La Martinière Monplaisir

Cours de MPSI

2 septembre 2017

Table des matières

Chapitre I

Nombres complexes

1 Corps des nombres complexes

1.1 Construction à partir de $\mathbb{R}$

Définition 1.1.1.
Soit E un ensemble. On appelle *loi de composition interne sur E* , ou plus simplement *loi (interne) sur E*, toute application de $E \times E$ dans E.

Remarque 1.1.2.
Une loi de composition interne est ce que vous appeliez auparavant une « opération » : l'addition des réels, la multiplication, l'addition des vecteurs...

Nous allons maintenant donner *une* construction de $\mathbb{C}$, ainsi que des opérations usuelles sur $\mathbb{C}$: addition et multiplication.

1. On suppose connu $\mathbb{R}$ muni de ses deux lois : l'addition $+$ et la multiplication $\times$.
2. Nous allons construire $\mathbb{C}$ comme l'ensemble des couples $(x, y) \in \mathbb{R}^2$, que nous munirons ensuite de deux lois. Le choix de $\mathbb{R}^2$ pour cette construction n'est pas essentiel (d'autres façons équivalentes de construire $\mathbb{C}$ existent). On ne considérera pas par la suite que $\mathbb{R}^2$ et $\mathbb{C}$ sont égaux, même s'il est parfois naturel de les identifier.
3. Construire $\mathbb{C}$ comme l'ensemble $\mathbb{R}^2$ n'est pas nécessairement très intuitif car on a l'impression que, pour construire $\mathbb{C}$, il faut chercher un sur ensemble de $\mathbb{R}$, or $\mathbb{R}^2$ n'en est pas un. L'idée est que l'ensemble $\mathbb{C}$ que nous allons construire contiendra une « copie » de $\mathbb{R}$. Par la suite, on identifiera cette copie et $\mathbb{R}$ lui-même.
4. Nous définissons donc deux lois de composition interne sur $\mathbb{R}^2$, notées provisoirement $\oplus$ et $\otimes$. Ce sont les lois telles que pour tout $(x, y) \in \mathbb{C}$ et tout $(x', y') \in \mathbb{C}$, on a :
$$(x, y) \oplus (x', y') = (x + x', y + y'),$$
$$(x, y) \otimes (x', y') = (xx' - yy', xy' + yx').$$
5. $\mathbb{R}^2$ muni de ces deux lois est appellé $\mathbb{C}$.
6. Nous identifions à présent, pour tout réel x, le réel x et l'élément de $\mathbb{C}$ $(x, 0)$. Cela signifie que, pour $x \in \mathbb{R}$, nous noterons maintenant x à la place de $(x, 0)$. Via cette identification, $\mathbb{R}$ peut être vu comme une partie de $\mathbb{C}$. En particulier 1 désigne le couple $(1, 0)$.
7. On peut remarquer qu'on a alors, pour tous réels x et x' :
$$x \oplus x' = (x, 0) \oplus (x', 0) = (x + x', 0) = x + x',$$
$$x \otimes x' = (x, 0) \otimes (x', 0) = (xx', 0) = xx'.$$
Autrement dit, sur $\mathbb{R}$, $\oplus$ se confond avec l'addition usuelle et $\otimes$ avec la multiplication usuelle. $\oplus$ et $\otimes$ sont donc des prolongements à $\mathbb{C}$ des lois usuelles de $\mathbb{R}$. On reprendra donc les notations $+$ et $\times$, le symbole $\times$ étant souvent omis, comme dans $\mathbb{R}$.
8. Nous avons décidé plus haut de noter 1 le complexe $(1, 0)$, nous décidons maintenant de noter i le complexe $(0, 1)$. Notons alors que pour tous réels x et y, on a
$$\begin{aligned} x + i \times y &= (x, 0) + (0, 1) \times (y, 0) \\ &= (x, 0) + (0, y) \\ &= (x, y). \end{aligned}$$
Par ailleurs,
$$\begin{aligned} i^2 &= (0 \times 0 - 1 \times 1, 0 \times 1 + 0 \times 1) \\ &= (-1, 0) \\ &= -1. \end{aligned}$$

Définition 1.1.3 (Parties réelle et imaginaire)**.**
Soit $z \in \mathbb{C}$. Alors il existe un unique couple $(x, y) \in \mathbb{C}$ vérifiant $z = x + iy$. Le réel x est appelé *partie réelle* de z et est noté $\mathrm{Re}(z)$, et le réel y est appelé *partie imaginaire* de z et est noté $\mathrm{Im}(z)$.

Démonstration.
Soit $(x, y) \in \mathbb{R}^2$. D'après ce qui précède $x + iy = (x, y)$, donc
$$z = x + iy \iff z = (x, y).$$
Il existe donc bien un unique couple (x, y) vérifiant $z = x + iy$. □

Remarque 1.1.4.
Pour tous z et z' dans $\mathbb{C}$, on a

$$z = z' \Leftrightarrow \mathrm{Re}(z) = \mathrm{Re}(z') \text{ et } \mathrm{Im}(z) = \mathrm{Im}(z').$$

Démonstration.
C'est une conséquence directe de la définition précédente. □

Définition 1.1.5 (Réels et imaginaires purs)**.**
Un complexe est dit *réel* si sa partie imaginaire est nulle. Il est dit *imaginaire pur* si sa partie réelle est nulle.

1.2 Propriétés des lois + et ×

a Commutativité

Proposition 1.2.1.
+ et × sont commutatives.

Démonstration.
Soit $z = x + iy$ et $z' = x' + iy'$ deux nombres complexes, avec x, x', y, y' des réels. Alors,

$$\begin{aligned} z + z' &= (x + x') + i(y + y') \\ &= (x' + x) + i(y' + y) \\ &= z' + z \end{aligned}$$

et

$$\begin{aligned} z \times z' &= (xx' - yy'') + i(x'y + xy') \\ &= (x'x - y'y) + i(xy' + x'y) \\ &= z' \times z. \end{aligned}$$

□

b Associativité

Proposition 1.2.2.
+ et × sont associatives.

Démonstration.
Soit $z = x+iy$, $z' = x'+iy'$ et $z'' = x''+iy''$ trois nombres complexes, avec x, x', x'', y, y', y'' des réels. Alors,

$$\begin{aligned} (z + z') + z'' &= [(x + x') + i(y + y')] + [x'' + iy''] \\ &= (x + x' + x'') + i(y + y' + y'') \\ &= (x + iy) + [(x' + x'') + i(y' + y'')] \\ &= z + (z' + z'') \end{aligned}$$

et

$$\begin{aligned} (z \times z') \times z'' &= [(xx' - yy'') + i(x'y + xy')] \times z'' \\ &= [(xx' - yy') + i(x'y + xy')](x'' + iy'') \\ &= (xx'x'' - yy'x'' - yx'y'' - xy'y'') \\ &\qquad + i(yx'x'' + xy'x'' + xx'y'' - yy'y'') \\ &= [x(x'x'' - y'y'') - y(y'x'' + x'y'')] \\ &\qquad + i[x(y'x'' + x'y'') + y(x'x'' - y'y'')] \\ &= (x + iy) \times [(x'x'' - y'y'') + i(y'x'' + x'y'')] \\ &= z \times (z' \times z''). \end{aligned}$$

□

c Distributivité de × sur +

Proposition 1.2.3.
La multiplication est distributive par rapport à l'addition.

Démonstration.
Soit $z = x+iy$, $z' = x'+iy'$ et $z'' = x''+iy''$ trois nombres complexes, avec x, x', x'', y, y', y'' des réels. Alors,

$$\begin{aligned} z \times (z' + z'') &= (x + iy) \times [(x' + x'') + i(y' + y'')] \\ &= xx' + xx'' - yy' - yy'' \\ &\qquad + i(yx' + yx'' + xy' + xy'') \\ &= [xx' - yy' + i(yx' + xy')] \\ &\qquad + [xx'' - yy'' + i(yx'' + xy'')] \\ &= (z \times z') + (z \times z''). \end{aligned}$$

□

d Éléments neutres

Définition 1.2.4.
Soit # une loi de composition interne sur un ensemble E. On dit que e est un élément neutre pour # si pour tout $x \in E$, $e\#x = x\#e = x$.

Proposition 1.2.5.
Soit E un ensemble muni d'une loi de composition interne #. Si # admet un élément neutre, alors celui-ci est unique.

Démonstration.
Soient e et e' deux neutres. Alors, e' étant neutre, on a $e\#e' = e$ et e étant neutre, on a $e\#e' = e'$. On a donc $e = e'$. □

Exemple 1.2.6.
L'addition sur l'ensemble des entiers naturels (resp. relatifs) admet un unique neutre : 0. L'addition sur l'ensemble des entiers naturels non nuls n'admet aucun neutre.

Proposition 1.2.7.
Dans $\mathbb{C}$, 0 est un élément neutre pour $+$, 1 est un élément neutre pour $\times$.

Démonstration.
Soit $z = x + iy \in \mathbb{C}$, avec $(x, y) \in \mathbb{R}^2$. Alors,

$$z+0 = (x+iy)+(0+i0) = (x+0)+i(y+0) = x+iy = z$$

et

$$\begin{aligned} z \times 1 &= (x+iy) \times (1+i0) \\ &= (1x - 0y) + i(1y + 0x) \\ &= x + iy \\ &= z. \end{aligned}$$

□

e Inverses

Définition 1.2.8.
Soient $(E, \#)$ un ensemble muni d'une loi interne, ayant un neutre e. On dit que $x \in E$ est *inversible* s'il existe un $x' \in E$ tel que $x\#x' = e$ **et** $x'\#x = e$.

Remarque 1.2.9.
Attention de bien vérifier les deux égalités, comme le montre l'exercice suivant.

Exercice 1.2.10.
On note $\mathscr{F}$ l'ensemble des applications de $\mathbb{N}$ dans $\mathbb{N}$, et on le munit de la lci $\circ$, qui dénote la composition de deux applications.

1. $(\mathscr{F}, \circ)$ a-t-il un élément neutre ?

2. Soient $f : \mathbb{N} \to \mathbb{N}$, $n \mapsto n+1$ et $g : \mathbb{N} \to \mathbb{N}$, $n \mapsto \begin{cases} 0 & \text{si } n = 0 \\ n-1 & \text{si } n \neq 0 \end{cases}$. Étudier $g \circ f$ et $f \circ g$. Que peut-on dire ?

Proposition 1.2.11.
Soit E un ensemble muni d'une lci ***associative*** $\#$ admettant un neutre e.

Pour tout élément x de E, si x est inversible pour $\#$, alors son inverse est unique.

Démonstration.
Soient y et y' deux inverses de x. Alors $y\#x = e$ donc $y\#x\#y' = e\#y' = y'$. D'autre part, $x\#y' = e$ donc $y\#x\#y' = y\#e = y$. □

Proposition 1.2.12.
Soit $z \in \mathbb{C}$.

z est inversible pour $+$, d'inverse $-z$.

Si $z \neq 0$, z est aussi inversible pour $\times$, d'inverse $z^{-1} = \dfrac{1}{z} = \dfrac{x - iy}{x^2 + y^2}$, où $x = \mathrm{Re}(z)$ et $y = \mathrm{Im}(z)$.

0 n'est pas inversible pour $\times$ dans $\mathbb{C}$.

Démonstration.
C'est simple pour l'addition.

Comme la multiplication complexe est commutative, on n'a besoin de vérifier qu'une égalité. Soit $z = x + iy \in \mathbb{C}$, avec $(x, y) \in \mathbb{R}^2 \setminus \{(0, 0)\}$. Alors $x^2 + y^2 \neq 0$ et

$$\begin{aligned} &\left[\frac{x}{x^2+y^2} - i\frac{y}{x^2+y^2}\right] \times (x+iy) \\ &= \frac{1}{x^2+y^2}\left[x^2 + y^2 + i(xy - yx)\right] \\ &= \frac{x^2+y^2}{x^2+y^2} \\ &= 1. \end{aligned}$$

Enfin, on vérifie aisément que 0 est absorbant : pour tout complexe z, $0z = 0$. Si 0 était inversible, son inverse z ne pourrait donc vérifier $0z = 1$, car $1 \neq 0$! □

Remarque 1.2.13.
Si z et z' sont deux nombres complexes, avec $z' \neq 0$, on note $\dfrac{z}{z'} = z \times (z')^{-1}$.

Définition 1.2.14.
On appelle *monoïde* tout couple $(G, \star)$ où G est un ensemble et

1. $\star$ est une loi de composition interne sur G ;
2. $\star$ est associative ;
3. et $\star$ possède un élément neutre.

On appelle *groupe* tout monoïde $(G, \star)$ dont tous les éléments sont inversibles.

On dit qu'un monoïde ou un groupe est *commutatif* si sa loi de composition interne l'est.

On appelle *anneau* tout triplet $(G, \star, \#)$ tel que

1. $(G, \star)$ est un groupe **commutatif** ;
2. $(G, \#)$ est un monoïde ;
3. et $\#$ est distributive par rapport à $\star$.

On dit qu'un anneau est *commutatif* si $\#$ est commutative.

Enfin, on appelle *corps* tout anneau **commutatif** $(G, \star, \#)$ tel que tout élément de G différent du neutre de $\star$ est inversible pour $\#$.

Exercice 1.2.15.
Chacun des ensembles $\mathbb{N}^*$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$ et $\mathbb{C}$, muni des lois usuelles, est-il un monoïde, un groupe, un anneau, un corps ?

1.3 Interprétation géométrique

Définition 1.3.1 (Affixe et image)**.**
Soit M un point du plan de coordonnées (x, y). On appelle *affixe* de M le complexe $x + iy$.

Soit z un complexe de partie réelle x et de partie imaginaire y. On appelle *image* de z le point du plan de coordonnées (x, y).

Remarque 1.3.2.
On peut identifier $\mathbb{C}$ et $\mathbb{R}^2$ au plan euclidien (l'ensemble des points du plan) muni d'un repère orthonormal direct $(O, \overrightarrow{i}, \overrightarrow{j})$, c'est-à-dire qu'un point du plan euclidien est identifié à ses coordonnées [1] dans $(O, \overrightarrow{i}, \overrightarrow{j})$.

On peut également identifier $\mathbb{C}$ et $\mathbb{R}^2$ à l'ensemble des vecteurs du plan, le vecteur $\overrightarrow{OM}$ étant identifié au point M, et donc à son affixe.

1. Notez la différence entre « identifié par » et « identifié à ».

Théorème 1.3.3 (Règles de calcul)**.**
On a les propriétés suivantes :

(i) Soient $\overrightarrow{u}$ et $\overrightarrow{u}'$ deux vecteurs d'affixes respectifs z et z', et soit $\lambda \in \mathbb{R}$. Alors le vecteur $\overrightarrow{u} + \lambda\overrightarrow{u}'$ a pour affixe $z + \lambda z'$. En particulier, pour tout couple de vecteurs, l'affixe de la somme de ces vecteurs est la somme des affixes et pour tout scalaire λ et tout vecteur $\overrightarrow{u}$ d'affixe z, l'affixe de $\lambda\overrightarrow{u}$ est λz.

(ii) Soient A et B deux points d'affixes respectifs a et b. Alors le vecteur $\overrightarrow{AB}$ a pour affixe $b-a$.

Démonstration. (i) Notons x et y respectivement les parties réelle et imaginaire de z, et x' et y' celles de z'. Alors $\overrightarrow{u}$ (resp. $\overrightarrow{u}'$) a pour coordonnées (x, y) (resp. (x', y')). $\overrightarrow{u} + \lambda\overrightarrow{u}'$ a alors pour coordonnées $(x+\lambda x', y+\lambda y')$, donc pour affixe $(x+\lambda x')+i(y+\lambda y')$. Or on a

$$\begin{aligned} z + \lambda z' &= (x + iy) + \lambda(x' + iy') \\ &= (x + \lambda x') + i(y + \lambda y') \end{aligned}$$

Donc $\overrightarrow{u} + \lambda\overrightarrow{u}'$ a bien pour affixe $z + \lambda z'$.
Il suffit alors d'étudier les cas particuliers où $\lambda = 1$, où $\overrightarrow{u} = \overrightarrow{0}$ et où $\overrightarrow{u} = \overrightarrow{0}$ et $\lambda = -1$ pour conclure.

(ii) Il suffit d'utiliser la relation fondamentale $\overrightarrow{AB} = \overrightarrow{OB} - \overrightarrow{OA}$ et le point précédent pour conclure.

□

Remarque 1.3.4.
Soit $b \in \mathbb{C}$. L'application

$$\begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & z + b \end{array}$$

s'interprète géométriquement comme la translation de vecteur d'affixe b.

1.4 Conjugué et module d'un nombre complexe

Définition 1.4.1.
On appelle *conjugué d'un complexe* z le complexe $\overline{z} = \mathrm{Re}(z) - i\,\mathrm{Im}(z)$.
On appelle *module d'un complexe* z le réel positif $|z| = \sqrt{\mathrm{Re}(z)^2 + \mathrm{Im}(z)^2}$.

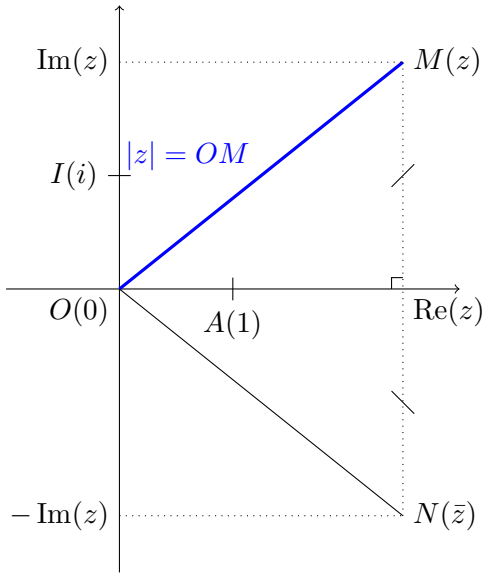


FIGURE I.1 – Interprétation géométrique du module et du conjugué de $z \in \mathbb{C}$.

Remarque 1.4.2.
Sur $\mathbb{R}$, le module coïncide avec la valeur absolue.

Proposition 1.4.3 (Règles de calcul)**.**
Soit $(z, z') \in \mathbb{C}^2$, on a les identités suivantes.

$$\begin{aligned} \mathrm{Re}(z) &= \frac{z+\overline{z}}{2} & \mathrm{Im}(z) &= \frac{z-\overline{z}}{2i} \\ \overline{z+z'} &= \overline{z}+\overline{z}' & \overline{z\times z'} &= \overline{z}\times\overline{z}' \\ \overline{\overline{z}} &= z & z\overline{z} &= |z|^2 \\ |\overline{z}| &= |z| & |zz'| &= |z|\times|z'| \end{aligned}$$

Si $z' \neq 0$,

$$\left|\frac{z}{z'}\right| = \frac{|z|}{|z'|} \quad \text{et} \quad \frac{\overline{z}}{z'} = \frac{\overline{z}}{\overline{z'}}.$$

Démonstration.
Ces identités sont élémentaires et se vérifient directement en posant $z = x + iy$, avec $(x, y) \in \mathbb{R}^2$.

L'égalité $z\overline{z} = |z|^2$ a déjà été vue lors du calcul de l'inver d'un nombre complexe.

Remarquons aussi que, facilement, $|zz'|^2 = zz'\overline{zz'} = zz'\overline{z}\overline{z'} = z\overline{z}z'\overline{z'} = |z|^2|z'|^2$. □

Corollaire 1.4.4.
Soit $z \in \mathbb{C}$, on a $z \in \mathbb{R} \Leftrightarrow \overline{z} = z$ et $z \in i\mathbb{R} \Leftrightarrow \overline{z} = -z$.

Proposition 1.4.5 (Comparaisons usuelles)**.**
Soit $z \in \mathbb{C}$, on a

$$|z| = 0 \Leftrightarrow z = 0,$$
$$|\,\mathrm{Re}(z)| \leqslant |z| \quad \text{et} \quad |\,\mathrm{Im}(z)| \leqslant |z|.$$

Démonstration.
Soit $z \in \mathbb{C}$, soit $x, y \in \mathbb{R}$ tels que $z = x + iy$. On a $0 \leqslant x^2 \leqslant x^2 + y^2$, ce qui prouve bien que si $|z| = 0$, alors $z = 0$ (l'autre implication est évidente). Cela prouve aussi que $\mathrm{Re}(z)^2 \leqslant |z|^2$, donc que $|\,\mathrm{Re}(z)| \leqslant |z|$ (*idem* pour $\mathrm{Im}(z)$). □

Corollaire 1.4.6.
Soit $a, b \in \mathbb{C}$, si $ab = 0$, alors $a = 0$ ou $b = 0$.

Théorème 1.4.7 (Inégalité triangulaire)**.**
Soit $z, z' \in \mathbb{C}$, on a

$$\big|\,|z| - |z'|\,\big| \leqslant |z \pm z'| \leqslant |z| + |z'|.$$

De plus, $|z + z'| = |z| + |z'|$ si et seulement s'il existe $(\lambda, \lambda') \in (\mathbb{R}^+)^2$ tel que $(\lambda, \lambda') \neq (0, 0)$ et $\lambda z = \lambda' z'$.

