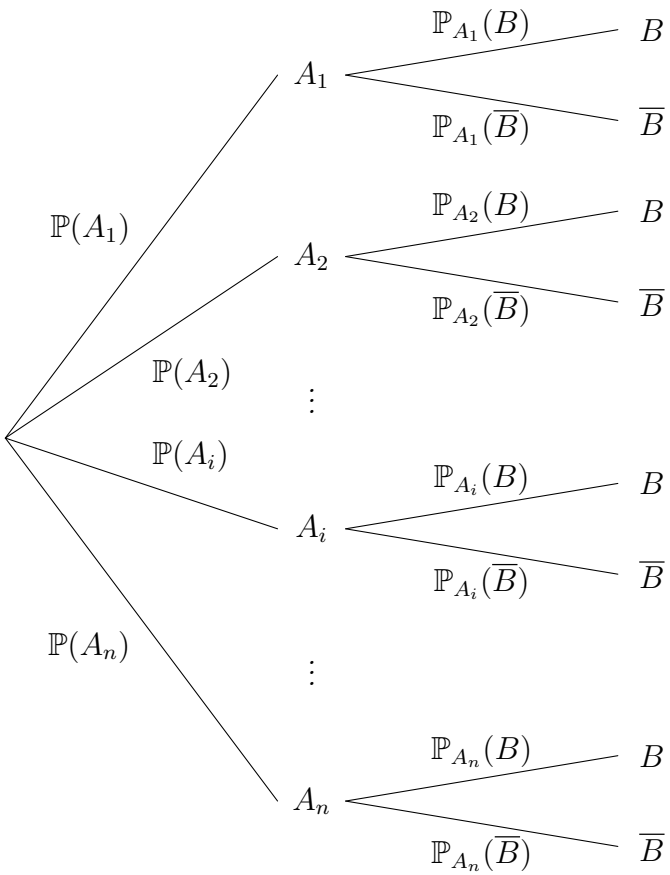
et la réécriture vient :

— directement de la définition des probabilités conditionnelles si $\mathbb{P}(A_i) \neq 0$;

— du fait que, si $\mathbb{P}(A_i) = 0$, alors $\mathbb{P}(B \cap A_i) = 0$ (par croissance).

□

Remarque III.11. *Tout l'enjeu est justement de trouver un système complet d'événements qui facilite les calculs des probabilités qui apparaissent dans la somme.*
Et à nouveau, le résultat se comprend bien avec un arbre :



Exemple III.12. *On considère une urne contenant n boules noires et b boules blanches. On tire sans remise trois boules, et on se demande la probabilité d'avoir une boule blanche au troisième tirage.*
Pour $i \in \{1, 2, 3\}$ notons B_i l'événement "tirer une boule blanche au tirage i". On veut calculer la probabilité de B_3. Pour cela, on utilise le système complet d'événements $B_1 \cap B_2$, $B_1 \cap \overline{B_2}$, $\overline{B_1} \cap B_1$, $\overline{B_1} \cap \overline{B_2}$, ce qui

donne :

$$\begin{aligned}\mathbb{P}(B_3) &= \mathbb{P}(B_1\cap B_2\cap B_3)+\mathbb{P}(B_1\cap\overline{B_2}\cap B_3)+\mathbb{P}(\overline{B_1}\cap B_1\cap B_3)+\mathbb{P}(\overline{B_1}\cap\overline{B_2}\cap B_3)\\ &= \frac{b}{b+n}\cdot\frac{b-1}{b+n-1}\cdot\frac{b-2}{b+n-2}+\frac{b}{b+n}\cdot\frac{n}{b+n-1}\cdot\frac{b-1}{b+n-2}\\ &\quad +\frac{n}{b+n}\cdot\frac{b}{b+n-1}\cdot\frac{b-1}{b+n-2}+\frac{n}{b+n}\cdot\frac{n-1}{b+n-1}\cdot\frac{b}{b+n-2}\\ &= \frac{b\cdot((b+n)^2-3(b+n)+2)}{(b+n)(b+n-1)(b+n-2)}=\frac{b}{b+n}\end{aligned}$$

Et notons que le résultat final est rassurant : si on échange les rôles de b et n, cela vient à calculer la probabilité de $\mathbb{P}(\overline{B_3})$, qui vaudrait donc $\frac{n}{b+n}$. Et on a bien que :

$$\mathbb{P}(B_3)+\mathbb{P}(\overline{B_3})=\frac{b}{b+n}+\frac{n}{b+n}=1.$$

Et surtout, on aurait pu prévoir ce résultat : le rôle des boules est symétrique : si on regarde nos triplets obtenus à la fin, on comprend bien que le fait de regarder la première ou la troisième boule ne change rien à la probabilité. Et il est immédiat que $\mathbb{P}(B_1)=\frac{b}{n+b}$ par un argument de dénombrement.

Théorème III.13 (Formule de Bayes)**.** *Si A, B sont des événements qui sont tous les deux de probabilité non nulle, alors :*

$$\mathbb{P}_B(A)=\frac{\mathbb{P}_A(B)\mathbb{P}(A)}{\mathbb{P}(B)}.$$

Démonstration. On a directement par définition que :

$$\mathbb{P}(A\cap B)=\mathbb{P}_B(A)\mathbb{P}(B)=\mathbb{P}_A(B)\mathbb{P}(A)$$

ce qui donne l'égalité en divisant par $\mathbb{P}(B)$. □

Remarque III.14. *La formule de Bayes s'utilise surtout lorsque l'on veut changer le prisme sous lequel on regarde deux événements : on connaît une probabilité conditionnelle et on veut calculer l'autre.*

Exemple III.15. *On considère un test de dépistage. Suivant les résultats du laboratoire :*

- *si une personne est malade : le test est positif dans 99% des cas ;*
- *si une personne n'est pas malade : le test est positif dans 0,1% des cas.*

Et on se demande à quel point le test est fiable, dans le sens où, si un test est positif, on veut savoir la probabilité que la personne testée soit malade.
Si on note T l'événement "le test est positif" et M l'événement "la personne est malade", on veut donc calculer $\mathbb{P}_T(M)$ en fonction de la probabilité $\mathbb{P}(M)=p$ d'être malade, ce qui se fait par la formule de Bayes :

$$P_T(M)=\frac{\mathbb{P}_M(T)\mathbb{P}(M)}{\mathbb{P}(T)}=\frac{0,99\cdot p}{\mathbb{P}(T)}$$

et on calcule $\mathbb{P}(T)$ par la formule des probabilités totales, ce qui donne (avec le système complet $\{M,\overline{M}\}$) :

$$\mathbb{P}(T)=\mathbb{P}_M(T)\mathbb{P}(M)+\mathbb{P}_{\overline{M}}(T)\mathbb{P}(\overline{M})=0,99\cdot p+0,001\cdot(1-p)=0,001+0.989\cdot p.$$

Et finalement on trouve que :

$$P_T(M)=\frac{0,99p}{0,001+0.989\cdot p}\simeq\frac{1}{\frac{10^{-3}}{p}+1}$$

ce qui donne par exemple :

— *avec* $p = 10^{-3}$ *: on a une chance sur* 2 *d'être malade avec un test positif ;*
— *avec* $p = 10^{-4}$ *: on a* 9% *de chance d'être malade avec un test positif.*

Corollaire III.16. *Si on considère* $\{A_1, \dots, A_n\}$ *un système complet d'événements, et* $B \in \mathcal{P}(\Omega)$*, alors :*

$$\forall i \in [\![1; n]\!],\ \mathbb{P}_B(A_i) = \frac{\mathbb{P}_{A_i}(B)\mathbb{P}(A_i)}{\sum_{j=1}^{n} \mathbb{P}(A_j)\mathbb{P}_{A_j}(B)}.$$

Démonstration. Découle du résultat précédent, et de la formule des probabilités totales pour changer $\mathbb{P}(B)$ en l'expression du dénominateur. □

Remarque III.17. *Pour le système complet* $\{A, \overline{A}\}$*, on retrouve que :*

$$\mathbb{P}_B(A) = \frac{\mathbb{P}_A(B)\mathbb{P}(A)}{\mathbb{P}(A)\mathbb{P}_A(B) + \mathbb{P}(\overline{A})\mathbb{P}_{\overline{A}}(B)}$$

et on retrouve la méthode employée dans l'exemple précédent.

III.3 Indépendance

Définition III.18. *Deux événements* A *et* B *sont dits* ***indépendants*** *si :* $\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B)$*.*

Exemples III.19.

1. *On lance un dé équilibré à* 6 *faces. Alors les événements* $A =$*"le montant est un nombre premier"* *et* $B =$*"le montant est un multiple de* 3*"* *sont indépendants.*
   On a : $A = \{2, 3, 5\}$*,* $B = \{3, 6\}$ *et* $A \cap B = \{3\}$*. Et comme on a une équiprobabilité on a directement que :*
   $$\mathbb{P}(A \cap B) = \frac{1}{6} = \frac{1}{2} \cdot \frac{1}{3} = \mathbb{P}(A) \cdot \mathbb{P}(B).$$
2. *On considère le fait de tirer une carte dans un jeu de cartes indiscernables. On considère les événements* $A =$*"tirer une dame"* *et* $B =$*"tirer un cœur". Dans ce cas, on a* $A \cap B =$*"tirer la dame de cœur".*
   Alors selon le type de jeu, les événements A *et* B *sont indépendants ou non :*
   — *dans un jeu de* 52 *cartes :*
   $$\mathbb{P}(A \cap B) = \frac{1}{52} = \frac{1}{13} \cdot \frac{1}{4} = \mathbb{P}(A) \cdot \mathbb{P}(B)$$
   donc A *et* B *sont indépendants ;*
   — *dans le même jeu, mais où on aurait perdu le roi de trèfle :*
   $$\mathbb{P}(A \cap B) = \frac{1}{51} \neq \frac{52}{51^2} = \frac{4}{51} \cdot \frac{13}{51} = \mathbb{P}(A) \cdot \mathbb{P}(B)$$
   donc A *et* B *ne sont pas indépendants ;*
   — *dans un jeu de tarot on a :*
   $$\mathbb{P}(A \cap B) = \frac{1}{78} \neq \frac{56}{78^2} = \frac{4}{78} \cdot \frac{14}{78} = \mathbb{P}(A) \cdot \mathbb{P}(B)$$
   donc A *et* B *ne sont pas indépendants.*

Proposition III.20. *Soient* A, B *deux événements avec* $\mathbb{P}(B) \neq 0$*. Alors les événements* A *et* B *sont indépendants si, et seulement si,* $\mathbb{P}(A) = \mathbb{P}_B(A)$*.*

Démonstration. On écrit directement, comme $\mathbb{P}(B) \neq 0$, que : $\mathbb{P}_B(A) = \dfrac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)}$. Et donc A et B sont indépendant si, et seulement si :

$$\mathbb{P}(A) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)} = \mathbb{P}_B(A)$$

□

Remarques III.21.

1. *On comprend bien avec ce résultat le terme d'indépendance : le fait d'avoir une information sur B ne donne aucune information sur A, dans la mesure où la probabilité de A n'est pas affectée par le fait que B soit réalisée ou non.*
2. *Si $\mathbb{P}(B) = 0$, alors B est indépendant de A : on a en effet $\mathbb{P}(A \cap B) \leq \mathbb{P}(B)$ (par croissance) donc $\mathbb{P}(A \cap B) = 0$, donc $\mathbb{P}(A \cap B) = \mathbb{P}(A) \cdot \mathbb{P}(B)$.*

Proposition III.22. *Si A et B sont deux événements indépendants, alors A et $\overline{B}$ le sont aussi.*

Démonstration. Par formule des probabilités totales, on a :

$$\mathbb{P}(A) = \mathbb{P}(A \cap B) + \mathbb{P}(A \cap \overline{B})$$

et ainsi : $\mathbb{P}(A \cap \overline{B}) = \mathbb{P}(A) - \mathbb{P}(A \cap B) = \mathbb{P}(A) - \mathbb{P}(A)\mathbb{P}(B) = \mathbb{P}(A) \cdot (1 - \mathbb{P}(B)) = \mathbb{P}(A)\mathbb{P}(\overline{B})$.
Donc A et $\overline{B}$ sont bien indépendants. □

Remarque III.23. *Comme le fait d'être indépendant défini une relation symétrique, on déduit que, si A et B sont indépendants, alors $\overline{A}$ et B également, de même que $\overline{A}$ et $\overline{B}$.*

Définition III.24. *Des événements $A_1, \ldots, A_n$ sont dits* ***(mutuellement) indépendants*** *si :*

$$\forall I \subset [\![1; n]\!],\ \mathbb{P}\left(\cap_{i \in I} A_i\right) = \prod_{i \in I} \mathbb{P}(A_i).$$

Remarque III.25. *Des événements mutuellement indépendants sont deux-à-deux indépendants, dans le sens où, avec les notations précédentes :*

$$\forall i, j \in [\![1; n]\!],\ i \neq j,\ \mathbb{P}(A_i \cap A_j) = \mathbb{P}(A_i)\mathbb{P}(A_j).$$

En revanche, la réciproque est fausse. Par exemple, on si on considère le lancer d'un dé rouge et d'un dé bleu équilibrés à 6 faces (chacun), on peut considérer les événements suivants :

$$A = \text{“le montant du dé bleu est pair”},\ B = \text{“le montant du dé rouge est pair”},$$

$$C = \text{“la somme des montants des dés est paire”}.$$

On a en effet par des méthodes de dénombrements que :

$$\mathbb{P}(A) = \frac{3 \times 6}{6 \times 6} = \frac{1}{2},\ \mathbb{P}(B) = \frac{6 \times 3}{6 \times 6} = \frac{1}{2},\ \mathbb{P}(C) = \frac{3 \times 3 + 3 \times 3}{6 \times 6} = \frac{1}{2}$$

et en notant que $A \cap B = A \cap C = B \cap C =$“les deux montants sont pairs”, on trouve :

$$\mathbb{P}(A \cap B) = \mathbb{P}(A \cap C) = \mathbb{P}(B \cap C) = \frac{1}{4}$$

ce qui donne bien que les événements A, B, C sont deux-à-deux indépendants.
Ils ne sont en revanche pas mutuellement indépendant comme on a $A \cap B \cap = A \cap B = A \cap C = B \cap C$, et ainsi :

$$\mathbb{P}(A \cap B \cap C) = \frac{1}{4} \neq \frac{1}{8} = \mathbb{P}(A)\mathbb{P}(B)\mathbb{P}(C).$$

Proposition III.26. *Si $A_1, \dots, A_n$ sont des événements mutuellement indépendants, et que l'on se donne pour tout $i \in [\![1; n]\!]$ un événement $B_i \in \{A_i, \overline{A_i}\}$, alors les événements $B_1, \dots, B_n$ sont mutuellement indépendants.*

Démonstration. On montre facilement que $\overline{A_1}, A_2, \dots, A_n$ sont mutuellement indépendants, ce qui se fait comme pour deux événements , en distinguant selon que $1 \in I$ ou non, suivant les notations de la définition. Le cas général se déduit par symétrie des rôles des A_i, en itérant. □

Chapitre 27

Espaces préhilbertiens

On ne considère ici que des $\mathbb{R}$-espaces vectoriels.

I Produits scalaires, espaces préhilbertiens, espaces euclidiens

I.1 Produits scalaires

Définition I.1. *Si E est un $\mathbb{R}$-espace vectoriel, une forme bilinéaire φ sur E est dite* ***symétrique*** *si :*

$$\forall x, y \in E,\ \varphi(x,y) = \varphi(y,x).$$

Exemples I.2.

1. *Le produit usuel sur $\mathbb{R}$ est bilinéaire symétrique.*
2. *Le produit scalaire usuel sur $\mathbb{R}^2$ est bilinéaire symétrique comme :*

$$\forall x_1, x_2, y_{1,2} \in \mathbb{R},\ (x_1,x_2)\cdot(y_1,y_2) = x_1y_1 + x_2y_2 = (y_1,y_2)\cdot(x_1,x_2)$$

   et on aurait pareil avec le produit scalaire sur $\mathbb{R}^3$.
3. *Plus généralement, pour tout $n \in \mathbb{N}^*$, la forme bilinéaire définie sur $\mathbb{R}^n$ par :*

$$\forall x_1,\dots,x_n,y_1,\dots,y_n \in \mathbb{R},\ \varphi\left((x_1,\dots,x_n),(y_1,\dots,y_n)\right) = \sum_{i=1}^{n} x_iy_i$$

   est symétrique.
4. *Si E est de dimension 2 et $\mathcal{B} = (e_1,e_2)$ est une base de E, alors $\det_{\mathcal{B}}$ est une forme bilinéaire sur E, mais n'est pas symétrique comme $\det_{\mathcal{B}}(e_1,e_2) = 1 \neq -1 = \det_{\mathcal{B}}(e_2,e_1)$.*
   En revanche, l'application :

$$\left\{\begin{array}{rcl} (\mathbb{R}^2)^2 & \to & \mathbb{R} \\ ((x_1,x_2),(y_1,y_2)) & \mapsto & x_1y_2 + x_2y_1 \end{array}\right.$$

   est bien symétrique.
5. *Si $E = \mathcal{C}_{pm}([a,b],\mathbb{R})$, alors l'application :*

$$\varphi : (f,g) \mapsto \int_a^b f(t)g(t)\mathrm{d}t$$

   est bilinéaire symétrique :

— *si $f_1, f_2 \in E$ et $\lambda, \mu \in \mathbb{R}$, alors :*

$$\varphi(\lambda f_1 + \mu f_2, g) = \int_a^b (\lambda f_1(t) + \mu f_2(t))\, g(t)\mathrm{d}t = \int_a^b (\lambda f_1(t)g(t) + \mu f_2(t)g(t))\, \mathrm{d}t$$

$$= \lambda \int_a^b f_1(t)g(t)\mathrm{d}t + \mu \int_a^b f_2(t)g(t)\mathrm{d}t = \lambda\varphi(f_1, g) + \mu\varphi(f_2, g)$$

ce qui prouve la linéarité à gauche ;

— *la linéarité à droite se montre de même, à l'aide de la bilinéarité du produit usuel sur $\mathbb{R}$ et de la linéarité de l'intégrale ;*

— *la symétrie découle directement de la symétrie du produit sur $\mathbb{R}$, comme :*

$$\forall f, g \in E,\ \varphi(f, g) = \int_a^b f(t)g(t)\mathrm{d}t = \int_a^b g(t)f(t)\mathrm{d}t = \varphi(g, f).$$

Remarque I.3. *L'aspect symétrique permet de montrer plus facilement la bilinéarité : une application de E^2 sur $\mathbb{R}$ symétrique est bilinéaire si, et seulement si, elle est linéaire à gauche ou à droite.*

Proposition I.4 (Identités remarquables)**.** *Si φ est une forme bilinéaire symétrique sur E, alors pour tous $x, y \in E$ on a :*

1. $\varphi(x + y, x + y) = \varphi(x, x) + 2\varphi(x, y) + \varphi(y, y)$;
2. $\varphi(x - y, x - y) = \varphi(x, x) - 2\varphi(x, y) + \varphi(y, y)$;
3. $\varphi(x + y, x - y) = \varphi(x - y, x + y)\varphi(x, x) - \varphi(y, y)$.

Démonstration.
Découle à chaque fois de la bilinéarité et de la symétrie. Plus précisément, si $x, y \in E$, alors :

$$\begin{array}{rcl} \varphi(x + y, x + y) & = & \varphi(x, x + y) + \varphi(y, x + y) \\ & = & \varphi(x, x) + \varphi(x, y) + \varphi(y, x) + \varphi(y, y)\ . \\ & = & \varphi(x, x) + 2\varphi(x, y) + \varphi(y, y) \end{array}$$

On déduit alors le deuxième point par linéarité, en changeant y en $-y$:

$$\varphi(x - y, x - y) \ = \ \varphi(x + (-y), x + (-y)) = \varphi(x, x) + 2\varphi(x, -y) + \varphi(-y, -y) = \varphi(x, x) - 2\varphi(x, y) + \varphi(y, y)$$

Et le troisième point se montre comme le premier :

$$\begin{array}{rcl} \varphi(x + y, x - y) & = & \varphi(x, x - y) + \varphi(y, x - y) \\ & = & \varphi(x, x) - \varphi(x, y) + \varphi(y, x) + \varphi(y, y)\ . \\ & = & \varphi(x, x) - \varphi(y, y) \end{array}$$

□

Remarque I.5. *Ce sont les mêmes formules que sur $\mathbb{R}$ (pour le produit usuel).*

Définition I.6 (Produit scalaire)**.** *Une forme bilinéaire symétrique φ sur E est un* ***produit scalaire*** *si elle est :*

1. ***définie*** *:*
$$\forall x \in E,\ \varphi(x, x) = 0 \Leftrightarrow x = 0;$$
2. ***positive*** *:*
$$\forall x \in E,\ \varphi(x, x) \geq 0.$$

Remarque I.7. *En général, si φ défini un produit scalaire sur E, on notera $\langle x, y\rangle$ ou $(x|y)$ au lieu de $\varphi(x, y)$. Et on pourra noter $\langle\cdot,\cdot\rangle$ ou $(\cdot|\cdot)$ pour désigner φ.*

Proposition-Définition I.8.

1. *Pour $n \in \mathbb{N}^*$, l'application : $(X, Y) \mapsto X^T \cdot Y$ définit un produit scalaire sur $\mathbb{R}^n$.*
2. *Pour $n, p \in \mathbb{N}^*$, l'application $(A, B) \mapsto \mathrm{tr}(A^T \cdot B)$ définit un produit scalaire sur $\mathcal{M}_{n,p}(\mathbb{R})$.*

Ces produits scalaires sont appelés ***produits scalaires canoniques*** *de $\mathbb{R}^n$ et $\mathcal{M}_{n,p}(\mathbb{R})$.*

Démonstration.
Si $X = (x_i), Y = (y_j) \in \mathbb{R}^n$, alors :

$$X^T \cdot Y = \sum_{i=1}^{n} x_i y_i$$

dont on a déjà dit qu'elle est bilinéaire symétrique.
On a de plus :

$$X^T \cdot X = \sum_{i=1}^{n} x_i^2 \geq 0$$

ce qui assure la positivité. Et pour le caractère défini :

$$X^T \cdot X = 0 \Leftrightarrow \sum_{i=1}^{n} x_i^2 = 0 \Leftarrow \forall i \in [\![1; n]\!],\ x_i = 0 \Leftrightarrow X = 0.$$

On a donc bien un produit scalaire.
Le cas de $\mathcal{M}_{n,p}(\mathbb{R})$ se montre de même en notant que, si $A = (a_{i,j}), B = (b_{i,j}) \in \mathcal{M}_{n,p}(\mathbb{R})$, on a :

$$\mathrm{tr}(A^T \cdot B) = \sum_{j=1}^{p} \left[A^T B\right]_{j,j} = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} \underbrace{[A^T]_{j,i}}_{=a_{i,j}} b_{i,j} \right) = \sum_{i=1}^{n} \sum_{j=1}^{p} a_{i,j} b_{i,j}$$

et donc :

$$\mathrm{tr}(A^T \cdot A) = \sum_{i=1}^{n} \sum_{j=1}^{p} a_{i,j}^2.$$

□

Remarque I.9. *On pourrait généraliser cette méthode pour créer des produits scalaires sur n'importe quel espace vectoriel de dimension finie : si on considère E de dimension $n \in \mathbb{N}^*$, et $(e_1, \ldots, e_n)$ une base de E, alors l'application :*

$$\varphi : \left\{ \begin{array}{rcl} E \times E & \to & \mathbb{R} \\ (\sum_{i=1}^n x_i e_i, \sum_{i=1}^n y_i e_i) & \mapsto & \sum_{i=1}^n x_i y_i \end{array} \right.$$

définit un produit scalaire sur E.
De plus, en munissant $\mathbb{R}^n$ du produit scalaire canonique, l'application :

$$\psi : \left\{ \begin{array}{rcl} E & \to & \mathbb{R}^n \\ \sum_{i=1}^n x_i e_i & \mapsto & (x_1, \ldots, x_n) \end{array} \right.$$

est un isomorphisme qui préserve le produit scalaire : c'est une ***isométrie****.*

Proposition I.10. *L'application :*

$$(f, g) \mapsto \int_a^b f(t) g(t) \mathrm{d}t$$

définit un produit scalaire sur $\mathcal{C}([a, b], \mathbb{R})$.

Démonstration. Le caractère bilinéaire symétrique a déjà été prouvé.
Si $f \in \mathcal{C}([a,b],\mathbb{R})$, on a :

$$\int_a^b f(t)^2 \mathrm{d}t \geq 0$$

par positivité de l'intégrale, donc on a bien une forme positive.
Et de plus, si $f \in \mathcal{C}([a,b],\mathbb{R})$, alors f^2 est continue positive sur $[a,b]$ et donc :

$$\int_a^b f(t)\mathrm{d}t = 0 \Leftrightarrow f^2 = 0 \Leftrightarrow f = 0$$

donc la forme est bien définie. □

Remarques I.11.