Démonstration.
On montre l'encadrement pour $|z + z'|$. Pour $|z - z'|$ il suffit de remplacer z' par $-z'$.

Pour montrer $|z + z'| \leqslant |z| + |z'|$, il suffit de montrer $|z + z'|^2 \leqslant (|z| + |z'|)^2$. Posons $d = (|z| + |z'|)^2 - |z + z'|^2$ et calculons d. On obtient successivement

$$\begin{aligned} d &= |z|^2 + |z'|^2 + 2|z||z'| - \big(z + z'\big)\big(\overline{z} + \overline{z'}\big) \\ &= 2|z||z'| - z\overline{z'} - z'\overline{z} \\ &= 2\left(|z||z'| - \frac{z\overline{z'} + z'\overline{z}}{2}\right) \\ &= 2\left(|z||\overline{z'}| - \frac{z\overline{z'} + \overline{z\overline{z'}}}{2}\right) \\ &= 2\big(|z\overline{z'}| - \mathrm{Re}\,(z\overline{z'})\big) \\ &\geqslant 0 \end{aligned}$$

On a donc $|z+z'| \leqslant |z| + |z'|$.

Pour la seconde inégalité : $|z| = |(z+z') + (-z')| \leqslant |z+z'| + |-z'|$, d'où $|z| - |z'| \leqslant |z+z'|$. On permute les rôles de z et z' et on a $|z'| - |z| \leqslant |z+z'|$, ce qui permet de conclure, car

$$\big|\, |z| - |z'| \,\big| = \max\big(|z| - |z'|; |z'| - |z|\big).$$

Montrons maintenant le cas d'égalité. Dans le cas où $z = z' = 0$, le résultat est immédiat.

Sinon, d'après la démonstration de l'inégalité triangulaire, l'égalité est vérifiée si et seulement si $\left|z\overline{z'}\right| = \mathrm{Re}\left(z\overline{z'}\right)$, *i.e.* si et seulement si $z\overline{z'}$ est un réel positif.

Dans le cas où $z' \neq 0$, on remarque que $\dfrac{z}{z'} = \dfrac{z\overline{z'}}{|z'|^2}$, donc l'égalité est vérifiée si et seulement si $\dfrac{z}{z'} \in \mathbb{R}_+$ si et seulement si il existe $\lambda \in \mathbb{R}_+$ tel que $z = \lambda z'$.

En inversant les rôles de z et z' dans le cas où $z' = 0$ on obtient le résultat voulu. □

Remarque 1.4.8.

• En pratique : on se sert de $z\overline{z} = |z|^2$ pour calculer la forme algébrique de l'inverse d'un complexe :

$$\frac{1}{z} = \frac{x - iy}{x^2 + y^2}$$

• Le module d'un complexe est la norme du vecteur ayant ce complexe pour affixe.

• En particulier, soit a et z deux complexes et $R \geqslant 0$. Notons M et A les points du plans d'affixes respectives z et a. Alors $|z-a|$ est la distance AM. Et M appartient au cercle (resp. disque ouvert, resp. disque fermé) de centre A et de rayon R si et seulement si $|z-a| = R$ (resp. $|z-a| < R$, resp. $|z-a| \leqslant R$).

• Géométriquement, il y a égalité dans l'inégalité triangulaire survient donc quand les images de z et z' sont sur une même demi-droite d'origine O.

• Le bloc « il existe $(\lambda, \lambda') \in (\mathbb{R}^+)^2$ tel que $(\lambda, \lambda') \neq (0,0)$ » s'écrit aussi « $\exists (\lambda, \lambda') \in (\mathbb{R}^+)^2 \setminus \{(0,0)\}$ » et se lit « il existe deux complexes λ et λ' non tous nuls ».

2 Groupe $\mathbb{U}$ des nombres complexes de module 1

2.1 Rappels de collège

Commençons par une première définition de trigonométrie.

Définition 2.1.1 (Fonction tangente)**.**
Notons A l'ensemble des réels congrus à $\dfrac{\pi}{2}$ modulo π :

$$A = \left\{ x \in \mathbb{R} \;\middle|\; \exists k \in \mathbb{Z}\ x = \frac{\pi}{2} + k\pi \right\}.$$

On appelle alors *fonction tangente*, notée tan, la fonction :

$$\begin{array}{rccc} \tan : & \mathbb{R}\backslash A & \to & \mathbb{R} \\ & t & \mapsto & \dfrac{\sin t}{\cos t} \end{array}.$$

Cette fonction sera étudiée plus en détail dans le chapitre sur les fonctions usuelles, mais il est utile de retenir les valeurs de tan en 0, $\pm\dfrac{\pi}{6}$, $\pm\dfrac{\pi}{4}$ et $\pm\dfrac{\pi}{3}$, l'allure de son graphe et le fait qu'elle est impaire.

Remarque 2.1.2.
On peut définir de la même manière la fonction *cotangente* :
Posons

$$B = \{x \in \mathbb{R},\ \exists k \in \mathbb{Z}\ x = k\pi\} = k\mathbb{Z}.$$

On appelle alors *fonction cotangente*, notée cotan, la fonction :

$$\begin{array}{rccc} \mathrm{cotan} : & \mathbb{R}\backslash B & \to & \mathbb{R} \\ & t & \mapsto & \dfrac{\cos t}{\sin t} \end{array}.$$

Attention : la fonction cotangente n'est pas égale à $\dfrac{1}{\tan}$. Pourquoi ?

2.2 Définition et caractérisation

Définition 2.2.1.
On note $\mathbb{U}$ l'ensemble des nombres complexes de module 1 : $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$. Muni de la multiplication usuelle entre complexes, c'est un groupe de neutre 1.

Remarque 2.2.2.
$\mathbb{U}$ est l'ensemble des affixes des points du cercle trigonométrique

Définition 2.2.3.
Soit $\theta \in \mathbb{R}$. On appelle *exponentielle complexe de* $i\theta$ le complexe $\mathrm{e}^{\,i\theta} = \cos\theta + i\sin\theta$.

 L'écriture $\mathrm{e}^{\,i\theta}$ n'est qu'une **notation** : en aucun cas il ne s'agit du réel e élevé à la puissance $i\theta$, ce qui n'a aucun sens.

Théorème 2.2.4.
Soient θ, $\theta' \in \mathbb{R}$ et $n \in \mathbb{N}$. On a :

(i) Les formules d'Euler :

$$\cos\theta = \frac{\mathrm{e}^{\,i\theta} + \mathrm{e}^{\,-i\theta}}{2}$$
$$\sin\theta = \frac{\mathrm{e}^{\,i\theta} - \mathrm{e}^{\,-i\theta}}{2i}$$

(ii) $\mathrm{e}^{\,i(\theta+\theta')} = \mathrm{e}^{\,i\theta}\mathrm{e}^{\,i\theta'}$;

(iii) $\mathrm{e}^{\,i\theta} \neq 0$; et $\overline{\mathrm{e}^{\,i\theta}} = \mathrm{e}^{\,-i\theta} = \dfrac{1}{\mathrm{e}^{\,i\theta}}$, donc $\mathrm{e}^{\,i\theta} \in \mathbb{U}$.

(iv) les formules de De Moivre :

$$\mathrm{e}^{\,in\theta} = \left(\mathrm{e}^{\,i\theta}\right)^n$$
$$\cos(n\theta) + i\sin(n\theta) = (\cos\theta + i\sin\theta)^n$$

(v) Si $\tan\dfrac{\theta}{2}$ est bien défini, alors en posant $t = \tan\dfrac{\theta}{2}$, on a $\mathrm{e}^{\,i\theta} = \dfrac{(1+it)^2}{1+t^2}$.

Démonstration.
On donne ici la démonstration utilisant les formules de trigonométrie, admises jusqu'ici. Ces formules peuvent se démontrer géométriquement. Consulter par exemple la page Wolfram

http ://preview.tinyurl.com/pzkqg5q

Une autre approche possible serait d'admettre la troisième propriété et d'en déduire toutes les autres, ainsi que les formules de trigonométrie.

(i) Facile.

(ii) Simple développement.

(iii) $\mathrm{e}^{\,i\theta} \times \mathrm{e}^{\,-i\theta} = \mathrm{e}^{\,i0} = 1$, donc $\mathrm{e}^{\,i\theta}$ et $\mathrm{e}^{\,-i\theta}$ sont inverses l'un de l'autre. En particulier $\mathrm{e}^{\,i\theta} \neq 0$.
Par ailleurs,

$$\begin{aligned}\mathrm{e}^{\,-i\theta} &= \cos(-\theta) + i\sin(-\theta)\\ &= \cos\theta - i\sin\theta\\ &= \overline{\mathrm{e}^{\,i\theta}}\end{aligned}$$

Donc $1 = \mathrm{e}^{\,-i\theta}.\overline{\mathrm{e}^{\,i\theta}} = \left|\mathrm{e}^{\,i\theta}\right|^2$, donc $\mathrm{e}^{\,i\theta} \in \mathbb{U}$.
On aurait aussi pu utiliser que $\cos^2\theta + \sin^2\theta = 1$.

(iv) Se démontre par une récurrence immédiate sur n.

(v) Ce point se déduit aisément des égalités $\cos\theta = \dfrac{1-t^2}{1+t^2}$ et $\sin\theta = \dfrac{2t}{1+t^2}$.
On peut aussi voir que, par la formule de De Moivre,

$$\begin{aligned}\mathrm{e}^{\,i\theta} &= \left(\mathrm{e}^{\,i\frac{\theta}{2}}\right)^2\\ &= \left(\cos\left(\frac{\theta}{2}\right) + i\sin\left(\frac{\theta}{2}\right)\right)^2\\ &= \cos^2\left(\frac{\theta}{2}\right)\left(1 + i\tan\left(\frac{\theta}{2}\right)\right)^2\\ &= \frac{(1+it)^2}{1+t^2}\end{aligned}$$

car, pour tout x pour lequel $\cos x \neq 0$, $1+\tan^2(x) = \dfrac{1}{\cos^2(x)}$.

□

Théorème 2.2.5 (Paramétrisation de $\mathbb{U}$)**.**
L'application

$$\begin{array}{ccc}\mathbb{R} & \to & \mathbb{C}\\ \theta & \mapsto & \mathrm{e}^{\,i\theta}\end{array}$$

est *un paramétrage de* $\mathbb{U}$, autrement dit, pour tout nombre complexe z on a

$$z \in \mathbb{U} \;\Leftrightarrow\; \exists\theta \in \mathbb{R} \quad z = \mathrm{e}^{\,i\theta} \qquad \text{(I.1)}$$

De plus, pour tout complexe $z \in \mathbb{U}$ donné, le paramètre correspondant est *unique à* 2π *près*, autrement dit, on a

$$\forall(\theta,\theta') \in \mathbb{R}^2 \quad \mathrm{e}^{\,i\theta} = \mathrm{e}^{\,i\theta'} \;\Leftrightarrow\; \theta = \theta'[2\pi] \qquad \text{(I.2)}$$

Remarque 2.2.6.
Ce résultat a une interprétation géométrique intuitive.

Démonstration.
Soit $z \in \mathbb{C}$. Montrons l'équivalence (I.1). L'implication de droite à gauche est évidente : s'il existe θ tel que z s'écrive $\sin\theta + i\cos\theta$, alors $|z|^2 = \sin^2\theta + \cos^2\theta = 1$, donc $z \in \mathbb{U}$. Réciproquement, soit $z \in \mathbb{U}$, alors $(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2 = 1$ donc il existe $\theta \in \mathbb{R}$ vérifiant $\operatorname{Re} z = \cos\theta$ et $\operatorname{Im} z = \sin\theta$.

Pour l'équivalence (I.2), il suffit de remarquer que pour tout couple (θ, θ') de réels, l'égalité $\mathrm{e}^{i\theta} = \mathrm{e}^{i\theta'}$ implique l'égalité des cosinus ainsi que des sinus de θ et θ', donc l'égalité de θ et θ' à 2π près. L'autre sens découle de la proposition 2.1.4. □

2.3 Technique de l'angle moitié

La factorisation suivante est indispensable. Pour tout $(x, y) \in \mathbb{R}^2$, on a

$$\begin{aligned}\mathrm{e}^{ix} + \mathrm{e}^{iy} &= \mathrm{e}^{i\frac{(x+y)}{2}}\left(\mathrm{e}^{i\frac{(x-y)}{2}} + \mathrm{e}^{-i\frac{(x-y)}{2}}\right)\\ &= 2\mathrm{e}^{i\frac{(x+y)}{2}}\cos\left(\frac{x-y}{2}\right)\end{aligned}$$

Cette technique permet en particulier de montrer

Proposition 2.3.1.
Soit $t \in \mathbb{R}$, alors

$$\begin{aligned}1 + \mathrm{e}^{it} &= \quad 2\mathrm{e}^{i\frac{t}{2}}\cos\left(\frac{t}{2}\right)\\ 1 - \mathrm{e}^{it} &= -2\mathrm{e}^{i\frac{t}{2}}i\sin\left(\frac{t}{2}\right)\end{aligned}$$

Démonstration.
Il suffit de remarquer que $1 = e^{i0}$ et d'appliquer la technique. □

2.4 Forme trigonométrique d'un nombre complexe

Définition 2.4.1.
Soit $z \neq 0$. Alors $z/|z| \in \mathbb{U}$, donc il existe $\theta \in \mathbb{R}$ vérifiant $z/|z| = \mathrm{e}^{i\theta}$, c'est-à-dire $z = |z|\mathrm{e}^{i\theta}$.

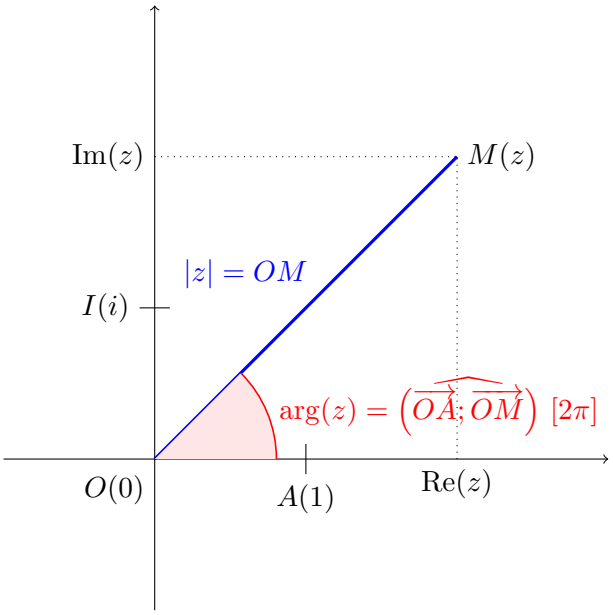


FIGURE I.2 – Interprétation géométrique du module et de l'argument de $z \in \mathbb{C}^*$.

Le réel θ est alors appelé ***un*** *argument* de z. Il existe à 2π près. Il existe alors un unique $\theta \in]-\pi, \pi]$ vérifiant $z = |z|\mathrm{e}^{i\theta}$. Ce réel est appelé *l'argument principal* de z, et noté $\arg z$.
L'écriture «$z = |z|\mathrm{e}^{i\theta}$» est appelée *écriture trigonométrique* de z.

Remarque 2.4.2.
1. Attention à la non unicité de l'argument.
2. Le complexe 0 n'a pas d'argument.
3. Pour tout z non nul, $(|z|, \arg z)$ est un couple de coordonnées polaires du point d'affixe z.

Proposition 2.4.3.
Soient $z, z' \in \mathbb{C}^*$. On a :

$$\begin{aligned}\arg\overline{z} &= -\arg z [2\pi]\\ \arg zz' &= \arg z + \arg z' [2\pi]\\ \text{et } \arg(1/z) &= -\arg z [2\pi].\end{aligned}$$

Démonstration.
Utiliser l'écriture trigonométrique. □

2.5 Racines $n^{\text{ièmes}}$

Définition 2.5.1.
Soient $z \in \mathbb{C}$ et $n \in \mathbb{N}^*$. On appelle *racine n-ième de z* tout complexe t tel que $t^n = z$.

Les racines de 1 sont appelées *racines n-ièmes de l'unité*.

L'ensemble des racines n-ièmes de l'unité est noté $\mathbb{U}_n$.

Remarque 2.5.2.
La notation $\sqrt[n]{.}$ est **interdite** sur les complexes quelconques. En effet, elle désigne l'application réciproque de la fonction $x \mapsto x^n$ qui n'est bijective que considérée comme application de $\mathbb{R}^+$ dans $\mathbb{R}^+$ si n est pair et de $\mathbb{R}$ dans $\mathbb{R}$ si n est impair.

Théorème 2.5.3. (i) La seule racine n-ième de zéro est zéro.

(ii) Soit $z \in \mathbb{C}$ non nul, donné sous une forme trigonométrique $z = re^{i\theta}$, avec $r > 0$. Alors z possède exactement n racines n-ièmes, qui sont les nombres complexes

$$\sqrt[n]{r} \times \mathrm{e}^{\left(\frac{i\theta}{n} + \frac{2ik\pi}{n}\right)}$$

pour k décrivant l'ensemble $[\![0, n-1]\!]$ (ou $[\![1, n]\!]$).

(iii) En particulier

$$\mathbb{U}_n = \left\{ \mathrm{e}^{\frac{2ik\pi}{n}} \;\middle|\; k \in [\![0, n-1]\!] \right\}$$

Démonstration. (i) Soit $t \in \mathbb{C}$. Alors $t \neq 0 \Rightarrow t^n \neq 0$ donc $t^n = 0 \Rightarrow t = 0$. On vérifie enfin que $t = 0 \Rightarrow t^n = 0$, pour $n > 0$.

(ii) Soit $(z, t) \in \mathbb{C}^2$, $z \neq 0$.
- 1er cas : $z = 1$: on note $\rho = |t|$ et $\varphi \in \mathbb{R}$ un argument de t. On a : $t^n = 1$ si et seulement si $\rho^n.\mathrm{e}^{in\varphi} = 1.\mathrm{e}^{i0}$ si et seulement si $\rho^n = 1$ et $n\varphi = 0[2\pi]$ si et seulement si $\rho = 1$ et $\varphi = \dfrac{2k\pi}{n}$.
- 2nd cas : z est quelconque non nul donc s'écrit sous la forme $re^{i\theta}$ où $r > 0$. On pose $\alpha = \sqrt[n]{r} \times \mathrm{e}^{i\theta/n}$, donc $\alpha^n = z$. Alors, si $t = \rho.\mathrm{e}^{i\varphi}$, $t^n = z$ si et seulement si $\left(\dfrac{t}{\alpha}\right)^n = 1$ et on utilise le premier cas.

□

Remarque 2.5.4 (Interprétation géométrique)**.**
Soit $n \geqslant 3$. Posons $z_i = \frac{2ik\pi}{n}$ et notons A_i le point d'affixe z_i pour $i \in [\![0, n-1]\!]$. Alors $A_0A_1 \dots A_n$ est un polygones réguliers à n côtés.

Les racines 2-ièmes de 1 sont -1 et 1 (racines carrées de 1).

En posant $j = \mathrm{e}^{2i\pi/3}$, les racines 3-ièmes de l'unité sont 1, j et j^2 (et on a $j^2 = \bar{j}$).

Cas $n = 4, 5, 6$.

Proposition 2.5.5.
Soit $n \in \mathbb{N}$, $n \geqslant 2$. Pour tout $z \in \mathbb{C}$ on a les égalités suivantes :

$$\prod_{\omega \in \mathbb{U}_n} (z - \omega) = \prod_{k=0}^{n-1} (z - \mathrm{e}^{\frac{2ik\pi}{n}}) = z^n - 1$$

$$\prod_{\omega \in \mathbb{U}_n \setminus \{1\}} (z - \omega) = \prod_{k=1}^{n-1} \left(z - \mathrm{e}^{\frac{2ik\pi}{n}}\right) = \sum_{k=0}^{n-1} z^k.$$

La somme des racines n-ièmes de l'unité est nulle, i.e. :

$$\sum_{\omega \in \mathbb{U}_n} \omega = \sum_{k=0}^{n-1} \mathrm{e}^{\frac{2ik\pi}{n}} = 0.$$

En particulier $1 + j + \bar{j} = 0$.

Démonstration.
Pour démontrer ce résultat on admettra provisoirement le résultat suivant : Pour tout entier n et tout polynôme P un polynôme de degré n admettant n racines distinctes z_1, …, z_n, de coefficient dominant α, on a

$$\forall z \in \mathbb{C} \quad P(z) = \alpha(z - z_1) \dots (z - z_n).$$

On admettra aussi la formule de sommation géométrique : pour tout $z \in \mathbb{C}$ et $n \in \mathbb{N}^*$,

$$z^n - 1 = (z - 1)(1 + z + \cdots + z^{n-1}).$$

La première égalité est une application directe du résultat admis, en posant $P : z \mapsto z^n - 1$; P est alors un polynôme de degré n et de coefficient dominant 1.