1. *La continuité est importante pour avoir l'aspect défini. Ainsi, la même application est une forme bilinéaire symétrique positive sur $\mathcal{C}_{pm}([a,b],\mathbb{R})$, mais ce n'est plus un produit scalaire.*
2. *Ce n'est pas non plus un produit scalaire sur $\mathcal{C}(\mathbb{R},\mathbb{R})$: la seule propriété que l'on aurait est que : $\langle f,f\rangle = 0 \Leftrightarrow f|_{[a,b]} = 0$.*
   En revanche, c'en est un sur $\mathbb{R}[X]$: la bilinéarité, symétrie, positivité sont claires. Et si $P \in \mathbb{R}[X]$ vérifie $\int_a^b P(t)^2\mathrm{d}t = 0$, alors P est nul sur $[a,b]$, donc nul.

Définition I.12. *Un **espace préhilbertien** est un espace vectoriel muni d'un produit scalaire.*
*Si cet espace est de dimension finie, on parlera d'**espace euclidien**.*

Remarque I.13. *Un même espace peut être muni de différents produits scalaires : il faudra donc préciser celui considéré.*

Exemple I.14. *L'espace $E = \mathbb{R}[X]$ est un espace préhilbertien pour les produits scalaires suivants :*

1. $(P,Q) \mapsto \int_a^b P(t)Q(t)\mathrm{d}t$ *(pour $a < b$) ;*
2. $(\sum a_n X^n, \sum b_n X^n) \mapsto \sum_{n=0}^{+\infty} a_n b_n$ *;*
3. $(P,Q) \mapsto \sum_{i=0}^{+\infty} P^{(i)}(a)Q^{(i)}(a)$ *(pour $a \in \mathbb{R}$).*

Proposition I.15. *Tout sous-espace d'un espace préhilbertien est un espace préhilbertien.*

Démonstration. Si E est muni du produit scalaire φ, alors φ définit également une forme bilinéaire symétrique définie positive sur tout sous-espace vectoriel de E comme toutes les propriétés à vérifier pour φ sont définies à l'aide de quantificateurs universel. □

Remarque I.16. *La réciproque est fausse, dans le sens où : si φ est une forme bilinéaire symétrique sur un espace E, et F est un sev de E pour lequel φ est un produit scalaire, alors φ n'est pas nécessairement un produit scalaire sur E.*

Exemple I.17. *Si $n \in \mathbb{N}$, alors $\mathbb{R}_n[X]$ est espace euclidien, et on peut prendre n'importe quel produit scalaire issu de $\mathbb{R}[X]$.*
Si $x_0,\ldots,x_n$ sont des réels deux-à-deux distincts, alors :

$$(P,Q) \mapsto \sum_{i=0}^{n} P(x_i)Q(x_i)$$

est un produit scalaire sur $\mathbb{R}_n[X]$ (mais pas sur $\mathbb{R}[X]$). On peut le montrer par le calcul, ou reconnaître le produit scalaire associé à la base des polynômes d'interpolation de Lagrange associés à la famille $(x_0,\ldots,x_n)$.

I.2 Norme associée à un produit scalaire

Définition I.18 (Norme et distance associées à un produit scalaire)**.** *On considère E un espace préhilbertien muni du produit scalaire $\langle\cdot,\cdot\rangle$. On appelle* ***norme associée à*** *$\langle\cdot,\cdot\rangle$ l'application :*

$$\|\cdot\| : \left\{ \begin{array}{ccc} E & \to & \mathbb{R}_+ \\ x & \mapsto & \|x\| = \sqrt{\langle x, x\rangle} \end{array} \right. .$$

La ***distance associée à*** *$\langle\cdot,\cdot\rangle$ est l'application :*

$$d : \left\{ \begin{array}{ccc} E\times E & \to & \mathbb{R}_+ \\ (x,y) & \mapsto & d(x,y) = \|x-y\| = \sqrt{\langle x-y, x-y\rangle} \end{array} \right. .$$

Exemple I.19. *Sur $\mathbb{R}^n$, la norme et la distance associées au produit scalaire canonique sont données par :*

$$\|(x_1,\dots,x_n)\| = \sqrt{\sum_{i=1}^n x_i^2} \text{ et } d\left((x_1,\dots,x_n),(y_1,\dots,y_n)\right) = \sqrt{\sum_{i=1}^n (x_i-y_i)^2}.$$

Et on retrouve les formules usuelles pour $n=2$ ou $n=3$.

Théorème I.20 (Inégalité de Cauchy–Schwarz)**.** *Si E est un espace préhilbertien muni du produit scalaire $\langle\cdot,\cdot\rangle$, alors :*

$$\forall x, y \in E,\ |\langle x, y\rangle| \leq \|x\| \cdot \|y\|$$

avec égalité si, et seulement si, les vecteurs x et y sont colinéaires.

Démonstration. Soient $x, y \in E$.
Si $y = 0$, alors l'inégalité est vérifiée : c'est même une égalité, et on a bien la condition d'égalité (comme le vecteur nul est colinéaire à tout vecteur).
Sinon, considérons l'application définie sur $\mathbb{R}$ par :

$$\forall t \in \mathbb{R},\ f(t) = \|x+ty\|^2 = \langle x+ty, x+ty\rangle.$$

Alors pour tout $t \in \mathbb{R}$, on a par bilinéarité et symétrie du produit scalaire :

$$f(t) = \langle x, x\rangle + 2t\langle x, y\rangle + t^2\langle y, y\rangle$$

donc f est une fonction polynomiale du second degré, comme $\langle y, y\rangle \neq 0$ (puisque $y \neq 0$).
De plus, pour tout $t \in \mathbb{R}$, on a : $f(t) \geq 0$ (par positivité du produit scalaire). Donc f est de signe constant.
Et donc le discriminant de f est négatif ou nul, c'est-à-dire :

$$\Delta = (2\langle x, y\rangle)^2 - 4\langle x, x\rangle \cdot \langle y, y\rangle = 4\left((\langle x, y\rangle)^2 - (\|x\| \cdot \|y\|)^2\right) \leq 0.$$

En passant à la racine carrée, on trouve bien que : $|\langle x, y\rangle| \leq \|x\| \cdot \|y\|$.
En cas d'égalité, on déduit que f a un discriminant nul, donc s'annule en un réel t. On a alors pour ce même t : $\langle x+ty, x+ty\rangle = 0$. Et comme le produit scalaire est défini, on a donc $x = -ty$, donc x et y sont bien colinéaires.
Réciproquement, si x et y sont colinéaires : comme $y \neq 0$, il existe $\lambda \in \mathbb{R}$ tel que $x = \lambda y$, et alors $f(-\lambda) = 0$.
D'où l'équivalence cherchée. □

Remarques I.21.

1. *On retrouve une situation déjà connue pour le produit scalaire sur $\mathbb{R}^2$:*

$$|\overrightarrow{u} \cdot \overrightarrow{v}| \leq \|\overrightarrow{u}\| \cdot \|\overrightarrow{v}\|.$$

2. *Le caractère défini est seulement indispensable pour montrer la situation d'égalité. Si on a seulement une forme bilinéaire symétrique positive φ, on trouve tout de même que :*

$$\forall x, y \in E,\ |\varphi(x,y)| \leq \sqrt{\varphi(x,x)} \cdot \sqrt{\varphi(y,y)}$$

en étudiant séparément selon que $\varphi(y,y) = 0$ ou $\varphi(y,y) \neq 0$. Et la situation d'égalité peut s'analyser en déterminant l'ensemble $\{x \in E \,|\, \varphi(x,x) = 0\}$.

Exemples I.22.

1. *Pour tous $x_1, \ldots, x_n, y_1, \ldots, y_n \in \mathbb{R}$, on a :*

$$\left|\sum_{i=1}^{n} x_i y_i\right| \leq \sqrt{\sum_{i=1}^{n} x_i^2}\sqrt{\sum_{i=1}^{n} y_i^2}$$

avec égalité si, et seulement si, les vecteurs $(x_1, \ldots, x_n) =$ et $(y_1, \ldots, y_n)$ sont colinéaires.
On retrouve l'inégalité entre moyennes arithmétique et quadratique :

$$\left|\frac{\sum_{i=1}^n x_i}{n}\right| = |\langle (x_1, \ldots, x_n), (1/n, \ldots, 1/n)\rangle| \leq \|(x_1, \ldots, x_n)\| \cdot \|(1/n, \ldots, 1/n)\| = \sqrt{\frac{\sum_{i=1}^n x_i^2}{n}}$$

avec égalité si, et seulement si, $x_1 = \cdots = x_n$.

2. *Si f, g sont deux fonctions continues sur $[a,b]$, alors :*

$$\left|\int_a^b f(t)g(t)\mathrm{d}t\right| \leq \sqrt{\int_a^b f(t)^2\mathrm{d}t}\sqrt{\int_a^b g(t)^2\mathrm{d}t}$$

avec égalité si, et seulement si, f est proportionnelle à g.
L'inégalité reste valable si f, g sont seulement continues par morceaux, mais on perd alors la condition d'égalité. Plus précisément, pour $f, g \in \mathcal{C}_{pm}([a,b], \mathbb{R})$, on aura égalité si, et seulement si, f est proportionnelle à g sauf éventuellement en un nombre fini de points.

Proposition I.23. *Si E est un espace préhilbertien, et $\|\cdot\|$ est la norme associée au produit scalaire sur E, alors pour tous $x, y \in E$ et $\lambda \in \mathbb{R}$ on a :*

1. $\|\lambda x\| = |\lambda| \cdot \|x\|$ *(positive homogénéité de degré 1, ou juste homogénéité) ;*
2. $\|x\| = 0 \Leftrightarrow x = 0$ *(séparation) ;*
3. $\|x + y\| \leq \|x\| + \|y\|$ *(inégalité triangulaire).*

De plus, dans l'inégalité triangulaire, il y a égalité si, et seulement si, x et y sont ***positivement colinéaires*** *(ou colinéaires de même sens), c'est-à-dire qu'il existe $\mu \in \mathbb{R}_+$ tel que $x = \mu y$ ou $y = \mu x$.*

Démonstration.

1. Par définition de la norme, on a :

$$\|\lambda x\| = \sqrt{\langle \lambda x, \lambda x\rangle} = \sqrt{\lambda^2\langle x, x\rangle} = |\lambda| \cdot \sqrt{\langle x, x\rangle} = |\lambda| \cdot \|x\|.$$

2. On a déjà par bilinéarité (ou le point précédent) que $\|0\| = 0$.
Réciproquement, si $\|x\| = 0$, alors $\langle x, x\rangle = \|x\|^2 = 0$ donc $x = 0$ (comme le produit scalaire est défini).

3. Pour $x, y \in E$, on a par inégalité de Cauchy–Schwarz :

$$\begin{array}{rcl} \|x+y\|^2 & = & \langle x+y, x+y\rangle = \langle x,x\rangle + 2\langle x,y\rangle + \langle y,y\rangle \\ & \leq & \|x\|^2 + 2\|x\|\cdot\|y\| + \|y\|^2 \\ & \leq & (\|x\| + \|y\|)^2 \end{array}$$

ce qui donne l'inégalité en passant à la racine carrée.
De plus, il y a égalité si, et seulement si, $\langle x, y\rangle = \|x\| \cdot \|y\|$.
Pour avoir une telle égalité, on doit donc déjà avoir égalité dans l'inégalité de Cauchy–Schwarz, donc x et y sont colinéaires. Le cas où $y = 0$ est immédiat (on a bien égalité, et x, y sont bien colinéaires de même sens). Sinon, on peut écrire $x = \lambda y$ pour $\lambda \in \mathbb{R}$, et on a alors :

$$\langle x, y\rangle = \lambda\langle x, x\rangle = \lambda\|x\|^2 \text{ et } \|x\| \cdot \|y\| = |\lambda| \cdot \|x\|^2$$

et ainsi on a l'égalité si, et seulement si, $\lambda \geq 0$

□

Remarques I.24.

1. *On retrouve les trois propriétés qu'on avait démontrées pour la norme $\|\cdot\|_\infty$ sur les fonctions continues par morceaux : ce sont en fait les trois propriétés qui justifient l'appellation de* ***norme****.*
2. *Pour l'inégalité triangulaire, on a même :*

$$|\|x\| - \|y\|| \leq \|x+y\| \leq \|x\| + \|y\|$$

avec égalité à droite (resp. à gauche) si, et seulement si, x et y sont colinéaire de même sens (resp. de sens opposés).

Corollaire I.25. *Avec les mêmes notations, si d est la distance associée au produit scalaire sur E, alors pour tous $x, y, z \in E$ on a :*

1. $d(x, y) = d(y, x)$;
2. $d(x, y) = 0 \Leftrightarrow x = y$;
3. $d(x, z) \leq d(x, y) + d(y, z)$.

Démonstration. Découle respectivement de la symétrie du produit scalaire, de son caractère défini, et de l'inégalité triangulaire pour la norme. □

Proposition I.26 (Identités remarquables)**.** *Si E est un espace préhilbertien muni d'un produit scalaire $\langle\cdot,\cdot\rangle$ et de norme associée $\|\cdot\|$, alors pour tous $x, y \in E$ on a :*

1. $\|x+y\|^2 = \|x\|^2 + 2\langle x, y\rangle + \|y\|^2$;
2. $\|x-y\|^2 = \|x\|^2 - 2\langle x, y\rangle + \|y\|^2$;
3. $\langle x+y, x-y\rangle = \|x\|^2 - \|y\|^2$.

Démonstration. Découle des identités remarquables avec les formes bilinéaires symétriques. □

Corollaire I.27 (Identités de polarisation)**.** *Avec les mêmes notations, on a :*

$$\langle x, y\rangle = \frac{1}{2}\left(\|x+y\|^2 - \|x\|^2 - \|y\|^2\right) \frac{1}{2}\left\|x\|^2 + \|y\|^2 - \|x-y\|^2\right) = \frac{1}{4}\left(\|x+y\|^2 - \|x-y\|^2\right).$$

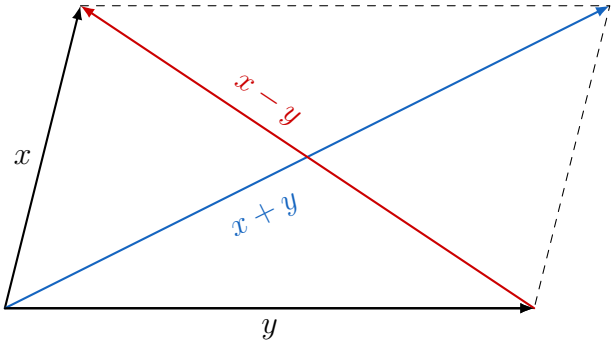
Démonstration. Découle directement des identités remarquables. □

Corollaire I.28 (Identité du parallélogramme)**.** *Avec les mêmes notations, on a :*

$$\|x+y\|^2 + \|x-y\|^2 = 2\left(\|x\|^2 + \|y\|^2\right).$$

Démonstration. On soustrait les deux premières identités de polarisation. □

Remarque I.29. *Le résultat veut dire que la somme des carrés des longueurs des diagonales d'un parallélogramme est égale à la somme des carrés des longueurs de ses côtés :*



Dont tout le monde connaît bien un cas particulier : quand il s'agit d'un rectangle, on retrouve le théorème de Pythagore.

II Vecteurs orthogonaux

II.1 Orthogonalité et orthonormalité

Définition II.1. *Si E est un espace préhilbertien muni d'un produit scalaire $\langle \cdot, \cdot \rangle$, on dit que $x, y \in E$ sont* ***orthogonaux****, ce que l'on note $x \perp y$, si $\langle x, y \rangle = 0$.*

Exemples II.2.

1. *Peu importe l'espace considéré : le vecteur nul est orthogonal à tout vecteur, et c'est le seul vecteur satisfaisant cette propriété.*
   C'est aussi le seul vecteur orthogonal à lui-même (comme un produit scalaire est défini).
2. *Sur $\mathbb{R}^2$ muni du produit scalaire canonique, les vecteurs (a, b) et $(-b, a)$ sont orthogonaux.*

Définition II.3. *Avec les mêmes notations, si X, Y sont deux parties de E, on dira que X et Y sont* ***orthogonales****, ce que l'on note $X \perp Y$, si tout vecteur de X est orthogonal à tout vecteur de Y :*

$$\forall (x, y) \in X \times Y,\ x \perp y.$$

Définition II.4. *Avec les mêmes notations, une famille $(x_i)_{i \in I}$ d'éléments de E est dite* ***orthogonale*** *si tous ses éléments sont deux-à-deux orthogonaux : $\forall i, j \in I,\ i \neq j \Rightarrow x_i \perp x_j$.*
Elle sera dite de plus ***orthonormale*** *(ou* ***orthonormée****) si tous ses vecteurs sont* ***unitaires*** *(c'est-à-dire de norme 1), c'est-à-dire si :*

$$\forall i, j \in I,\ \langle x_i, x_j \rangle = \delta_{i,j}.$$

Exemples II.5.

1. *Pour le produit scalaire canonique, les bases canoniques de $\mathbb{R}^n$ ou de $\mathcal{M}_{n,p}(\mathbb{R})$ sont orthonormées.*
2. *Plus généralement, si $\mathcal{B} = (e_1, \dots, e_n)$ est une base de E, elle est orthonormée pour le produit scalaire :*

$$\left\langle \sum_{i=1}^{n} x_i e_i, \sum_{i=1}^{n} y_i e_i \right\rangle = \sum_{i=1}^{n} x_i y_i.$$

   Par exemple, si $x_0, \dots, x_n$ sont des réels deux-à-deux distincts, la famille des polynômes d'interpolation de Lagrange associés forme une famille orthonormale pour le produit scalaire défini sur $\mathbb{R}_n[X]$ par : $\langle P, Q \rangle = \sum_{i=0}^{n} P(x_i) Q(x_i)$.

3. *Sur $\mathcal{C}([0,2\pi],\mathbb{R})$, la famille $(f_k)_{k\in\mathbb{N}}$ définit par $f_k : x \mapsto \cos(kx)$ est une famille orthogonale pour le produit scalaire : $\langle f,g\rangle = \int_0^{2\pi} f(t)\mathrm{g}(t)\mathrm{d}t$.*
On a pour $k,l \in \mathbb{N}$ avec $k \neq l$, on a :

$$\begin{aligned}\langle f_k, f_l\rangle &= \int_0^{2\pi} f_k(t)f_l(t)\mathrm{d}t = \int_0^{2\pi}\cos(kt)\cos(lt)\mathrm{d}t\\ &= \frac{1}{2}\int_0^{2\pi}\cos((k+l)t)\mathrm{d}t + \frac{1}{2}\int_0^{2\pi}\cos((k-l)t)\mathrm{d}t\\ &= \frac{1}{2}\left[\frac{1}{k+l}\sin((k+l)t)\right]_0^{2\pi} + \frac{1}{2}\left[\frac{1}{k+l}\sin((k-l)t)\right]_0^{2\pi}\\ &= 0\end{aligned}$$

ce qui donne bien le caractère orthogonal.
En revanche, elle n'est pas orthonormée. Pour tout $k \in \mathbb{N}$, on a :

$$\langle f_k f_k\rangle = \int_0^{2\pi}\cos^2(kt)\mathrm{d}t = \int_0^{2\pi}\frac{\cos(2kt)+1}{2}\mathrm{d}t = \begin{cases} 2\pi & si \quad k=0\\ \pi & si \quad k\neq 0\end{cases}$$

En revanche, la famille $\left(\dfrac{f_k}{\sqrt{(1+\delta_{0,k})\pi}}\right)_{k\in\mathbb{N}}$ *est orthonormée.*

Proposition II.6. *Une famille orthogonale de vecteurs non nuls est libre.*

Démonstration. Considérons $(x_1,\dots,x_n)$ une famille orthogonale de vecteurs non nuls. Soient $\lambda_1,\dots,\lambda_n \in \mathbb{R}$ tels que $\sum_{i=1}^n \lambda_i x_i$. Alors pour tout $j \in [\![1;n]\!]$, on a :

$$0 = \langle 0, x_j\rangle = \left\langle \sum_{i=1}^n \lambda_i x_i, x_j\right\rangle = \sum_{i=1}^n \lambda_i\langle x_i, x_j\rangle = \lambda_j\|x_j\|^2$$

et donc, comme $x_j \neq 0$, alors $\|x_j\| \neq 0$ donc $\lambda_j = 0$.
Et donc la famille est libre. □

Remarque II.7. *On retrouve notamment un résultat vu pendant l'année, à savoir que la famille $(x \mapsto \cos(kx))_{k\in\mathbb{N}}$ est une famille libre.*

Corollaire II.8. *Toute famille orthonormée est libre.*

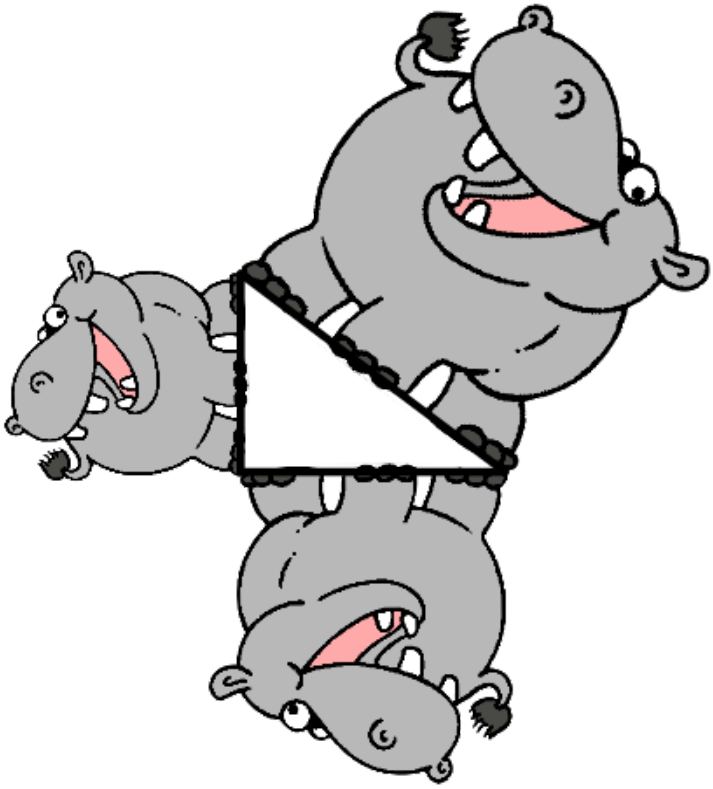
Théorème II.9 (de Pythagore)**.** *Si E est un espace préhilbertien et $x,y \in E$, alors x et y sont orthogonaux si, et seulement si, $\|x+y\|^2 = \|x\|^2 + \|y\|^2$.*

Démonstration. On a par identité remarquable :

$$\|x+y\|^2 = \|x\|^2 + \|y\|^2 + 2\langle x,y\rangle$$

ce qui donne bien que $\|x+y\|^2 = \|x\|^2 + \|y\|^2$ si, et seulement si, $\langle x,y\rangle = 0$, c'est-à-dire que x et y sont orthogonaux. □

Remarque II.10. *Les formulations autour des triangles rectangles, et les similarités entre les mots "hypoténuse" et "hippopotame" ont entraîner de nombreuses déformations de ce théorème. De nombreuses blagues à la qualité discutable autour de théorème autour d'hippopotames par exemple. Ou sinon le fait que le fait d'accoler la même figure aux côtés d'un triangle rectangle, en la dilatant suivant un rapport correspondant à la longueur du côté, donne que l'aire de la figure adjacente à l'hypoténuse est égale à la somme des aires des deux autres. Et c'est même valable lorsque les figures représentent des hippopotames :*



Corollaire II.11. *Si $(x_1, \dots, x_n)$ est une famille orthogonale, on a :*

$$\left\| \sum_{i=1}^{n} \right\|^2 = \sum_{i=1}^{n} \|x_i\|^2$$

Démonstration. Par récurrence. □

Remarque II.12. *On pouvait aussi procéder par calcul direct, par propriétés d'une forme bilinéaire symétrique. Plus généralement, on obtient pour tout famille :*

$$\left\| \sum_{i=1}^{n} x_i \right\|^2 = \sum_{i=1}^{n} \sum_{j=1}^{n} \langle x_i, x_j \rangle = \sum_{i=1}^{n} \|x_i\|^2 + \sum_{i \neq j} \langle x_i, x_j \rangle$$

ce qui permet de voir au passage que l'on n'a plus l'équivalence lorsque l'on considère plus de deux vecteurs.

II.2 Le processus d'orthonormalisation de Gram–Schmidt

Théorème II.13 (Orthonormalisation de Gram–Schmidt)**.** *Si E est un espace préhilbertien, et $(e_1, \dots, e_n)$ est une famille libre d'éléments de E, alors il existe une famille orthonormée $(x_1, \dots, x_n)$ de E telle que :*

$$\forall k \in [\![1; n]\!],\ \mathrm{Vect}(e_1, \dots, e_k) = \mathrm{Vec}(x_1, \dots, x_k).$$

Plus précisément, on peut construire les x_k récursivement : si on a déjà construit les vecteurs $x_1, \dots, x_{k-1}$, alors on peut poser $x_k = \dfrac{x_k^*}{\|x_k^*\|}$, où :

$$x_k^* = e_k - \sum_{i=1}^{k-1} \langle e_k, x_i \rangle x_i.$$

Démonstration. On considère la famille (x_k) construite comme dans l'énoncé du théorème. On va montrer par récurrence sur $k \in [\![1;n]\!]$ que la famille $(x_1,\dots,x_k)$ est orthonormée, et vérifie $\text{Vect}(e_1,\dots,e_k) = \text{Vect}(x_1,\dots,x_k)$.
Si $k=1$: comme la famille $(e_1,\dots,e_n)$ est libre, alors $e_1 \neq 0$, et ainsi $x_1 = \dfrac{e_1}{\|e_1\|}$ est un vecteur unitaire : la famille (x_1) est orthonormée, et engendre bien $\text{Vect}(e_1)$.
Supposons que $(x_1,\dots,x_k)$ soit orthonormée avec $\text{Vect}(x_1,\dots,x_k) = \text{Vect}(e_1,\dots,e_k)$. Alors pour tout $j \in [\![1;k]\!]$ on a :

$$\begin{aligned}
\langle x_{k+1}^*, x_j\rangle &= \left\langle e_{k+1} - \textstyle\sum_{i=1}^k \langle e_{k+1}, x_i\rangle x_i, x_j \right\rangle \\
&= \langle e_{k+1}, x_j\rangle - \textstyle\sum_{i=1}^k \langle \langle e_{k+1}, x_i\rangle x_i, x_j\rangle \\
&= \langle e_{k+1}, x_j\rangle - \textstyle\sum_{i=1}^k \langle e_{k+1}, x_i\rangle \underbrace{\langle x_i, x_j\rangle}_{=\delta_{i,j}} \\
&= \langle e_{k+1}, x_j\rangle - \langle e_{k+1}, x_j\rangle \\
&= 0
\end{aligned}$$

ce qui montre déjà que la famille $(x_1,\dots,x_k,x_{k+1}^*)$ est orthogonale.
De plus, on a que x_{k+1}^* est non nul, car sinon on aurait :

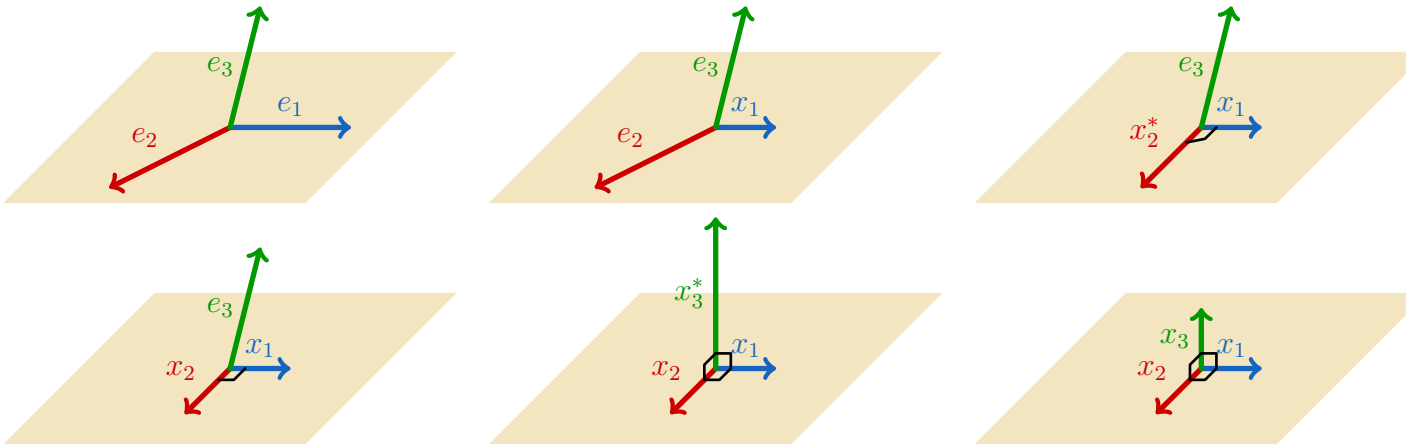
$$e_{k+1} = \sum_{i=1}^k \langle e_{k+1}, x_i\rangle x_i \in \text{Vect}(x_1,\dots,x_k) = \text{Vect}(e_1,\dots,e_k)$$

ce qui contredirait la liberté de la famille $(e_1,\dots,e_{k+1})$.
Et donc $x_{k+1} = \dfrac{x_{k+1}^*}{\|x_{k+1}^*\|}$ est bien défini. Et la famille $(x_1,\dots,x_{k+1})$ est donc une famille orthogonale dont tous les vecteurs sont unitaires : c'est une famille orthonormée.
Par hypothèse de récurrence, on a : $x_1,\dots,x_k \in \text{Vect}(e_1,\dots,e_k)$. Par construction, on a $x_{k+1} \in \text{Vect}(x_1,\dots,x_k,e_k$ $\text{Vect}(e_1,\dots,e_{k+1})$. Mais la famille $(e_1,\dots,e_{k+1})$ est libre (sous-famille d'une famille libre), donc c'est une base de $\text{Vect}(e_1,\dots,e_{k+1})$, qui est donc de dimension $k+1$.
Et comme la famille $(x_1,\dots,x_{k+1})$ est libre (car orthonormée), c'est donc une base de $\text{Vect}(e_1,\dots,e_{k+1})$, ce qui prouve bien par son côté générateur que $\text{Vect}(e_1,\dots,e_{k+1}) = \text{Vect}(x_1,\dots,x_{k+1})$. □

Remarques II.14.

1. *La récursivité de la construction se comprend bien avec $n=2$:*
   - *on transforme e_1 en le divisant par sa norme pour le rendre unitaire ;*
   - *on transforme e_2 en lui retirant $\langle e_2, x_1\rangle x_1$ pour le rendre orthogonal à e_1, qu'on renormalise pour le rendre unitaire également.*

   Et on verra le sens plus général qui se cache derrière.



2. *Il existe des énoncés légèrement différents qui permettent d'assurer l'unicité de la base $(x_1, \dots, x_n)$. Il suffit par exemple d'imposer que pour tout $k \in [\![1; n]\!]$, $\langle e_k x_k \rangle > 0$ et on a alors l'unicité d'une telle base (celle donnée par la construction du théorème). On peut notamment observer que, si (e_i) est orthonormée, alors la famille (x_i) rendue par l'algorithme de Gram–Schmidt est égale à la famille (e_i).*

Exemple II.15. *On considère $\mathbb{R}[X]$ muni du produit scalaire : $\langle P, Q \rangle = \int_0^1 P(t)Q(t)\mathrm{d}t$. Appliquons l'algorithme de Gram–Schmidt à la famille $(P_0 = 1, P_1 = X, P_2 = X^2)$ (qui est bien libre) pour construire une famille orthonormée (Q_0, Q_1, Q_2) :*

— *On a directement : $\|P_0\|^2 = \int_0^1 1\mathrm{d}t = 1$, donc $Q_0 = \dfrac{P_0}{\|P_0\|} = \dfrac{P_0}{1} = 1$.*

— *Pour Q_1, on a déjà :*

$$Q_1^* = P_1 - \langle X, Q_0 \rangle Q_0 = X - \left(\int_0^1 t \cdot 1\mathrm{d}t \right) \cdot 1 = X - \frac{1}{2}$$

et donc :

$$\|Q_1^*\|^2 = \int_0^1 \left(t - \frac{1}{2} \right)^2 \mathrm{d}t = \frac{1}{12}$$

donc finalement :

$$Q_1 = \frac{Q_1^*}{\|Q_1^*\|} = \sqrt{12} \left(X - \frac{1}{2} \right) = \sqrt{3}\,(2X - 1)$$

— *Pour Q_2, on a déjà :*

$$\begin{aligned} Q_2^* &= P_2 - \langle P_2, Q_0 \rangle Q_0 - \langle P_2, Q_1 \rangle Q_1 \\ &= X^2 - \left(\int_0^1 t^2 \mathrm{d}t \right) \cdot 1 - \sqrt{3} \left(\int_0^1 t^2 (2t - 1)\mathrm{d}t \right) \cdot \sqrt{3}(2X - 1) \\ &= X^2 - \frac{1}{3} - \frac{1}{2}\,(2X - 1) = X^2 - X + \frac{1}{6} \end{aligned}$$

et donc :

$$\|Q_2^*\|^2 = \int_0^1 \left(t^2 - t + \frac{1}{6} \right)^2 \mathrm{d}t = \frac{1}{180}$$

donc finalement :

$$Q_2 = \frac{Q_2^*}{\|Q_2^*\|} = \sqrt{180} \left(X^2 - X + \frac{1}{6} \right) = \sqrt{5}\left(6X^2 - 6X + 1 \right).$$

Et finalement, la famille $\left(1, \sqrt{3}(2X - 1), \sqrt{5}(6X^2 - 6X + 1)\right)$ est une famille orthonormale pour ce produit scalaire sur $\mathbb{R}[X]$.

Remarque II.16. *Le théorème de Pythagore permet de gagner un peu de temps dans les calculs. On a en effet, que les x_i sont orthogonaux, et donc pour tout k la famille $(x_1, \dots, x_{k+1}, x_k^*)$ est orthogonale, et donc :*

$$\|e_k\|^2 = \left\| x_k^* + \sum_{i=1}^{k-1} \langle e_k, x_i \rangle x_i \right\|^2 = \|x_k^*\|^2 + \sum_{i=1}^{k-1} \langle e_k, x_i \rangle^2 \underbrace{\|x_i\|^2}_{=1}$$

et donc :

$$\|x_k\|^2 = \|e_k\|^2 - \sum_{i=1}^{k-1} \langle e_k, x_i \rangle^2$$

Par exemple, dans le calcul précédent, on pouvait calculer $\|Q_2^*\|$ un peu plus rapidement, en utilisant que :

$$\|Q_2^*\|^2 = \|P_2\|^2 - \langle P_2, Q_1 \rangle^2 - \langle P_2, Q_0 \rangle^2 = \frac{1}{5} - \frac{1}{9} - \frac{1}{12} = \frac{1}{180}.$$

II.3 Bases orthonormées

Définition II.17. *Une **base orthonormée** (abrégé en bon) d'un espace préhilbertien E est une famille orthonormée qui est une base de E.*

Exemples II.18.

1. *Les bases canoniques de $\mathbb{R}^n$ ou $\mathcal{M}_{n,p}(\mathbb{R})$ sont des bon pour les produits scalaires canoniques.*
2. *Plus généralement, n'importe quelle base est une base orthonormée pour le produit scalaire qu'on lui avait associé.*
3. *Dans $\mathbb{R}_2[X]$ muni du produit scalaire $\langle P, Q\rangle = \int_0^1 P(t)Q(t)\mathrm{d}t$, la famille $\big(1, \sqrt{3}(2X-1), \sqrt{5}(6X^2-6X+$ est une base orthonormée.*
4. *Pour un espace de dimension 1, les bases orthonormées sont exactement les familles à un vecteur unitaire.*

Théorème II.19.

1. *Tout espace euclidien possède une base orthonormée.*
2. *Dans un espace euclidien, toute famille orthonormée peut être complétée en une base orthonormée.*

Démonstration.

1. Tout espace de dimension finie admet une base, donc un espace euclidien admet toujours une base. L'algorithme de Gram–Schmidt appliqué à cette base donne une base orthonormée.
2. Tout famille orthonormée est libre, donc par théorème de la base incomplète peut être complétée en une base. Lui appliquer l'algorithme de Gram–Schmidt permettra d'avoir une base orthonormée, et ne changera pas les premiers vecteurs, donc permet de compléter la base initiale en une base orthonormée.

□

Remarques II.20.

1. *Le second résultat s'appelle le théorème de la base orthonormale incomplète.*
2. *L'algorithme de Gram–Schmidt ne fait rien si la famille est déjà orthonormée. Si elle est seulement orthogonale, l'algorithme divise chaque vecteur par sa norme.*

Proposition II.21. *Si E est un espace euclidien, et $(e_1, \dots, e_n)$ est une bon de E, alors pour tout $x \in E$ on a :*

$$x = \sum_{i=1}^{n} \langle x, e_i\rangle e_i$$

c'est-à-dire que les coordonnées de x dans $(e_1, \dots, e_n)$ sont : $(\langle x, e_1\rangle, \dots, \langle x, e_n\rangle)$.

Démonstration. Notons $x = \sum_{i=1}^n x_i e_i$ (c'est-à-dire que $(x_1, \dots, x_n)$ sont les coordonnées de x). Alors pour tout $j \in [\![1; n]\!]$:

$$\langle x, e_j\rangle = \left\langle \sum_{i=1}^{n} x_i e_i, e_j \right\rangle = \sum_{i=1}^{n} x_i \langle e_i, e_j\rangle = \sum_{i=1}^{n} x_i \delta_{i,j} = x_j$$

ce qui donne bien le résultat. □

Proposition II.22. *Soit E un espace euclidien, $\mathcal{B} = (e_1, \dots, e_n)$ une bon de E et $x, y \in E$. On note $X = \mathrm{Mat}_{\mathcal{B}}(x) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ et $Y = \mathrm{Mat}_{\mathcal{B}}(y) = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$. Alors :*

$$\langle x, y\rangle = X^T Y = \sum_{i=1}^{n} x_i y_i \text{ et } \|x\| = \sqrt{X^T X} = \sqrt{\sum_{i=1}^{n} x_i^2}.$$

Démonstration. Avec les mêmes notations, on a directement par bilinéarité :

$$\langle x, y\rangle = \left\langle \sum_{i=1}^{n} x_i e_i, \sum_{j=1}^{n} y_j e_j \right\rangle = \sum_{i,j} x_i y_j \langle e_i, e_j\rangle = \sum_{i,j} x_i y_j \delta_{i,j} = \sum_{i=1}^{n} x_i y_i = X^T Y$$

ce qui donne l'expression pour le produit scalaire.
Et l'expression pour la norme se déduit directement de la définition, comme $\|x\| = \sqrt{\langle x, x\rangle}$. □

Remarques II.23.

1. *La proposition précédente permet d'exprimer facilement les x_i, y_i à l'aide des produits scalaires $\langle x, e_i\rangle, \langle y, e_i\rangle$ et permettent d'adapter les expressions précédentes aux vecteurs et espaces considérés.*
2. *Une autre manière de formuler est que, étant donné un produit scalaire, une base orthonormée revient à choisir une base dont le produit scalaire associé est celui déjà considéré.*

III Espaces orthogonaux

III.1 Supplémentaire orthogonal

Définition III.1 (Orthogonal d'une partie)**.** *Soient E un espace préhilbertien, et X une partie de E. On appelle **orthogonal** de X (dans E) l'ensemble :*

$$X^\perp = \{y \in E \,|\, \forall x \in X,\ x \perp y\}.$$

Exemples III.2.

1. *On a toujours $\emptyset^\perp = E = \{0\}^\perp$ (le vecteur nul est orthogonal à tout vecteur) et $E^\perp = \{0\}$ (et c'est le seul). Comme c'est même le seul vecteur orthogonal à lui-même, on déduit que $X \cap X^\perp = \{0\}$ ou $\emptyset$.*
2. *Dans $\mathbb{R}^3$ muni du produit scalaire canonique, pour tous $a, b, c \in \mathbb{R}$ on a :*

   $$\{(x, y, z) \in \mathbb{R}^3 \,|\, ax + by + cz = 0\} = \{(a, b, c)\}^\perp.$$

   puisqu'on a directement que $\langle (x, y, z), (a, b, c)\rangle = ax + by + cz$.
3. *Si X, Y sont deux parties de E, elles sont orthogonales si, et seulement si, $X \subset Y^\perp$. Par symétrie des rôles, on déduit que $X \subset Y^\perp$ si, et seulement si, $Y \subset X^\perp$, ce qu'on montrera plus tard.*

Proposition III.3. *Si X, Y sont deux parties d'un espace préhilbertien E, alors :*

1. *$X^\perp$ est un sous-espace vectoriel de E ;*
2. *si $X \subset Y$, alors $Y^\perp \subset X^\perp$;*
3. *$X^\perp = (\mathrm{Vect}(X))^\perp$.*

Démonstration.

1. Comme le vecteur nul est orthogonal à tout vecteur, on a : $0 \in X^\perp$.
   Si $y_1, y_2 \in X^\perp$ et $\lambda, \mu \in \mathbb{R}$, alors pour tout $x \in X$ on a :

   $$\langle \lambda y_1 + \mu y_2, x\rangle = \lambda\langle y_1, x\rangle + \mu\langle y_2, x\rangle = 0$$

   donc $\lambda y_1 + \mu y_2 \in X^\perp$.
   C'est donc bien un sous-espace vectoriel de E.

2. Supposons que $X \subset Y$. Soit $z \in Y^\perp$. Alors :
$$\forall y \in Y,\ \langle z, y\rangle = 0$$
puis par inclusion de X dans Y :
$$\forall x \in X,\ \langle z, x\rangle = 0$$
ce qui donne que $z \in X^\perp$, et donc $Y^\perp \subset X^\perp$.
3. On a déjà, comme $X \subset \mathrm{Vect}(X)$, l'inclusion $\mathrm{Vect}(X)^\perp \subset X^\perp$.
Pour l'autre inclusion, considérons $y \in X^\perp$ et $x \in \mathrm{Vect}(X)$. Notons $x = \sum_{i=1}^n \lambda_i x_i$ pour $x_1, \dots, x_n \in X$. Alors par bilinéarité :
$$\langle y, x\rangle = \sum_{i=1}^n \lambda_i \underbrace{\langle y, x_i\rangle}_{=0} = 0$$
et donc on a bien que $y \in \mathrm{Vect}(X)^\perp$.

□

Remarques III.4.

1. *On voit ainsi l'aspect central des espaces vectoriels quand on travaille avec des espaces orthogonaux : déjà l'orthogonal d'une partie (quelconque) est toujours un espace vectoriel ; et ensuite il suffit de regarder les orthogonaux des espaces vectoriels, et pour les étudier il suffit d'étudier l'orthogonalité par rapport aux éléments d'une famille génératrice. Par exemple, si $F = \mathrm{Vect}(e_1, \dots, e_n)$, alors on a l'équivalence :*
$$x \in F^\perp \Leftrightarrow \forall i \in [\![1; n]\!],\ x \perp e_i.$$
2. *Pour montrer que $X^\perp$ est un espace vectoriel, on pouvait aller plus vite en montrant que c'est une intersection d'espaces vectoriels :*
$$X^\perp = \cap_{x\in X} \mathrm{Ker}\,(y \mapsto \langle x, y\rangle)$$
en utilisant la linéarité à droite du produit scalaire.

Exemple III.5. *On considère $\mathbb{R}_2[X]$ muni du produit scalaire $\langle P, Q\rangle = \sum_{k=-1}^1 P(k)Q(k)$. Pour déterminer $\mathbb{R}_1[X]^\perp$, on note que $(1, X)$ est une base de $\mathbb{R}_1[X]$, et si $P = aX^2 + bX + c \in \mathbb{R}_2[X]$ on a :*
— $\langle P, 1\rangle = P(-1)\cdot 1 + P(0)\cdot 1 + P(1)\cdot 1 = (a - b + c) + c + (a + b + c) = 2a + 3c$;
— $\langle P, X\rangle = P(-1)\cdot -1 + P(0)\cdot 0 + P(1)\cdot 1 = -(a - b + c) + 0 + (a + b + c) = 2b$.
Et ainsi on a les équivalences :
$$P \in \mathbb{R}_1[X]^\perp \Leftrightarrow \langle P, 1\rangle = \langle P, X\rangle = 0 \Leftrightarrow 2a + 3c = 0 = 2b$$
ce qui donne que $\mathbb{R}_1[X]^\perp = \mathrm{Vect}(3X^2 - 2)$.

Proposition III.6. *Si X est une partie d'un espace préhilbertien E, alors $X \subset (X^\perp)^\perp$.*

Démonstration. Si $x \in X$, alors pour tout $y \in X^\perp$ on a : $\langle x, y\rangle = 0$. Et donc $x \in (X^\perp)^\perp$. □

Remarque III.7. *Comme l'orthogonal est un espace vectoriel, on ne peut espérer une égalité que si X est un espace vectoriel. Mais même en imposant cette condition on n'a pas toujours l'égalité.*

Théorème-Définition III.8 (Supplémentaire orthogonal)**.** *Si E est un espace préhilbertien (quelconque) et F un sous-espace vectoriel de E* ***de dimension finie****, alors : $F^\perp$ est un supplémentaire de F dans E. C'est même le seul supplémentaire de F qui soit orthogonal à F. On l'appelle* ***le supplémentaire orthogonal de*** *F.*
De plus, on a $\left(F^\perp\right)^\perp = F$.

Démonstration. On a déjà que $F \cap F^\perp = \{0\}$, ce qui montre que F et $F^\perp$ sont en somme directe.
Reste à montrer que $E = F + F^\perp$. Considérons $(f_1, \dots, f_n)$ une base orthonormé de F (qui existe bien comme F est de dimension finie.
Soit $x \in E$. Alors pour tout $j \in [\![1; n]\!]$ on a :

$$\left\langle x - \sum_{i=1}^{n} \langle x, f_i\rangle f_i, f_j \right\rangle = \langle x, f_j\rangle - \sum_{i=1}^{n} \langle x, f_i\rangle \underbrace{\langle f_i, f_j\rangle}_{\delta_{i,j}} = \langle x, f_j\rangle - \langle x, f_j\rangle = 0$$

ce qui assure que $x - \sum_{i=1}^{n} \langle x, f_i\rangle f_i \in F^\perp$.
Et on a ainsi que :

$$x = \underbrace{\sum_{i=1}^{n} \langle x, f_i\rangle f_i}_{\in F} + \underbrace{x - \sum_{i=1}^{n} \langle x, f_i\rangle f_i}_{\in F^\perp} \in F + F^\perp$$

ce qui assure bien que F et $F^\perp$ sont supplémentaires.

Pour l'unicité, considérons G un supplémentaire de F dans E orthogonal à F. Comme F et G sont orthogonaux, on a déjà que $G \subset F^\perp$.
Pour l'autre inclusion, considérons $x \in F^\perp$. On a déjà que $E = F \oplus G$, donc il existe $x_F \in F$ et $x_G \in G$ tels que $x = x_F + x_G$. Et ainsi :

$$\|x_F\|^2 = \langle x_F, x_F\rangle = \langle x_F, x - x_G\rangle = 0 - 0 = 0$$

et donc $x_F = 0$, c'est-à-dire que $x = x_G \in G$, ce qui prouve la seconde inclusion.
Et finalement $G = F^\perp$, ce qui prouve l'unicité.

Pour le dernier résultat, on a déjà prouvé que $F \subset \left(F^\perp\right)^\perp$.
Pour l'autre inclusion, soit $x \in \left(F^\perp\right)^\perp$. On pose $x = x_1 + x_2$ où $x_1 \in F$ et $x_2 \in F^\perp$. Alors :

$$\|x_2\|^2 = \langle x_2, x_2\rangle = \langle x_2, x - x_1\rangle = \langle x_2, x\rangle - \langle x_2, x_1\rangle = 0 - 0 = 0$$

et donc $x_2 = 0$, c'est-à-dire que $x = x_1 \in F$, ce qui prouve bien que $\left(F^\perp\right)^\perp = F$. □

Remarques III.9.

1. *En prenant F de dimension finie dans E de dimension infinie, les conclusions du théorème restent valable pour $F^\perp$, qui est de dimension infinie. Ainsi, il n'est pas nécessaire d'avoir un espace de dimension finie pour avoir $(F^\perp)^\perp = F$. Et on pourrait avoir même F et $F^\perp$ de dimension infinie : par exemple, si $F = \mathrm{Vect}(1, X^2, \dots, X^{2n}, \dots)$ dans $\mathbb{R}[X]$ muni du produit scalaire associé à sa base canonique, on trouve $F^\perp = \mathrm{Vect}(X, X^3, \dots, X^{2n+1}, \dots)$, et on a bien $\mathbb{R}[X] = F \oplus F^\perp$.*
2. *On voit apparaître un résultat important : on n'avait pas l'unicité du supplémentaire, mais l'orthogonalité permet de l'acquérir.*
3. *Si E est euclidien, on a directement toutes les hypothèses sur F.*
4. *On notera parfois $E = F \oplus^\perp G$ pour notifier que F et G sont supplémentaires orthogonaux.*

Exemple III.10. *Dans $\mathcal{M}_n(\mathbb{R})$ muni de son produit scalaire canonique, les espaces $\mathcal{S}_n(\mathbb{R})$ et $\mathcal{A}_n(\mathbb{R})$ sont supplémentaires orthogonaux l'un de l'autre.*
On a en effet l'orthogonalité, comme pour toutes matrices $S \in \mathcal{S}_n(\mathbb{R})$ et $A \in \mathcal{A}_n(\mathbb{R})$ on a :

$$\langle A, S\rangle = \mathrm{tr}(A^T S) = -\mathrm{tr}(AS) = -\mathrm{tr}(SA) = -\mathrm{tr}(S^T A) = -\langle S, A\rangle = \langle A, S\rangle$$

et donc $\langle A, S\rangle = 0$.
Et le fait qu'ils soient supplémentaire a déjà été montré plusieurs fois.
Donc finalement : $\mathcal{S}_n(\mathbb{R}) = \mathcal{A}_n(\mathbb{R})^\perp$

Corollaire III.11. *Si E est un espace euclidien, alors pour tout sous-espace vectoriel F de E on a :* $\dim(F^\perp) = \dim(E) - \dim(F)$.