La seconde est une application directe du même résultat en considérant $P : z \mapsto \sum_{k=0}^{n-1} z^k$. De plus $n \neq 1$ donc $\mathrm{e}^{\frac{2i\pi}{n}} \neq 1$ donc

$$\sum_{k=0}^{n-1} \mathrm{e}^{\frac{2ik\pi}{n}} = \sum_{k=0}^{n-1} \left(\mathrm{e}^{\frac{2i\pi}{n}}\right)^k = \frac{1 - \left(\mathrm{e}^{\frac{2i\pi}{n}}\right)^n}{1 - \mathrm{e}^{\frac{2i\pi}{n}}} = 0$$

□

3 Équations du second degré

3.1 Calcul des racines carrées d'un complexe sous forme algébrique

Soit z et t deux complexes. On veut résoudre explicitement l'équation $t^2 = z$, d'inconnue z, que nous noterons (E).

On peut écrire z sous la forme $x + iy$ avec $(x, y) \in \mathbb{R}^2$ et t sous la forme $a+ib$, où $(a, b) \in \mathbb{R}^2$.

Pour résoudre (E), il y a une astuce très utile

Astuce.
Soit t et z deux complexes. Alors

$$t^2 = z \iff \begin{cases} t^2 = z \\ \text{et } |t|^2 = |z| \end{cases}$$

On en déduit successivement :

$$(E) \iff \begin{cases} a^2 - b^2 + i2ab = x + iy \\ \text{et } a^2 + b^2 = \sqrt{x^2 + y^2} \end{cases}$$

$$(E) \iff \begin{cases} a^2 - b^2 = x \\ \text{et } 2ab = y \\ \text{et } a^2 + b^2 = \sqrt{x^2 + y^2} \end{cases}$$

$$(E) \iff \begin{cases} a^2 = \dfrac{x + \sqrt{x^2 + y^2}}{2} \\ \text{et } b^2 = \dfrac{-x + \sqrt{x^2 + y^2}}{2} \\ \text{et } 2ab = y \end{cases}$$

Exercice 3.1.1.
Trouver les racines carrées de $z = 3 - 4i$.

3.2 Résolution des équations du second degré

Théorème 3.2.1.
Soient a, b, $c \in \mathbb{C}$ avec $a \neq 0$. Les solutions de l'équation $az^2 + bz + c = 0$ d'inconnue $z \in \mathbb{C}$ sont $\dfrac{-b \pm \delta}{2a}$, où δ est l'une quelconque des deux racines carrées du discriminant $\Delta = b^2 - 4ac$. La somme de ces solutions vaut $-\dfrac{b}{a}$ et leur produit $\dfrac{c}{a}$.

Démonstration.
Pour tout $z \in \mathbb{C}$, on a

$$\begin{aligned} az^2 + bz + c &= a\Big(z^2 + \frac{b}{a}z + \frac{c}{a}\Big) \\ &= a\left[\Big(z + \frac{b}{2a}\Big)^2 - \frac{b^2}{4a^2} + \frac{c}{a}\right] \\ &= a\left[\Big(z + \frac{b}{2a}\Big)^2 - \frac{b^2 - 4ac}{4a^2}\right] \\ &= a\left[\Big(z + \frac{b}{2a}\Big)^2 - \Big(\frac{\delta}{2a}\Big)^2\right] \\ &= a\left[z + \frac{b}{2a} - \frac{\delta}{2a}\right]\left[z + \frac{b}{2a} + \frac{\delta}{2a}\right] \\ &= a\Big(z - \frac{-b - \delta}{2a}\Big)\Big(z - \frac{-b + \delta}{2a}\Big) \end{aligned}$$

On calcule finalement :

$$\frac{-b - \delta}{2a} + \frac{-b + \delta}{2a} = -\frac{b}{a},$$
$$\frac{-b - \delta}{2a} \times \frac{-b + \delta}{2a} = \frac{b^2 - \delta^2}{4a^2} = \frac{c}{a}.$$

□

Remarque 3.2.2.
• Avec $\alpha, \beta \in \mathbb{C}$, on a la relation suivante :

$$(X - \alpha)(X - \beta) = X^2 - (\alpha + \beta)X + \alpha\beta.$$

• On peut donc connaître la somme et le produit des deux racines sans connaître les racines. Réciproquement, si l'on connaît la somme et le produit de deux nombres complexes, alors on connaît une équation polynomiale du second degré dont ils sont exactement les racines.

Exercice 3.2.3.
Trouver a et b tels que $ab = 2$ et $a + b = i$.

4 Techniques de calcul

4.1 Formules trigonométriques

Nous avons utilisé les formules de trigonométrie (cf. formulaire de trigonométrie) dans la démons-

tration de 2.1.4.

Néanmoins, les propriétés de l'exponentielle « de $i\theta$ » permettent de retrouver ces formules, dans le cas inenvisageable où vous les auriez oubliées.

Par exemple : développer $\mathrm{e}^{\,i(a+b)}$ de deux manières différentes, identifier les expressions obtenues et retrouver les formules donnant $\sin(a+b)$ et $\cos(a+b)$.

4.2 Technique de l'angle moitié

Déjà vu. Elles permet aussi de retrouver les formules de factorisation du type $\cos(a)+\cos(b)$.

4.3 Factorisation

Utilise la technique de l'angle moitié, souvent après avoir identifié la somme en question comme la partie réelle ou imaginaire d'un type de somme bien connue. On admet temporairement les formules suivantes.

Sommation géométrique : Pour tout $z \in \mathbb{C}$ et $n \in \mathbb{N}$,

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

Binôme de Newton : Pour tout $(a,b) \in \mathbb{C}^2$ et $n \in \mathbb{N}$,

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

On peut calculer les coefficients binomiaux $\binom{n}{k}$ avec le triangle de Pascal.

Exemple 4.3.1.

$$\sum_{k=0}^{n} \cos(4kx) = \begin{cases} \frac{\sin(2(n+1)x)\cos(2nx)}{\sin(2x)} & \text{si } x \notin \frac{\pi}{2}\mathbb{Z} \\ n+1 & \text{si } x \in \frac{\pi}{2}\mathbb{Z} \end{cases}$$

4.4 Linéarisation

Méthode pour supprimer les produits et puissances dans une expression en cosinus et sinus :

1- Utiliser la formule d'Euler et développer.

2- Regrouper les puissances pour réutiliser les formules d'Euler, mais dans l'autre sens.

Exemple 4.4.1.

$$\cos^3 x = \frac{1}{4}\cos(3x) + \frac{3}{4}\cos x$$
$$\sin^3(x)\cos^2(x) = -\frac{1}{16}\sin(5x) + \frac{1}{8}\sin(x) + \frac{1}{16}\sin(3x)$$

4.5 L'exponentielle complexe

Définition 4.5.1.
Soit $z \in \mathbb{C}$, donné sous forme algébrique $z = x+iy$. On appelle *exponentielle de z* notée $\mathrm{e}^{\,z}$ le nombre complexe $\mathrm{e}^{\,z} = \mathrm{e}^{\,x}\mathrm{e}^{\,iy}$.

Remarque 4.5.2.
$\mathrm{e}^{\,z}$ n'est toujours pas une puissance : ce n'est qu'une notation.

Exemple 4.5.3.
$\mathrm{e}^{\,2+i\pi/2} = i\mathrm{e}^{\,2}$.

Théorème 4.5.4. (i) l'exponentielle complexe est $2i\pi$-périodique.

(ii) pour tous $z, z' \in \mathbb{C}$, $\mathrm{e}^{\,z+z'} = \mathrm{e}^{\,z}.\mathrm{e}^{\,z'}$: on dit que l'exponentielle transforme les sommes en produits.

(iii) l'exponentielle complexe ne s'annule pas.

(iv) pour tous $z \in \mathbb{C}$ et $t \in \mathbb{C}^*$, on a

$$\mathrm{e}^{\,z} = t \iff \exists k \in \mathbb{Z} \quad z = \ln|t| + i\arg t + 2ik\pi$$

Démonstration. (i) facile.

(ii) Séparer parties réelle et imaginaire.

(iii) L'exponentielle ne s'annule pas sur $\mathbb{R}$, et $\mathrm{e}^{\,i\theta}$ non plus (déjà vu).

(iv) $\mathrm{e}^{\,z} = t$ si et seulement si $\mathrm{e}^{\,\mathrm{Re}\,z} = |t|$ et $\mathrm{Im}\,z = \arg t[2\pi]$.

□

Remarque 4.5.5.
L'exponentielle n'est ni surjective, ni injective, et il n'existe pas de « logarithme complexe ».

5 Nombres complexes et géométrie plane

5.1 Colinéarité et orthogonalité

a Interprétation géométrique du rapport

Théorème 5.1.1.
Soit z et z' deux complexes non nuls. On note $\overrightarrow{u}$ et $\overrightarrow{u}'$ les vecteurs d'affixes respectives z et z'. Alors

$$\left|\frac{z'}{z}\right| = \frac{\|\overrightarrow{u}'\|}{\|\overrightarrow{u}\|}$$
$$\arg\left(\frac{z'}{z}\right) = (\overrightarrow{u}, \overrightarrow{u}') \quad [2\pi]$$

Démonstration.
Le premier point est immédiat, le second découle de l'interprétation géométrique de l'argument. En notant $\overrightarrow{i}$ le vecteur d'affixe 1, et en posant $\theta = \arg z$, on a $z = |z|(\cos\theta + i\sin\theta)$, donc $(\overrightarrow{i}, \overrightarrow{u}) = \arg z \quad [2\pi]$. De même $(\overrightarrow{i}, \overrightarrow{u}') = \arg z' [2\pi]$. D'où

$$\begin{aligned}(\overrightarrow{u}, \overrightarrow{u}') &= (\overrightarrow{i}, \overrightarrow{u}') - (\overrightarrow{i}, \overrightarrow{u}) && [2\pi]\\ &= \arg z' - \arg z && [2\pi]\\ &= \arg\left(\frac{z'}{z}\right) && [2\pi]\end{aligned}$$

□

Corollaire 5.1.2.
Soit A, B et M trois points deux à deux distincts d'affixes respectives a, b et z. Alors

(i) A, B et M sont alignés si et seulement si $\dfrac{z-a}{z-b} \in \mathbb{R}$;

(ii) $(AM)\perp(BM)$ si et seulement si $\dfrac{z-a}{z-b} \in i\mathbb{R}$.

Exemple 5.1.3.
i, 1 et $2-i$ sont alignés, et $1+i$, 2 et $-2i$ forment un angle droit en 2.

5.2 Transformations usuelles

Définition 5.2.1 (Transformations usuelles du plan)**.**
Soit M et M' deux points du plan, $\overrightarrow{u}$ un vecteur, Ω un point du plan, $\theta \in \mathbb{R}$ et $\lambda \in \mathbb{R}^*$.

1. La translation de vecteur $\overrightarrow{u}$ est l'application qui envoie M sur M', vérifiant $\overrightarrow{MM'} = \overrightarrow{u}$.
2. La rotation de centre Ω et d'angle θ est l'application qui fixe Ω et qui envoie tout point M différent de Ω, sur M' vérifiant $\Omega M = \Omega M'$ et $(\widehat{\overrightarrow{\Omega M}, \overrightarrow{\Omega M'}}) = \theta[2\pi]$.
3. L'homothétie de centre Ω et de rapport λ est l'application qui envoie M sur M', vérifiant $\overrightarrow{\Omega M'} = \lambda\overrightarrow{\Omega M}$.

Théorème 5.2.2.
Soit M un point d'affixe z, et Ω un point d'affixe ω.

(i) Soit $\overrightarrow{u}$ un vecteur d'affixe u. L'image de M par la translation de vecteur $\overrightarrow{u}$ a pour affixe le nombre complexe $z+u$;

(ii) Soit $\lambda \in \mathbb{R}$. L'image de M par l'homothétie de centre Ω et de rapport λ a pour affixe le nombre complexe $\omega + \lambda(z-\omega)$;

(iii) Soit $\theta \in \mathbb{R}$. L'image de M par la rotation de centre Ω et d'angle de mesure θ a pour affixe le nombre complexe $\omega + \mathrm{e}^{i\theta}(z-\omega)$. En particulier, iz est l'affixe de l'image de M par la rotation de centre O et d'angle de mesure $\frac{\pi}{2}$;

(iv) L'image de M par la symétrie centrale de centre O a pour affixe le nombre complexe $-z$;

(v) L'image de M par la symétrie par rapport à l'axe des abscisses (Ox) a pour affixe le nombre complexe $\overline{z}$;

(vi) L'image de M par la symétrie par rapport à l'axe des ordonnées (Oy) a pour affixe le nombre complexe $-\overline{z}$.

Démonstration. (i) L'image M' de M est telle que $\overrightarrow{OM'} = \overrightarrow{OM} + \overrightarrow{u}$. On traduit cela en termes d'affixes.

(ii) $\overrightarrow{\Omega M'} = \lambda\overrightarrow{\Omega M}$, donc $z' - \omega = \lambda(z - \omega)$.

(iii) $\Omega M' = \Omega M$ et $(\overrightarrow{\Omega M'}, \overrightarrow{\Omega M}) = \theta[2\pi]$, donc $|z - \omega| = |z' - \omega|$ et $\arg(z' - \omega) - \arg(z - \omega) = \theta[2\pi]$, d'où $z' - \omega = \mathrm{e}^{i\theta}(z - \omega)$.

(iv) C'est une homothétie de centre O et de rapport -1.

(v) Déjà vu.

(vi) On compose.

□

Exemple 5.2.3. 1. L'homothétie de centre $(2 - i)$ et de rapport 3 s'écrit : $z \mapsto 3(z - 2 + i) + 2 - i = 3z - 4 + 2i$.

2. La rotation de centre 0 et d'angle $\dfrac{\pi}{2}$ s'écrit $z \mapsto iz$.

3. La rotation de centre $(1 + i)$ et d'angle $\dfrac{2\pi}{3}$ s'écrit $z \mapsto j(z - 1 - i) + 1 - i$.

5.3 Similitudes et isométries

Définition 5.3.1.
Soit $\lambda > 0$. On appelle *similitude (plane) de rapport* λ toute application f du plan dans lui-même telle que pour tous points M, N on ait :

$$f(M)f(N) = \lambda MN$$

On appelle *isométrie (plane)* toute application f du plan dans lui-même telle que pour tous points M, N on ait :

$$f(M)f(N) = MN$$

Remarque 5.3.2. 1. Comme le nom l'indique (racines grecques), les isométries préservent les distances.

2. Les isométries sont les similitudes de rapport 1.

3. La composée de deux isométries est une isométrie.

4. La composée de deux similitudes est une similitude de rapport le produit des rapports de celles-ci.

5. Il est clair que toute similitude est injective. On verra ci-dessous que toute similitude est en fait bijective.

Exemple 5.3.3.
Les translations, les rotations, les symétries et les homothéties sont des similitudes.

Dans la suite de ce chapitre, on identifiera le plan complexe et $\mathbb{C}$, c'est-à-dire qu'on identifiera un point avec son affixe. Les applications du plan dans lui-même sont donc les applications de $\mathbb{C}$ dans lui-même. En ce qui concerne les similitudes, on a alors le résultat suivant :

Théorème 5.3.4. (i) Les similitudes planes sont exactement toutes les applications de la forme $z \mapsto az + b$ ou $z \mapsto a\overline{z} + b$, où $(a, b) \in \mathbb{C}^2$ avec $a \neq 0$;

(ii) Les isométries planes sont exactement toutes les applications de la forme $z \mapsto az + b$ ou $z \mapsto a\overline{z} + b$, où $(a, b) \in \mathbb{C}^2$, et $|a| = 1$.

Démonstration.
Soit f une application de la forme $z \mapsto a\overline{z}+b$, où $(a, b) \in \mathbb{C}^2$ avec a non nul.

Alors, soit $(z, z') \in \mathbb{C}^2$. On a $|f(z') - f(z)| = |a|\left|\overline{z'} - \overline{z}\right| = |a||z' - z|$. Donc f est une similitude de rapport $|a|$.

De même, toute application f de la forme $z \mapsto az + b$, où $(a, b) \in \mathbb{C}^2$ et $a \neq 0$ est également une similitude de rapport $|a|$.

Donc les application de la forme données dans l'énoncé du théorème sont bien des similitudes dans le cas général et des isométries dans le cas où $|a| = 1$.

Il reste à montrer que toutes les similitudes et les isométries sont de la forme donnée dans l'énoncé.

1. Remarquons tout d'abord qu'il existe une unique isométrie plane fixant 0, 1 et i. En effet, soit f une telle isométrie, c'est-à-dire vérifiant $f(0) = 0$, $f(1) = 1$ et $f(i) = i$.

   Alors, soit $z \in \mathbb{C}$. z s'écrit sous la forme $x + iy$ et $f(z)$ sous la forme $x' + iy'$ où $(x, y, x', y') \in \mathbb{R}^4$.

   On a $|f(z) - f(0)| = |z - 0|$, donc $x'^2 + y'^2 = x^2 + y^2$.

   De plus $|f(z) - f(1)| = |z - 1|$, donc $(x' - 1)^2 + y'^2 = (x - 1)^2 + y^2$.

   Par soustraction de ces deux égalités, on déduit $x' = x$.

   En outre, $|f(z) - f(i)| = |z - i|$, donc $x'^2 + (y' - 1)^2 = x^2 + (y - 1)^2$.

Par soustraction de cette égalité à la première, on déduit $y' = y$.

On a donc $f(z) = z$.

Donc f est nécessairement l'identité.

Réciproquement l'identité est bien une isométrie fixant 0, 1 et i.

2. Montrons maintenant qu'il existe deux isométries planes et deux seulement fixant 0 et 1. Soit f une telle isométrie. $f(i)$ s'écrit sous la forme $x + iy$ où $(x, y) \in \mathbb{R}^2$.

   On a $|f(i) - f(0)| = |i - 0| = 1$, donc $x^2 + y^2 = 1$. De plus $|f(i) - f(1)| = |i - 1|$, donc $(x - 1)^2 + y^2 = 2$.

   Par soustraction de ces deux égalités, on a donc $2x - 1 = -1$, donc $x = 0$. On en déduit $y^2 = 1$, donc $y = 1$ ou $y = -1$.

   Si $y = 1$, alors $f(i) = i$ et d'après ce qui précède, f est nécessairement l'identité.

   Sinon, $y = -1$ et $f(i) = -i$. Notons $s : z \mapsto \overline{z}$. s est bien une isométrie donc $s \circ f$ est une isométrie. Or $s \circ f$ fixe 0, 1 et i. Donc c'est l'identité : $s \circ f = \mathrm{Id}$, donc $s \circ s \circ f = s \circ \mathrm{Id}$, donc $f = s$.

   On a donc $f = \mathrm{Id}$ ou $f = s$.

   Réciproquement s et Id sont bien des isométries fixant 0 et 1.

3. Montrons maintenant que toute similitude fixant 0 est de la forme $z \mapsto az$ ou de la forme $z \mapsto a\overline{z}$ avec $a \neq 0$.

   Soit f une telle similitude. Alors posons $a = f(1)$. On a $f(0) = 0$ et f est injective donc $a \neq 0$. Notons alors g la similitude $z \mapsto z/a$. $g \circ f$ est une similitude fixant 0 et 1.

   Donc son rapport est 1 : c'est une isométrie. On a donc $g \circ f = \mathrm{Id}$ ou $g \circ f = s$ (où $s : z \mapsto \overline{z}$).

   En composant à gauche par $z \mapsto az$, on en déduit que f est l'application $z \mapsto az$ ou $z \mapsto a\overline{z}$.

4. Montrons maintenant le résultat. Soit f une similitude. Alors posons $b = f(0)$ et $g : z \mapsto z - b$. $g \circ f$ est une similitude fixant 0, donc est de la forme $z \mapsto az$ ou $z \mapsto a\overline{z}$. En composant à gauche par $z \mapsto z + b$, on en déduit que f est de la forme $z \mapsto az + b$ ou de la forme $z \mapsto a\overline{z} + b$ avec $a \neq 0$.

   Dans les deux cas, le rapport de la similitude est $|a|$. Si f est de plus une isométrie, on a donc de plus $|a| = 1$.

□

Définition 5.3.5 (Similitude directe/indirecte)**.** On distingue les similitudes directes et indirectes :

(i) Toute similitude plane de la forme $z \mapsto az + b$, avec $a, b \in \mathbb{C}$ et $a \neq 0$ préserve les angles orientés de vecteurs, et est dite *directe*.

(ii) Toute similitude plane de la forme $z \mapsto a\overline{z} + b$, avec $a, b \in \mathbb{C}$ et $a \neq 0$ renverse les angles orientés de vecteurs, et est dite *indirecte*.

Démonstration. (i) Soient $a, b \in \mathbb{C}$ tels que $a \neq 0$ et soit f la similitude $z \mapsto az + b$. Soient en outre u, v et w trois points distincts. Leurs images respectives par f sont notées u', v' et w'. Alors

$$\frac{u' - w'}{u' - v'} = \frac{(au + b) - (aw + b)}{(au + b) - (av + b)} = \frac{a(u - w)}{a(u - v)} = \frac{u - w}{u - v}$$

d'où égalité des arguments de ces expressions, et l'égalité des angles recherchée.