Exemple III.12. *Dans le cas d'un hyperplan, tout supplémentaire (donc en particulier le supplémentaire orthogonal) est une droite. Et donc tout vecteur non-nul a orthogonal à un hyperplan H engendre $H^\perp$.*
Et en reprenant l'orthogonal, on déduit que : $H = \text{Vect}(a)^\perp = \{a\}^\perp$.
On retrouve dans $\mathbb{R}^3$ *que :*

$$\{(x,y,z) \in \mathbb{R}^3 \,|\, ax + by + cz = 0\} = \{(a,b,c)\}^\perp$$

et plus généralement on avait vu que, étant donné $(e_1, \dots, e_n)$ une base de E, un hyperplan est donné par une équation du type $\sum_{i=1}^n a_i x_i = 0$, où les x_i sont les coordonnées dans la base (e_i) des points considérés, et les a_i sont des coefficients qui dépendent de l'hyperplan.
Et cet hyperplan est directement $\{(a_1, \dots, a_n)\}^\perp$ pour le produit scalaire associé à $(e_1, \dots, e_n)$.

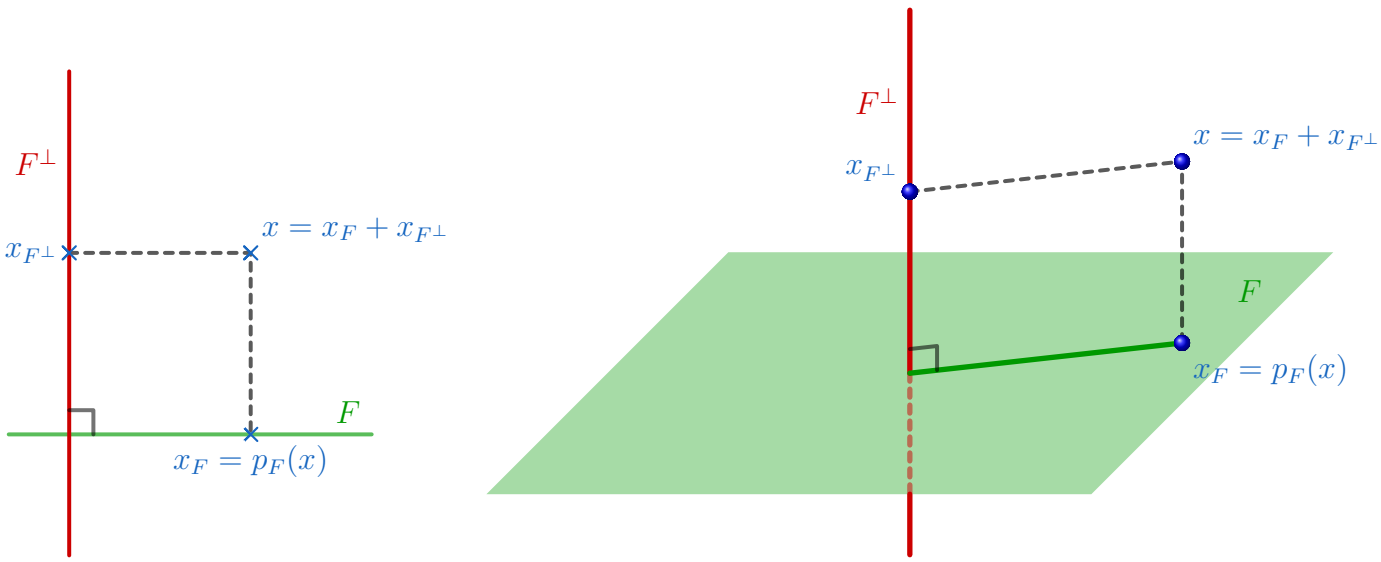
Corollaire III.13. *Si E est un espace euclidien, les hyperplans sont exactement les orthogonaux de droites. Plus précisément, si on considère $\mathcal{B} = (e_1, \dots, e_n)$ une base orthonormée de E, et H l'hyperplan d'équation $\sum_{i=1}^n a_i x_i = 0$, alors $H = \text{Vect}\left((a_1, \dots, a_n)\right)^\perp$.*

Démonstration. Le premier résultat découle directement des dimensions, comme les hyperplans sont exactement les espaces de dimension n, donc leur orthogonal est une droite. Et inversement l'orthogonal d'une droite est bien un hyperplan.
Le second résultat découle du lien entre expression du produit scalaire et coordonnées dans une base orthonormée. □

Remarque III.14. *Avec les mêmes notations, le vecteur $n = \sum_{i=1}^n a_i e_i$ est un* ***vecteur normal*** *à H. Tout élément non nul de $H^\perp = \text{Vect}(n)$ est également appelé vecteur normal.*

III.2 Projecteur orthogonal

Définition III.15. *Si E est un espace préhilbertien, et F est un sous-espace vectoriel de E* ***de dimension finie****, on appelle* ***projecteur orthogonal sur*** *F le projecteur p_F sur F parallèlement à $F^\perp$.*
Pour $x \in E$, on dira que p_F est le ***projeté orthogonal*** *de x sur F.*



Remarques III.16.

1. *L'unicité du supplémentaire orthogonal permet de ne pas préciser les deux espaces supplémentaires (comme on le ferait normalement pour un projecteur).*

2. *Étant donné un projecteur $p \in \mathcal{L}(E)$, c'est un projecteur orthogonal si, et seulement si,* $(\mathrm{Im}p)^\perp = \mathrm{Ker}p$.

Proposition III.17. *Si F est un sous-espace vectoriel de dimension finie E préhilbertien, en notant $(f_1, \dots, f_n)$ une base de F et p_F la projection orthogonale sur F, on a :*

$$\forall x \in E,\ p_F(x) = \sum_{i=1}^{n} \langle x, f_i \rangle f_i.$$

De plus, $p_F(x)$ est l'unique élément de F tel que $x - p_F(x) \in F^\perp$.

Démonstration. En reprenant les mêmes notations, on a directement que :

$$x = \underbrace{\left(x - \sum_{i=1}^{n} \langle x, f_i \rangle f_i\right)}_{\in F^\perp} + \underbrace{\sum_{i=1}^{n} \langle x, f_i \rangle f_i}_{\in F} = \underbrace{x - p_F(x)}_{\in F^\perp} + \underbrace{p_F(x)}_{\in F}$$

et donc, par unicité de l'écriture (comme F et $F^\perp$ sont en somme directe), on a bien que $p_F(x) = \sum_{i=1}^{n} \langle x, f_i \rangle f_i$.
Si $y \in F$ vérifie que $x - y \in F^\perp$, alors :

$$p_F(y) = y \text{ et } 0 = p_F(x - y) = p_F(x) - p_F(y)$$

donc $y = p_F(x)$. □

Remarques III.18.

1. *On a ainsi deux méthodes pour calculer un projeté orthogonal : ou bien on passe par une base orthonormée, ou bien on utilise la caractérisation de la fin de la proposition. Et c'est souvent cette seconde méthode qui est plus efficace, car la première demande de déterminer une base orthonormée ce qui peut prendre du temps, et cela fait aussi apparaître des racines carrées, alors que la seconde permet de faire des calculs dans une base quelconque.*
2. *On retrouve l'expression de l'algorithme de Gram–Schmidt. Si on reprend les notations de l'algorithme, on a que, pour tout $k \in [\![1; n]\!]$, la famille $(x_1, \dots, x_k)$ est une base orthonormée de $F_k = \mathrm{Vect}(e_1, \dots, e_k)$, et on a donc $x_{k+1}^* = e_{k+1} - p_k(e_{k+1})$, où p_k est la projection orthogonale sur F_k.*
3. *Pour le dernier résultat, on pouvait aussi constater que pour tout $i \in [\![1; n]\!]$, on a : $\langle x - y, f_i \rangle = 0$, et donc $\langle x, f_i \rangle = \langle y, f_i \rangle$ par linéarité à gauche. De sorte que, par expression des coordonnées en base orthonormée :*

$$y = \sum_{i=1}^{n} \langle y, f_i \rangle f_i = \sum_{i=1}^{n} \langle x, f_i \rangle f_i = p_F(x).$$

Corollaire III.19. *On considère H un hyperplan d'un espace euclidien E, et n un vecteur normal à H, alors en notant p_H la projection orthogonale sur H on a :*

$$\forall x \in E,\ p_H(x) = x - \frac{\langle x, n \rangle}{\|n\|^2} n.$$

Remarque III.20. *Si n est unitaire, on a même plus simplement :*

$$\forall x \in E,\ p_H(x) = x - \langle x, n \rangle n.$$

Exemple III.21. *Considérons* $E = \mathcal{C}([0, 2\pi], \mathbb{R})$ *muni du produit scalaire* $\langle f, g\rangle = \int_0^{2\pi} f(t)g(t)\mathrm{d}t$.
On pose $F = \mathrm{Vect}(\cos, \sin)$*, qui est un espace de dimension* 2*. Et on veut déterminer le projeté orthogonal sur* F *de la fonction* id.
On procède suivant les deux méthodes précédentes. On calcule déjà tous les produits scalaires dont on aura besoin :

$$\|\cos\|^2 = \int_0^{2\pi} \cos^2(t)\mathrm{d}t = \pi = \|\sin\|^2$$

(en linéarisant par exemple)

$$\langle \cos, \sin\rangle = \int_0^{2\pi} \cos(t)\sin(t)\mathrm{d}t = 0$$

(en linéarisant, ou par changement de variable $u = \cos(t)$ *ou* $u = \sin t$*)*

$$\int_0^{2\pi} te^{it}\mathrm{d}t = -2i\pi \text{ donc } \langle \mathrm{id}, \sin\rangle = -2\pi \text{ et } \langle \mathrm{id}, \cos\rangle = 0$$

(en calculant la première intégrale par intégration par parties)
Et avec ces calculs on déduit :

— *par base orthonormée : la base* $(\cos, \sin)$ *est déjà orthogonale, donc la famille* $\left(\frac{\cos}{\sqrt{\pi}}, \frac{\sin}{\sqrt{\pi}}\right)$ *est une base orthonormée de* F*. Et la projection orthogonale de* id *sur* F *est donc :*

$$\left\langle \mathrm{id}, \frac{\cos}{\sqrt{\pi}}\right\rangle \frac{\cos}{\sqrt{\pi}} + \left\langle \mathrm{id}, \frac{\sin}{\sqrt{\pi}}\right\rangle \frac{\sin}{\sqrt{\pi}} = \frac{\langle \mathrm{id}, \cos\rangle}{\pi}\cos + \frac{\langle \mathrm{id}, \sin\rangle}{\pi}\sin = -2\sin.$$

— *par caractérisation d'un projecteur : on note* $p(\mathrm{id}) = \lambda\cos + \mu\sin$*. Et on a* $\mathrm{id} - p(\mathrm{id}) \in F^\perp$*, ce qui donne :*

$$0 = \langle \mathrm{id} - p\mathrm{id}, \cos\rangle = \langle \mathrm{id} - \lambda\cos - \mu\sin, \cos, \cos\rangle = \langle \mathrm{id}, \cos\rangle - \lambda\|\cos\|^2 - \mu\langle \sin, \cos\rangle = -\lambda\pi$$

$$0 = \langle \mathrm{id} - p\mathrm{id}, \sin\rangle = \langle \mathrm{id} - \lambda\cos - \mu\sin, \cos, \sin\rangle = \langle \mathrm{id}, \sin\rangle - \lambda\langle \cos, \sin\rangle - \mu\|\sin\|^2 = -2\pi - \mu\pi$$

et donc $\lambda = 0$ *et* $\mu = -2$*, ce qui donne* $p(\mathrm{id}) = -2\sin$.

III.3 Distance à un espace vectoriel

Définition III.22 (Distance d'un point à une partie)**.** *Étant donné un espace préhilbertien* E*, un élément* $x \in E$ *et une partie non vide* A *de* E*, on appelle* ***distance de*** x ***à*** A*, notée* $\mathrm{d}(x, A)$*, la quantité :*

$$\mathrm{d}(x, A) = \inf_{a\in A} \mathrm{d}(x, a) = \inf_{a\in A} \|x - a\|.$$

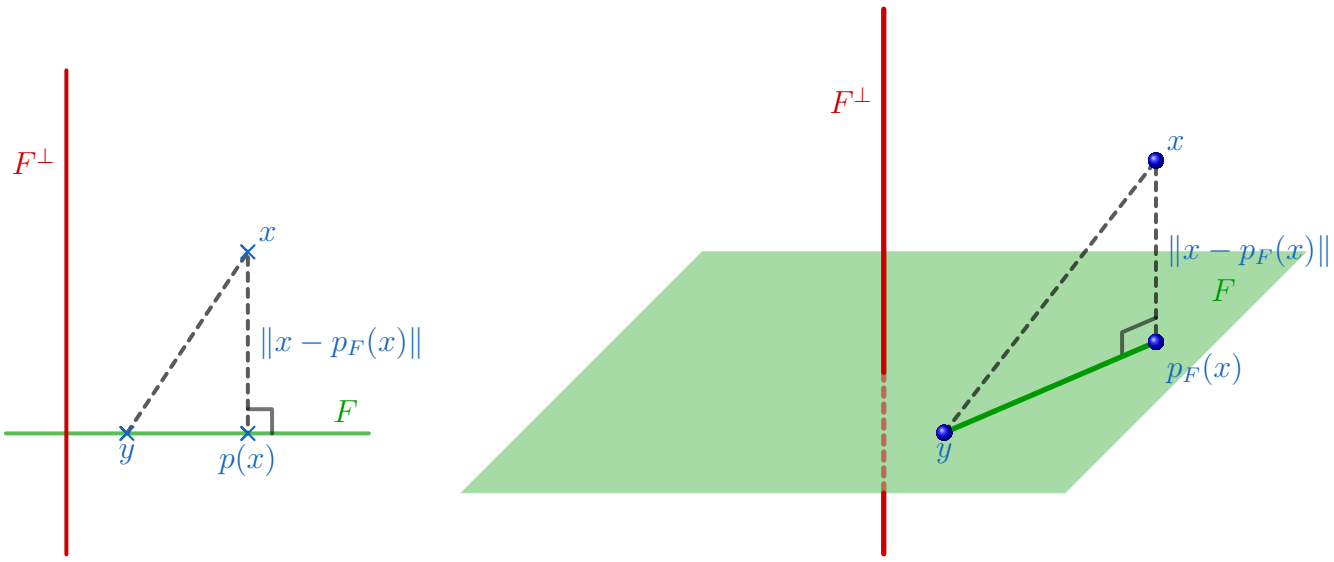
Remarques III.23.

1. *Comme* A *est supposé non vide, alors* $\mathrm{d}(x, A)$ *est la borne inférieure d'une partie non vide minorée de* $\mathbb{R}_+$*, donc c'est un réel positif ou nul.*
2. *Si* $x \in A$*, on a* $\mathrm{d}(x, A) = 0$*. Mais la réciproque est fausse pour des parties* A *quelconques. Par exemple, si on se place sur* $\mathbb{R}$*, alors pour tout* $x \in \mathbb{R}$ *on a* $\mathrm{d}(x, \mathbb{Q}) = 0$ *(par densité de* $\mathbb{Q}$ *dans* $\mathbb{R}$*).*

Théorème III.24. *Soit* E *est un espace préhilbertien, et* F *un sous-espace vectoriel de* E ***de dimension finie****. On note* p_F *la projection orthogonale sur* F*.*
Alors pour tout $x \in E$*,* $p_F(x)$ *est l'unique élément de* F *qui réalise la distance de* x *à* F*, c'est à dire que l'on a :*

$$\forall y \in F,\ \mathrm{d}(x, F) = \|x - y\| \Leftrightarrow y = p_F(x).$$

Démonstration.



Soit $y \in F$. Alors :

$$x - y = \underbrace{(x - p_F(x))}_{\in F^\perp} + \underbrace{(p_F(x) - y)}_{\in F}$$

Et donc par théorème de Pythagore :

$$\|x - y\|^2 = \|x - p_F(x)\|^2 + \|p_F(x) - y\|^2$$

ce qui donne bien que $\|x - y\| \geq \|x - p_F(x)\|$, avec égalité si, et seulement si, $\|y - p_F(x)\| = 0$, c'est-à-dire $y = p_F(x)$. □

Remarques III.25.

1. *Une conséquence est que, dans le cadre du théorème, la distance n'est plus seulement une borne inférieure : c'est un minimum.*
2. *On peut reformuler ce résultat en termes d'extrema : la fonction $x \mapsto \mathrm{d}(x, y)$, définie sur F, atteint un minimum global strict en F.*
3. *La dernière formule montre aussi comme alléger les calculs avec le théorème de Pythagore : il suffit de calculer $\|x\|^2$ et $\|p_F(x)\|^2$ (ce qui revient à prendre $y = 0$) et on trouve :*

$$\mathrm{d}(x, F)^2 = \|x - p_F(x)\|^2 = \|x\|^2 - \|p_F(x)\|^2$$

ce qui fait apparaître au passage que l'on a toujours $\|x\| \geq \|p_F(x)\|$ pour un projecteur orthogonal (c'est d'ailleurs une caractéristique des projecteurs orthogonaux).

Corollaire III.26. *Considérons H un hyperplan d'un espace euclidien E, de vecteur normal n. Alors :*

$$\forall x \in E,\ \mathrm{d}(x, H) = \frac{|\langle x, n\rangle|}{\|n\|}.$$

Exemple III.27. *On cherche à calculer :*

$$A = \inf_{a,b \in \mathbb{R}} \int_0^1 \left(e^t - a - bt - ct^2\right)^2 \mathrm{d}t$$

qui est bien défini comme toutes les intégrales ci-dessus sont positives.

Considérons l'espace $\mathcal{C}([0,1],\mathbb{R})$ *muni du produit scalaire* $\langle f,g\rangle = \int_0^1 f(t)g(t)\mathrm{d}t$. *Alors on a :*

$$A = \inf_{a,b\in\mathbb{R}} \|t\mapsto e^t - a - bt - ct^2\|^2 = \mathrm{d}(\exp,\mathbb{R}_2[x])^2.$$

Pour calculer cette distance, on passe la projection orthogonale sur $F=\mathbb{R}_2[X]$. *Comme on a déjà montré que la famille* $(1,\sqrt{3}(2X-1),\sqrt{5}(6X^2-6X+1))$ *est une base orthonormée de* $\mathbb{R}_2[X]$ *pour ce produit scalaire, on déduit que le projeté orthogonal de* exp *est :*

$$p_F(\exp) = \langle \exp,1\rangle\cdot 1 + \Big\langle \exp,\sqrt{3}(2X-1)\Big\rangle\cdot\sqrt{3}(2X-1) + \Big\langle \exp,\sqrt{5}(6X^2-6X+1)\Big\rangle\cdot\sqrt{5}(6X^2-6X+1)$$

Pour calculer ces quantités, on calcule $a_k = \int_0^1 e^t t^k\mathrm{d}t$ *pour* $k\in\{0,1,2\}$. *On a :*

— *pour* $k=0$ *:* $a_0 = \int_0^1 e^t\mathrm{d}t = e-1$ *;*

— *pour* $k=1$ *:* $a_1 = \int_0^1 te^t\mathrm{d}t = [te^t]_0^1 - \int_0^1 e^t\mathrm{d}t = e - a_1 = 1$ *;*

— *pour* $k=2$ *:* $a_2 = \int_0^1 t^2e^t\mathrm{d}t = [t^2e^t]_0^1 - 2\int_0^1 te^t = e - 2a_1 = e-2$.

Par linéarité on déduit :

$$\langle \exp,1\rangle = a_0 = e-1$$

$$\Big\langle \exp,\sqrt{3}(2X-1)\Big\rangle = \sqrt{3}(2a_1-a_0) = \sqrt{3}(3-e)$$

$$\Big\langle \exp,\sqrt{5}(6X^2-6X+1)\Big\rangle = \sqrt{5}(6a_26a_1+a_0) = \sqrt{5}(7e-19)$$

Et donc $\|p_F(\exp)\|^2 = (e-1)^2 + 3(3-e)^2 + 5(7e-19)^2 = 249e^2 - 1350e + 1833$.

Et comme $\|\exp\|^2 = \int_0^1 e^{2t}\mathrm{d}t = \dfrac{e^2-1}{2}$, *on déduit que :*

$$A = \frac{-497e^2+2700e-3667}{2} \simeq 3\cdot 10^{-5}$$

et que A *est un minimum, atteint pour* $a+bX+cX^2 = p_F(\exp)$, *ce qui donne :*

$$a = 39e-105,\ b = 588-216e \text{ et } c = 210e-570.$$

À titre de comparaison, si on avait voulu approcher exp *par son développement de Taylor en* 0, *on aurait eu :*

$$\int_0^1 \left(e^t - 1 - t - \frac{t^2}{2}\right)^2 \mathrm{d}t = \frac{15e^2-90e+134}{30} \simeq 7\cdot 10^{-3}$$

et avec le développement en 1 *:*

$$\int_0^1 \left(e^t - e - e(t-1) - \frac{e(t-1)^2}{2}\right)^2 \mathrm{d}t = \frac{-31e^2+90e-15}{30} \simeq 2\cdot 10^{-2}$$

et on trouverai une valeur environ de $2\cdot 10^{-4}$ *avec un développement de Taylor en* $1/2$ *(ce qui est à peu près la meilleure valeur que l'on puisse faire avec un développement de Taylor).*

Chapitre 28

Variables aléatoires

I Variables aléatoires

I.1 Variables aléatoires et événements

Définition I.1 (Variable aléatoire)**.** *Étant donné Ω l'univers d'une expérience aléatoire, et E un ensemble quelconque, on appelle* ***variable aléatoire sur Ω à valeurs dans*** *E tout application $X : \Omega \to E$.*
On parle de ***variable aléatoire réelle*** *lorsque $E \subset \mathbb{R}$.*

Remarques I.2.

1. *L'idée d'une variable aléatoire est de simplifier notre problème, en regroupant ensemble certaines issues, qui joueraient le même rôle.*
2. *Comme au premier chapitre de probabilités, on ne considèrera que des ensembles Ω finis dans ce chapitre. Et, quitte à restreindre X, on pourra alors toujours considérer E fini également.*
3. *On peut composer à gauche une variable aléatoire par une fonction quelconque, et avoir ainsi une nouvelle variable aléatoire. Si $X : \Omega \to E$ est une variable aléatoire, et $f : E \to F$ est une fonction quelconque, alors $f \circ X$, qu'on notera plus simplement $f(X)$, est une variable aléatoire.*

Exemples I.3.

1. *Si on tire deux dés à 6 faces, on peut considérer la variable aléatoire X qui, à un tirage donné, associe la somme des montants.*
   On passe alors de 36 tirages à seulement 11 sommes.
2. *On peut considérer une urne, dans laquelle sont placées des boules blanches et noires, que l'on tire n fois. Et on peut considérer la variable aléatoire qui, étant donnés une suite de tirages, associe le rang du premier tirage où on a tiré une boule blanche, ou 0 comme image si on ne tire jamais de boule blanche. Ainsi, si on note $a_i \in \{B, N\}$ la couleur de la boule au i-ème tirage, la variable aléatoire considérée est définie par :*

$$X : (a_1, \dots, a_n) \mapsto \begin{cases} 0 & \text{si } \forall i \in [\![1; n]\!],\ a_i = N \\ \min\{i \in [\![1; n]\!] \mid a_i = B\} & \text{sinon} \end{cases}$$

Remarque I.4.
Une variable aléatoire permet de passer d'un ensemble d'issues Ω à un ensemble E quelconque.
Inversement, étant donnée une variable aléatoire X à valeurs dans E et une partie A de E, on peut considérer l'événement $X^{-1}(A)$, qu'on notera plus simplement $[X \in A]$ ou $(X \in A)$. Si $A = \{a\}$, on notera $[X = a]$ au lieu de $[X \in \{a\}]$, et dans le cas de variables aléatoires réelles, pour tous $a, b \in \mathbb{R}$ avec $a < b$, on notera respectivement $[X \leq a]$, $[X \geq a]$, $[a \leq X \leq b]$ au lieu de $[X \in]-\infty; a]]$, $[X \in [a; +\infty[]$ et $[X \in [a; b]]$ (et les notations idoines pour des inégalités strictes).