(ii) On obtient, de la même façon,

$$\frac{u' - w'}{u' - v'} = \overline{\left(\frac{u - w}{u - v}\right)}$$

d'où le résultat.

□

Exemple 5.3.6.
Translations, rotations et homothéties vs. symétries axiales.

Théorème 5.3.7 (Caractérisation géométrique)**.** Toute similitude plane directe est soit une translation, soit la composée d'une homothétie de rapport strictement positif et d'une rotation de même centre. Dans ce second cas, si f est la composée d'une homothétie de centre ω et de rapport $\lambda > 0$, et d'une rotation de centre ω et d'angle de mesure θ, alors on dit que f est la *similitude (directe) de centre ω, de rapport λ et d'angle de mesure θ.*

Toute isométrie plane directe est soit une translation, soit une rotation.

Démonstration.
Soient $(a, b) \in \mathbb{C}$ tels que $a \neq 0$ et soit f la similitude $z \mapsto az + b$. Si $a = 1$, alors f est une translation de vecteur d'affixe b. Supposons donc que $a \neq 1$. Alors f possède un

unique point fixe, $\omega = \dfrac{b}{1-a}$. On a alors :

$$\begin{aligned} f(z) - \omega &= f(z) - f(\omega) \\ &= (az+b) - (a\omega + b) \\ &= a(z-\omega) \\ &= |a| \times \underbrace{\underbrace{\left(\mathrm{e}^{\,i \arg a}(z-\omega)\right)}_{\text{rotation de centre } \omega \text{ et d'angle de mesure } \arg a}}_{\text{homothétie de centre } \omega \text{ et de rapport } |a| > 0} \\ &= \mathrm{e}^{\,i \arg a} \times \underbrace{\underbrace{\left(|a|(z-\omega)\right)}_{\text{homothétie de centre } \omega \text{ et de rapport } |a| > 0}}_{\text{rotation de centre } \omega \text{ et d'angle de mesure } \arg a} \end{aligned}$$

Le résultat sur les isométries découle immédiatement de celui sur les similitudes. □

Exemple 5.3.8.
L'application $f \;\; z \mapsto (1+i)z + 2$ est la similitude directe de centre $2i$, de rapport $\sqrt{2}$ et d'angle de mesure $\dfrac{\pi}{4}$.

Chapitre II

Quelques fondamentaux

1 Propositions

Définition 1.0.1.
Une *proposition* est un énoncé qui peut prendre deux valeurs de vérité : « vrai » (V) ou « faux » (F).

Exemple 1.0.2.
• $2 > 7$
• Pour tout nombre réel x, il existe un entier n tel que $n \leqslant x < n + 1$.

2 Connecteurs logiques

Définition 2.0.1.
Un **connecteur logique** est un outil mathématique permettant de construire une proposition à partir d'une ou plusieurs propositions.

Définition 2.0.2.
La *table de vérité* d'une proposition construite à partir de connecteurs logiques est la donnée de la valeur de vérité de cette proposition pour chaque jeu de valeur de vérité des propositions prises en argument des connecteurs.

Définition 2.0.3.
Deux propositions sont dites ***équivalentes*** si elles ont la même table de vérité. On utilise alors le connecteur $\equiv$.

Les paragraphes suivants présentent les connecteurs logiques les plus utilisés en mathématiques.

2.1 Négation

Définition 2.1.1.
Soit p une proposition. La proposition « non p », notée $\neg p$, est la proposition qui est vraie quand p est fausse, et fausse quand p est vraie. Sa table de vérité est :

p	$\neg p$
V	F
F	V

Théorème 2.1.2 (Loi de la double négation)**.**
Soit p une proposition, p et « non (non p) » sont deux propositions équivalentes, ce qui s'écrit :

$$p \equiv \neg(\neg p).$$

Démonstration.
Avec une table de vérité :

p	$\neg p$	$\neg(\neg p)$
V	F	V
F	V	F

□

2.2 Conjonction « et » et disjonction « ou »

Définition 2.2.1.
Soient p et q deux propositions.
— La *conjonction* de p et q est une proposition dite « p et q » et notée $p \wedge q$, qui est vraie si p et q sont vraies, et qui est fausse sinon.
— La *disjonction* de p et q est une proposition dite « p ou q » et notée $p \vee q$, qui est fausse si p et q sont fausses, et qui est vraie sinon.
Les tables de vérités de ces connecteurs sont donc :

p	q	$p \wedge q$	$p \vee q$
V	V	V	V
F	V	F	V
F	F	F	F
V	F	F	V

Remarque 2.2.2.
Il existe un autre « ou », le « ou exclusif » : si p et q sont deux propositions, la proposition « p ou

exclusif q » est vraie si et seulement si p est vraie ou q est vraie, mais pas les deux. Autrement dit, cette proposition est fausse si et seulement si p et q ont même valeur de vérité.
Dans la vie courante, on utilise intuitivement le ou exclusif. Ex : fromage ou dessert.
Très classique : un logicienne, enceinte, croise un ami.
L'ami : « c'est un garçon ou une fille ? »
La logicienne : « Oui. »

Proposition 2.2.3 (Tiers exclu)**.**
Pour toute proposition p, $p \vee \neg p$ est vraie.

Proposition 2.2.4 (Non contradiction)**.**
Pour toute proposition p, $p \wedge \neg p$ est fausse.

Démonstration.
Écrire les tables de vérités de $p \vee \neg p$ et $p \wedge \neg p$. □

Théorème 2.2.5 (Lois de De Morgan)**.**
Soit p et q deux propositions.

1. $\neg(p \wedge q) \equiv (\neg p) \vee (\neg q)$.
2. $\neg(p \vee q) \equiv (\neg p) \wedge (\neg q)$.

Démonstration. 1. Construire les tables de vérité de ces deux propositions et constater que ce sont les mêmes.

2. Par le premier point et la loi de double négation,

$$\begin{aligned}\neg(p \vee q) &\equiv \neg([\neg\neg p] \vee [\neg\neg q]) \\ &\equiv \neg(\neg[(\neg p) \wedge (\neg q)]) \\ &\equiv (\neg p) \wedge (\neg q).\end{aligned}$$

□

Exemple 2.2.6.
• Nier « je n'aime ni le chocolat ni la vanille ».
• Dans $\mathbb{R}^2$, dessiner l'ensemble $\{(x, y) \in \mathbb{R}^2 \mid x < 2 \text{ et } y \leqslant 3\}$, dessiner et décrire son complémentaire.

Exercice 2.2.7.
Soit p, q et r trois propositions. À quoi sont logiquement équivalentes $p \wedge (q \vee r)$ et $p \vee (q \wedge r)$?

2.3 Implication

Définition 2.3.1.
Soient p et q deux propositions. On appelle $p \Rightarrow q$, qui se dit « p implique q », ou « si p alors q », la proposition $(\neg p) \vee q$. Dans l'implication $p \Rightarrow q$, p est l'antécédent, q le conséquent.

Exercice 2.3.2.
Construire la table de vérité de $p \Rightarrow q$.

Remarque 2.3.3.
En pratique, pour démontrer une implication, on commence toujours, bêtement, par « supposons p vraie ». Il faut alors montrer que sous cette hypothèse q est vraie.

— $p \Rightarrow q$ peut être vraie même si p et q n'ont rien à voir. Par exemple : si $1 \geqslant 0$ alors l'eau mouille.
— $p \Rightarrow q$ est toujours vraie si p est fausse (le faux implique n'importe quoi) ou q est vraie. Ainsi, si « $0 \neq 0$ » alors « $0 = 0$ »(cela peut paraître étonnant, on reviendra dessus à la fin du paragraphe « équivalence ») .
— $p \Rightarrow q$ n'implique ni que p est vraie ni que q est vraie. Par exemple : Si les pommes étaient des citrouilles, Newton serait mort assommé. Ou bien : si je mesurais 2 m 20, je serais entraîneur de basket.

Proposition 2.3.4 (Modus Ponens)**.**
Soit p et q deux proposition. Si $p \Rightarrow q$ est vraie et si p est vraie, alors q est vraie.
Autrement dit, $[p \wedge (p \to q)] \Rightarrow q$ est toujours vraie.

Démonstration.
Consulter la table de vérité de $p \Rightarrow q$ ou de $[p \wedge (p \to q)] \Rightarrow q$. □

Théorème 2.3.5 (Négation d'une implication)**.**
Soit p et q deux propositions, alors $\neg(p \Rightarrow q) \equiv (p \wedge (\neg q))$.

Démonstration.
C'est une conséquence simple de la loi de De Morgan. □

Exemple 2.3.6.
En pratique, pour montrer $p \Rightarrow q$ est fausse on peut trouver un exemple où p est vraie mais où q est fausse.

Ainsi, avoir 18 ans n'implique pas d'avoir droit de vote (ex : si on a casier judiciaire). De même, mesurer 2 m 20 n'implique pas d'être un joueur de basket.

Théorème 2.3.7 (Contraposition)**.**
Soit p et q deux propositions, alors $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$.

Démonstration.
C'est une conséquence simple de la loi de double négation. □

Remarque 2.3.8.
On peut formaliser ainsi le principe de « démonstration par l'absurde » : on veut montrer que p est vraie, sachant qu'une certaine proposition q est fausse.

On suppose alors que p est fausse et si l'on arrive à montrer que q est vraie : on a obtenu une contradiction ! En fait on a montré $\neg p \Rightarrow q$, et donc $\neg q \Rightarrow p$. Comme $\neg q$ est vraie, on a p qui est vraie.

Exemple 2.3.9.
Un entier ne peut pas être pair et impair.

Démonstration.
Soit n pair et impair. Alors il existe $k, k' \in \mathbb{Z}$ tels que $n = 2k = 2k' + 1$, donc $k - k' = 1/2$ est un entier, ce qui est absurde. □

2.4 Équivalence

Définition 2.4.1.
Soient p et q deux propositions. La proposition $p \Leftrightarrow q$, qui se lit « p équivaut à q », est la proposition qui est vraie si et seulement si p et q ont la même valeur de vérité.

Exercice 2.4.2.
Construire la table de vérité de $p \Leftrightarrow q$.

Théorème 2.4.3 (Équivalence et double implication)**.**
Soit p et q deux propositions, alors

$$(p \Leftrightarrow q) \equiv ([p \Rightarrow q] \wedge [q \Rightarrow p])$$

Démonstration.
Il suffit d'écrire les tables de vérités de ces propostions. □

Définition 2.4.4.
$q \Rightarrow p$ est appelée la *réciproque* de $p \Rightarrow q$.

• En pratique : pour montrer $p \Leftrightarrow q$, il y a 3 méthodes :

1. Montrer $p \Leftrightarrow p_1 \Leftrightarrow p_2 \ldots \Leftrightarrow q$ où les p_i sont des propositions intermédiaires ;
2. Montrer $q \Rightarrow p$ puis $p \Rightarrow q$;
3. Montrer $p \Rightarrow q$ puis la contraposée de sa réciproque, i.e. $\neg p \Rightarrow \neg q$

Définition 2.4.5.
Soient p et q deux propositions.
On dit que la proposition p est *nécessaire* pour avoir la proposition q si $q \Rightarrow p$ est vraie.
On dit que la proposition p est *suffisante* pour avoir la proposition q si $p \Rightarrow q$ est vraie.
On dit que la proposition p est *nécessaire et suffisante* pour avoir la proposition q si $q \Leftrightarrow p$ est vraie.

Remarque 2.4.6.
Revenons sur la table de vérité de l'implication.

Intuitivement, si p est vraie et q fausse, $p \Rightarrow q$ est fausse. De même, si p et q sont vraies, on conçoit que $p \Rightarrow q$ le soit.

Dans les deux autres cas, l'intuition se perd. Constatons que si $p \Rightarrow q$ était vraie si p était fausse et q vraie, ou si $p \Rightarrow q$ était fausse si p et q étaient fausses, la table de l'implication serait la même que celle d'une autre connecteur logique déjà connu (construire et identifier les tables de tous les connecteurs possibles de deux propositions pour s'en convaincre).

Exemple 2.4.7.
Montrons que $\sqrt{2} \notin \mathbb{Q}$.

Démonstration.
On montre d'abord que, si n est un entier, alors « n est pair » si et seulement si « n^2 est pair ».

Si n est pair, son reste dans la division euclidienne par 2 est nul : il existe $k \in \mathbb{Z}$ tel que $n = 2k$. Donc $n^2 = 2 \times 2k^2$ est pair.

Si n est impair, son reste dans la division euclidienne par 2 n'est pas nul, donc vaut 1 : il existe $k \in \mathbb{Z}$ tel que $n = 2k + 1$. Donc $n^2 = 2 \times (2k^2 + 2k) + 1$ est impair.

On vient bien de montrer l'équivalence annoncée.

Puis, on suppose que $\sqrt{2} \in \mathbb{Q}$ et l'on écrit $\sqrt{2}$ sous forme fractionnelle irréductible : il existe $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ sans diviseurs communs autres que 1 ou -1, tels que $\sqrt{2} = \frac{p}{q}$.

On élève au carré : $p^2 = 2q^2$, donc p^2 est pair, donc p aussi. Il existe donc $p' \in \mathbb{Z}$ tel que $p = 2p'$, et l'on a alors $q^2 = 2p'^2$, donc q^2 est pair et q est pair aussi.

Ainsi, p et q ont bien un diviseur non trivial, 2, c'est absurde, donc $\sqrt{2} \notin \mathbb{Q}$. □

Remarque 2.4.8.
Vous remarquerez que les symboles $\Rightarrow$ et $\Leftrightarrow$ n'ont pas été utilisés dans la démonstration précédente. C'est normal : ils servent à construire des phrases formelles, pas à les démontrer. On ne les utilise donc JAMAIS dans une démonstration : à la place, on rédige EN FRANÇAIS, en utilisant par exemple la conjonction de coordination « donc ».

3 Quantificateurs universel et existentiel

3.1 Définition

Définition 3.1.1.
On appelle *prédicat* toute proposition dépendant d'une ou plusieurs variables, et qui, pour chaque jeu de valeurs de ces variables, prend la valeur V ou F.

Exemple 3.1.2.
$P(x, y) \equiv x + y = 2$.

Définition 3.1.3.
Si P est un prédicat qui dépend de la variable x et éventuellement d'autres variables, alors $\forall x, P(x)$ et $\exists x, P(x)$ sont deux prédicats qui ne dépendent pas de x et :

- $\forall x, P(x)$ est vrai si, pour toutes les valeurs de x, $P(x)$ est vrai ;
- $\exists x, P(x)$ est vrai s'il existe une valeur de x pour laquelle $P(x)$ est vrai.

$\forall$ est appelé *quantificateur universel* et $\exists$ est le *quantificateur existentiel*.

Remarque 3.1.4.
On spécifiera tout le temps dans les quantificateurs les ensembles sur lesquels sont considérées les variables. On écrira par exemple

$$\forall x \in \mathbb{R},\ x^2 \geqslant 0$$

et

$$\forall a \in \mathbb{R},\ \exists n \in \mathbb{Z},\ a \geqslant n.$$

Remarque 3.1.5.
Si P est un prédicat d'une variable, $\forall x, P(x)$ est un prédicat de zéro variables, c'est-à-dire une proposition.

Exemple 3.1.6.
• Soit $P(x, y) \equiv xy = 0$. Alors $\forall x \in \mathbb{R}, \forall y \in \mathbb{R},\ P(x, y)$ est fausse, mais $\exists x \in \mathbb{R}, \forall y \in \mathbb{R},\ P(x, y)$ est vraie.
• Soit $P'(x) \equiv x.0 = 0$: alors $\forall x \in \mathbb{C},\ P'(x)$ est vraie.

 Les quantificateurs sont des symboles mathématiques utilisés pour construire des phrases mathématiques. Ils ne sont en aucun cas à utiliser au cours d'une démonstration. En pratique :

- Pour montrer que $\forall x \in E, P(x)$ est vraie, on commencera (presque) toujours par écrire « Soit x un élément de E » : x est maintenant fixé (et pris quelconque), on peut maintenant montrer $P(x)$.
- Pour montrer que $\exists x \in E, P(x)$ est vraie, il « suffira » d'exhiber une valeur de x dans E telle que $P(x)$ soit vraie.

Remarque 3.1.7.
Dans les propositions $\forall x, P(x)$ et $\exists x, P(x)$, la variable x est muette. On peut donc remplacer la lettre x par n'importe quelle autre lettre.

Par exemple, $\exists x \in \mathbb{R}, x^2 = -1$ est la même proposition que $\exists \xi \in \mathbb{R}, \xi^2 = -1$ et que $\exists \heartsuit \in \mathbb{R}, \heartsuit^2 = -1$

3.2 Permutation de quantificateurs

Proposition 3.2.1.
On peut permuter les $\forall$ entre eux et les $\exists$ entre eux.

Démonstration.
Admis. □

Remarque 3.2.2.
On abrégera parfois $\forall x \in E,\ \forall y \in E,\ P(x,y)$ en $\forall x, y \in E,\ P(x,y)$. C'est aussi équivalent à $\forall (x,y) \in E^2,\ P(x,y)$.

Exemple 3.2.3.
$\forall x \in \mathbb{N}, \forall y \in \mathbb{N}, x.y \geqslant 0 \equiv \forall y \in \mathbb{N}, \forall x \in \mathbb{N}, x.y \geqslant 0$
$\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y \leqslant 0 \equiv \exists y \in \mathbb{R}, \exists x \in \mathbb{R}, x + y \leqslant 0$

 On ne peut en général pas permuter un $\forall$ et un $\exists$.

Exemple 3.2.4.
Comparer les propositions : « pour toute poule il existe un oeuf d'où est sortie la poule » et « il existe un oeuf d'où sont sorties toutes les poules ».

Exercice 3.2.5.
Donner un exemple formel du dernier point.

3.3 Négation

Proposition 3.3.1.
Soit P un prédicat.

1. La négation de $\forall x P(x)$ est $\exists x, \neg P(x)$.
2. La négation de $\exists x, P(x)$ est $\forall x, \neg P(x)$.

Démonstration.
Admis. □

• En pratique, il faut savoir nier une phrase avec des $\forall$ et $\exists$.

Exemple 3.3.2.
$\forall x \in \mathbb{R}, \exists y \in \mathbb{Z}$ tq $x \leqslant y$ se nie en $\exists x \in \mathbb{R}$ tq $\forall y \in \mathbb{Z}, x > y$.

3.4 Le pseudo-quantificateur $\exists!$

Pour simplifier la rédaction, il existe le pseudo-quantificateur $\exists!$. La proposition $\exists! x, P(x)$ signifie : il existe un unique x tel que $P(x)$. Pour démontrer une telle proposition, il faut montrer d'un côté la partie existence, et d'un autre côté la partie unicité.

Exercice 3.4.1.
Écrire $\exists! x, P(x)$ en n'utilisant que les symboles $\forall$ et $\exists$.

3.5 Quantificateurs et inégalités.

On commet souvent un abus d'écriture, notamment en analyse, en raccourciçant la phrase

$$\forall x \in \mathbb{R},\ [x \geqslant M \Rightarrow P(x)]$$

en

$$\forall x \geqslant M, P(x).$$

Dans la deuxième écriture, la quantification porte implicitement sur x et non sur M (qui doit avoir été fixé ou quantifié auparavant). De plus, le domaine de P n'est plus explicitement défini.

Exemple 3.5.1.
Soit $(u_n)_{n\in\mathbb{N}}$ une suite de nombres réels, la proposition « $u_n \xrightarrow[n\to+\infty]{} +\infty$ » (qui se lit « (u_n) tend vers $+\infty$ ») s'écrit formellement

$$\forall A \in \mathbb{R},\ \exists n_0 \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geqslant n_0 \Rightarrow u_n \geqslant A,$$

mais on l'écrira plutôt

$$\forall A \in \mathbb{R},\ \exists n_0 \in \mathbb{N},\ \forall n \geqslant n_0,\ u_n \geqslant A.$$

4 Raisonnement par récurrence

L'objectif de cette partie est de montrer comment rédiger une récurrence, à partir d'exemples, en présentant en particulier quelques erreurs courantes, mais aussi de présenter une autre technique de démonstration, extrêmement puissante, appelée principe du minimum.

Il y a plusieurs façons possibles de rédiger une récurrence. Néammoins l'expérience montre que les étudiants qui essaient de l'écrire de façon originale l'écrivent rarement correctement.

En d'autres termes : nous vous conseillons *très fortement* de suivre les modèles donnés ici, mais vous êtes absolument libres de ne pas suivre les conseils ci-dessous. Pour mémoire, dans 9 cas sur dix, ceux qui n'ont pas suivi le modèle donné ici rédigent mal leurs raisonnements par récurrence et perdent en conséquence les points correspondants dans leurs DS.

Pour fixer les idées, nous travaillerons essentiellement sur des exemples, et parfois sur des exemples très simples.

4.1 Principe du minimum

Définition 4.1.1.
Soit E un ensemble de réels. On appelle *minimum* de E, tout réel x vérifiant $x \in E$ et $\forall y \in E \quad x \leqslant y$.

Remarque 4.1.2.
1. Certains ensembles de réels n'admettent pas de minimum. Exemples : $]0,1]$, $]0,1]$, $\mathbb{R}$, $\mathbb{R}_+^*$, $\mathbb{R}_-$.
2. Tout ensemble de réels admet **au plus** un minimum.

Lorsqu'il existe, le minimum d'un ensemble E est noté $\min(E)$.

L'ensemble des entiers naturels possède la propriété fondamentale suivante qu'on admettra :

Proposition 4.1.3.
Tout ensemble E d'entiers naturels non vide admet un minimum.

Remarque 4.1.4.
Pour tout ensemble d'entiers naturels E, on a

$$\forall x \in [\![0, \min(E)[\![\quad x \notin E.$$

Corollaire 4.1.5.
Tout sous-ensemble de $\mathbb{Z}$ minoré (resp. majoré) non vide admet un minimum (resp. maximum).

Proposition 4.1.6 (Principe du minimum)**.**
Soit P un prédicat sur les entiers naturels. Supposons qu'il existe au moins un entier rendant faux le prédicat P. Alors l'ensemble des entiers naturels sur lesquels P est faux admet un plus petit élément n_0 et on a
1. non $(P(n_0))$,
2. et $\forall n \in [\![0, n_0[\![\quad P(n)$.

Exercice 4.1.7.
Soit N un entier non-nul et a_0, a_1, …, a_N des réels. On pose

$$\begin{array}{rccc} f: & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & \displaystyle\sum_{k=0}^{N} a_k x^k \end{array}.$$

On suppose $\forall x \in \mathbb{R} \quad f(x) = 0$.

Montrer que les coefficients a_0, a_1, …, a_N sont tous nuls.

Indication : si ces coefficients ne sont pas tous nuls, on pourra s'intéresser au plus grand coefficient a_k non-nul et regarder la limite de f en $+\infty$.

4.2 Principe de récurrence simple

a Principe utilisé

Définition 4.2.1.
Soit P un prédicat sur les entiers naturels. Pour $n \in \mathbb{N}$, on dit que P est *héréditaire au rang* n si et seulement si on a $P(n) \Rightarrow P(n+1)$ (autrement dit, P n'est pas héréditaire au rang n si et seulement si on a $P(n)$ et $\neg P(n+1)$)

On dit que P est *héréditaire* sur $\mathbb{N}$ si et seulement si P est héréditaire à tout rang, c'est-à-dire si et seulement si on a :

$$\forall n \in \mathbb{N} \qquad (P(n) \Rightarrow P(n+1))$$

Exemple 4.2.2.

Le prédicat : $P(n) : \sum_{k=0}^{n} k = n^2$ est-il héréditaire ?

Et le prédicat $Q(n) : \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$?

Et le prédicat $R(n) : \sum_{k=0}^{n} k = 2 + \frac{n(n+1)}{2}$?

Théorème 4.2.3 (Principe de récurrence simple)**.**
Soit P un prédicat sur les entiers naturels. Supposons qu'on a $P(0)$ et que P est héréditaire. Alors P est vraie pour tout entier naturel n.

Démonstration.
Il suffit d'appliquer le principe du minimum à $\neg P$: s'il existe un entier naturel n tel que $P(n)$ est fausse, on peut alors considérer le plus petit de ces entiers, noté n_0. Comme $P(0)$ est vraie, $n_0 > 0$ et donc $n_0 - 1 \in \mathbb{N}$. Ainsi, $P(n_0 - 1)$ est vraie et, comme P est héréditaire, $P(n_0)$ est aussi vraie, ce qui est absurde. On obtient donc bien que $\forall n \in \mathbb{N},\ P(n)$. □

Exemple 4.2.4.

Soit n un entier naturel. Montrons que $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.

Pour tout $n \in \mathbb{N}$, notons $P(n)$ l'assertion

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

Montrons $\forall n \in \mathbb{N}\ P(n)$ par récurrence.

— Montrons $P(0)$.
On a
$$\sum_{k=0}^{0} k = 0 = \frac{0(0+1)}{2},$$
donc on a $P(0)$.

— Soit $n \in \mathbb{N}$. Supposons $P(n)$ et montrons $P(n+1)$.
Alors, on a
$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$$
Ainsi,
$$\begin{aligned}\sum_{k=0}^{n+1} k &= \left(\sum_{k=0}^{n} k\right) + n + 1 \\ &= \frac{n(n+1)}{2} + n + 1 \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+2)(n+1)}{2},\end{aligned}$$
donc on a $P(n+1)$.

On a donc
$$\forall n \in \mathbb{N}\ P(n).$$

4.3 Erreurs classiques

Nous listons ici des erreurs fréquemment trouvées dans les copies.

Mauvaise définition de l'assertion Forme classique de cette erreur :

Notons $P(n)$ l'assertion
$$\text{«}\forall n \in \mathbb{N}\ \sum_{k=0}^{n} k = \frac{n(n+1)}{2}\text{»}$$

Explications : cette définition, mathématiquement, signifie exactement la même chose que :

Notons $P(n)$ l'assertion
$$\text{«}\forall p \in \mathbb{N}\ \sum_{k=0}^{p} k = \frac{p(p+1)}{2}\text{»}$$

Autrement dit, $P(n)$ ne dépend pas de n. Inutile alors de tenter une démonstration par récurrence...

Variante 1 :

Notons $P(n)$ l'assertion

«pour tout $n \in \mathbb{N}$, $\sum_{k=0}^{p} k = \frac{n(n+1)}{2}$».

Variante 2 :

Notons $P(n)$ l'assertion «$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$ pour tout $n \in \mathbb{N}$».

En revanche, la formulation suivante est acceptable, bien qu'à éviter :

Notons $P(n)$ l'assertion «$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$» pour tout $n \in \mathbb{N}$.

Mauvaise énonciation de l'objectif Forme classique de cette erreur :

Pour $n \in \mathbb{N}$, notons $P(n)$ l'assertion

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

Montrons $P(n)$ par récurrence.

Explications : on ne précise pas ici ce qu'est n. De plus, le principe de récurrence ne montre pas $P(n)$ pour un n donné mais pour tout n. Il convient donc d'écrire

Montrons $\forall n \in \mathbb{N}$ $P(n)$ par récurrence

ou une variante, comme

Montrons par récurrence que pour tout entier naturel n on a $P(n)$.

Mauvaise démonstration de l'hérédité Forme classique de cette erreur :

Supposons $\forall n \in \mathbb{N}$ $P(n)$.

Montrons $\forall n \in \mathbb{N}$ $P(n+1)$.

Explications : une fois que l'on a supposé $\forall n \in \mathbb{N}$ $P(n)$, il n'y a pas beaucoup de travail à fournir pour montrer $\forall n \in \mathbb{N}$ $P(n)$ ...

Variante 1 :

Supposons $\forall n \in \mathbb{N}$ $P(n)$.

Montrons $P(n+1)$.

Variante 2 :

Supposons, pour tout entier naturel n, $P(n)$ et montrons $P(n+1)$

Variante 3 :

Supposons, pour tout entier naturel n, $P(n)$ et montrons pour tout entier naturel n, $P(n+1)$.

4.4 Bonne définition d'une suite

Notons $(u_n)_{n\in\mathbb{N}}$ la suite définie par

$$\begin{cases} u_0 = 5 \\ \text{et } \forall n \in \mathbb{N}\ u_{n+1} = 2 + \sqrt{u_n - 1} \end{cases}$$

Montrer que la suite u est bien définie.

Ici, le terme «bien définie» signifie non seulement que pour tout n, on a bien donné une expression pour définir u_n mais aussi que cette expression est définie, c'est-à-dire qu'elle a mathématiquement un sens.

Pour n donné, montrer que u_n est bien définie est un préalable à la démonstration de toute propriété de u_n.

Ici, il s'agit de montrer que pour tout n l'expression $2 + \sqrt{u_n - 1}$ est bien définie, c'est-à-dire que $u_n - 1$ est positif ou nul, autrement dit $u_n \geqslant 1$.

Pour n donné, on voit alors que d'une part, pour montrer que u_{n+1} est bien défini, il va falloir montrer tout d'abord $u_n \geqslant 1$ et d'autre part, pour montrer $u_n \geqslant 1$, on va avoir besoin au préalable de s'assurer que u_n est bien défini.

Autrement dit : on va avoir besoin de démontrer simultanément ces deux propriétés.

Pour $n \in \mathbb{N}$, notons $P(n)$ l'assertion

«u_n est bien défini et $u_n \geqslant 1$»

Montrons $\forall n \in \mathbb{N}$ $P(n)$ par récurrence :

— On a clairement $P(0)$.
— Soit $n \in \mathbb{N}$. Supposons $P(n)$ et montrons $P(n+1)$.
u_n est bien défini et $u_n \geqslant 1$.
Donc $u_n - 1 \geqslant 0$.
Donc $\sqrt{u_n - 1}$ est bien défini.
Donc u_{n+1} est bien défini, et de plus

$$u_{n+1} \geqslant 2 + \sqrt{u_n - 1} \geqslant 2 \geqslant 1$$

Donc on a $P(n+1)$.
On a donc

$$\forall n \in \mathbb{N}\ P(n)$$

La suite u est donc bien définie (et de plus pour tout entier naturel n, $u_n \geqslant 1$).

Problème de définition non étudié On trouve parfois la réponse erronée suivante :

> Pour tout entier naturel n, $n = 0$ ou n est de la forme $k+1$. On a donné une définition à u_n dans chacun de ces deux cas, donc u est bien définie.

Manifestement, l'auteur du texte ci-dessus n'a pas compris que la définition $u_{n+1} = 2 + \sqrt{u_n - 1}$ pouvait poser problème.

4.5 Récurrence double

a Énoncé

Notons u la suite définie par :

$$\begin{cases} u_0 = 2 \\ u_1 = 3 \\ \forall n \in \mathbb{N},\ u_{n+2} = 1 + \sqrt{u_n + u_{n+1} - 2} \end{cases}$$

Montrer que u est bien définie.

On s'aperçoit vite qu'il va falloir montrer simultanément que u_n est bien défini et qu'on a $u_n \geqslant 1$.

On va donc, pour tout $n \in \mathbb{N}$, définir $P(n)$ comme l'assertion

$$\text{«}u_n \text{ est bien défini et } u_n \geqslant 1\text{»}$$

De plus, pour montrer cette P à un rang donné, il va falloir supposer qu'elle est vérifiée au deux rangs précédents.

Il ne suffit donc pas de chercher à démontrer P par récurrence. Pour répondre à cette question on va utiliser un principe de récurrence double, dans lequel l'initialisation consiste à montrer $P(0)$ et $P(1)$ et la démonstration de l'hérédité consiste à montrer

$$\forall n \in \mathbb{N}\ \Big(\big(P(n) \text{ et } P(n+1)\big) \Rightarrow P(n+2)\Big)$$

b Par récurrence double

Pour tout $n \in \mathbb{N}$, notons $P(n)$ la propriété

$$\text{«}u_n \text{ est bien défini et } u_n \geqslant 1\text{»}$$

Montrons $\forall n \in \mathbb{N}\ P(n)$ par récurrence double.
— On a clairement $P(0)$.
— On a clairement $P(1)$.
— Soit $n \in \mathbb{N}$. Supposons $P(n)$ et $P(n+1)$ et montrons $P(n+2)$.
u_n et u_{n+1} sont bien définis et de plus $u_n \geqslant 1$ et $u_{n+1} \geqslant 1$.
Donc $u_n + u_{n+1} - 2 \geqslant 0$.
Donc u_{n+2} est bien défini et de plus, $u_{n+2} = 1 + \sqrt{u_n + u_{n+1} - 2} \geqslant 1$.
Donc on a $P(n+2)$.
On a donc

$$\forall n \in \mathbb{N}\ P(n)$$

En particulier la suite u est bien définie.

c Énoncé du principe

Théorème 4.5.1 (Principe de récurrence double)**.**
Soit P un prédicat portant sur $\mathbb{N}$. Si :
- $P(0)$ et $P(1)$ sont vrais,
- pour tout $n \in \mathbb{N}$, si $P(n)$ et $P(n+1)$ sont vrais alors $P(n+2)$ est vrai,

alors $\forall n \in \mathbb{N},\ P(n)$.

Démonstration.
On peut montrer par récurrence simple que pour tout $n \in \mathbb{N}$, $Q(n)$: « $P(n)$ et $P(n+1)$ ».

Ou bien on peut utiliser le principe du minimum : si P n'est pas toujours vrai, on considère le plus petit entier pour lequel P est faux *etc.* □

4.6 Récurrence triple, etc.

On peut, de la même façon, avoir besoin de principes de récurrence triple, quadruple, ...

Si cela s'avère nécessaire, on pourra les utiliser sans démonstration.

Ainsi, appliquer le principe de récurrence triple pour démontrer $\forall n \in \mathbb{N}\ P(n)$ consistera à démontrer d'une part $P(0)$, $P(1)$ et $P(2)$, et d'autre part à démontrer que pour tout $n \in \mathbb{N}$, si on a $P(n)$ et $P(n+1)$ et $P(n+2)$ alors on a $P(n+3)$.

Là encore, si l'on préfère, on pourra se passer d'une récurrence triple et utiliser simplement la récurrence ordinaire. Il suffira pour cela de définir, pour tout $n \in \mathbb{N}$, $Q(n)$ comme

$$\text{«}P(n) \text{ et } P(n+1) \text{ et } P(n+2)\text{»}$$

et de montrer $\forall n \in \mathbb{N}\ Q(n)$ par récurrence simple.

Enfin, on peut évidemment là aussi se passer de tout principe de récurrence en utilisant le principe du minimum.

4.7 Récurrence forte

Enfin, il existe des cas où ni une récurrence simple, ni une récurrence double, ni une récurrence triple ne semblent suffire.

Dans ces cas, on pourra utiliser le principe de récurrence forte.

a Énoncé

Notons u la suite définie par

$$\begin{cases} u_0 = \sqrt{1/2} - 1 \\ \text{et } \forall n \in \mathbb{N}\ u_{n+1} = \sqrt{1/2 + n + 1 + \sum_{k=0}^{n} u_k} - 1 \end{cases}$$

Montrez que u est bien définie.

On s'aperçoit assez vite qu'on peut espérer montrer que pour tout $n \in \mathbb{N}$, on a $u_n \geqslant -1$. Mais pour montrer la propriété pour n donné, il va falloir supposer qu'elle est vraie pour toutes les entiers naturels strictement inférieurs.

On va donc utiliser le principe de récurrence forte.

Celui-ci peut s'énoncer comme suit :

1. Étant donné un entier naturel n, on dit qu'une propriété P est *fortement héréditaire au rang n* si
$$\Big(\forall m \in [\![0, n]\!]\ P(m)\Big) \Rightarrow P(n+1)$$
(ou de façon équivalente, si $P(0)$ et $P(1)$ et ...et $P(n)$ implique $P(n+1)$)
2. On dit qu'une propriété P est *fortement héréditaire* si pour tout entier naturel n, P est fortement héréditaire au rang n.
3. Le principe de récurrence forte dit simplement qu'une propriété P vraie en 0 et fortement héréditaire est vraie pour tout entier naturel.

Remarque 4.7.1.
Dire que P est fortement héréditaire au rang n est équivalent à dire que n ne peut pas être l'entier minimum pour lequel P est faux.

Exemple 4.7.2.
On peut montrer que tout prédicat héréditaire est fortement héréditaire. La réciproque est fausse comme le montre le prédicat P défini comme suit : pour $n \in \mathbb{N}$, $P(n)$ est l'assertion «$n(n-2) \neq 0$».

b Par le principe de récurrence forte

Pour tout $n \in \mathbb{N}$, notons $P(n)$ la propriété

$$\text{«}u_n \text{ est bien défini et } u_n \geqslant -1\text{»}$$

Montrons par récurrence forte que pour tout $n \in \mathbb{N}$, on a $P(n)$.

— On a clairement $P(0)$.

— Soit $n \in \mathbb{N}$. Supposons que pour tout $m \in \mathbb{N}$ vérifiant $m \leqslant n$, on a $P(m)$.
Montrons $P(n+1)$.
Pour tout $k \in \{0, \ldots, n\}$, u_k est bien défini, donc la somme $\sum_{k=0}^{n} u_k$ est bien définie.

En outre, pour tout $k \in \{0, \dots, n\}$, $u_k \geqslant -1$, donc

$$\sum_{k=0}^{n} u_k \geqslant \sum_{k=0}^{n} -1 = -n - 1$$

Donc

$$1/2 + n + 1 + \sum_{k=0}^{n} u_k \geqslant 0$$

Donc u_{n+1} est bien défini, et de plus, on a

$$u_{n+1} = \sqrt{1/2 + n + 1 + \sum_{k=0}^{n} u_k} - 1 \geqslant -1$$

Donc on a $P(n+1)$

Par le principe de récurrence forte, on a donc

$$\forall n \in \mathbb{N}\ P(n)$$

Donc u est bien définie.

c Énoncé du principe

Théorème 4.7.3 (Principe de récurrence forte)**.** Soit P un prédicat portant sur $\mathbb{N}$. Si :

- $P(0)$ est vrai,
- pour tout $n \in \mathbb{N}$, si $P(0)$, $P(1)$, ..., $P(n)$ sont vrais, alors $P(n+1)$ est vrai,

alors $\forall n \in \mathbb{N},\ P(n)$.

Démonstration.
On peut montrer par récurrence simple que pour tout $n \in \mathbb{N}$, $R(n)$: « $P(0)$ et $P(1)$ et ... et $P(n)$ ».

Ou bien on peut utiliser le principe du minimum : si P n'est pas toujours vrai, on considère le plus petit entier pour lequel P est faux *etc.* □

4.8 Récurrence à partir d'un certain rang

Il s'agit maintenant de faire démarrer la récurrence à un autre rang que le rang 0.

Énoncé Soit u une suite, n_0 un entier et α un réel strictement positif.

On suppose que pour tout $n \geqslant n_0$, on a

$$|u_{n+1}| \leqslant \alpha |u_n|$$

Montrer

$$\forall n \geqslant n_0 \quad |u_n| \leqslant \alpha^{n-n_0} |u_{n_0}|$$

Modèle proposé Pour tout $n \geqslant n_0$, notons $P(n)$ la propriété $|u_n| \leqslant \alpha^{n-n_0}$.

Montrons par récurrence que pour tout $n \geqslant n_0$, $P(n)$ est vraie.

— On a $|u_{n_0}| = \alpha^{n_0-n_0}|u_{n_0}|$. Donc on a $P(n_0)$.

— Soit $n \geqslant n_0$. Supposons $P(n)$.
Montrons $P(n+1)$.
On a $|u_{n+1}| \leqslant \alpha |u_n|$ car $n \geqslant n_0$.
Par ailleurs $|u_n| \leqslant \alpha^{n-n_0}|u_{n_0}|$.
Donc $\alpha |u_n| \leqslant \alpha^{n+1-n_0}|u_{n_0}|$.
Donc $|u_{n+1}| \leqslant \alpha^{n+1-n_0}|u_{n_0}|$.
On a donc $P(n+1)$

On a donc

$$\forall n \geqslant n_0\ P(n)$$

4.9 Quelques récurrences fausses

Exercice : chercher l'erreur dans les pseudo-démonstrations ci-dessous.

a Suite négative minorée par un réel positif...

Notons u la suite définie par

$$\begin{cases} u_0 = \dfrac{\pi}{4} \\ \forall n \in \mathbb{N}\ u_{n+1} = 6u_n - 4 \end{cases}$$

(il est clair que u est bien définie)
Montrons que pour tout $n \in \mathbb{N}$, $u_n \geqslant \frac{4}{5}$.
Pour tout $n \in \mathbb{N}$, notons $P(n)$ la propriété

$$\text{«}u_n \geqslant \frac{4}{5}\text{»}$$

Montrons $\forall n \in \mathbb{N}\ P(n)$ par récurrence.

— On a $P(0)$.

— Soit $n \in \mathbb{N}$. Supposons $P(n)$. Montrons $P(n+1)$.
On a :

$$\begin{aligned} & & u_n &\geqslant \frac{4}{5} \\ \text{donc} & & 6u_n &\geqslant \frac{24}{5} \\ \text{donc} & & 6u_n - 4 &\geqslant \frac{24 - 5 \times 4}{5} \\ \text{donc} & & u_{n+1} &\geqslant \frac{4}{5}. \end{aligned}$$

Ainsi, on a $P(n+1)$.
Donc on a $\forall n \in \mathbb{N}\ P(n)$

Calculons les valeurs approchées des premiers termes de la suite avec Python :

```
def f(x) :
  """Calcule 6*x-4, précondition  : x réel"""
  return 6 * x - 4

from math import pi
x = pi / 4 # u_0
u = [x] # Contient u_0
for i in range(5) :
  x = f(x) # Calcule le terme suivant de u
  u.append(x) # Ajoute le nouveau terme
print(u) # Affiche les valeurs calculées
```

On obtient les valeurs suivantes :

$$\begin{aligned} u_0 &\approx 0.7853982 \\ u_1 &\approx 0.7123890 \\ u_2 &\approx 0.2743339 \\ u_3 &\approx -2,3539967 \\ u_4 &\approx -18.12398 \\ u_5 &\approx -112.74388 \end{aligned}$$

Autrement dit, u_5 est négatif et devrait être supérieur à $\frac{4}{5}\ldots$

b n valeurs sont égales

Montrons que pour tout entier n non nul, et tout n-uplet $(x_1, \ldots, x_n)$, on a

$$x_1 = x_2 = \ldots = x_n$$

Autrement dit : toutes les composantes d'un n-uplet sont égales.