Proposition I.5. *Si $X : \Omega \to E$ est une variable aléatoire, alors $\{[X = a] \mid a \in E\}$ est un système complet d'événements, qu'on appelle système complet d'événements associé à X.*

Démonstration. On utilise que E s'écrit comme l'union disjointe : $E = \cup_{a\in E}\{a\}$.
Le caractère disjoint assure que les événements $[X = a]$ sont deux à deux incompatibles. Et le fait que ce soit un recouvrement assure que l'on a bien un recouvrement de Ω. □

Exemple I.6. *Pour un lancé de deux dés à 6 faces, la variable aléatoire X qui correspond à la somme des montants des dés vérifie $X(\Omega) = [\![2; 12]\!]$, et on a :*

$$[X = 2] = \{(1, 1)\},\ [X = 3] = \{(1, 2), (2, 1)\},\ \ldots$$

$$\ldots,\ [X = 10] = \{(6, 4), (5, 5), (4, 6)\},\ [X = 11] = \{(6, 5), (5, 6)\},\ [X = 12] = \{(6, 6)\}.$$

I.2 Loi d'une variable aléatoire

Définition I.7 (Loi d'une variable aléatoire)**.** *Étant donnée une variable aléatoire X sur un espace probabilisé $(\Omega, \mathbb{P})$, la **loi** de X est l'application :*

$$\mathbb{P}_X : \left\{ \begin{array}{rcl} \mathcal{P}\left(X(\Omega)\right) & \to & [0; 1] \\ A & \mapsto & \mathbb{P}(X \in A) \end{array} \right.$$

Proposition I.8. *La loi $\mathbb{P}_X$ définit une probabilité sur $X(\Omega)$.*

Démonstration. On a déjà que :

$$\mathbb{P}_X(X(\Omega)) = \mathbb{P}(X \in X(\Omega)) = \mathbb{P}(\Omega) = 1$$

De plus, si $A, B \in \mathcal{P}\left(X(\Omega)\right)$ sont disjoints, alors :

$$[X \in (A \cup B)] = X^{-1}\left(A \cup B\right) = X^{-1}(A) \cup X^{-1}(B) = [X \in A] \cup [X \in B]$$

et cette dernière union est disjointe également. Et donc par définition de $\mathbb{P}_X$ on déduit que :

$$P_X\left(A \cup B\right) = \mathbb{P}\left([X \in A] \cup [X \in B]\right) = \mathbb{P}\left([X \in A]\right) + \mathbb{P}\left([X \in B]\right) = \mathbb{P}_X(A) + \mathbb{P}_X(B)$$

ce qui donne bien l'additivité.
Donc $\mathbb{P}_X$ est bien une probabilité sur $X(\Omega)$. □

Remarque I.9. *Le point important est d'avoir une probabilité sur Ω, qu'on transforme en une loi pour X. Si on considère $A \subset \Omega$ tel que $\mathbb{P}(A) \neq 0$, on a vu que $\mathbb{P}_A$ définit une probabilité sur Ω : une probabilité conditionnelle définit donc une nouvelle loi, qu'on appelle **loi conditionnelle** (de la variable aléatoire X sachant A).*

Proposition I.10. *Si X est une variable aléatoire sur un univers **fini** Ω, alors la loi de X est entièrement déterminée par la famille $\left(\mathbb{P}_X(\{x\}) = \mathbb{P}(X = x)\right)_{x\in X(\Omega)}$, qui est une distribution de probabilités sur $X(\Omega)$. Plus précisément, si $A \in \mathcal{P}\left(X(\Omega)\right)$, on a :*

$$\mathbb{P}_X(A) = \sum_{x\in A} \mathbb{P}(X = x).$$

Démonstration. Découle du résultat analogue pour les probabilités, qui donne la bijection entre probabilité et distribution de probabilités. □

Remarque I.11. *On définit alors une relation d'équivalence sur les variables aléatoires, en notant $X \sim Y$ si $\mathbb{P}_X = \mathbb{P}_Y$. On dira alors que X et Y suivent (ou ont) la même loi.*

Corollaire I.12. *Si Ω est un ensemble fini muni de la probabilité uniforme $\mathbb{P}$, et $X : \Omega \to E$ est une variable aléatoire, alors :*

$$\forall A \in \mathcal{P}(E), P_X(A) = \frac{|X^{-1}(A)|}{|\omega|}.$$

Exemple I.13. *lancer de deux dés équilibrés à 6 faces*

Proposition I.14. *Si $X, Y : \Omega \to E$ sont deux variables aléatoires de même loi, et f une fonction définie sur E, alors $f(X)$ et $f(Y)$ suivent la même loi.*
Plus précisément, cette loi est donnée par :

$$\forall A \in \mathcal{P}\left(f(X(\Omega))\right),\ \mathbb{P}_{f(X)}(A) = \mathbb{P}(f(X) \in A) = \sum_{x \in X(\Omega),\ f(x) \in A} \mathbb{P}(X = x).$$

Démonstration. immédiat □

I.3 Variables aléatoires usuelles

Définition I.15 (loi uniforme)**.** *Étant donné E un ensemble fini non vide, on dit qu'une variable aléatoire X sur Ω suit une* ***loi uniforme sur*** *E si :*

$$X(\Omega) = E \text{ et } \forall A \subset E,\ \mathbb{P}(X \in A) = \frac{|A|}{|E|}$$

ce que l'on note $X \sim \mathcal{U}(E)$.

Exemple I.16. *Si on considère un dé équilibré à n faces, la loi qui donne le montant du dé suit la loi $\mathcal{U}(\llbracket 1; n \rrbracket)$.*

Définition I.17 (Loi de Bernoulli)**.** *Soit $p \in [0; 1]$. On dit qu'une variable aléatoire X sur Ω suit une* ***loi de Bernoulli de paramètre*** *p si :*

$$X(\Omega) = \{0; 1\} \text{ et } \mathbb{P}(X = 1) = p,\ \mathbb{P}(X = 0) = 1 - p$$

ce que l'on note $X \sim \mathcal{B}(p)$.

Exemple I.18. *On considère une pièce déséquilibrée, qui tombe sur Pile avec probabilité p (et Face avec probabilité $1 - p$). Alors la variable aléatoire qui vaut 1 si la pièce fait Pile et 0 sinon suit une loi de Bernoulli de paramètre p.*
Plus généralement, une expérience qui a deux issues peut-être modélisée par une variable aléatoire de Bernoulli : par exemple si on considère une loterie avec 48 participant, si on considère la variable aléatoire qui vaut 1 si on gagne et 0 si on perd, elle suit une loi de Bernoulli de paramètre $p = \frac{1}{48}$.

Définition I.19 (Loi binomiale)**.** *Soit $p \in [0; 1]$ et $n \in \mathbb{N}^*$. On dit qu'une variable aléatoire X sur Ω suit une* ***loi binomiale de paramètres*** *n* ***et*** *p si :*

$$X(\Omega) = \llbracket 0; n \rrbracket \text{ et } \forall k \in \llbracket 0; n \rrbracket,\ \mathbb{P}(X = k) = \binom{n}{k} p^k (1 - p)^{n-k}$$

ce que l'on note $X \sim \mathcal{B}(n, p)$.

Exemple I.20. *On considère une pièce déséquilibrée, qui tombe sur Pile avec probabilité p (et Face avec probabilité $(1-p)$), qu'on lance n fois* ***de manière indépendante****. Alors la variable aléatoire du nombre de Pile après les n lancers suit une loi binomiale de paramètres n et p.*
Pour avoir $X = k$, on a à choisir les $\binom{n}{k}$ possibilités pour choisir les k lancers qui feront Pile et les $(n-k)$ lancers qui feront Face. Une fois ces choix, on a une probabilité de p^k (par indépendance) que les lancers choisis fassent Pile, et $(1-p)^{n-k}$ que les autres donnent Face. Ce qui donne bien la loi voulue.

II Couples (et plus) de variables aléatoires

II.1 Lois conjointes et marginales

Définition II.1 (Couples de variables aléatoires)**.** *Étant donné deux variables aléatoires $X : \Omega \to E$ et $Y : \Omega \to F$, l'application :*

$$(X,Y) : \left\{ \begin{array}{ccc} \Omega & \to & E \times F \\ \omega & \mapsto & (X(\omega), Y(\omega)) \end{array} \right.$$

est une variable aléatoire appelle ***couple de variables aléatoires sur*** Ω.

Remarque II.2. *De manière analogue, on parle de n-uplets de variables aléatoires.*

Définition II.3 (Lois conjointes et marginales)**.** *On considère (X,Y) un couple de variables aléatoires sur Ω :*

1. *la loi de la variable aléatoire (X,Y) est appelée* ***loi conjointe*** *du couple (X,Y) ;*
2. *les lois de X et de Y sont appelées respectivement première et seconde* ***loi marginale*** *du couple (X,Y).*

Remarque II.4. *Pour la loi conjointe, si $(x,y) \in E \times F$, on notera $\mathbb{P}(X = x, Y = y)$ pour la probabilité de l'événement $[X = x] \cap [Y = y]$.*

Proposition II.5. *Si (X,Y) est un couple de variable aléatoire, alors :*

$$\forall x \in X(\Omega),\ \mathbb{P}(X = x) = \sum_{y \in Y(\Omega)} \mathbb{P}(X = x, Y = y)$$

$$\forall y \in Y(\Omega),\ \mathbb{P}(Y = y) = \sum_{x \in X(\Omega)} \mathbb{P}(X = x, Y = y)$$

Démonstration. On applique la formule des probabilités totales aux systèmes complets d'événements $\{[Y = y] \,|\, y \in Y(\Omega)\}$ et $\{[X = x] \,|\, x \in X(\Omega)\}$. □

Remarque II.6. *Autrement dit, les lois marginales se déduisent de la loi conjointe. Mais la réciproque est fausse : par exemple, si on lance deux dés équilibrés à 6 faces, et qu'on considère X la variable aléatoire correspondant au montant du premier dé, et Y celle du second. Alors X et Y suivent la même loi, mais les couples (X,X) et (X,Y) ne suivent pas la même loi, puisque pour tous $k,l \in [\![1;6]\!]$ on a :*

$$\mathbb{P}(X = k, Y = l) = \frac{1}{36} \text{ et } \mathbb{P}(X = k, X = l) = \frac{\delta_{k,l}}{6}$$

II.2 Indépendance de variables aléatoires

Définition II.7. *Si $X : \Omega \to E$ et $Y : \Omega \to F$ sont des variables aléatoires, on dit qu'elles sont* ***indépendantes*** *si : pour tout $A \in \mathcal{P}(E)$ et $B \in \mathcal{P}(F)$ les événements $[X \in A]$ et $[Y \in B]$ sont indépendants, c'est-à-dire que :*

$$\mathbb{P}([X \in A] \cap [Y \in B]) = \mathbb{P}(X \in A)\mathbb{P}(Y \in B)$$

et on note alors : $X \perp Y$.

Remarque II.8. *La définition s'étend à davantage de variables aléatoires. Comme pour les événements, il y a une différence entre le fait d'être mutuellement indépendants, ou d'être indépendant deux à deux.*

Proposition II.9. *Si X, Y sont deux variables aléatoires, elles sont indépendantes si, et seulement si, pour tout $(x,y) \in X(\Omega) \times Y(\Omega)$ les événements $[X = x]$ et $[Y = y]$ sont indépendants, c'est-à-dire que :*

$$\mathbb{P}(X = x, Y = y) = \mathbb{P}(X = x)\mathbb{P}(Y = y).$$

Démonstration. Notons déjà que, si X et Y sont indépendants, en appliquant la définition aux singletons $\{x\}$ et $\{y\}$ on a bien le résultat.
Réciproquement, si pour tout $(x,y) \in X(\Omega) \times Y(\Omega)$ on a $\mathbb{P}(X=x, Y=y) = \mathbb{P}(X=x)\mathbb{P}(Y=y)$. Soit $A \in \mathcal{P}(X(\Omega))$ et $B \in \mathcal{P}(Y(\Omega))$. Alors par propriété des lois de variables aléatoires :

$$\mathbb{P}(X \in A) = \sum_{x \in A} \mathbb{P}(X=x),\ \mathbb{P}(Y \in B) = \sum_{y \in B} \mathbb{P}(Y=y)$$

$$\mathbb{P}((X,Y) \in A \times B) = \mathbb{P}([X \in A] \cap [Y \in B]) = \sum_{(x,y) \in A \times B} \mathbb{P}([X=x] \cap [Y=y])$$

ce qui donne en faisant apparaître une somme double par produit :

$$\begin{array}{rcl} \mathbb{P}(X \in A)\mathbb{P}(Y \in B) & = & \left(\sum_{x \in A} \mathbb{P}(X=x)\right)\left(\sum_{y \in B} \mathbb{P}(Y=y)\right) \\ & = & \sum_{(x,y) \in A \times B} \mathbb{P}(X=x)\mathbb{P}(Y=y) \\ & = & \sum_{(x,y) \in A \times B} \mathbb{P}([X \in A] \cap [Y \in B]) \end{array}$$

donc X et Y sont bien indépendantes. □

Remarque II.10. *Le point important est que l'indépendance permet de passer de la loi conjointe aux lois marginales.*

Exemple II.11. *Si $X_1, \dots, X_n$ sont des variables aléatoires indépendantes suivant chacune une loi de Bernoulli de paramètre p, alors la variable aléatoire $X_1 + \cdots + X_n$ suit une loi binomiale de paramètres n et p.*

Proposition II.12 (Lemme des coalitions)**.** *Si $X_1, \dots, X_n$ sont des variables aléatoires indépendantes, et $m \in [\![1; n]\!]$ tel que les variables aléatoires $f(X_1, \dots, X_m)$, $g(X_{m+1}, \dots, X_n)$ sont bien définies, alors elles sont indépendantes.*

Démonstration. Découle du résultat précédent, en raisonnant avec les distributions de probabilités. □

Exemple II.13. *Si $X_1, \dots, X_k$ sont des variables aléatoires indépendantes suivant des lois binomiales de paramètres n_1 et p, …,n_k et p, alors :*

$$\sum_{i=1}^{k} X_i \sim \mathcal{B}\left(\sum_{i=1}^{k} n_i, p\right).$$

III Espérance et variance

III.1 Espérance d'une variable aléatoire

Définition III.1. *Si X est une variable aléatoire **réelle ou complexe** sur un ensemble fini Ω, on définit son **espérance** comme :*

$$\mathrm{E}(X) = \sum_{x \in X(\Omega)} x\mathbb{P}(X=x)$$

Remarques III.2.

1. *Si Ω est fini, alors $X(\Omega)$ également, donc la somme ci-dessus a toujours un sens. On verra l'année prochaine, pour les variables aléatoires discrète, que l'on peut étendre la définition à des ensembles $X(\Omega)$ dénombrables, à condition que la famille $(x\mathbb{P}(X=x))_{x \in X(\Omega)}$ soit sommable.*
2. *L'espérance se comporte comme une somme, donc également comme une intégrale, et on verra qu'elle possède des propriétés communes avec ces deux autres notions.*

3. *L'espérance correspond à la moyenne des valeurs prises par X, pondérées par les probabilités associées : c'est donc un indicateur sur les valeurs prises par X en moyenne. On dira notamment qu'une variable aléatoire est* ***centrée*** *si son espérance est nulle.*

Théorème III.3 (Espérance des lois usuelles)**.**

1. *Si X suit une loi uniforme sur $E = \{x_1, \dots, x_n\} \subset \mathbb{C}$, alors :* $\mathrm{E}(X) = \dfrac{1}{n}\sum_{i=1}^{n} x_i$.
   En particulier, si $E = \{m\}$ (variable aléatoire constante) on a $\mathrm{E}(X) = m$, *et si $E = [\![a; b]\!]$ (pour $a, b \in \mathbb{Z}$) on a :* $\mathrm{E}(X) = \dfrac{a+b}{2}$.
2. *Si $X \sim \mathcal{B}(p)$, alors* $\mathrm{E}(X) = p$.
3. *Si $X \sim \mathcal{B}(n, p)$, alors* $\mathrm{E}(X) = np$.

Exemple III.4. *Si $A \subset \Omega$, la variable aléatoire 1_A suit une loi de Bernoulli de paramètre $\mathbb{P}(A)$.*

Proposition III.5. *Si X est une variable aléatoire réelle ou complexe sur un espace probabilisé $(\Omega, \mathbb{P})$ fini, alors :*

$$\mathrm{E}(X) = \sum_{\omega \in \Omega} X(\omega)\mathbb{P}(\{\omega\}).$$

Démonstration. Par sommation par paquets (cas de sommes finies), en notant que $[X = x] = \cup_{\omega\in\Omega,\ X(\omega)=x}\{\omega\}$. □

Proposition III.6 (Linéarité de l'espérance)**.** *Si X, Y sont deux variables aléatoires réelles ou complexes sur Ω et $\lambda, \mu \in \mathbb{R}$ (ou $\mathbb{C}$), alors :*

$$\mathrm{E}\left[\lambda X + \mu Y\right] = \lambda \mathrm{E}\left[X\right] + \mu \mathrm{E}\left[Y\right].$$

En particulier, on a :

$$E(X) = E\left(\mathrm{Re}(X)\right) + iE\left(\mathrm{Im}(X)\right).$$

Exemples III.7. *somme de dés*
espérance Binomiale à partir de Bernoulli

Proposition III.8 (Positivité de l'espérance)**.** *Si X est une variable aléatoire à valeurs dans $\mathbb{R}_+$, alors :*

$$\mathrm{E}(X) \geq 0$$

avec égalité si, et seulement si, $\mathbb{P}(X = 0) = 1$.

Démonstration. somme de nombres positifs ou nuls
cas d'égalité donne $\mathbb{P}(X = a) = 0$ si $a > 0$, et donc $\mathbb{P}(X = 0) = 1$. □

Remarque III.9. *Presque sûrement nulle/constante*

Corollaire III.10 (Croissance de l'espérance)**.** *Si X et Y sont deux variables aléatoires telles que $X \leq Y$, alors* $\mathrm{E}(X) \leq \mathrm{E}(Y)$.

Démonstration. Par linéarité et positivité. □

Proposition III.11 (Inégalité triangulaire)**.**

$$|E(X)| \leq E(|X|)$$

avec égalité ssi X d'argument (signe) constant.

Proposition III.12 (Théorème de transfert)**.** *Si X est une variable aléatoire sur Ω et $f : X(\Omega) \to \mathbb{R}$, alors :*

$$\mathrm{E}\left(f(X)\right) = \sum_{x \in X(\Omega)} f(x)\mathbb{P}(X = x)$$

Démonstration. Découle de la sommation par paquets. □

Remarque III.13. *application aux couples)*

Corollaire III.14. *Si X, Y sont deux variables aléatoires réelles, alors :*

$$\mathrm{E}(XY) = \sum_{(x,y) \in X(\Omega) \times Y(\Omega)} xy\mathbb{P}(X = x, Y = y)$$

En particulier, si X et Y sont indépendantes, alors :

$$\mathrm{E}(XY) = \mathrm{E}(X)\mathrm{E}(Y).$$

Démonstration. on applique le transfert au couple (X, Y) et à la fonction $(x, y) \mapsto xy$.
En cas d'indépendance, on reconnait une somme double. □

Remarque III.15. *Généralisation à davantage de va indépendantes.*

Théorème III.16 (Inégalité de Markov)**.** *Si X est une variable aléatoire **positive** et $a > 0$, alors :*

$$\mathbb{P}(X \geq a) \leq \frac{\mathrm{E}(X)}{a}$$

Démonstration. On pose $Y = a \cdot \mathbb{1}_{[X \geq a]} = \begin{cases} a & \text{si} \quad X \geq a \\ 0 & \text{si} \quad X < a \end{cases}$.
On a donc $Y \leq X$, et par croissance de l'espérance :

$$E(Y) \leq E(X)$$

Mais par linéarité :

$$E(Y) = a \cdot E(\mathbb{1}_{[X \geq a]} = a \cdot \mathbb{P}(X \geq a)$$

ce qui donne bien l'inégalité de Markov en divisant par $a > 0$. □

Remarque III.17. *permet de localiser un peu mieux les variables aléatoires*

III.2 Variance

Définition III.18 (Variance et écart type)**.** *Si X est une variable aléatoire réelle, on définit sa **variance** comme :*

$$V(X) = \mathrm{E}\left((X - \mathrm{E}(X))^2\right)$$

*et son **écart type** comme :*

$$\sigma(X) = \sqrt{V(X)}.$$

*On dira que X est **réduite** si $V(X) = 1$.*

Remarque III.19. *le "$-E(X)$" permet d'avoir une va centrée, puisque la variance permet d'avoir la dispersion d'une va, c'est-à-dire à quel point elle est en moyenne éloignée de sa moyenne (ici avec un écart quadratique)*
Plus généralement, on a les moments d'ordre $k \in \mathbb{N}$ définis par $m_k(X) = E(X^k)$, et les moments centrés d'ordre k comme $E\left((X - E(X))^k\right)$, c'est-à-dire que la variance est le moment centré d'ordre 2.

Proposition III.20 (Formule de Koenig–Huygens)**.** *Si X est une variable aléatoire réelle, alors :*

$$V(X) = E(X^2) - E(X)^2$$

Démonstration. calcul direct en notant que $(X - E(X))^2 = X^2 - 2E(X)X + E(X)^2$ et en utilisant la linéarité de l'espérance. □

Proposition III.21. *Si X est une va réelle, alors :*

1. *$V(X) \geq 0$, avec égalité ssi X est ps constante ($\mathbb{P}(X = E(X)) = 1$) ;*
2. *si $a, b \in \mathbb{R}$, alors : $V(aX + b) = a^2 V(X)$.*

Corollaire III.22. *Si X est une variable aléatoire réelle qui n'est pas presque sûrement constante, alors la variable aléatoire $Y = \dfrac{X - E(X)}{\sigma(X)}$ est bien définie, et est centrée réduite ($E(Y) = 0$ et $V(Y) = 1$).*

Théorème III.23 (Variance des lois usuelles)**.**

1. *Si X suit une loi uniforme sur E fini, alors :*
   Si $E = \{m\}$ (variable aléatoire constante) on a $\mathrm{V}(X) = 0$.
   Si $E = [\![a; b]\!]$ (pour $a, b \in \mathbb{Z}$) on a : $\mathrm{V}(X) = \dfrac{(b - a + 1)^2 - 1}{12}$.
   En particulier, si $E = [\![1; n]\!]$ on a : $\mathrm{V}(X) = \dfrac{n^2 - 1}{12}$.
2. *Si $X \sim \mathcal{B}(p)$, alors $\mathrm{V}(X) = p(1 - p)$.*
3. *Si $X \sim \mathcal{B}(n, p)$, alors $\mathrm{E}(X) = np(1 - p)$.*

Théorème III.24 (Inégalité de Bienaymé–Tchebychev)**.** *Si X est une variable aléatoire réelle, pour tout $a > 0$ on a :*

$$\mathbb{P}\left(|X - E(X)| \geq a\right) \leq \frac{V(X)}{a^2}$$

Démonstration. On applique Markov à $Y = (X - E(X))^2$, qui est bien positive, avec a^2, en notant que :

$$[|X - E(X)| \geq a] = \left[Y \geq a^2\right]$$

pour $a > 0$. □

Exemple III.25. *Application type "loi des grands nombres" : on tire une pièce (peut-être truquée) qui tombe sur pile avec probabilité p. On lance n fois cette pièce, et on note le nombre de Pile obtenus. On veut savoir à quel point le résultat obtenu est fiable.*
Si on note N le nombre de Pile obtenus, et $F = \dfrac{N}{n}$ la fréquence associée, alors $N \sim \mathcal{B}(n, p)$ (par indépendance des lancers), donc $E(N) = np$ puis par linéarité $E(F) = p$.
Par Bienaymé–Tchebychev, si on veut savoir à $0,01$ près la valeur de p, on utilise que :

$$\mathbb{P}\left(|F - p| \geq 0.01\right) = \mathbb{P}\left(|N - E(N)| \geq 0.01\right) \leq \frac{V(N)}{(0.01n)^2} = \frac{np(1-p)}{10^{-4}n^2} = \frac{10^{-4}}{n} p(1-p) \leq \frac{2500}{n}$$

Donc si on veut avoir moins d'une chance sur 10 de faire une erreur de plus de $0,01$ sur la valeur de p, il suffit de lancer 25000 fois la pièce et de regarder la fréquence d'apparition de Pile.

III.3 Covariance

Définition III.26 (Covariance)**.** *Si X, Y sont deux variables aléatoires réelles, on définit la* ***covariance*** *de X et Y comme :*

$$\mathrm{Cov}(X,Y) = \mathrm{E}\left(X - E(X)\right)\mathrm{E}\left(Y - E(Y)\right).$$

On dira que X et Y sont ***décorrélées*** *si* $\mathrm{Cov}(X,Y) = 0$.

Proposition III.27 (Formule de Huygens)**.** *cov(X,Y) = E(XY)-E(X)E(Y)*

Corollaire III.28. *Si X, Y indépendantes, alors elles sont décorrelées.*

Remarque III.29. *Réciproque fausse. Contre exemple : $X \sim \mathcal{U}(\{-1,0,1\})$ et $Y = X^2$. On trouve que $cov(X,Y) = 0$, mais $X = 0 \Leftrightarrow Y = 0$ donc pas indépendantes.*

Proposition III.30. *L'application* cov *est une forme bilinéaire qui vérifie pour toutes variables aléatoires X, Y :*

1. $\mathrm{cov}(X,Y) = \mathrm{cov}(Y,X)$ *(symétrie)*
2. $\mathrm{cov}(X,X) = V(X) \geq 0$ *(positivité)*

Remarque III.31. *Pas défini, donc pas un produit scalaire sur les va réelles. Mais c'en est un sur les va centrées !*

Proposition III.32. *Si X, Y va réelles :*

$$\mathrm{V}(X+Y) = \mathrm{V}(X) + \mathrm{V}(Y) + 2\mathrm{Cov}(X,Y).$$

Corollaire III.33. *Si X, Y indépendantes : $V(X+Y) = V(X) + V(Y)$.*

Corollaire III.34. $V\left(\sum X_i\right) = \sum V(X_i) + 2\sum_{i<j}\mathrm{Cov}(X_i,X_j)$
si indépendantes : $V(\sum X_i) = \sum V(X_i)$.