Pour tout $n \geqslant 1$, notons $P(n)$ la propriété

«pour tout n-uplet $(x_1, \ldots, x_n)$, on a $x_1 = x_2 = \ldots = x_n$.»

Montrons $\forall n \geqslant 1\ P(n)$ par récurrence.
— On a clairement $P(1)$.
— Soit $n \geqslant 1$.
Supposons $P(n)$ et montrons $P(n+1)$.
Soit $(x_1, \ldots, x_{n+1})$ un $n+1$-uplet.
$(x_1, \ldots, x_n)$ est un n-uplet donc on a

$$x_1 = x_2 = \ldots = x_n$$

$(x_2, \ldots, x_{n+1})$ est un n-uplet donc on a

$$x_2 = \ldots = x_{n+1}$$

Donc on a

$$x_1 = x_2 = \ldots = x_{n+1}$$

Donc on a $P(n+1)$.
On a donc $\forall n \geqslant 1\ P(n)$.

c Toutes les puissances valent 1

Soit $a \in \mathbb{R}^*$. Montrons que pour tout entier naturel non-nul n, on a $a^{n-1} = 1$.
Notons $P(n)$ la propriété «$a^{n-1} = 1$».
Montrons $\forall n \geqslant 1 \quad P(n)$ par récurrence forte.
— On a clairement $P(1)$.
— Soit $n \geqslant 1$.
Supposons $\forall m \in [\![1, n]\!] \quad P(m)$.
Montrons $P(n+1)$.
On a

$$\begin{aligned} a^{n+1-1} &= a^n \\ &= \frac{a^{n-1} \times a^{n-1}}{a^{(n-1)-1}} \end{aligned}$$

Or par hypothèse de récurrence, $P(m)$ est vraie pour tout $m \leqslant n$, donc $P(n)$ et $P(n-1)$ sont vraies.
Donc $a^{n-1} = 1$ et $a^{(n-1)-1} = 1$.
D'où :

$$a^{n+1-1} = \frac{1 \times 1}{1}$$

Donc on a $P(n+1)$.

On a donc

$$\forall n \geqslant 1 \quad P(n)$$

Chapitre III

Un peu de calcul

1 Le symbole somme : Σ

Définition 1.0.1.
Soient I un ensemble **fini** et $(z_i)_{i\in I}$ une famille de nombres complexes indexée par I (c'est-à-dire il existe une application $z : I \to \mathbb{C}$ et on note $z_i = z(i)$). La somme des z_i, i parcourant l'ensemble I, est notée $\sum_{i\in I} z_i$.
Dans le cas où $I = [\![m, n]\!]$, où m, $n \in \mathbb{Z}$ sont tels que $m \leqslant n$, on la note plus couramment $\sum_{k=m}^{n} z_k$ ou $\sum_{m\leqslant k\leqslant n} z_k$. Elle vaut $z_m + z_{m+1} + z_{m+2} \ldots + z_n$.
Dans le cas où $I = [\![m, n]\!] \times [\![p, q]\!]$ où m, n, p et $q \in \mathbb{Z}$ sont tels que $m \leqslant n$ et $p \leqslant q$, on la note plus couramment $\sum_{m\leqslant k\leqslant n,\ p\leqslant \ell\leqslant q} z_{k\ell}$.

Remarque 1.0.2.
On pourrait formellement définir ces symboles par récurrence sur le nombre d'objets sommés.

Remarque 1.0.3.
Dans une expression du type $\sum_{k=m}^{n} f(k)$, on dit que la variable k est *muette*. En effet, on peut remplacer la lettre k par un autre nom de variable non encore utilisé, sans changer le sens de l'expression. Ainsi $\sum_{k=m}^{n} f(k)$, $\sum_{i=m}^{n} f(i)$ et $\sum_{\text{Brandon}=m}^{n} f(\text{Brandon})$ sont synonymes. Par contre on ne peut pas écrire $\sum_{m=m}^{n} f(m)$, $\sum_{n=m}^{n} f(n)$ ou $\sum_{f=m}^{n} f(f)$, qui n'ont aucun sens.

On essaiera bien entendu de garder des notations cohérentes avec le contexte ... et raisonnables.

Remarque 1.0.4.
On peut donner le même sens à ce symbole dans un groupe commutatif, dont la loi est notée $+$.

Proposition 1.0.5 (Changements d'indice)**.**
Soit $n, m \in \mathbb{Z}$, tels que $m \leqslant n$.

1. Si f est une application, et $I = [\![m, n+1]\!]$, alors $\sum_{k=m}^{n} f(k+1) = \sum_{k=m+1}^{n+1} f(k)$.
2. $\sum_{k=0}^{n} f(k) = \sum_{k=0}^{n} f(n-k)$ et $\sum_{k=1}^{n} f(k) = \sum_{k=0}^{n-1} f(n-k)$.

Démonstration. 1. On le montre par récurrence sur n, en ayant fixé un entier m.
Si $n = m$, alors

$$\sum_{k=m}^{n} f(k+1) = f(m+1) = \sum_{k=m+1}^{n+1} f(k).$$

Soit un entier $n \geqslant m$, supposons que l'identité soit vraie au rang n. Alors,

$$\begin{aligned}\sum_{k=m}^{n+1} f(k+1) &= \sum_{k=m}^{n} f(k+1) + f(n+1+1)\\ &= \sum_{k=m+1}^{n+1} f(k) + f(n+2)\\ &= \sum_{k=m+1}^{n+2} f(k).\end{aligned}$$

Ainsi, la propriété est vraie au rang $n+1$ et l'on peut conclure par récurrence.

2. On montre la première par récurrence sur n.
Si $n = 0$, alors

$$\sum_{k=0}^{n} f(k) = f(0) = f(n-0) = \sum_{k=0}^{n} f(n-k).$$

Soit un entier naturel n, supposons que l'identité soit vraie au rang n. Alors,

$$\begin{aligned}\sum_{k=0}^{n+1} f(k) &= \sum_{k=0}^{n} f(k) + f(n+1)\\ &= \sum_{k=0}^{n} f(n-k) + f(n+1)\\ &= \sum_{k=1}^{n+1} f(n+1-k) + f(n+1-0)\\ &= \sum_{k=0}^{n+1} f(n+1-k).\end{aligned}$$

Ainsi, la propriété est vraie au rang $n+1$ et l'on peut conclure par récurrence.
La seconde identité se déduit immédiatement de celle-là avec un décalage d'indice.

□

Exemple 1.0.6.
$$\sum_{i=3}^{6} i^2 = \sum_{i=2}^{5} (i+1)^2$$
$$= \sum_{i=0}^{3} (i+3)^2 = \sum_{i=0}^{3} (6-i)^2.$$

Le résultat suivant est fondamental. Savoir repérer une somme télescopique et la simplifier (ou, réciproquement, faire apparaître une somme télescopique à la place de la différence de deux termes) est un *savoir faire* important.

Théorème 1.0.7 (Simplification téléscopique)**.**
Soit $(z_k)_{m\leqslant k\leqslant n+1}$ une famille de nombres complexes. Alors :

$$\sum_{k=m}^{n} (z_{k+1} - z_k) = z_{n+1} - z_m.$$

Remarque 1.0.8.
Ceci est l'analogue discret du résultat d'intégration $\int_a^b f'(t)\,\mathrm{d}t = f(b) - f(a)$, pour les fonctions f éligibles.

Démonstration.
Commencer par écrire la somme « à la main »avec des « petits points » pour voir. Ensuite, par changement d'indice :

$$\begin{aligned}\sum_{k=m}^{n} (z_{k+1} - z_k) &= \sum_{k=m}^{n} z_{k+1} - \sum_{k=m}^{n} z_k \\ &= \sum_{k=m+1}^{n+1} z_k - \sum_{k=m}^{n} z_k \\ &= z_{n+1} - z_m.\end{aligned}$$

□

Remarque 1.0.9.
La dernière égalité se comprend intuitivement, on peut la montrer formellement par récurrence sur n.

Exemple 1.0.10.
Calculer la somme $\displaystyle\sum_{k=1}^{n} \frac{1}{k(k+1)}$.

Théorème 1.0.11 (Sommes doubles et permutation des Σ)**.**
Soit $(z_{ij})_{m\leqslant i,j\leqslant n}$ une famille de nombres complexes. Alors :

1. $\displaystyle\sum_{m\leqslant i,j\leqslant n} z_{ij} = \sum_{i=m}^{n}\sum_{j=m}^{n} z_{ij} = \sum_{j=m}^{n}\sum_{i=m}^{n} z_{ij}.$
2. $\displaystyle\sum_{m\leqslant i\leqslant j\leqslant n} z_{ij} = \sum_{i=m}^{n}\sum_{j=i}^{n} z_{ij} = \sum_{j=m}^{n}\sum_{i=m}^{j} z_{ij}.$
3. $\displaystyle\sum_{m\leqslant i<j\leqslant n} z_{ij} = \sum_{i=m}^{n-1}\sum_{j=i+1}^{n} z_{ij} = \sum_{j=m+1}^{n}\sum_{i=m}^{j-1} z_{ij}.$

Démonstration.
On se contentera de dessiner un tableau. □

2 Le symbole produit : Π

Le symbole Π est au produit ce que le symbole Σ est à la somme.

Définition 2.0.1.
Soient I un ensemble **fini** et $(z_i)_{i\in I}$ une famille de nombres complexes indexée par I. Le produit des z_i, i parcourant l'ensemble I, est noté $\displaystyle\prod_{i\in I} z_i$.

Définition 2.0.2 (Factorielle)**.**
Pour tout $n \in \mathbb{N}\backslash\{0\}$ (noté aussi $\mathbb{N}^\times$), on appelle *factorielle* n, notée $n!$ le nombre

$$n! = \prod_{k=1}^{n} k = 1 \times 2 \times 3 \ldots \times n.$$

Par convention, $0! = 1$.

Exemple 2.0.3.
Il est bon de connaître les 5 ou 6 premières factorielles : $0! = 1$, $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, $5! = 120$ et $6! = 720$.

Les nombres factoriels vérifient la relation de récurrence suivante.

Proposition 2.0.4.
Pour tout $n \in \mathbb{N}$, $(n+1)! = (n+1) \times n!$.

Démonstration.
Immédiat. □

Théorème 2.0.5 (Simplification téléscopique)**.**
Soit $(z_k)_{m \leqslant k \leqslant n+1}$ une famille de nombres complexes non nuls. Alors : $\prod_{k=m}^{n} \frac{z_{k+1}}{z_k} = \frac{z_{n+1}}{z_m}$.

Il y a pour les produits l'exact analogue du théorème 1.0.11 pour les sommes, et la démonstration est elle aussi analogue.

 En général on ne peut pas permuter les Σ et les Π. Par exemple, calculer $\sum_{i=1}^{3} \prod_{j=1}^{2} 1$ et $\prod_{j=1}^{2} \sum_{i=1}^{3} 1$.

Remarque 2.0.6.
Dans le cas d'un produit de nombres réels strictement positifs, on pensera souvent à appliquer le logarithme pour se rammener à une somme.

3 Quelques formules à connaître

Théorème 3.0.1.
Soit n un entier naturel. Alors

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

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

Démonstration.
Les deux se démontrent facilement par récurrence. Par curiosité et pour s'entraîner, voici deux autres démonstrations :

(i) On note $S_n = \sum_{k=0}^{n} k$. On fait un changement d'indice : $S_n = \sum_{k=0}^{n} (n-k)$ et on développe : $S_n = \sum_{k=0}^{n} n - \sum_{k=0}^{n} k = n(n+1) - S_n$, d'où $2S_n = n(n+1)$.

(ii) On note $S'_n = \sum_{k=0}^{n} k^2$. Pour tout $k \in [\![0, n]\!]$, on a : $(k+1)^3 - k^3 = 3k^2 + 3k + 1$. On somme tout ça de 0 à n, et on obtient, après simplification téléscopique du membre de gauche : $(n+1)^3 = 3S'_n + 3\frac{n(n+1)}{2} + n + 1$. Ça se simplifie pour donner le résultat voulu.

□

Définition 3.0.2 (Coefficients binomiaux)**.**
Soit $(n, k) \in \mathbb{N}^2$ tels que $k \leqslant n$. On appelle *coefficient binomial*, aussi lu *« k parmi n »*, le réel noté $\binom{n}{k}$ valant $\frac{n!}{k!(n-k)!}$.
On étend cette définition à tout $(n, k) \in \mathbb{N} \times \mathbb{Z}$ en posant $\binom{n}{k} = 0$ pour $k > n$ ou $k < 0$.

Remarque 3.0.3.
On utilisera souvent :

$$\binom{n}{k} = \frac{\prod_{i=n-k+1}^{n} i}{\prod_{j=1}^{k} j} = \frac{n \times n-1 \times \cdots \times n-k+1}{k \times k-1 \times \cdots \times 1}.$$

Théorème 3.0.4 (Formule du triangle de Pascal)**.**
Soit $(n, k) \in \mathbb{N}^* \times \mathbb{Z}$. Alors

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

Démonstration.
Se fait par un calcul direct. □

Remarque 3.0.5.
Cette formule permet de calculer par récurrence tous les coefficients binomiaux, en les représentant par exemple dans le triangle de Pascal.

Corollaire 3.0.6.
Soit $(n,k) \in \mathbb{N} \times \mathbb{Z}$, $\binom{n}{k}$ est un entier.

Démonstration.
La démonstration se fait par récurrence sur n, avec l'hypothèse : « $\forall k \in [\![0,n]\!]$, $\binom{n}{k}$ est un entier », en utilisant la formule de Pascal pour l'hérédité. □

Théorème 3.0.7.
Sur un arbre représentant les répétitions d'une même expérience aléatoire, le coefficient binomial k parmi n compte le nombre de chemins réalisant k succès pour n répétitions. En particulier, c'est un entier.

La figure 1 illustre le calcul de ces coefficients pour 4 répétitions.

Démonstration.
Pour $n \in \mathbb{N}^*$, notons H_n la proposition : « pour tout $k \in [\![0,n]\!]$, il y a $\binom{n}{k}$ chemins réalisant k succès pour n répétitions. »

— H_1 est évidente ;

— Soit $n \in \mathbb{N}^*$ vérifiant H_n. Montrons H_{n+1}.
Soit $k \in [\![0,n+1]\!]$. Montrons qu'il y a $\binom{n+1}{k}$ chemins réalisant k succès pour $n+1$ répétitions.
Il est immédiat qu'il n'y a qu'un chemin réalisant 0 succès pour $n+1$ répétitions. Or $\binom{n+1}{0} = 1$.
De même, il n'y a qu'un chemin réalisant $n+1$ succès pour $n+1$ répétitions. Or $\binom{n+1}{n+1} = 1$.
Le résultat est donc démontré si $k = 0$ ou $k = n+1$. Supposons donc maintenant $k \in [\![1,n]\!]$. Comptons le nombre de chemins réalisant k succès pour $n+1$ répétitions : pour un tel chemin, regardons le résultat de la dernière répétition. Si c'est un succès, cela signifie que parmi les n premières répétitions, $k-1$ succès ont été réalisés ; si c'est un échec, cela signifie que parmi les n premières répétitions, k succès ont été réalisés.
Réciproquement, pour tout chemin réalisant $k-1$ succès pour les n premières répétitions il y a un chemin réalisant k succès pour $n+1$ répétitions dont la dernière répétition est un succès et pour tout chemin réalisant k succès pour les n premières répétitions, il y a un chemin réalisant k succès pour $n+1$ répétitions dont la dernière répétition est un échec.
Par conséquent, le nombre de chemins réalisant k succès pour $n+1$ répétitions est égal au nombre de chemins réalisant k succès pour n répétitions plus le nombre de chemins réalisant $k-1$ succès pour n répétitions. D'après l'hypothèse de récurrence, le nombre de chemins réalisant k succès pour $n+1$ répétitions vaut donc $\binom{n}{k-1} + \binom{n}{k}$, ce qui, d'après la formule de Pascal, vaut bien $\binom{n+1}{k}$.
Donc on a H_{n+1}.

On a donc, pour tout $n \in \mathbb{N}^*$, H_n. □

Remarque 3.0.8.

• $\binom{n}{k}$ est aussi égal au nombre de possibilités de choisir k éléments dans un ensemble de n éléments.

• Considérons un goban de taille $n+1$ fois $n+1$. On le coupe le long d'une diagonale, et on n'en conserve que la moitié. On pose cette moitié sur une table, le long de sa diagonale, verticalement. On numérote alors de 0 à n les intersections de cette diagonale, de gauche à droite.
Une fourmi ce trouvant en haut, sur le coin opposé à la diagonale, décide de descendre sur la table en suivant les lignes du goban, mais en se dirigeant toujours vers le bas. À chaque intersection de lignes, deux choix s'offrent donc à elle.
On peut alors montrer que le nombre de chemins par lesquels la fourmi peut atteindre la $k$ème intersection de la diagonale est exactement $\binom{n}{k}$.

Proposition 3.0.9.
Soit $n \in \mathbb{N}^*$ et $k \in [\![0,n]\!]$. On a $\binom{n}{k} = \binom{n}{n-k}$.

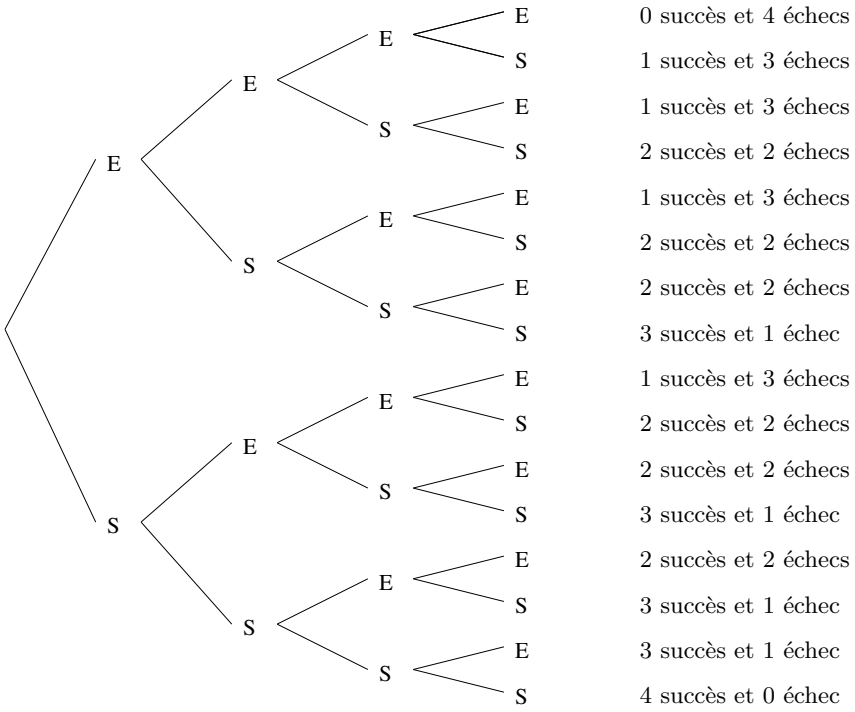


FIGURE III.1 – Chemins des succès et échecs pour 4 répétitions d'une expérience

Démonstration.
Remarquer que $k = n - (n - k)$! □

La formule suivant n'est pas exigible mais est fort utile.

Proposition 3.0.10.
Soit $n \in \mathbb{N}^*$ et $0 < k \leqslant n$, alors $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$.

Démonstration.
Facile et laissée en exercice. □

Théorème 3.0.11 (Formule du binôme de Newton)**.**
Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{C}$. On a :

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

Démonstration.
Par récurrence. □

Corollaire 3.0.12.
Soit $n > 0$. $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ et $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$.

Théorème 3.0.13.
Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{C}$. Alors :

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

Démonstration.
Développement et simplification téléscopique. □

Corollaire 3.0.14.
Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{C}$. Alors,

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

Démonstration.
$a^{2n+1}+b^{2n+1} = a^{2n+1}-(-b)^{2n+1}$ et on utilise le théorème précédent. □

Corollaire 3.0.15 (Formule de sommation géométrique)**.**
Soient $n \in \mathbb{N}$ et $z \in \mathbb{C}$. Alors,

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

Démonstration.
— Si $z = 1$: on somme n fois 1.
— Sinon, $z^n - 1 = z^n - 1^n = (z-1)\sum_{k=0}^{n-1} z^k 1^{n-1-k} = \sum_{k=0}^{n-1} z^k$.

□

4 Calcul matriciel élémentaire

Même si quelques définitions et démonstrations théoriques sont données ici, le seul but de cette section et de savoir effectuer des opérations élémentaires sur des matrices simples. Le chapitre sur les matrices reprendra tout cela de manière plus poussée, au second semestre, et fera ensuite le lien entre les matrices et les applications linéaires.

n, m, p, q et r désignent des entiers naturels non nuls, et $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

4.1 Définitions élémentaires

Définition 4.1.1.
On appelle *matrice de taille* $n \times p$ (ou à n lignes et p colonnes), à valeurs (ou coefficients) dans $\mathbb{K}$, toute famille de np éléments de $\mathbb{K}$, ces éléments étant notés $(a_{ij})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant p}$, et présentés sous la forme d'un tableau de la manière suivante :

$$A = \begin{pmatrix} a_{1,1} & \dots & a_{1,p} \\ \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,p} \end{pmatrix}.$$

On note $A = (a_{ij})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant p}$, les $(a_{i,j})$ étant les *coefficients* de la matrice A, $a_{i,j}$ étant le coefficient de la i^{e} ligne et de la j^{e} colonne.

La matrice $(a_{i,j})_{1\leqslant j\leqslant n}$ est la i^{e} ligne de A, parfois notée $a_{i,*}$.

La matrice $(a_{i,j})_{1\leqslant i\leqslant n}$ est la j^{e} colonne de A, parfois notée $a_{*,j}$.

Remarque 4.1.2.
Le premier indice indique toujours la ligne et le second indice indique toujours la colonne. En général (mais attention quand même), on les note respectivement i et j.

Exemple 4.1.3.
Donner la matrice $(i \times j)_{1\leqslant i\leqslant 3, 1\leqslant j\leqslant 5}$.

Définition 4.1.4.
— L'ensemble des matrices de taille $n \times p$ est noté $\mathscr{M}_{n,p}(\mathbb{K})$.
— On appelle *matrice carrée d'ordre* n toute matrice de taille $n \times n$. L'ensemble des matrices carrées d'ordre n est noté $\mathscr{M}_n(\mathbb{K})$.
— On appelle *matrice nulle d'ordre* n la matrice carrée d'ordre n dont tous les coefficients sont nuls. On la note simplement 0_n, ou 0 sans référence à sa taille s'il n'y a pas d'ambiguïté.
— On appelle *matrice identité d'ordre* n la matrice $(\delta_{i,j})_{1\leqslant i,j\leqslant n}$. On la note I_n, ou Id_n.
— On appelle *matrice diagonale* toute matrice carrée $(a_{ij})_{1\leqslant i,j\leqslant n}$ telle que pour tous $i, j \in [\![1, n]\!]$, $i \neq j \Rightarrow a_{i,j} = 0$.
— On appelle *matrice triangulaire supérieure* (resp. *inférieure*) toute matrice carrée $(a_{ij})_{1\leqslant i,j\leqslant n}$ telle que pour tous $i, j \in [\![1, n]\!]$ tells que $i > j$ (resp. $i < j$), $a_{ij} = 0$.

Remarque 4.1.5. 1. On note généralement les matrices par des lettres majuscules, et la famille des coefficients par la lettre minuscule correspondante.

2. On identifie les matrices colonnes de $\mathscr{M}_{n,1}(\mathbb{K})$ avec les éléments de $\mathbb{K}^n$.
3. On se gardera d'identifier les matrices lignes avec les éléments de $\mathbb{K}^n$ car on préfère les identifier avec d'autres objets mathématiques (on verra cela plus tard).

4.2 Opérations sur les matrices

Définition 4.2.1.
Soient $A = (a_{ij})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant p}$ et $B = (b_{ij})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant p}$ deux matrices **de même taille**, et $\lambda \in \mathbb{K}$ un scalaire.

Addition On appelle *somme* de A et B la matrice $(a_{ij} + b_{ij})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant p}$, notée $A + B$.

Produit par un scalaire On note λA la matrice $(\lambda a_{ij})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant p}$.

 Attention aux tailles des matrices : on ne peut additionner n'importe quoi avec n'importe quoi.

Exemple 4.2.2.
$$\begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} + 2\begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 1 \\ 1 & 8 \end{pmatrix}.$$

Définition 4.2.3 (Produit matriciel)**.**
Soient $A \in \mathscr{M}_{n,p}(\mathbb{K})$ et $B \in \mathscr{M}_{p,q}(\mathbb{K})$. On appelle *produit de A par B noté AB* la matrice de $\mathscr{M}_{n,q}(\mathbb{K})$ de coefficients $\left(\sum_{k=1}^{p} a_{ik}b_{kj}\right)$.

 Gare aux dimensions, on ne peut pas multiplier n'importe quelle matrices.

Exemple 4.2.4. — On tâchera d'organiser les produits comme suit :

$$\begin{array}{c} \\ \text{Dim. OK} \\ \\ \underbrace{\begin{pmatrix} 2 & 1 \\ 1 & 0 \\ 4 & 2 \end{pmatrix}}_{A} \end{array} \quad \overbrace{\begin{pmatrix} 1 & 0 & 2 \\ -1 & 3 & 2 \end{pmatrix}}^{B} \\ \underbrace{\begin{pmatrix} 1 & 3 & 6 \\ 1 & 0 & 2 \\ 2 & 6 & 12 \end{pmatrix}}_{=AB}$$

— Le produit impossible :

$$\begin{pmatrix} 1 & 3 & 0 \\ 2 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix}.$$

 Ce produit comporte plein de pièges :

• Il n'est pas commutatif, par exemple : $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Et même pire, AB peut exister mais pas BA.

• Le produit de deux matrices non nulles peut valoir la matrice nulle. Exemple : $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, alors $AA = 0$, $AB = 0$ et $BA \neq 0$.

• On ne peut pas « simplifier » dans un produit. Ici : $A \times A = A \times B$ mais $A \neq B$.

Proposition 4.2.5.
Le produit matriciel est :

Associatif : si $A \in \mathscr{M}_{n,p}(\mathbb{K})$, $B \in \mathscr{M}_{p,q}(\mathbb{K})$, $C \in \mathscr{M}_{q,r}(\mathbb{K})$, alors $(AB)C$ et $A(BC)$ sont dans $\mathscr{M}_{n,r}(\mathbb{K})$ et sont égales, notées ABC.

Bilinéaire : si A, B, C, D sont des matrices de taille convenable, et si $\lambda \in \mathbb{K}$, alors $(A + \lambda B)C = AC + \lambda BC$ et $A(C + \lambda D) = AC + \lambda AD$.

Les matrices nulles et identité jouent un rôle bien particulier. Si $A \in \mathscr{M}_{n,p}(\mathbb{K})$ et $q \in \mathbb{N}^*$, alors

Neutre à gauche : $I_n A = A$

Neutre à droite : $AI_p = A$
Mult. par 0 **à gauche :** $0_{q,n}A = 0_{q,p}$
Mult. par 0 **à droite :** $A0_{p,q} = 0_{n,q}$

Démonstration.
Bien qu'un peu technique, nous donnons ici la démonstration ; nous en verrons plus tard une autre.

1. $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij})$. Ainsi,
$$BC = \left(\sum_{k=1}^{q} b_{ik}c_{kj}\right)_{1\leqslant i\leqslant p, 1\leqslant j\leqslant r}$$
et
$$A(BC) = \left(\sum_{\ell=1}^{p} a_{i\ell} \times \left(\sum_{k=1}^{q} b_{\ell k}c_{kj}\right)\right)_{1\leqslant i\leqslant n, 1\leqslant j\leqslant r}.$$
Or, si $1 \leqslant i \leqslant n$ et $1 \leqslant j \leqslant r$,
$$\begin{aligned}\sum_{\ell=1}^{p} a_{i\ell} \times \left(\sum_{k=1}^{q} b_{\ell k}c_{kj}\right) &= \sum_{\ell=1}^{p} a_{i\ell} \times \sum_{k=1}^{q} b_{\ell k}c_{kj}\\ &= \sum_{\ell=1}^{p}\sum_{k=1}^{q} a_{i\ell}b_{\ell k}c_{kj}\\ &= \sum_{k=1}^{q}\sum_{\ell=1}^{p} a_{i\ell}b_{\ell k}c_{kj}\\ &= \sum_{k=1}^{q}\left(\sum_{\ell=1}^{p} a_{i\ell}b_{\ell k}\right) \times c_{kj},\end{aligned}$$
qui est le coefficient i, j de $(AB)C$. D'où l'égalité voulue.
2. *idem*
3. $I_nA = \left(\sum_{k=1}^{n} \delta_{ik}a_{kj}\right) = (\delta_{ii}a_{ij}) = (a_{ij}) = A.$
4. Direct.

□

Remarque 4.2.6.
Par associativité, il y a 5 manières de calculer $ABCD$ qui conduisent toutes au même résultat : $((AB)C)D = (A(BC))D = A((BC)D) = A(B(CD)) = (AB)(CD)$. Mais le temps de calcul est-il le même dans les 5 cas ? C'est le problème de la *multiplication matricielle enchaînée* (Matrix chain multiplication ou Matrix Chain Ordering Problem (MCOP) en anglais). Plus généralement, le problème est de savoir dans quel ordre effectuer les produits pour calculer le plus efficacement possible un produit de matrices $M_1.M_2.\cdots.M_n$. Ce problème peut se résoudre par programmation dynamique, ce qui est au programme en option informatique, mais même si ce n'est pas toujours la solution optimale, il vaut mieux commencer par les produits qui font apparaître des « petites » matrices.

Précisément, le produit d'une matrice $n \times p$ par une matrice $p \times q$ nécessite de l'ordre de $n \times p \times q$ opérations. Ainsi, si $A \in \mathscr{M}_{10,100}(\mathbb{K})$, $B \in \mathscr{M}_{100,5}$ et $C \in \mathscr{M}_{5,50}$, le calcul de $(AB)C$ demande de l'ordre de $(10 \times 100 \times 5) + 10 \times 5 \times 50 = 7\,500$ opérations, alors que celui de $A(BC)$ en demande de l'ordre de $100 \times 5 \times 50 + 10 \times 100 \times 50 = 75\,000$.

4.3 Matrices carrées

Remarque 4.3.1.
Si A et B sont deux matrices carrées d'ordre n, alors AB et BA sont définies et également de taille n. On dit que le produit matriciel est une *loi de composition interne* de $\mathscr{M}_n(\mathbb{K})$.

De plus, $\mathrm{I}_n.A = A.\mathrm{I}_n = A$. On dit que I_n est le *neutre* de $\mathscr{M}_n(\mathbb{K})$ pour le produit matriciel.

Enfin, la propriété de bilinéarité montrée précédemment montre que $(\mathscr{M}_n(\mathbb{K}), +, \times)$ a une structure d'anneau, non commutatif.

Définition 4.3.2 (Puissances d'une matrice carrée)**.**
On les définit par récurrence : si $M \in \mathscr{M}_n(\mathbb{K})$, alors, $M^0 = \mathrm{I}_n$, $M^1 = M$, et pour tout $k \in \mathbb{N}$, $M^{k+1} = M \times M^k$ (on a donc, pour tout $k \in \mathbb{N}^*$, $M^k = \underbrace{M \times M \ldots \times M}_{k \text{ fois}}$. Ainsi pour tout $k \in \mathbb{N}$, on a $M^n \in \mathscr{M}_n(\mathbb{K})$.

Remarque 4.3.3.
On remarque que les puissances d'une même ma-

trice commutent entre elles :

$$\begin{aligned} M^k \times M^j &= \underbrace{M \times M \ldots \times M}_{k \text{ fois}} \times \underbrace{M \times M \ldots \times M}_{j \text{ fois}} \\ &= \underbrace{M \times M \ldots \times M}_{(k+j) \text{ fois}} \\ &= \underbrace{M \times M \ldots \times M}_{j \text{ fois}} \times \underbrace{M \times M \ldots \times M}_{k \text{ fois}} \\ &= M^j \times M^k. \end{aligned}$$

Théorème 4.3.4 (Formule du binôme de Newton)**.**
Elle est valable pour les matrices *carrées qui* ***commutent***.

Soit $n \in \mathbb{N}^*$ et $p \in \mathbb{N}$, soit $A, B \in \mathscr{M}_n(\mathbb{K})$ vérifiant $AB = BA$. Alors,

$$(A+B)^p = \sum_{k=0}^{p} \binom{p}{k} A^k B^{p-k}.$$

Démonstration.
Reprendre la démonstration du binôme de Newton pour des complexes, en repérant bien à quel endroit le fait que les deux matrices commutent intervient. □

Exemple 4.3.5.
Calculer A^2 avec

$$\begin{aligned} A &= \begin{pmatrix} 1 & 1 & 1 \\ 2 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 1 \\ 2 & -1 & 0 \\ 0 & -2 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 2 & 0 \end{pmatrix} \\ &= B + C. \end{aligned}$$

Calculer A^3 avec

$$\begin{aligned} A &= \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 4 & 6 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 1 & 2 \end{pmatrix} + \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 3 & 4 \end{pmatrix} \\ &= B + C. \end{aligned}$$

Définition 4.3.6.
Soit $A \in \mathscr{M}_n(\mathbb{K})$. On dit que A est *inversible* s'il existe une matrice $B \in \mathscr{M}_n(\mathbb{K})$ telle que $AB = BA = \mathrm{I}_n$.

Dans ce cas B est unique, est appelée *l'inverse de* A et est notée A^{-1}.

On note $GL_n(\mathbb{K})$ l'ensemble des matrices carrées d'ordre n à coefficients dans $\mathbb{K}$ inversibles.

Exercice 4.3.7.
Montrer que la matrice $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ étudiée précédemment n'est pas inversible.

Enfin, le cas particulier des matrices carrées d'ordre 2 est à connaître sur le bout des doigts.

Définition 4.3.8.
Le déterminant d'une matrice *carrée d'ordre* 2 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est $\det A = ad - bc$.

Proposition 4.3.9.
Une matrice, carrée d'ordre 2, notée $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est $\det A = ad - bc$ est inversible si et seulement si son déterminant est non nul. Le cas échéant, $A^{-1} = \dfrac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Démonstration.
Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on a toujours (le vérifier par le calcul)

$$A^2 - (a+d)A + (ad-bc)I_2 = 0.$$

Alors, si $\det A \neq 0$, avec $B = \dfrac{1}{\det A}((a+d)I_2 - A)$, on a $AB = BA = I_2$ donc A est inversible, d'inverse B.

Réciproquement, si $\det A = 0$, alors $A(A-(a+d)I_2) = 0$. Si A est inversible, en multipliant par cet inverse on obtient que A est diagonale, puis que $a = 0$ ou que $d = 0$ ... Dans les deux cas, $A^2 = 0$ donc A ne peut être inversible (à vous de réfléchir pourquoi !). □

5 Systèmes linéaires et pivot de Gauss

5.1 Définitions

Définition 5.1.1.
On appelle *système linéaire à n équations et p inconnues* tout système de la forme :

$$\begin{cases} a_{11}x_1 & + & \dots & + & a_{1p}x_p & = & b_1 \\ \cdot & & \cdot & & \cdot & & \\ \cdot & & \cdot & & \cdot & & \\ a_{n1}x_1 & + & \dots & + & a_{np}x_p & = & b_n \end{cases}$$

où les a_{ij} et les b_i sont dans $\mathbb{K}$, et les x_i sont les inconnues.
On dit que le système est *compatible* s'il admet une solution.
Le *système homogène associé* est le système :

$$\begin{cases} a_{11}x_1 & + & \dots & + & a_{1p}x_p & = & 0 \\ \cdot & & \cdot & & \cdot & & \\ \cdot & & \cdot & & \cdot & & \\ a_{n1}x_1 & + & \dots & + & a_{np}x_p & = & 0 \end{cases}$$

Dans la suite nous noterons S le premier système et S_H son système homogène associé, et nous noterons Sol et Sol_H leurs ensembles de solutions respectifs.

Le système S peut aussi s'écrire sous forme matricielle $AX = B$, avec $A = (a_{ij})_{1\leqslant i\leqslant n,\ 1\leqslant j\leqslant p}$, $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$ et $B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$.
S_H s'écrit alors $AX = 0$.

5.2 Interprétation géométrique

a Dans le plan

Si $n = 2$, chaque ligne du système s'interprète comme l'équation d'une droite dans le plan. Chaque droite y est en effet représentée par une équation cartésienne. On « sait » de plus que l'intersection de deux droites est

- soit l'ensemble vide (droites parallèles distinctes) ;
- soit une droite (droites confondues) ;
- soit un point (droites non parallèles).

Ainsi, l'ensemble des solutions est soit vide, soit un point, soit représente une droite.

b Dans l'espace

Si $n = 3$, chaque ligne du système s'interprète comme l'équation d'un plan dans l'espace. Chaque plan y est en effet représenté par une équation cartésienne. On « sait » de plus que l'intersection de deux plans est

- soit l'ensemble vide (plans parallèles distincts) ;
- soit un plan (plans confondus) ;
- soit une droite (plans non parallèles).

De plus, on « sait » que l'intersection d'un plan et d'une droite est

- soit l'ensemble vide (droite parallèle au plan, non inclue dedans) ;
- soit une droite (droite inclue dans le plan) ;
- soit un point (droite non parallèle au plan).

Ainsi, l'ensemble des solutions est soit vide, soit un point, soit représente une droite, soit représente un plan.

5.3 Structure des solutions

Théorème 5.3.1. 1. Sol_H contient toujours l'élément $(0, \dots, 0)$. S'il n'est pas réduit à cet élément, il est infini.

2. L'ensemble Sol est :
   • soit vide ;
   • soit non vide, et dans ce cas, si $X_0 = (x_1, \dots, x_p)$ est un élément de Sol, alors $\mathrm{Sol} = \{X_0 + X_H,\ X_H \in \mathrm{Sol}_H\}$, ce que l'on note $\mathrm{Sol}_H + (x_1, \dots, x_p)$.
   Par conséquent, Sol contient 0, 1 ou une infinité d'éléments.

Démonstration.
On utilise les notations matricielles, le système S s'écrivant $S : AX = B$, avec $A \in \mathscr{M}_{n,p}(\mathbb{K})$ et $B \in \mathscr{M}_{p,1}(\mathbb{K})$. Le

système homogène associé à S est $S_H : AX = 0$. Soit $X, Y \in \mathscr{M}_{n,1}(\mathbb{K})$ et $\lambda, \mu \in \mathbb{K}$. On a bien

$$A \times \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

donc le vecteur nul est solution du système homogène. De plus, si X et Y sont solutions de S_H, alors

$$A(\lambda X + \mu Y) = \lambda AX + \mu AY = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Notamment, si X est une solution de S_H, tous les vecteurs colinéaires à X seront aussi solution de S_H, donc S_H est infini.

Ensuite, soit $X_0 \in \mathscr{M}_{n,1}(\mathbb{K})$ solution de S. On a

$$\begin{aligned} X \in \mathrm{Sol} &\Leftrightarrow AX = B \\ &\Leftrightarrow AX = AX_0 \\ &\Leftrightarrow A(X - X_0) = 0 \\ &\Leftrightarrow X - X_0 \in \mathrm{Sol}_H, \end{aligned}$$

ce qui montre bien que $\mathrm{Sol} = \{ X_0 + X_H \mid X_H \in \mathrm{Sol}_H \}$. □

Exemple 5.3.2.
On considère le système

$$\begin{cases} x + 3y = 2 \\ 2y + z = 1 \end{cases}$$

Le système homogène associé est

$$\begin{cases} x + 3y = 0 \\ 2y + z = 0 \end{cases}$$

Si $(x, y, z) \in \mathbb{R}^3$, on a

$$\begin{cases} x + 3y = 0 \\ 2y + z = 0 \end{cases} \Leftrightarrow \begin{pmatrix} x \\ y \\ z \end{pmatrix} = y \begin{pmatrix} -3 \\ 1 \\ -2 \end{pmatrix}.$$

Ainsi, l'ensemble des solutions homogènes est une droite vectorielle dirigée par le vecteur de coordonnées $(-3, 1, -2)$.

De même, si $(x, y, z) \in \mathbb{R}^3$, on a

$$\begin{cases} x + 3y = 2 \\ 2y + z = 1 \end{cases} \Leftrightarrow \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} + y \begin{pmatrix} -3 \\ 1 \\ -2 \end{pmatrix}.$$

Ainsi, l'ensemble des solutions du système est une droite passant par le point de coordonnées $(2, 0, 1)$ et dirigée par le vecteur de coordonnées $(-3, 1, -2)$.

5.4 Opérations sur les lignes d'un système

Définition 5.4.1.
On dit que deux systèmes linéaires sont *équivalents* s'ils ont le même ensemble de solutions.

Si i et j sont deux indices différents compris entre 1 et n, et λ est un scalaire, on note :
• $L_i \leftrightarrow L_j$ l'opération consistant à échanger les $i^{\text{ème}}$ et $j^{\text{ème}}$ lignes du système S ;
• $L_i \leftarrow \lambda L_i$ l'opération consistant à multiplier par λ la $i^{\text{ème}}$ ligne du système ;
• $L_i \leftarrow L_i + \lambda L_j$ l'opération consistant à ajouter la $j^{\text{ème}}$ ligne multipliée par λ à la $i^{\text{ème}}$ ligne du système.