Démonstration. par récurrence □

Remarque III.35. *En prenant $X_1, \ldots, X_n$ indépendantes qui suivent une même loi de Bernoulli de paramètre p, on retrouve la variance d'une loi binomiale.*

Chapitre 29

Fonctions à deux variables

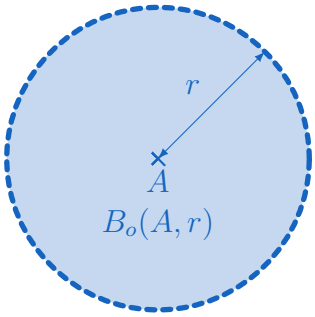
On considère ici l'espace $\mathbb{R}^2$, muni de sa structure euclidienne par son produit scalaire canonique, et on note $\|\cdot\|$ la norme associée.

I Fonctions continues à deux variables

I.1 Topologie de $\mathbb{R}^2$ euclidien

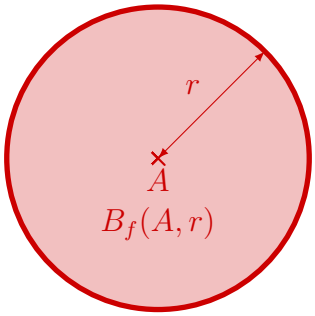
Définition I.1 (Boules ouvertes/fermées)**.** *Si $A \in \mathbb{R}^2$ et $r > 0$, on définit la* ***boule ouverte de centre*** *A* ***et de rayon*** *r comme :*

$$B_o(A,r) = \{x \in \mathbb{R}^2 \,|\, \|x - A\| < r\}$$



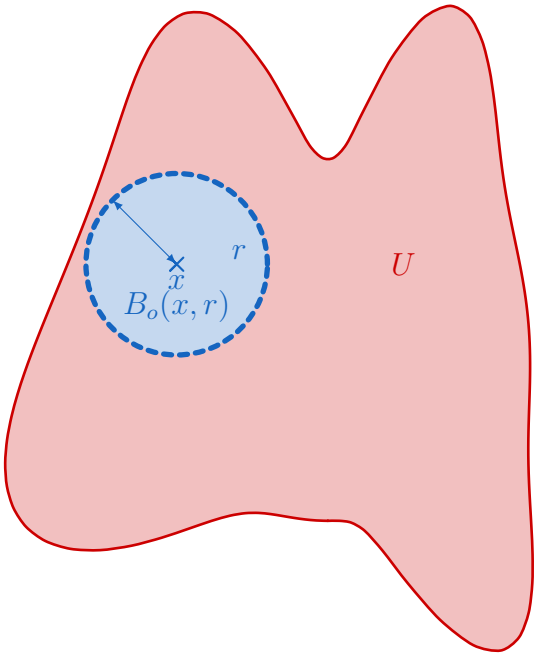
et la ***boule fermée de centre*** *A* ***et de rayon*** *r comme :*

$$B_f(A,r) = \{x \in \mathbb{R}^2 \,|\, \|x - A\| \leq r\}.$$



Remarque I.2. *La boule ouverte (resp. fermée) de centre A de rayon r joue dans $\mathbb{R}^2$ le même rôle que l'intervalle ouvert $]a-r, a+r[$ (resp. le segment $[a-r, a+r]$) dans $\mathbb{R}$. Et lien entre les boules ouvertes/fermées est le même que celui entre les intervalles ouverts/fermés : on retire on on rajoute le bord.*

Définition I.3 (Voisinage)**.** *Soit $x \in \mathbb{R}^2$ et $U \subset \mathbb{R}^2$. On dit que U est un* ***voisinage*** *de x s'il existe $r > 0$ tel que : $B_o(x,r) \subset U$.*



Remarques I.4.

1. *Si U est un voisinage de x, alors nécessairement $x \in U$.*
2. *La réciproque est fausse : si $x \in U$, U est un voisinage de x à moins que x soit "au bord" de U. Et c'est l'intérêt de travailler avec des boules (ouvertes ou fermées), puisqu'elle ont des éléments partout autour de leur centre.*

Définition I.5 (Ouverts)**.** *Un sous-ensemble U de $\mathbb{R}^2$ est un **ouvert** s'il est un voisinage de chacun de ses points, c'est-à-dire s'il vérifie l'une des conditions équivalentes suivantes :*

$$\forall x \in U,\ \exists r > 0,\ B_o(x,r) \subset U$$

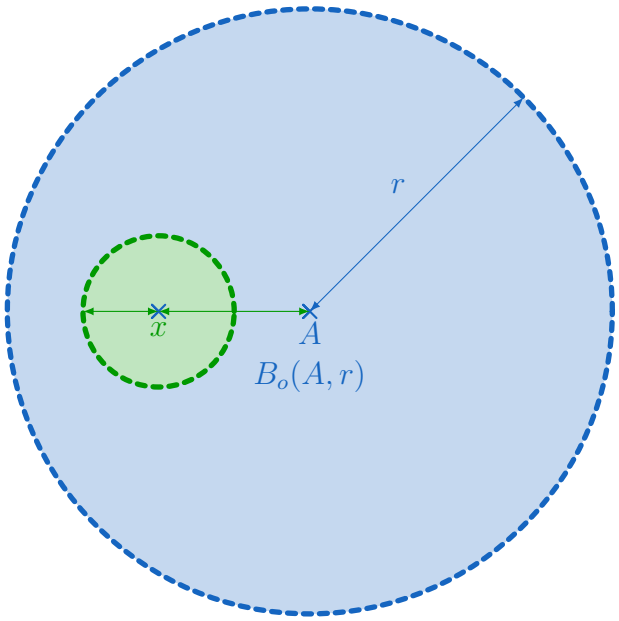
$$\forall x \in U,\ \exists r > 0,\ \|x - y\| < r \Rightarrow y \in U$$

Remarque I.6. *Que ce soit pour les voisinages ou les ouverts, on peut changer les boules ouvertes par des boules fermées dans les définitions. Le point important étant que, si $x \in \mathbb{R}^2$ et $r > 0$, alors : $B_f(x, r/2) \subset B_o(x,r)$.*

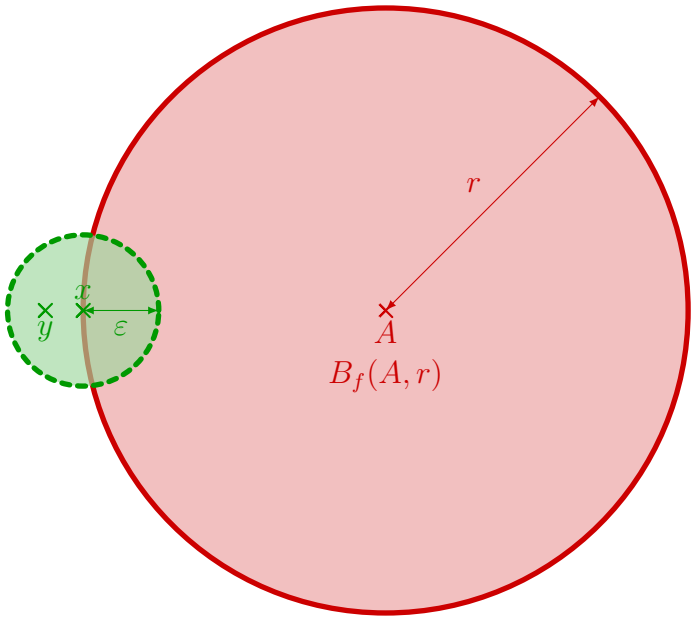
Exemples I.7.

1. *Les boules ouvertes sont des ouverts.*
   Soit $A \in \mathbb{R}^2$ et $r > 0$. Montrons que la boule ouverte $U = B_o(A,r)$ est un ouvert. Soit donc $x \in U$. Alors on a : $B_o\left(x, \dfrac{r - \|x - A\|}{2}\right) \subset U$. En effet, on a pour tout $y \in \mathbb{R}^2$:

$$\begin{aligned} y \in B_o\left(x, \frac{r - \|x - A\|}{2}\right) &\Rightarrow \|y - x\| < \frac{r - \|x - A\|}{2} \\ &\Rightarrow \|y - A\| \underset{\text{inégalité triangulaire}}{\leq} \|y - x\| + \|x - A\| \leq \frac{r - \|x - A\|}{2} + \|x - A\| \leq \\ &\Rightarrow y \in U \end{aligned}$$



2. *Les boules fermées ne sont pas des ouverts.*
   Soit $A \in \mathbb{R}^2$ *et* $r > 0$. *Montrons que la boule fermée* $V = B_f(A,r)$ *n'est pas un ouvert. Prenons* $x \in \mathbb{R}^2$ *tel que* $\|x - A\| = r$ *et considérons* $\varepsilon > 0$. *Alors* $B_o(x,\varepsilon) \not\subset V$, *tandis que* $x \in V$.
   Prenons $y = \dfrac{A + \left(r + \frac{\varepsilon}{2}\right)(x - A)}{r}$. *Alors :*
   — $\|y - x\| = \left\|\dfrac{\varepsilon/2}{r}(x - A)\right\| = \dfrac{\varepsilon/2}{\cancel{r}}\cancel{\|x - A\|} < \varepsilon$;
   — $\|y - A\| \left\|\dfrac{r + \varepsilon/2}{r}(x - A)\right\| = \dfrac{r + \varepsilon/2}{\cancel{r}}\cancel{\|x - A\|} > r.$
   ce qui montre bien que $B_f(A,r)$ *n'est pas un voisinage de* x, *donc n'est pas un ouvert.*



Proposition I.8.

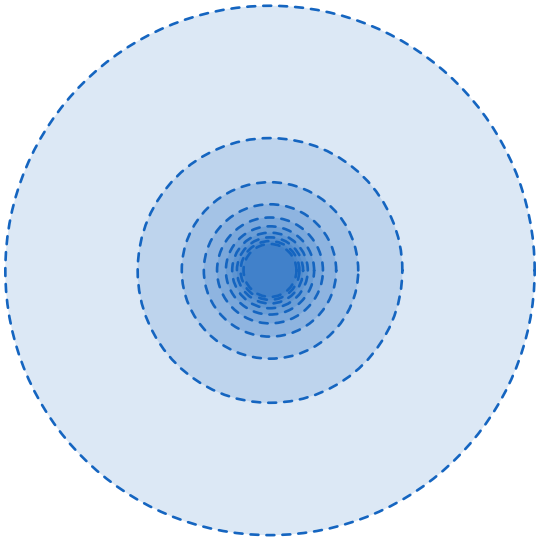
1. *Une union (quelconque) d'ouverts est un ouvert.*
2. *Une intersection* ***d'un nombre fini*** *d'ouverts est un ouvert.*

Démonstration. à faire □

Remarque I.9. *Le fait que les ouverts soient en nombre fini pour l'intersection est fondamental. Par exemple on a :*

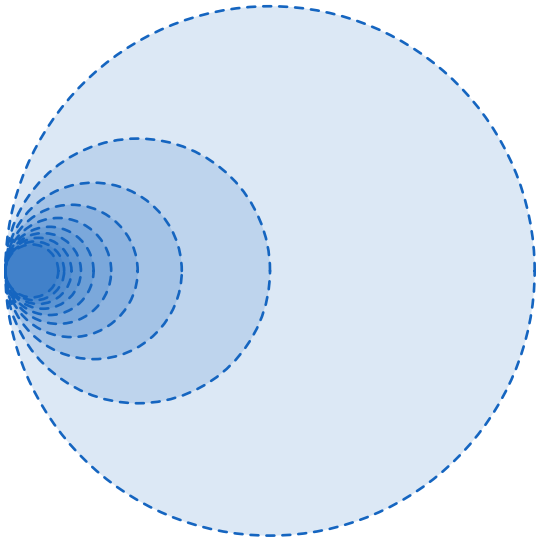
$$\cap_{n\in\mathbb{N}^*} B_o(0,1/n) = \{0\}$$

qui n'est pas un ouvert.



De plus, même si les ouverts sont inclus les uns dans les autres, une intersection infinie d'ouverts peut être vide. Par exemple on a :

$$\cap_{n\in\mathbb{N}^*} B_o((1/n,0),1/n) = \emptyset.$$



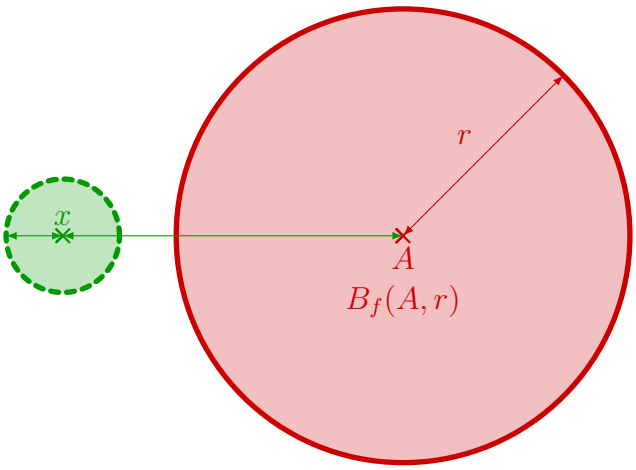
Définition I.10 (Fermés)**.** *Un sous-ensemble $F \subset \mathbb{R}^2$ est dit* ***fermé*** *si son complémentaire $\mathbb{R}^2 \setminus F$ est un ouvert.*

Proposition I.11.

1. *Une intersection quelconque de fermés est un fermé.*
2. *Une intersection* ***d'un nombre fini*** *de fermés est un fermé.*

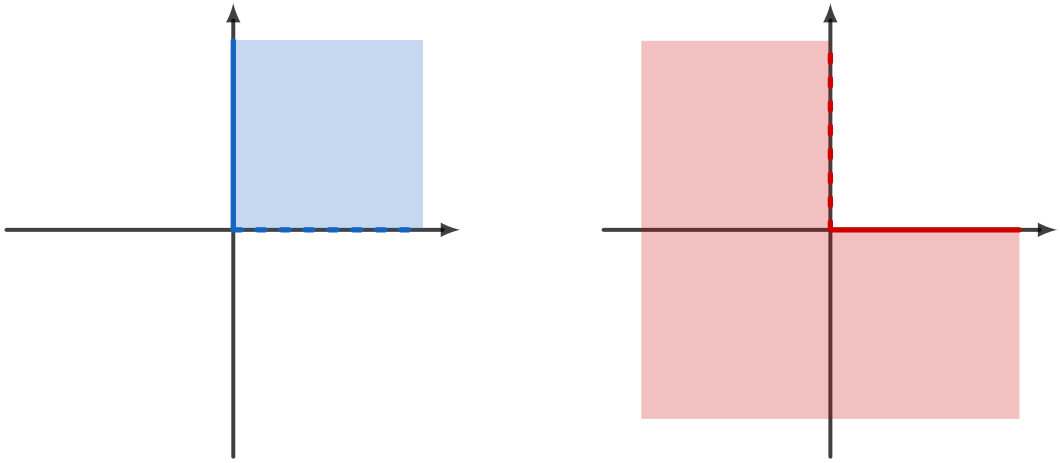
Démonstration. Comme pour les ouverts, ou comme corollaire en utilisant les règles de de Morgan. □

Exemple I.12. *Une boule fermée est un fermé.*



Remarques I.13.

1. *On a exactement la même situation que sur* $\mathbb{R}$.
2. *Comme dans* $\mathbb{R}$, *il existe des ensembles qui ne sont ni ouverts, ni fermés. Par exemple, l'ensemble* $\mathbb{R}_+ \times \mathbb{R}_+^*$ *n'est ni ouvert, ni fermé.*



À l'inverse, il existe des ensembles ouverts et fermés : il s'agit de $\emptyset$ *et* $\mathbb{R}^2$, *et ce sont les seuls.*

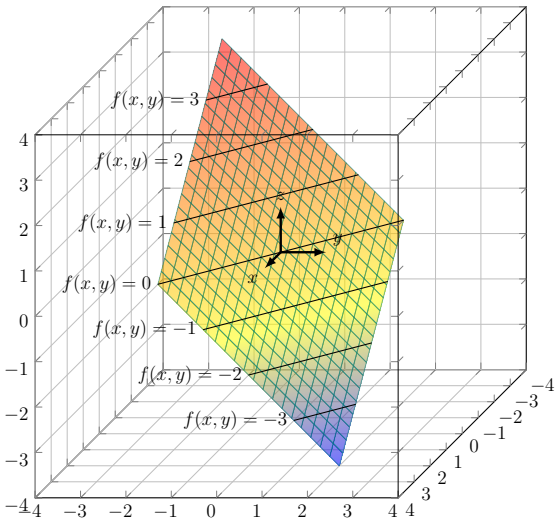
I.2 Fonctions (continues) de $\mathbb{R}^2$ dans $\mathbb{R}$.

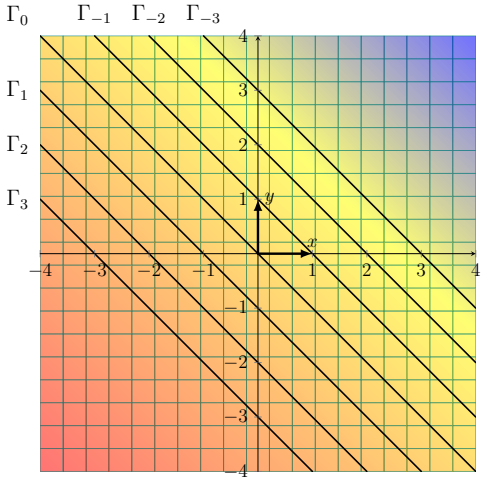
Définition I.14 (Fonction à deux variables)**.** *On a appelle* ***fonction à deux variables*** *une application d'un ensemble* $E \subset \mathbb{R}^2$ *dans* $\mathbb{R}$.
Son ***graphe*** *est la surface* $S = \{(x, y, f(x, y)) \,|\, (x, y) \in E\}$.
Si $\lambda \in f(E)$, *on appelle* ***ligne (ou courbe) de niveau*** *(associée à la valeur* λ*) l'ensemble :* $\Gamma_\lambda = f^{-1}(\{\lambda\}) = \{(x, y) \,|\, (x, y) \in E,\ f(x, y) = \lambda\}$.

Remarque I.15. *En général, comme on le verra dans les exemples, les lignes de niveau sont des courbes, mais ce n'est pas toujours le cas. Par exemple, si* f *est la fonction nulle sur* $\mathbb{R}^2$, *alors* $\Gamma_0 = \{(x, y) \,|\, x, y \in \mathbb{R}\}$ *est le plan* $\mathbb{R}^2$.
Le cas général se comprend assez bien : on intersecte le graphe de f *(qui se ressemble localement à un plan) avec le plan d'équation* $z = \lambda$, *ce qui donne localement une intersection de deux plans distincts, donc une droite. Et on garde la même structure en la projetant sur le plan d'équation* $z = 0$, *ce qui donne bien une courbe.*
Et c'est la méthode générale pour comprendre graphiquement les courbes de niveaux : la courbe Γ_λ *est la projection orthogonale (pour le produit scalaire canonique de* $\mathbb{R}^3$*) sur le plan d'équation* $z = 0$ *de l'intersection du graphe de* f *avec le plan d'équation* $z = \lambda$.

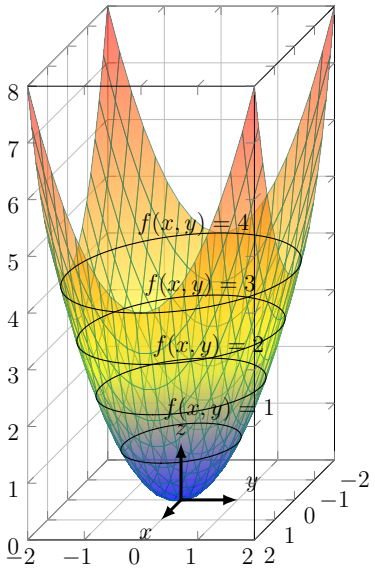
Exemples I.16.

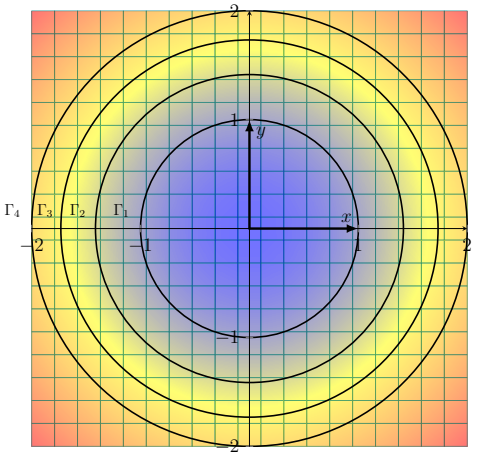
1. *Le plan d'équation $x+y+z=0$ est le graphe de la fonction :* $f : \begin{cases} \mathbb{R}^2 & \to & \mathbb{R} \\ (x,y) & \mapsto & -x-y \end{cases}$. *La ligne de niveau associée à la valeur 0 est :* $\Gamma_0 = \{(a,-a) \,|\, a \in \mathbb{R}\} = \{(x,y) \in \mathbb{R}^2 \,|\, x+y=0\}$ *(qui est même une droite). Et plus généralement, pour tout $\lambda \in \mathbb{R}$ on a :* $\Gamma_\lambda = \{(a-\lambda,-a) \,|\, a \in \mathbb{R}\} = \{(x,y) \in \mathbb{R}^2 \,|\, x+y+\lambda=0\}$. *Donc les lignes de niveaux sont exactement les droites du plan de pente -1.*





2. *La fonction* $g : \begin{cases} \mathbb{R}^2 & \to & \mathbb{R} \\ (x,y) & \mapsto & x^2+y^2 \end{cases}$ *a pour graphe l'hyperboloïde de révolution d'axe (Oz) d'équation : $z = x^2+y^2$.*
Pour tout $\lambda \in \mathbb{R}_+$, la ligne de niveau associée est un cercle : $\Gamma_\lambda = \{(x,y) \,|\, x^2+y^2 = \lambda\}$. *Et les lignes de niveau sont même exactement les cercles de centre $(0,0)$, comme* $\mathrm{Img} = \mathbb{R}_+$.





Proposition I.17. *L'ensemble des courbes de niveau non vides forme une partition de l'ensemble de définition de f.*

Remarque I.18. *La partition correspond à la relation d'équivalence sur D_f définie par :*

$$(x,y) \sim (x',y') \Leftrightarrow f(x,y) = f(x',y').$$

Définition I.19 (Continuité d'une fonction à deux variables)**.** *Une fonction à deux variables f définie sur un ensemble E est dite* ***continue*** *en $a \in E$ si :*

$$\forall \varepsilon > 0,\ \exists \eta > 0,\ \forall (x,y) \in E,\ \|(x-y)-a\| \leq \eta \Rightarrow |f(x,y)-f(a)| \leq \varepsilon.$$

Remarque I.20. *Les inégalités qui apparaissent dans l'implication peuvent être remplacées par des inégalités strictes sans changer la définition. Et on peut ainsi reformuler la définition avec des boules (ouvertes ou fermées) :*

$$\forall \varepsilon > 0,\ \exists \eta > 0,\ f\left(B_o(a,\eta)\right) \subset B_o(f(a),\varepsilon)$$

où $B_o(a,\eta) = \{(x,y) \in \mathbb{R}^2 \,|\, \|(x,y)-a\| < \eta\}$ *(boule ouverte au sens de* $\mathbb{R}^2$*) et* $B_o(f(a),\varepsilon) = \{x \in \mathbb{R} \,|\, |x-f(a)| < \varepsilon\} =]f(a)-\varepsilon; f(a)+\varepsilon[$ *(boule ouverte au sens de* $\mathbb{R}$*).*

Définition I.21. *Une fonction à deux variable est dite* ***continue*** *si elle est continue en tout point de son ensemble de définition.*

Théorème I.22. *Si* $f : U \to \mathbb{R}$ *est une fonction à deux variables définie sur* U *ouvert de* $\mathbb{R}^2$*, alors* f *est continue si, et seulement si, l'image réciproque de tout ouvert (au sens de* $\mathbb{R}$*) est un ouvert (au sens de* $\mathbb{R}^2$*).*

Remarque I.23. *Que ce soit pour le théorème ou pour la définition, on retrouve une situation analogue à celle sur* $\mathbb{R}$ *: l'image réciproque par une application continue d'un voisinage est un voisinage. Le point clé de la démonstration du théorème est que l'on peut écrire un ouvert (de* $\mathbb{R}$ *comme de* $\mathbb{R}^2$*) comme une union (éventuellement infinie) de boules ouvertes, et qu'une union (finie ou non) d'ouverts est un ouvert.*

Exemple I.24. *La fonction* f *définie sur* $\mathbb{R}^2$ *par :*

$$f : \left\{ \begin{array}{ccc} \mathbb{R}^2 & \to & \mathbb{R} \\ (x,y) & \mapsto & \left\{ \begin{array}{lll} \dfrac{xy}{x^2+y^2} & si & (x,y) \neq (0,0) \\ 0 & si & (x,y) = (0,0) \end{array} \right. \end{array} \right.$$

n'est pas continue en $(0,0)$*.*
On peut voir que :

- *si* $x \neq 0$ *:* $f(x,0) = 0 \underset{x\to 0}{\to} 0$ *;*
- *si* $y \neq 0$ *:* $f(0,y) = 0 \underset{y\to 0}{\to} 0$*.*

Donc la seule valeur de $f(0,0)$ *pour que* f *soit continue serait* 0*.*
Soit $(x,y) \in \mathbb{R}^2 \setminus \{(0,0)\}$*. Considérons* $\rho \geq 0$ *et* $\theta \in \mathbb{R}$ *tels que :* $(x,y) = (\rho\cos(\theta), \rho\sin(\theta))$ *(ce qui revient à raisonner en coordonnées polaires). Alors faire tendre* (x,y) *vers* $(0,0)$ *revient à faire tendre* ρ *vers* 0*.*
Mais on a : $f(\rho\cos(\theta), \rho\sin(\theta)) = \dfrac{\rho^2\cos(\theta)\sin(\theta)}{\rho^2} = \cos(\theta)\sin(\theta)$*.*
Et on trouve par exemple pour $\theta = \dfrac{\pi}{4}$ *que :*

$$f(\rho\cos(\theta), \rho\sin(\theta)) = \frac{1}{2} \underset{\rho\to 0}{\not\to} 0 = f(0,0)$$

ce qui montre bien que f *n'est pas continue en* 0*.*

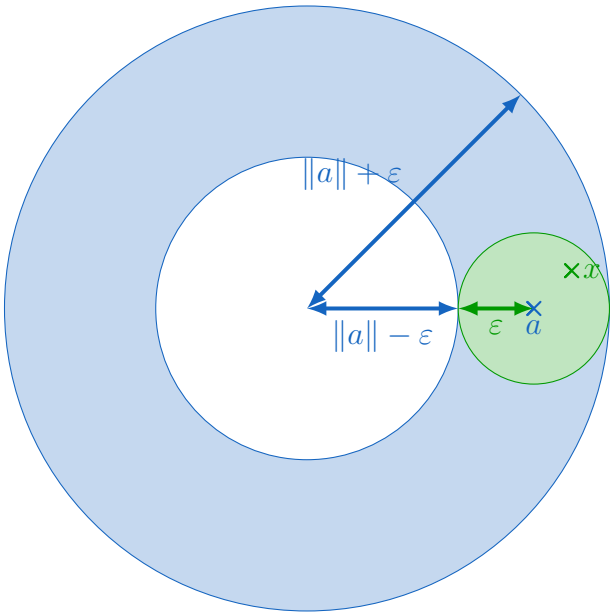
Remarque I.25. *L'utilisation du passage en coordonnées polaires est souvent efficace pour étudier la continuité d'une fonction en* $(0,0)$*. Cela permet de se ramener à la recherche d'une limite pour* ρ *tendant vers* 0*, de manière indépendante du choix de* θ*.*
Et on peut se ramener à cette situation dans le cas général : si on veut étudier la continuité en $a \in \mathbb{R}^2$*, on pose* $(x,y) = a + (\rho\cos(\theta), \rho\sin(\theta))$*.*
Le point important est que l'on veut tendre vers a *(ou vers* $(0,0)$ *si on reprend l'exemple précédent) suivant toutes les directions. Et même avec des chemins tortueux (ce qui revient à faire varier* θ*), en prenant seulement garde au fait que* ρ *tend vers* 0*.*

Exemples I.26.

1. *Les fonctions constantes sont continues : on peut voir que, dans la définition, tout η convient, peu importe la valeur de ε.*
2. *La norme* $\|\cdot\| : \left\{ \begin{array}{ccc} \mathbb{R}^2 & \to & \mathbb{R} \\ x & \mapsto & \|x\| \end{array} \right.$ *est une application continue.*

   Par inégalité triangulaire, on a en effet pour tout $x, a \in \mathbb{R}^2$ et tout $\varepsilon > 0$ que :

$$\|x - a\| \leq \varepsilon \Rightarrow |\|x\| - \|a\|| \leq \varepsilon.$$



3. *Les projections :*

$$\left\{ \begin{array}{ccc} \mathbb{R}^2 & \to & \mathbb{R} \\ (x,y) & \mapsto & x \end{array} \right. \text{ et } \left\{ \begin{array}{ccc} \mathbb{R}^2 & \to & \mathbb{R} \\ (x,y) & \mapsto & y \end{array} \right.$$

   sont également continues.

   Par exemple, pour la première, on a pour tous $x, y, a, b \in \mathbb{R}$:

$$\|(x,y) - (a,b)\| = \sqrt{(x-a)^2 + (y-b)^2} \geq \sqrt{(x-a)^2} = |x - a|.$$

   Et ainsi, pour tout $\varepsilon > 0$:

$$\|(x,y) - (a,b)\| \leq \varepsilon \Rightarrow |x - a| \leq \varepsilon.$$

Remarque I.27. *Le dernier exemple s'inscrit dans un résultat plus général : toute application linéaire sur un espace de dimension finie est continue.*

Proposition I.28. *La somme, le produit, le quotient, la composée et la combinaison linéaire d'applications continues (à deux variables ou à variables réelles) sont continues dès lors qu'elles sont bien définies.*

Démonstration. Se montre comme dans le cas réel. □

Corollaire I.29. *Les fonctions polynomiales sur $\mathbb{R}^2$, c'est-à-dire de la forme : $(x,y) \mapsto \sum_{i=0}^{n} \sum_{j=0}^{m} a_{i,j} x^i y^j$ pour $n, m \in \mathbb{N}$ et $(a_{i,j})$ famille de réels, sont continues sur $\mathbb{R}^2$.*

Démonstration. C'est directement une combinaison linéaire de produits itérés des applications $(x,y) \mapsto x$ et $(x,y) \mapsto y$. □

Corollaire I.30. *Si f, g sont des fonctions continues sur $\mathbb{R}$ (ou un sous-ensemble de $\mathbb{R}$), alors les fonctions $(x,y) \mapsto f(x) + g(y)$ et $(x,y) \mapsto f(x) \cdot g(y)$ sont continues sur leur ensemble de définition.*

Démonstration. Par continuité d'une composée, puis par continuité d'une somme ou d'un produit, en composant f et g avec les applications $(x,y) \mapsto x$ et $(x,y) \mapsto y$ pour voir que $(x,y) \mapsto f(x)$ et $(x,y) \mapsto g(y)$ sont continues (en tant que fonctions à deux variables). □

II Dérivées partielles

II.1 Fonctions partielles et dérivées partielles

Définition II.1 (Fonctions partielles)**.** *Si $f : U \to \mathbb{R}$ pour $U \subset \mathbb{R}^2$ est une fonction à deux variables, et $(x_0, y_0) \in U$, on appelle* ***première fonction partielle*** *(resp. seconde fonction partielle) de f la fonction $x \mapsto f(x, y_0)$ (resp. la fonction $y \mapsto f(x_0, y)$.*

Remarque II.2. *En pratique, on travaillera avec des fonctions définies sur des ouverts. Si on reprend les notations, et que l'on note $r > 0$ tel que $B_o((x_0, y_0), r) \subset U$, alors les fonction partielles de f sont définies sur les intervalles $]x_0 - r; x_0 + r[$ et $]y_0 - r, y_0 + r[$, ce qui permet de faire une étude locale en x_0 et en y_0 (étude de dérivabilité par exemple). Il suffit en fait que U soit un voisinage de (x_0, y_0).*

Définition II.3 (Dérivées partielles)**.** *Avec les mêmes notations, et en supposant U ouvert, on dit que f admet une* ***dérivée partielle*** *en (x_0, y_0) suivant la première (resp. la seconde) variable si la première (resp. la seconde) fonction partielle de f en y_0 (resp. en x_0) est dérivable en x_0 (resp. en y_0).*
On note alors $\dfrac{\partial f}{\partial x}(x_0, y_0)$ et $\dfrac{\partial f}{\partial y}(x_0, y_0)$ les nombres dérivés ainsi obtenus, appelés dérivées partielles de f.

Remarque II.4. *Les dérivées partielles d'une fonction à deux variables s'expriment comme dérivées de fonctions à variable réelle, et donc comme limite de taux d'accroissement. On a concrètement :*

$$\begin{cases} \dfrac{\partial f}{\partial x}(x_0, y_0) = \lim\limits_{x \to x_0} \dfrac{f(x, y_0) - f(x_0, y_0)}{x - x_0} = \lim\limits_{h \to 0} \dfrac{f(x_0 + h, y_0) - f(x_0, y_0)}{h} \\ \dfrac{\partial f}{\partial y}(x_0, y_0) = \lim\limits_{y \to y_0} \dfrac{f(x_0, y) - f(x_0, y_0)}{y - y_0} = \lim\limits_{h \to 0} \dfrac{f(x_0, y_0 + h) - f(x_0, y_0)}{h} \end{cases}.$$

Remarque II.5. *Le fait de ne regarder que les fonctions partielles fait perdre beaucoup d'information par rapport à f. Par exemple, une fonction qui admet des dérivées partielles suivant les deux variables n'est même pas nécessairement continue.*
On peut reprendre la fonction f définie sur $\mathbb{R}^2$ par :

$$f : \begin{cases} \mathbb{R}^2 & \to & \mathbb{R} \\ (x, y) & \mapsto & \begin{cases} \dfrac{xy}{x^2 + y^2} & si \quad (x, y) \neq (0, 0) \\ 0 & si \quad (x, y) = (0, 0) \end{cases} \end{cases}$$

dont on a vu qu'elle n'est pas continue en $(0, 0)$.
Ses fonctions partielles en $(0, 0)$ sont les fonctions :

$$\varphi : x \mapsto f(x, 0) = 0 \text{ et } \psi : y \mapsto f(0, y) = 0$$

qui sont constantes, donc dérivables de dérivée nulle. Et ainsi f admet bien des dérivées partielles en 0, et plus précisément :

$$\frac{\partial f}{\partial x}(0, 0) = \varphi'(0) = 0 \text{ et } \frac{\partial f}{\partial y}(0, 0) = \psi'(0) = 0.$$

Proposition II.6. *La somme, le produit, le quotient, la composée et la combinaison linéaire d'applications admettant des dérivées (partielles pour les fonctions à deux variables, classique pour les fonctions à variables réelles) admettent également des dérivées (au même sens) dès lors qu'elles sont bien définies.*

Remarque II.7. *Le calcul explicite de ces dérivées (partielles ou non) se fait en reprenant les définitions, et en passant éventuellement par les fonctions partielles, ce qui ramène le calcul à des dérivées de fonctions à variables réelles, donc on connaît le comportement vis-à-vis des produits, quotients, combinaisons linéaires, etc.*

Définition II.8 (Gradient)**.** *Si $f : U \to \mathbb{R}$, pour U ouvert de $\mathbb{R}^2$, admet des dérivées partielles en $(x_0, y_0) \in U$, on appelle* ***gradient de*** *f* ***en*** *(x_0, y_0) le vecteur :*

$$\nabla f(x_0, y_0) = \left(\frac{\partial f}{\partial x}(x_0, y_0), \frac{\partial f}{\partial y}(x_0, y_0) \right).$$

Remarque II.9. *Le principal intérêt du gradient est de pouvoir manipuler simultanément les deux dérivées partielles d'une fonction. Et la dérivation de combinaisons linéaires ou de produits s'énonce alors facilement. Par exemple, si f, g sont deux fonctions à deux variables admettant des dérivées partielles (donc un gradient) en (x_0, y_0), et $\lambda, \mu \in \mathbb{R}$, alors :*

$$\nabla(\lambda f + \mu g)(x_0, y_0) = \lambda \nabla f(x_0, y_0) + \mu \nabla g(x_0, y_0) \text{ et } \nabla(f \cdot g)(x_0, y_0) = g(x_0, y_0)\nabla f(x_0, y_0) + f(x_0, y_0)\nabla g(x_0, y_0).$$

II.2 Fonctions de classe $\mathcal{C}^1$ sur un ouvert de $\mathbb{R}^2$

Définition II.10 (Fonction de classe $\mathcal{C}^1$)**.** *Une fonction à deux variables $f : U \to \mathbb{R}$, pour U ouvert de $\mathbb{R}^2$ est dite (de classe) $\mathcal{C}^1$ si elle admet des dérivées partielles continues sur U.*

Remarque II.11. *Les dérivées partielles d'une fonction à deux variables sont également des fonctions à deux variables : c'est donc dans ce sens qu'on entend la continuité.*

Proposition II.12. *La somme, le produit, le quotient, la composée et la combinaison linéaire d'applications $\mathcal{C}^1$ (à deux variables ou à variables réelles) sont $\mathcal{C}^1$ dès lors qu'elles sont bien définies.*

Exemples II.13.

1. *Si f, g sont deux fonctions (à variable réelle) $\mathcal{C}^1$ sur $\mathbb{R}$, alors les applications :*

   $$\varphi : (x, y) \mapsto f(x) + g(y) \text{ et } \psi : (x, y) \mapsto f(x)g(y)$$

   sont $\mathcal{C}^1$ sur $\mathbb{R}^2$.
   On a en effet les dérivées partielles :

   $$\left\{ \begin{array}{l} \dfrac{\partial \varphi}{\partial x}(x, y) = f'(x) \\ \dfrac{\partial \varphi}{\partial y}(x, y) = g'(y) \end{array} \right. \quad \text{et} \quad \left\{ \begin{array}{l} \dfrac{\partial \psi}{\partial x}(x, y) = g(y)f'(x) \\ \dfrac{\partial \psi}{\partial y}(x, y) = f(x)g'(y) \end{array} \right.$$

   qui sont bien des fonctions continues sur $\mathbb{R}^2$.
2. *Considérons l'application $f : (x, y) \mapsto ax + by$, pour $a, b \in \mathbb{R}$ (c'est-à-dire que f est l'application linéaire de $\mathbb{R}^2$ dans $\mathbb{R}$ dont la matrice dans les bases canoniques est $\begin{pmatrix} a & b \end{pmatrix}$).*
   Alors on a les dérivées partielles :

   $$\frac{\partial f}{\partial x}(x, y) = a \text{ et } \frac{\partial f}{\partial y}(x, y) = b$$

   qui sont bien continues (en tant que fonctions constantes). Et on a même : $\nabla f(x, y) = (a, b)$.
3. *Si $f : (x, y) \mapsto \sum_{i,j} a_{i,j} x^i y^j$ est une fonction polynomiale, alors elle admet les dérivées partielles :*

   $$\frac{\partial f}{\partial x}(x, y) = \sum_{i \geq 1, j} a_{i,j} \cdot i \cdot x^{i-1} y^j \text{ et } \frac{\partial f}{\partial y}(x, y) = \sum_{j \geq 1, i} a_{i,j} \cdot j \cdot x^i y^{j-1}$$

   qui sont continues (en tant que fonctions polynomiales), donc les fonctions polynomiales (sur $\mathbb{R}^2$) sont de classe $\mathcal{C}^1$.

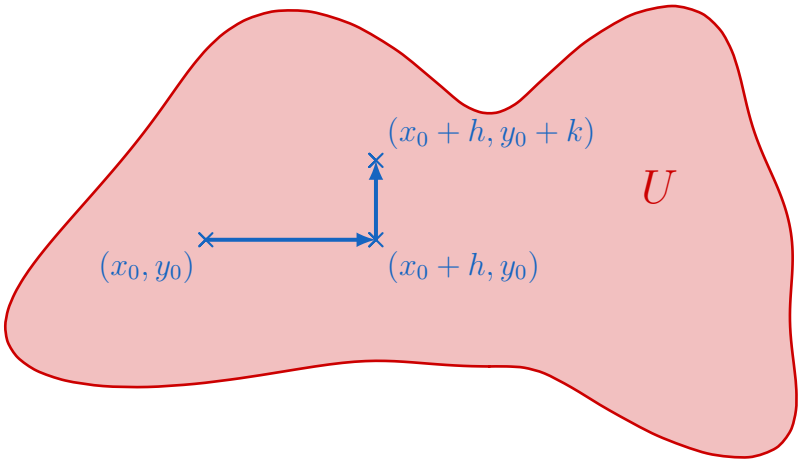
II.3 Formules de Taylor

Théorème II.14 (Formule de Taylor à l'ordre 1)**.** *Soit f une fonction de classe $\mathcal{C}^1$ sur un ouvert U de $\mathbb{R}^2$. On considère $(x_0, y_0) \in U$. Alors pour tout $(h, k) \in \mathbb{R}^2$ tel que $(x_0 + h, y_0 + k) \in U$, on a :*

$$f(x_0 + h, y_0 + k) = f(x_0, y_0) + \frac{\partial f}{\partial x}(x_0, y_0)h + \frac{\partial f}{\partial y}(x_0, y_0)k + \mathrm{o}\left(\|(h, k)\|\right)$$

où $\mathrm{o}\left(\|(h, k)\|\right) = \|(h, k)\| \cdot \varepsilon(h, k)$ *avec* $\varepsilon(h, k) \underset{(h,k)\to(0,0)}{\to} 0$.

Démonstration. en intégrant les inégalités de continuité sur un chemin bien choisi



□

Remarques II.15.

1. *Le fait de travailler sur un ouvert U fait que l'on peut légitimement étudier $f(x, y)$ pour (x, y) proche de (x_0, y_0), c'est-à-dire pour (h, k) proche de $(0, 0)$.*
2. *Si on reprend les mêmes notations, la formule de Taylor s'exprime à l'aide du gradient comme :*

$$f\left((x_0, y_0) + (h, k)\right) = f\left(x_0, y_0\right) + \langle \nabla f(x_0, y_0), (h, k)\rangle + \mathrm{o}\left(\|(h, k)\|\right)$$

Corollaire II.16. *Une fonction $\mathcal{C}^1$ est continue.*

Démonstration. En passant à la limite dans la formule de Taylor. □

Remarques II.17.

1. *Ces résultats marque la différence entre les fonctions à deux variables et les fonctions à variable réelle : alors qu'il suffisait d'être dérivable pour être continu et avoir un développement limité d'ordre 1 dans le cas réel, les dérivées partielles ne suffisent pas pour les fonctions à deux variables (qui ne sont même pas continues a priori).*
2. *On peut s'intéresser aux fonctions qui coïncident avec leur développement de Taylor à l'ordre 1. Dans le cas réel, il s'agissait des fonctions affines. Dans le cas des fonctions à deux variables aussi : il s'agit des fonctions affines sur $\mathbb{R}^2$, c'est à dire de la forme $(x, y) \mapsto a + f(x, y)$, où a est un réel quelconque, et f est une forme linéaire sur $\mathbb{R}^2$.*

Définition II.18 (Plan tangent)**.** *Si f est une fonction de classe $\mathcal{C}^1$ sur un ouvert U de $\mathbb{R}^2$, et $(x_0, y_0) \in U$, on appelle* ***plan tangent*** *à la surface d'équation $z = f(x, y)$ le plan d'équation :*

$$z - z_0 = \frac{\partial f}{\partial x}(x_0, y_0)(x - x_0)\frac{\partial f}{\partial y}(x_0, y_0)(y - y_0)$$

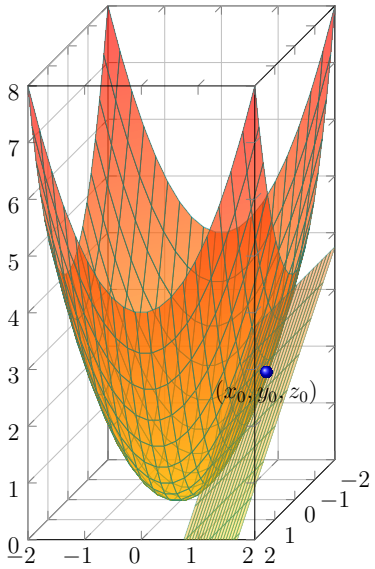
où on a posé $z_0 = f(x_0, y_0)$.

Remarque II.19. *Du fait de la formule de Taylor, le plan tangent correspond à la meilleure approximation du graphe de f (qui n'est autre que la surface d'équation $z = f(x, y)$) par un plan. Le terme de plan "tangent" permet de faire l'analogie avec le cas réel : la dérivée d'une fonction permet d'exprimer sa tangente, qui est la droite qui approxime le mieux sa courbe.*

Exemple II.20. *Considérons la fonction : $f : \left\{ \begin{array}{ccc} \mathbb{R}^2 & \to & \mathbb{R} \\ (x,y) & \mapsto & x^2+y^2 \end{array} \right.$, qui est de classe $\mathcal{C}^1$ (en tant que fonction polynomiale). Alors pour tout $(x, y) \in \mathbb{R}^2$ on a : $\nabla f(x, y) = (2x, 2y)$.*
Le plan tangent au point (x_0, y_0) est donc le plan d'équation :

$$z - (x_0^2 + y_0^2) = 2x_0(x - x_0) + 2y_0(y - y_0)$$

c'est-à-dire : $2x_0x + 2y_0y - z = x_0^2 + y_0^2$.



III Manipulation de fonctions de classe $\mathcal{C}^1$

III.1 Dérivée directionnelle

Définition III.1 (Dérivée directionnelle)**.** *Si $f : U \to \mathbb{R}$ pour U ouvert de $\mathbb{R}^2$, et $v \in \mathbb{R}^2$, on dit que f a une **dérivée (directionnelle)** suivant le vecteur v en $(x_0, y_0) \in U$ si la quantité :*

$$\lim_{t \to 0} \frac{f((x_0, y_0) + tv) - f(x_0, y_0)}{t}$$

existe et est finie.
On note alors $\partial_v f(x_0, y_0)$ cette limite.

Remarque III.2. *La dérivée directionnelle revient à la dérivée en 0 de la fonction (réelle) $t \mapsto f((x_0, y_0) + tv)$. Cette fonction est d'ailleurs bien définie en 0, comme on travaille sur un ouvert, et donc pour t suffisamment petit on a bien $(x_0, y_0) + tv \in U$.*

Exemple III.3. *Pour $v = (1, 0)$, on a pour tout $t \neq 0$:*

$$\frac{f((x_0, y_0) + tv) - f(x_0, y_0)}{t} = \frac{f(x_0 + t, y_0) - f(x_0, y_0)}{t}$$

et donc f a une dérivée directionnelle suivant $v = (1, 0)$ en (x_0, y_0) si, et seulement si, elle a une première dérivée partielle en (x_0, y_0).

De même, elle a une seconde dérivée partielle si, et seulement si, elle a une dérivée suivant le vecteur $(0,1)$.
Et on a même égalité entre dérivée partielle et dérivée directionnelle correspondante dans ces deux cas, sous réserve d'existence.

Proposition III.4. *Si f est de classe $\mathcal{C}^1$ sur un ouvert U de $\mathbb{R}^2$, alors elle admet des dérivées partielles suivant tout vecteur en tout point. Plus précisément, la dérivée suivant le vecteur $u=(u_1,u_2)$ en (x_0,y_0) est :*

$$\partial_u f(x_0,y_0) = \langle \nabla f(x_0,y_0), u\rangle = \frac{\partial f}{\partial x}(x_0,y_0)u_1 + \frac{\partial f}{\partial y}(x_0,y_0)u_2.$$

Démonstration. Par formule de Taylor. □

Remarque III.5. *Le terme de dérivée directionnel est un peu trompeur, puisque ce n'est pas seulement la direction de u qui importe, mais aussi son sens et sa norme. Plus précisément, si $u\in\mathbb{R}^2$ et $\lambda\in\mathbb{R}$, avec f qui admet une dérivée directionnelle suivant le vecteur u en (x_0,y_0), alors elle admet une dérivée directionnelle suivant le vecteur λu, et on a :*

$$\partial_{\lambda u} f(x_0,y_0) = \lambda \partial_u f(x_0,y_0).$$

III.2 Utilisation de courbes paramétrées

Proposition III.6. *Soient $f:U\to\mathbb{R}$, pour U ouvert de $\mathbb{R}^2$, une fonction de classe $\mathcal{C}^1$, et $x,y:I\to\mathbb{R}$, pour I intervalle de $\mathbb{R}$, deux fonctions de classe $\mathcal{C}^1$ telles que : $\forall t\in I,\ (x(t),y(t))\in U$. Alors la fonction $F:t\mapsto f(x(t),y(t))$ est $\mathcal{C}^1$ sur I avec :*

$$\forall t\in I,\ F'(t) = \frac{\partial f}{\partial x}(x(t),y(t))\cdot x'(t) + \frac{\partial f}{\partial y}(x(t),y(t))\cdot y'(t) = \langle \nabla f(x(t),y(t)), (x'(t),y'(t))\rangle .$$

Démonstration. Par formule de Taylor de x et y, qu'on réinjecte dans celle de f, on trouve une formule de Taylor pour F. Ceci donne bien la dérivée de F annoncée, qui est bien continue (comme somme, produit et composée de fonctions continues), ce qui donne bien que F est $\mathcal{C}^1$. □

Remarque III.7. *L'idée derrière est de bien choisir les fonctions x et y pour que l'ensemble $\{(x(t),y(t))\,|\,t\in I\}$ (qui est en toute généralité une courbe) donne un ensemble intéressant.*
Par exemple, si on considère le cercle de centre (x_0,y_0) et de rayon $r\in\mathbb{R}$, on peut utiliser l'un des paramétrages suivants :

$$\begin{cases} x(t) &= x_0 + r\cos(t) \\ y(t) &= y_0 + r\sin(t) \end{cases},\ t\in[0;2\pi] \text{ ou } \begin{cases} x(t) &= x_0 + r\dfrac{1-t^2}{1+t^2} \\ y(t) &= y_0 + r\dfrac{2t}{1+t^2} \end{cases},\ t\in\mathbb{R}$$

Exemple III.8. *Reprenons la fonction $f:(x,y)\mapsto x^2+y^2$. Prenons $r\in\mathbb{R}$, et considérons x,y définies sur $\mathbb{R}$ par : $\forall t\in\mathbb{R}$, $\begin{cases} x(t) &= r\cos(t) \\ y(t) &= r\sin(t) \end{cases}$ (c'est-à-dire que l'on utilise une paramétrisation du cercle de centre $(0,0)$ de rayon $|r|$).*
Alors x,y sont $\mathcal{C}^1$ sur $\mathbb{R}$ avec : $\forall t\in\mathbb{R}$, $\begin{cases} x'(t) &= -r\sin(t) \\ y'(t) &= r\cos(t) \end{cases}$. De sorte que la fonction $F:t\mapsto f(x(t),y(t))$ est $\mathcal{C}^1$ sur $\mathbb{R}$ avec :

$$\forall t\in\mathbb{R},\ F'(t) = \langle \nabla f(x(t),y(t)), (x'(t),y'(t))\rangle = -2r^2\cos(t)\sin(t) + 2r^2\cos(t)\sin(t) = 0$$

donc F est constante.
Ce qui est bien cohérent avec l'étude des lignes de niveaux de f, dont la projection sur le plan (Oxy) sont exactement les cercles de centre O.

Corollaire III.9. *Si $\gamma : I \to U$ est une courbe paramétrée de classe $\mathcal{C}^1$, et $f : U \to \mathbb{R}$ est une fonction à deux variables de classe $\mathcal{C}^1$, alors $f \circ \gamma$ est de classe $\mathcal{C}^1$ sur I, avec :*

$$\forall t \in I,\ (f \circ \gamma)'(t) = \langle \nabla f(\gamma(t)), \gamma'(t) \rangle .$$

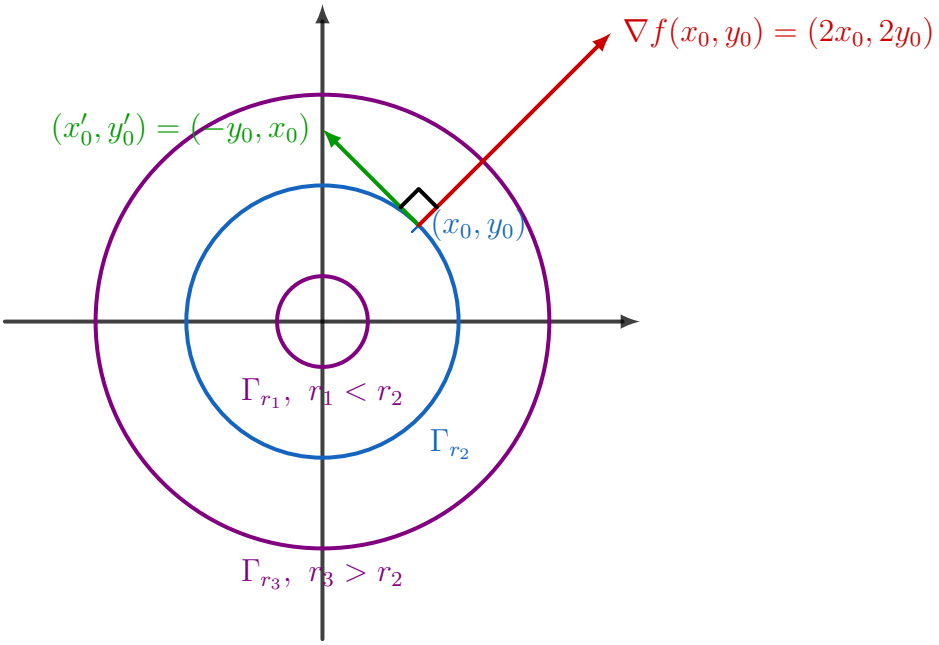
Remarque III.10. *Ce n'est qu'une reformulation du résultat précédent, mais cela permet de retrouver sensiblement la même formule que la dérivée d'une composée (pour les fonctions réelles), à la différence près que le produit usuel de $\mathbb{R}$ a été remplacé par le produit scalaire.*

Corollaire III.11. *Les gradients sont orthogonaux aux lignes de niveaux.*

Démonstration. Considérons $f : U \to \mathbb{R}$ de classe $\mathcal{C}^1$, pour U ouvert de $\mathbb{R}^2$, Γ_λ une ligne de niveau de f, et $\gamma : I \to U$ de classe $\mathcal{C}^1$ telle que : $\forall t \in I, \gamma(t) \in \Gamma_\lambda$.
Alors l'application $F = f \circ \gamma$ est constante, de valeur λ. Donc sa dérivée est nulle, ce qui donne que : $\langle \nabla f(\gamma(t)), \gamma'(t) \rangle = 0$, donc $\nabla f(\gamma(t))$ et $\gamma'(t)$ sont bien orthogonaux pour tout t.
Le premier vecteur est directement le gradient, tandis que le second est tangent à la courbe γ. Ce qui donne bien le résultat. □

Remarque III.12. *Plus généralement, les valeurs prises par f grandissent d'autant plus vite sur une courbe que celle-ci va dans le même sens que le gradient.*

Exemple III.13. *Reprenons la fonction $f : (x, y) \mapsto x^2 + y^2$ et les notations de l'exemple précédent. Suivant la paramétrisation utilisée, le vecteur tangent à Γ_{r^2} en (x_0, y_0) est le vecteur $(-y_0, x_0)$, qui est bien orthogonal au gradient à f en (x_0, y_0) puisque l'on a : $\nabla f(x_0, y_0) = (2x_0, 2y_0)$.*



Corollaire III.14. *Soient f, φ, ψ des fonctions à deux variables de classe $\mathcal{C}^1$, telles que : $g : (u, v) \mapsto f(\varphi(u, v), \psi(u, v))$ est bien définie. Alors g est de classe $\mathcal{C}^1$, avec :*

$$\frac{\partial g}{\partial x}(u,v) = \frac{\partial f}{\partial x}(\varphi(u,v),\psi(u,v))\frac{\partial \varphi}{\partial x}(u,v) + \frac{\partial f}{\partial y}(\varphi(u,v),\psi(u,v))\frac{\partial \psi}{\partial x}(u,v)$$

$$\frac{\partial g}{\partial y}(u,v) = \frac{\partial f}{\partial x}(\varphi(u,v),\psi(u,v))\frac{\partial \varphi}{\partial y}(u,v) + \frac{\partial f}{\partial y}(\varphi(u,v),\psi(u,v))\frac{\partial \psi}{\partial y}(u,v)$$

Démonstration. On applique le résultat précédent avec $x : t \mapsto \varphi(u + t, v)$ et $\psi : t \mapsto \psi(u + t, v)$ pour avec la première dérivée partielle, et avec $x : t \mapsto \varphi(u, v + t)$ et $\psi : t \mapsto \psi(u, v + t)$ pour la seconde, ce qui donne bien les expressions des dérivées partielles de g, qui sont bien $\mathcal{C}^1$ comme on reconnaît des sommes, produits ou composées de fonctions continues. □

Remarques III.15.

1. *Il faut bien prendre garde au fait que la dérivée partielle* $\dfrac{\partial g}{\partial x}$ *veut dire que l'on dérive par rapport à la première variable de* g. *Avec les notations de l'énoncé, cela revient à dériver l'expression* $f(\varphi(u,v),\psi(u,v))$ *par rapport à* u. *Et pour éviter les confusions, on pourra parfois écrire* $\dfrac{\partial g}{\partial u}$ *au lieu de* $\dfrac{\partial g}{\partial x}$.
2. *Comme les calculs de dérivées de composées dans le cas réel, l'intérêt est de simplifier un problème différentiel (d'équation différentiel ou de calcul d'intégrale) par un changement de variable adapté.*

Exemple III.16. *Considérons les applications* φ,ψ *définies par :*

$$\forall (r,\theta)\in\mathbb{R}_+^*\times]0;\pi[,\ (\varphi(r,\theta),\psi(r,\theta))=(r\cos(\theta),r\sin(\theta))$$

ce qui revient à paramétrer en polaire l'ensemble $\mathbb{R}\times\mathbb{R}_+^*$ *par des applications* $\mathcal{C}^1$.
On considère f *de classe* $\mathcal{C}^1$ *sur* $\mathbb{R}\times\mathbb{R}_+^*$, *et on définit la fonction* g *sur* $\mathbb{R}_+^*\times]0;\pi[$ *par :*

$$\forall (r,\theta)\in\mathbb{R}_+^*\times]0;\pi[,\ g(r,\theta)=f(r\cos(\theta),r\sin(\theta)).$$

Alors g *est de classe* $\mathcal{C}^1$ *sur* $\mathbb{R}_+^*\times]0;\pi[$ *et pour tout* $(r,\theta)\in\mathbb{R}_+^*\times]0;\pi[$ *on a :*

$$\begin{array}{rcl}
\dfrac{\partial g}{\partial r}(r,\theta) &=& \dfrac{\partial f}{\partial x}(r\cos(\theta),r\sin(\theta))\dfrac{\partial \varphi}{\partial r}(r,\theta)+\dfrac{\partial f}{\partial y}(r\cos(\theta),r\sin(\theta))\dfrac{\partial \psi}{\partial r}(r,\theta)\\
&=& \dfrac{\partial f}{\partial x}(r\cos(\theta),r\sin(\theta))\cos(\theta)+\dfrac{\partial f}{\partial y}(r\cos(\theta),r\sin(\theta))\sin(\theta)\\
\dfrac{\partial g}{\partial \theta}(r,\theta) &=& \dfrac{\partial f}{\partial x}(r\cos(\theta),r\sin(\theta))\dfrac{\partial \varphi}{\partial \theta}(r,\theta)+\dfrac{\partial f}{\partial y}(r\cos(\theta),r\sin(\theta))\dfrac{\partial \psi}{\partial \theta}(r,\theta)\\
&=& \dfrac{\partial f}{\partial x}(r\cos(\theta),r\sin(\theta))\cdot(-r\sin(\theta))+\dfrac{\partial f}{\partial y}(r\cos(\theta),r\sin(\theta))\cdot(r\cos(\theta))
\end{array}$$

Utilisons la fonction $g=f\circ(\varphi,\psi)$ *pour trouver toutes les fonctions* f *de classe* $\mathcal{C}^1$ *de* $\mathbb{R}\times\mathbb{R}_+^*$ *dans* $\mathbb{R}^2$ *telles que :*

$$\forall (x,y)\in\mathbb{R}\times\mathbb{R}_+^*,\ x\frac{\partial f}{\partial x}(x,y)+y\frac{\partial f}{\partial y}(x,y)=\sqrt{x^2+y^2}.$$

Considérons f *une fonction de classe* $\mathcal{C}^1$. *Alors elle vérifie l'équation précédente si, et seulement si, la fonction* g *construite ci-dessus vérifie :*

$$\forall (r,\theta)\in\mathbb{R}_+^*\times]0;\pi[,\ r\frac{\partial g}{\partial r}=\underbrace{r\cos(\theta)}_{=x}\frac{\partial f}{\partial x}(r\cos(\theta),r\sin(\theta))+\underbrace{r\sin(\theta)}_{=y}\frac{\partial f}{\partial x}(r\cos(\theta),r\sin(\theta))=\underbrace{\sqrt{x^2+y^2}}_{=r}$$

c'est-à-dire si, et seulement si, la fonction g *ainsi construite vérifie :*

$$\forall (r,\theta)\in\mathbb{R}_+^*\times]0;\pi[,\ \frac{\partial g}{\partial r}=1.$$

C'est le cas si, pour tout $\theta\in]0;\pi[$, *il existe un réel* λ_θ *(dépendant de* θ *a priori) tel que :*

$$\forall r\in\mathbb{R}_+^*,\ g(r,\theta)=r+\lambda_\theta.$$

Et donc les fonctions g *correspondant aux solutions sont exactement les fonctions de la forme :*

$$g:\left\{\begin{array}{rcl}\mathbb{R}_+^*\times]0;\pi[&\to& \mathbb{R}\\ (r,\theta) &\mapsto& r+h(\theta)\end{array}\right.$$

pour h fonction de classe $\mathcal{C}^1$ de $]0;\pi[$ dans $\mathbb{R}$.
On revient alors à f facilement, ce qui dit que les fonctions f cherchées sont toutes de la forme :

$$f : \left\{ \begin{array}{rcl} \mathbb{R} \times \mathbb{R}_+^* & \to & \mathbb{R} \\ (x,y) & \mapsto & \sqrt{x^2+y^2} + h\left(\text{Arccos}\left(\dfrac{x}{\sqrt{x^2+y^2}}\right)\right) \end{array} \right.$$

pour h fonction de classe $\mathcal{C}^1$ de $]0;\pi[$ dans $\mathbb{R}$.

Remarque III.17. *On a ici restreint les ensembles d'étude de sorte que l'application (φ,ψ) réalise une bijection de $\mathbb{R}_+^*\times]0;\pi[$ dans $\mathbb{R}\times\mathbb{R}_+^*$: ceci n'est pas obligatoire, comme pour les changements de variables, mais permet plus facilement de travailler dans les deux sens (passer de f à g et inversement). Sinon, il faudrait procéder par analyse–synthèse.*

III.3 Extrema

Définition III.18 (Extrema)**.** *Si f est définie sur un sous-ensemble A de $\mathbb{R}^2$, à valeurs dans $\mathbb{R}$, et $a \in A$, on dit que :*

1. *f possède un **maximum (global)** en a si :*

$$\forall x \in A,\ f(x) \leq f(a)$$

*et on dit de plus que maximum est **strict** si on a de plus : $f(x) = f(a) \Leftrightarrow x = a$;*

2. *f possède un **maximum local** en a s'il existe $\varepsilon > 0$ tel que $f|_{B_o(a,\varepsilon)\cap A}$ possède un maximum en a, c'est-à-dire si :*

$$\exists \varepsilon > 0,\ \forall x \in B_o(a,\varepsilon) \cap A,\ f(x) \leq f(a);$$

et ce maximum est dit strict s'il est strict au sens précédent pour $f|_{B_o(a,\varepsilon)\cap A}$ quitte à réduire la valeur de ε.

*On définit de manière analogue la notion de **minimum** (local ou global, strict ou non) en inversant l'inégalité précédente.*
*On parlera plus généralement d'**extremum** (local ou global, strict ou non).*

Définition III.19 (Point critique)**.** *Si f est une fonction de classe $\mathcal{C}^1$ sur un ouvert U de $\mathbb{R}^2$, et $a \in U$, on dit que f possède un **point critique** en a si : $\nabla f(a) = 0$, c'est-à-dire si :*

$$\frac{\partial f}{\partial x}(a) = \frac{\partial f}{\partial y}(a) = 0.$$

Théorème III.20. *Si f est définie sur un ouvert U de $\mathbb{R}^2$ et $a \in U$, tels que f possède un extremum en a et que f est $\mathcal{C}^1$ sur un voisinage de a, alors f admet un point critique en a.*

Démonstration. Il suffit d'utiliser le résultat correspondant pour les fonctions à variable réelle, qu'on applique aux fonctions partielles de f, qui sont bien $\mathcal{C}^1$ sur un voisinage de a et qui possèdent également un extremum en a. □

Remarques III.21.

1. *Comme sur $\mathbb{R}$, le fait d'avoir un point critique est une condition nécessaire mais non suffisante pour avoir un extremum. De plus, la nature de cet éventuel extremum nécessite de faire une étude plus poussée de f (par développement limités par exemple pour avoir un extremum local, ou par des jeux de réécriture pour un extremum global). Et du fait de l'équation du plan tangent, un point critique correspond à un point sur le graphe en lequel le plan tangent horizontal.*

2. *Le fait d'être $\mathcal{C}^1$ et de travailler sur un ouvert est fondamental. Ainsi, pour étudier les extrema d'une fonction qui ne serait pas $\mathcal{C}^1$ partout, et qui ne serait pas définit sur un ouvert, ou étudiera d'un côté les points en lesquels f n'est pas $\mathcal{C}^1$, et les points au bord (qui peuvent être des extrema sans être des points critiques), et dans un second temps les points critiques (qui sont les seuls lieux possibles d'existence d'extrema).*

Exemples III.22.

1. *Considérons* $f : \left\{ \begin{array}{ccc} \mathbb{R}^2 & \to & \mathbb{R} \\ (x,y) & \mapsto & x^2+y^2 \end{array} \right.$ *. Alors f est $\mathcal{C}^1$ sur $\mathbb{R}^2$, qui est un ouvert : tous les extrema de f sont des points critiques.*
Mais pour $(a,b) \in \mathbb{R}^2$, on a :

$$\nabla f(a,b) = 0 \Leftrightarrow (2a,2b) = (0,0) \Leftrightarrow a = b = 0$$

donc $(0,0)$ est le seul point critique de f, et donc le seul extremum possible.
Mais $f(0,0) = 0$, qui est un minimum global strict car :

$$\forall (x,y) \in \mathbb{R}^2,\ f(x,y) = x^2+y^2 \geq 0 \text{ et } f(x,y) = 0 \Leftrightarrow x^2+y^2 = 0 \Leftrightarrow x = y = 0.$$

2. *Soit* $f : \left\{ \begin{array}{ccc} \mathbb{R}^2 & \to & \mathbb{R} \\ (x,y) & \mapsto & 4x^2-4xy+y^2-6x+2y \end{array} \right.$ *. Alors f est de classe $\mathcal{C}^1$ sur l'ouvert $\mathbb{R}^2$ (en tant que fonction polynomiale), donc tous ses extrema sont des points critiques. Et on a :*

$$\forall (x,y) \in \mathbb{R}^2,\ \frac{\partial f}{\partial x} = 8x-4y-6 \text{ et } \frac{\partial f}{\partial y} = -4x+2y+2.$$

Pour tout $(a,b) \in \mathbb{R}^2$, on a donc :

$$\begin{array}{rcl} \nabla f(a,b) = 0 & \Leftrightarrow & \left\{ \begin{array}{rcl} 8a-4b-6 & = & 0 \\ -4a+2b+2 & = & 0 \end{array} \right. \\ & \Leftrightarrow & \left\{ \begin{array}{rcl} -2 & = & 0 \\ -4a+2b+2 & = & 0 \end{array} \right. \end{array}$$

et donc f n'admet pas de point critique, comme le dernier système n'a pas de solution.
Donc f ne possède pas d'extremum, peu importe sa nature.

3. *Soit* $f : \left\{ \begin{array}{ccc} \mathbb{R}^2 & \to & \mathbb{R} \\ (x,y) & \mapsto & x^2(1+y)^3+y^2 \end{array} \right.$ *. Alors f est $\mathcal{C}^1$ sur l'ouvert $\mathbb{R}^2$ (en tant que fonction polynomiale), donc tous ses extrema sont des points critiques. Et on a :*

$$\forall (x,y) \in \mathbb{R}^2,\ \frac{\partial f}{\partial x} = 2(1+y)^3 x \text{ et } \frac{\partial f}{\partial y} = 3x^2(1+y)^2+2y.$$

Pour tout $(a,b) \in \mathbb{R}^2$, on a donc :

$$\begin{array}{rcl} \nabla f(a,b) = 0 & \Leftrightarrow & \left\{ \begin{array}{rcl} 2(1+b)^3 a & = & 0 \\ 2a^2(1+b)^2+2b & = & 0 \end{array} \right. \\ & \Leftrightarrow & \left\{ \begin{array}{rcl} a & = & 0 \\ 2b & = & 0 \end{array} \right. \text{ ou } \left\{ \begin{array}{rcl} b & = & -1 \\ 2b & = & 0 \end{array} \right. \\ & \Leftrightarrow & a = b = 0 \end{array}$$

donc le seul point critique est $(0,0)$.

Pour étudier sa nature en tant qu'extremum éventuel, étudions $f(x,y)$ pour $(x,y) \in \mathbb{R}^2$ tendant vers $(0,0)$. Pour un tel (x,y), on a :

$$\begin{aligned} f(x,y) &= x^2(1+3y+3y^2+y^3)+y^2 \\ &= x^2+y^2+3x^2y+3y^2x^2+x^2y^3 \\ &= (x^2+y^2)\left(1+\frac{3x^2y+3y^2x^2+x^2y^3}{x^2+y^2}\right) \end{aligned}.$$

Mais on a aussi par inégalité classique : $|xy| \leq \dfrac{x^2+y^2}{2}$. Et donc par inégalité triangulaire on déduit que :

$$\left|\frac{3x^2y+3y^2x^2+x^2y^3}{x^2+y^2}\right| \leq \frac{3}{2}|x|+\frac{3}{2}|xy|+\frac{1}{2}|xy^2| \underset{(x,y)\to(0,0)}{\to} 0$$

et donc, pour ε suffisamment petit, on a : $\left|\dfrac{3x^2y+3y^2x^2+x^2y^3}{x^2+y^2}\right| \leq \dfrac{1}{2}$.

Et finalement, pour un tel ε on a :

$$\forall (x,y) \in B_o((0,0),\varepsilon),\ f(x,y)-f(0,0)=f(x,y) \geq \frac{x^2+y^2}{2} \geq 0$$

avec égalité si, et seulement si : $x=y=0$. On a donc un minimum local strict en $(0,0)$, et c'est le seul extremum de f sur $\mathbb{R}^2$.
Ce n'est pas un minimum global, car f n'est pas minorée. On a par exemple pour tout $y \in \mathbb{R}$:

$$f(1,y)=(1+y)^3+y^2 \underset{y\to\pm\infty}{\sim} y^3$$

et donc :

$$\lim_{y\to+\infty} f(1,y)=+\infty \text{ et } \lim_{y\to-\infty} f(1,y)=-\infty.$$

Théorème III.23 (des bornes atteintes)**.** *Si F est un ensemble fermé et borné de $\mathbb{R}^2$, alors toute fonction continue sur F admet un maximum et un minimum sur F.*

Remarque III.24. *L'intérêt est qu'un tel théorème assure l'existence des extrema, et aide donc à la recherche.*

Exemple III.25. *Étudions la fonction $f : (x,y) \mapsto x+y$ sur $F = B_f((0,0),r)$ (pour $r \in \mathbb{R}_+$ fixé). On a déjà que f est $\mathcal{C}^1$ sur F (et en particulier continue), donc par théorème des bornes atteintes elle atteint son maximum et son minimum en des points de F.*
De tels points, s'ils n'étaient pas au bord de F, serait donc sur l'ensemble $U = B_o((0,0),r)$, qui est un ouvert, et seraient donc aussi des points en lesquels $f|_U$ atteint un extremum : ce serait donc des points critiques. Mais on a directement que, pour tout $(x,y) \in F$: $\nabla f(x,y)=(1,1) \neq 0$, donc f n'a pas de points critique.
Ces points sont donc nécessairement au bord, c'est-à-dire sur l'ensemble $\mathcal{C}_r = \{(x,y)\,|\,x^2+y^2=r^2\} = \{(r\cos(t), r\sin(t))\,|\,t \in \mathbb{R}\}$.
Pour trouver ces points, il suffit d'étudier les extrema de la fonction (à variable réelle) :

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ t & \mapsto & f(r\cos(t), r\sin(t)) \end{array} \right.$$

qui est une fonction $\mathcal{C}^1$ (comme composée de fonctions $\mathcal{C}^1$), et donc ses extrema correspondent à des points critiques (au sens des fonctions à variable réelle).
On a pour tout $t \in \mathbb{R}$:

$$\varphi(t) = r\cos(t)+r\sin(t)$$

et donc pour tout $t \in \mathbb{R}$*, on a :*

$$\varphi'(t) = r\left(-\sin(t) + \cos(t)\right)$$

ce qui donne que les points critiques de φ*, et donc nécessairement les points en lesquels elle atteint un extremum, sont les réels* t *tels que :* $\cos(t) = \sin(t)$*. C'est-à-dire les éléments de* $\dfrac{\pi}{4} + \pi\mathbb{Z}$*. De telles valeurs correspondent à* $(x, y) \in \left\{\pm\left(\dfrac{\sqrt{2}}{2}, \dfrac{\sqrt{2}}{2}\right)\right\}$*.*

Comme il y a deux valeurs, et que parmi ces deux valeurs une (au moins) correspond à un maximum et l'autre à un minimum, il suffit de voir laquelle est la plus grande et laquelle la plus petite. Et comme on a :

$$f\left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right) = \sqrt{2} > -\sqrt{2} = f\left(-\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2}\right)$$

on déduit que, sur F*, la fonction* f *admet un maximum global en* $\left(\dfrac{\sqrt{2}}{2}, \dfrac{\sqrt{2}}{2}\right)$ *et un minimum global en* $\left(\dfrac{\sqrt{2}}{2}, \dfrac{\sqrt{2}}{2}\right)$*, et pas d'autre extremum (local ou global).*

Comme f *n'atteint d'extremum en aucun autre point, ces extrema sont d'ailleurs nécessairement stricts.*