 Il faut effectuer ces opérations sur toute la ligne du système sans oublier le membre de droite.

Exemple 5.4.2.
Donner des exemples.

Théorème 5.4.3.
• Le système obtenu à partir de S après avoir effectué une opération $L_i \leftrightarrow L_j$ ou une opération $L_i \leftarrow L_i + \lambda L_j$ est encore équivalent à S.
• **Si** $\lambda \neq 0$, alors le système obtenu à partir de S après avoir effectué une opération $L_i \leftrightarrow \lambda L_i$ est encore équivalent à S.

Démonstration.
Si l'on a effectué $L_i \leftrightarrow L_j$, il suffit de la réeffectuer pour revenir au système de départ.

Si l'on a effectué $L_i \leftarrow L_i + \lambda L_j$, il suffit d'effectuer $L_i \leftarrow L_i - \lambda L_j$ pour revenir au système de départ.

Si $\lambda \neq 0$ et si l'on a effectué $L_i \leftrightarrow \lambda L_i$, il suffit d'effectuer $L_i \leftrightarrow \lambda^{-1} L_i$ pour revenir au système de départ. □

5.5 Algorithme du pivot

L'idée du pivot de Gauss pour résoudre un système est de de se ramener à un système simple à résoudre, grâce à une succession d'opérations sur les lignes. Ainsi, l'on se ramène d'abord à un système triangulaire (processus d'*élimination*), puis, si cela est possible, à un système diagonal (processus de *remontée*).
Pour étudier d'abord les cas les plus simples et finir par le cas général, étudions ces étapes à rebours.

a Cas d'un système diagonal

Si le système S est *diagonal*, c'est-à-dire si A est une matrice diagonale dans l'écriture $AX = B$ du système, alors le système se résout de manière immédiate.

Exemple 5.5.1.
Résoudre les systèmes $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1 \end{pmatrix} X = \begin{pmatrix} 2 \\ 1 \\ -2 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} X = \begin{pmatrix} 2 \\ 1 \\ -2 \end{pmatrix}$.

On remarque que s'il n'y a aucun zéro sur la diagonale, il y a une unique solution, sinon il n'y a aucune solution, ou une infinité de solutions.

b Cas d'un système triangulaire inversible

Un cas un peu plus compliqué est celui ou le système est *triangulaire*, c'est-à-dire si A est une matrice triangulaire dans l'écriture $AX = B$ du système.
Nous ne traiterons pour l'instant que le cas où A n'a aucun zéro sur la diagonale (on peut alors montrer qu'elle est inversible).
Pour fixer les idées, supposons A triangulaire supérieure.
Le système a donc cette allure :

$$\begin{cases} a_{11}x_1 & +a_{12}x_2 & +\dots & & +a_{1n}x_n & = b_1 \\ & a_{22}x_2 & +\dots & & +a_{2n}x_n & = b_2 \\ & & \dots & & +\dots & = \dots \\ & & \dots & & +\dots & = \dots \\ & & a_{n-1,n-1}x_{n-1} & & +a_{n-1,n}x_n & = b_{n-1} \\ & & & & a_{nn}x_n & = b_n \end{cases}$$

On obtient alors facilement :

$$x_n = \frac{b_n}{a_{nn}}$$

puis

$$x_{n-1} = \frac{b_{n-1} - a_{n-1,n}x_n}{a_{n-1,n-1}}$$

et, par récurrence (descendante),

$$\text{pour tout } k \in [\![1, n-1]\!],\ x_k = \frac{b_k - \sum_{i=k+1}^{n} a_{k,i}x_i}{a_{k,k}}.$$

Ces relations permettent de calculer les x_k par récurrence.

Nous pouvons également appliquer une succession d'opérations sur les lignes du système pour se ramener de manière équivalente à un système diagonal.
Ce processus est parfois appelé principe de *remontée* car l'on y fait apparaître des zéros dans le haut de la matrice du système, en partant des lignes du bas.
Cette méthode peut être présentée en utilisant une suite de systèmes équivalents.
Il existe une présentation plus visuelle et plus rapide à rédiger. Par exemple, considérons le système

$$\begin{cases} x & +y & -z & = & 2 \\ & -2y & +z & = & 1 \\ & & -z & = & 3 \end{cases}.$$

Nous pouvons l'écrire

$$\left(\begin{array}{ccc|c} 1 & 1 & -1 & 2 \\ 0 & -2 & 1 & 1 \\ 0 & 0 & -1 & 3 \end{array}\right).$$

Les opérations à effectuer sont alors bien visibles : dans un premier temps, nous allons faire apparaître des zéros dans toute la dernière colonne de la partie de gauche du système, sauf à la dernière ligne. Pour cela, effectuons les opérations $L_1 \leftarrow L_1 - L_3$ et $L_2 \leftarrow L_2 + L_3$, et nous obtenons (sans oublier d'effectuer également ces opérations sur la partie de droite du système !)

$$\left(\begin{array}{ccc|c} 1 & 1 & 0 & -1 \\ 0 & -2 & 0 & 4 \\ 0 & 0 & -1 & 3 \end{array}\right)$$

ce qui correspond au système

$$\left\{\begin{array}{rcrcl} x & + & y & = & -1 \\ & & -2y & = & 4 \\ & & -z & = & 3 \end{array}\right.$$

équivalent au premier. Ensuite, nous effectuons l'opération $L_1 \leftarrow L_1 + \frac{1}{2}L_2$. Ou plutôt,pour simplifier dès à présent la deuxième ligne et obtenir la valeur de y, nous pouvons effectuer $L_2 \leftarrow -\frac{1}{2}L_2$, et ensuite $L_1 \leftarrow L_1 - L_2$, ce qui donne

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & -1 & 2 \end{array}\right)$$

ce qui correspond au système

$$\left\{\begin{array}{rcr} x & = & 1 \\ y & = & -2 \\ -z & = & 3 \end{array}\right.$$

qui est bien diagonal. Il vient alors directement

$$\left\{\begin{array}{rcr} x & = & 1 \\ y & = & -2 \\ z & = & -3 \end{array}\right. .$$

Exemple 5.5.2.
Résoudre le système

$$\begin{pmatrix} 1 & 2 & 0 & 4 \\ 0 & -2 & 3 & 0 \\ 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \\ 3 \\ 1 \end{pmatrix}.$$

Exemple 5.5.3.
Résoudre, en fonction de la valeur du paramètre p, le système

$$\begin{pmatrix} 1 & 2 & 0 \\ 0 & p & 3 \\ 0 & 0 & p(p-1) \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \\ 3 \end{pmatrix}.$$

c Cas d'un système triangulaire non inversible

S'il y a un zéro sur la diagonale d'un système triangulaire, ce dernier n'est pas inversible. On obtient un certain nombre de lignes de la forme $0 = c_i$, où les c_i sont des constantes. Si un de ces c_i est non nul, le système n'admet pas de solution, sinon, des lignes se simplifient.
Nous n'évoquerons ce cas que lorsque $p \leqslant 3$ et $n \leqslant 3$.
Les solutions du système s'interprètent simplement en termes géométriques.

• si $p = 2$, l'ensemble des solutions est soit vide, soit un singleton, soit une droite du plan, soit le plan tout entier.

Exemple 5.5.4.
Résoudre les systèmes :

1. $\left\{\begin{array}{rcr} y & = & 2 \\ y & = & 1 \end{array}\right.$

2. $\left\{\begin{array}{rcrcl} x & + & y & = & 2 \\ & & 2y & = & 1 \end{array}\right.$

• si $p = 3$, l'ensemble des solutions est soit vide, soit un singleton, soit une droite de l'espace, soit un plan de l'espace, soit l'espace tout entier.

Exemple 5.5.5.
Résoudre les systèmes :

1. $\left\{\begin{array}{rcrcrcl} x & + & y & + & z & = & 1 \\ & & & & z & = & 2 \\ & & & & z & = & 1 \end{array}\right.$

2. $\left\{\begin{array}{rcrcrcl} x & + & y & + & z & = & 1 \\ & & y & + & z & = & 2 \\ & & & & z & = & 1 \end{array}\right.$

d Systèmes échelonnés

Nous généralisons ici le cas précédent, quand la matrice du système n'est pas carrée.

Le système S est dit échelonné de rang $r \in \{0, 1, \ldots, \min(n,p)\}$ s'il est de la forme :

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \ldots + a_{1,r}x_r + \ldots + a_{1,p}x_p = b_1 \\ \qquad\quad a_{2,2}x_2 + \ldots + a_{2,r}x_r + \ldots + a_{2,p}x_p = b_2 \\ \qquad\qquad\quad \ddots \quad a_{r,r}x_r + \ldots + a_{r,p}x_r = b_r \\ \qquad\qquad\qquad\qquad\qquad\qquad 0 = b_{r+1} \\ \qquad\qquad\qquad\qquad\qquad\qquad \vdots \quad\quad \vdots \\ \qquad\qquad\qquad\qquad\qquad\qquad 0 = b_p \end{cases}$$

où les coefficients $a_{1,1}, \ldots, a_{r,r}$ sont tous non nuls.

Si S est échelonné, il est compatible (possède au moins une solution) si et seulement $b_{r+1} = \cdots = b_p = 0$. Dans ce cas, chacune des premières lignes s'interprète comme l'équation d'un « hyperplan » de dimension $p-1$ dans $\mathbb{K}^p$. Le système possède une unique solution si et seulement si $r = p$ et une infinité de solutions si et seulement si $r < p$.

Nous n'évoquerons ce cas que lorsque $p \leqslant 3$ et $n \leqslant 3$.
Les solutions du système s'interprètent simplement en termes géométriques.

• si $p = 2$, l'ensemble des solutions est soit vide, soit un singleton, soit une droite du plan, soit le plan tout entier.

Exemple 5.5.6.
Résoudre les systèmes :

1. $\begin{cases} x + y = 2 \\ 0 = 1 \end{cases}$
2. $x + y = 1$

• si $p = 3$, l'ensemble des solutions est soit vide, soit un singleton, soit une droite de l'espace, soit un plan de l'espace, soit l'espace tout entier.

Exemple 5.5.7.
Résoudre les systèmes :

1. $\begin{cases} x + y + z = 1 \\ y + z = 2 \end{cases}$
2. $x + y + z = 1$

e Cas général

Nous allons maintenant voir la méthode d'élimination qui permet de se ramener à un système échelonné.
Dans le système de départ, choisissons une ligne, et une variable. Le but est d'éliminer cette variable dans les autres lignes. Il est donc souvent intéressant de choisir une variable qui apparaît dans un minimum de lignes, comme cela une partie du travail est déjà fait.
Si la variable choisie est x et que la ligne conservée L est de la forme $ax + by + \ldots$ et que l'on veuille éliminer x d'une ligne L' de la forme $cx + dy + \ldots$, il suffit d'effectuer l'opération $L' \leftarrow L' - \frac{c}{a}L$. La ligne L' devient alors $\left(d - \frac{bc}{a}\right)y + \ldots$.
Après avoir éliminé la variable choisie dans toutes les lignes sauf celle conservée, on ne touche plus à cette dernière ligne, et on réitère le procédé avec les lignes restantes, en choisissant une autre variable. Oncontinue jusqu'à ce que le système soit triangulaire ou trivialement sans solution.

Exemple 5.5.8.
Considérons le système $\begin{cases} x + y + z = 1 \\ x - 2y + z = 2 \\ 2x - z = 1 \end{cases}$ que l'on écrira sous forme matricielle $\left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 1 & -2 & 1 & 2 \\ 2 & 0 & -1 & 1 \end{array}\right)$. Puisque y n'apparaît pas dans la dernière ligne, choisissons d'éliminer y dans les deux premières lignes. Afin d'éviter de manipuler des fractions, nous choisissons de conserver la première ligne, car le coefficient devant y y est 1.
Effectuons l'opération $L_2 \leftarrow L_2 + 2L_1$: le système est donc équivalent à $\left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 3 & 0 & 3 & 4 \\ 2 & 0 & -1 & 1 \end{array}\right)$.
On choisit ensuite d'éliminer z de la seconde ligne en utilisant la dernière ligne, car la variable z y a un coefficient égal à -1. Après l'opération $L_2 \leftarrow L_2 + 3L_3$, il vient : $\left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 9 & 0 & 0 & 7 \\ 2 & 0 & -1 & 1 \end{array}\right)$.
Le système obtenu n'a pas l'air très tri-

angulaire ... en fait il l'est si on le réécrit $\begin{pmatrix}1&1&1\\0&-1&2\\0&0&9\end{pmatrix}\begin{pmatrix}y\\z\\x\end{pmatrix}=\begin{pmatrix}1\\1\\7\end{pmatrix}$, ce qui revient à faire des échanges de lignes et de variables dans le dernier système obtenu.

Il vient finalement $\begin{cases} x &= &\frac{7}{9}\\ y &= &-\frac{1}{3}\\ z &= &\frac{5}{9}\end{cases}$.

Exemple 5.5.9.

Considérons le système $\begin{cases} x &+y &+z &= &1\\ x &-2y &+z &= &2\\ 2x &+y &-z &= &1\\ &2y &+z &= &2\end{cases}$.

Codons-le et exécutons l'algorithme du pivot. Il vient successivement :

$$\left(\begin{array}{ccc|c}1&1&1&1\\1&-2&1&2\\2&1&-1&1\\0&2&1&2\end{array}\right)\begin{array}{rcl}L_2&\leftarrow&L_2-L_1\\L_3&\leftarrow&L_3-2L_1\end{array} \quad \text{(III.1)}$$

$$\left(\begin{array}{ccc|c}1&1&1&1\\0&-3&0&1\\0&-1&-3&-1\\0&2&1&2\end{array}\right)\begin{array}{rcl}L_3&\leftarrow&L_3+3L_4\end{array} \quad \text{(III.2)}$$

$$\left(\begin{array}{ccc|c}1&1&1&1\\0&-3&0&1\\0&5&0&5\\0&2&1&2\end{array}\right) \quad \text{(III.3)}$$

Or les deuxième et troisième lignes sont contradictoires, donc le système n'a pas de solution.

Remarque 5.5.10.

Si A est une matrice carrée inversible, alors le système $AX = B$ a une unique solution qui est $X = A^{-1}B$.

La résolution des systèmes 2×2 inversibles peut être effectuée très simplement ainsi.

Exemple 5.5.11.

Résoudre $\begin{pmatrix}1&2\\2&3\end{pmatrix}X=\begin{pmatrix}1\\-2\end{pmatrix}$.

Chapitre IV

Théorie des ensembles

La première partie de ce chapitre est donnée dans un but culturel et ne sera pas nécessairement traitée en cours.

1 Un peu d'histoire

La théorie des ensembles doit son succès au fait qu'elle fournit des fondements solides pour toutes les mathématiques actuelles. En théorie des ensembles, tous les objets mathématiques sont des ensembles : les nombres sont des ensembles, les fonctions sont des ensembles, ...

Nous n'allons pas entrer dans les détails de la théorie. Nous allons tout d'abord nous contenter de la définition suivante pour les ensembles :

Définition 1.0.1 (Pseudo-définition)**.**
Un *ensemble* est une collection d'objets appelés *éléments*. On note $x \in E$ si l'objet x est un élément de l'ensemble E, $x \notin E$ sinon.

Même si cela ressemble à une définition, il y a un problème de taille : cette pseudo-définition repose sur la notion de *collection*, qui n'est pas définie !

En fait, on s'aperçoit qu'on ne parvient pas à définir ce qu'*est* un ensemble mais qu'on peut essayer de le définir par les propriétés qu'on attend de lui.

Pour l'instant, on peut simplement dire qu'on manipule des objets mathématiques, qu'on appelle ensembles, et qu'on dispose d'un prédicat à deux arguments, le prédicat d'appartenance, noté $\in$.

1.1 La crise des fondements

Historiquement, la notion d'ensemble a été introduite au XIXe siècle par Cantor puis formalisés notamment par Frege, qui introduit les ensembles à partir de la notion de prédicat. Essentiellement, il se donne un axiome [1] appelé *schéma de compréhension (non restreinte)* disant qu'étant donné un prédicat P quelconque à un argument, on peut définir un ensemble E, appelé ensemble des x tels que $P(x)$, noté $\{ x \mid P(x) \}$, tel que les éléments de E sont exactement les objets mathématiques x tels que $P(x)$. Pour tout objet mathématique x, on a donc :

$$x \in E \iff P(x)$$

Malheureusement on s'est aperçu bientôt que cet axiome conduisait à un paradoxe, appelé paradoxe de Russel ou paradoxe du barbier :

Exercice 1.1.1 (Paradoxe du barbier)**.**
Dans une ville de Crète, le barbier rase tous les hommes qui ne se rasent pas eux-mêmes. Le barbier se rase t-il lui-même ?

Ce paradoxe est à rapprocher du paradoxe d'Épiménide le Crétois [2] :

> «Tous les crétois sont toujours menteurs.»
>
> Épiménide le Crétois
> (VII^{e} siècle av. J.-C.)

Exercice 1.1.2 (Paradoxe de Russel)**.**
On dira qu'un ensemble x est anormal et on notera $A(x)$ si $x \in x$. On dira qu'un ensemble x est normal dans le cas contraire ($x \notin x$) et on notera $N(x)$. Notons E l'ensemble des ensembles normaux. E est-il normal ?

Ce paradoxe, trouvé indépendamment par Zermelo en 1900 et par Russel en 1901 a conduit à une crise profonde de la théorie des ensembles.

Pour résoudre ce paradoxe, il y a essentiellement deux façons de voir les choses :

1. La théorie des ensembles permet de mettre dans un même ensembles des objets de niveau différents. Par exemple on peut considérer l'ensemble $\{ 1, \sin, \mathbb{R} \}$ qui contient à la fois un nombre, une fonction et un ensemble de nombres, ce qui semble assez incongru et qui fait qu'on peut en arriver à se poser la question de l'appartenance d'un ensemble à lui-même, ce qui conduit au paradoxe. Pour

1. Techniquement, il s'agit en fait de ce qu'on appelle un schéma d'axiomes

2. Attention : En 270 avant J.-C., Philétas de Cos serait mort d'insomnie voire se serait suicidé à cause de ce parallogisme.

éviter ce problème, on peut essayer de classer les ensembles par niveau : on peut se dire qu'il y a des objets de niveau 0 avec lesquels on peut former les ensembles de niveau 1, avec lesquels on peut former les ensembles de niveau 2, etc. et s'interdire d'écrire une proposition de la forme $x \in y$ si x n'est pas de niveau inférieur à y. Du coup, se poser la question $x \in x$ n'est pas possible et on ne peut pas tomber dans le paradoxe. Cette solution, esquissée en 1903 puis véritablement développée en 1908 par Russel, a donné ce qu'on appelle la théorie des types. C'est une solution lourde qui avait quasiment disparu jusqu'à ce qu'on lui trouve des applications très intéressantes en informatique.

2. On peut préciser les règles de formation des ensembles pour qu'on ne puisse pas construire un ensemble avec n'importe quel prédicat : on restreint le schéma de compréhension mentionné plus haut. De cette façon, on peut se poser la question $x \in x$ pour chaque ensemble x mais on ne peut pas construire l'ensemble $\{\, x \in x \,\}$. C'est la solution choisie par Zermelo (en 1908), complétée par la suite par Fraenkel, Skolem et Zermelo (dans les années 1920) et clarifiée par Von Neumann par la suite. Connue sous le nom ZFC (Zermelo-Fraenkel avec axiome du choix), c'est la théorie qui a été adoptée quasi universellement par les mathématiciens.

1.2 Théorie des ensembles ZFC

ZFC repose sur les dix axiomes [3] suivants :

Axiome 1.2.1 (Extensionnalité)**.**
Si deux ensembles ont les mêmes éléments alors ils sont égaux.

3. En fait la compréhension et le remplacement sont techniquement des schémas d'axiomes, le schéma de compréhension pourrait être supprimé car il découle de celui de remplacement, l'axiome de l'ensemble de vide pourrait aussi être supprimé, et le 9e est optionnel, car il est sans impact sur l'essentiel des mathématiques.

Axiome 1.2.2 (de l'ensemble vide)**.**
Il existe un ensemble sans élément.

Axiome 1.2.3 (de la paire)**.**
Si x et y sont deux objets, il existe un ensemble contenant x et y et eux seuls comme éléments. Il se note $\{\, x, y \,\}$.

Axiome 1.2.4 (de la réunion)**.**
Étant donné un ensemble (d'ensembles) E, il existe un ensemble R dont les éléments sont exactement les éléments des éléments de E, c'est-à-dire vérifiant, pour tout x :

$$x \in R \iff \exists X \in E \; x \in X$$

Axiome 1.2.5 (de l'ensemble des parties)**.**
Étant donné un ensemble E, il existe un ensemble, noté $\mathscr{P}(E)$ dont les éléments sont exactement les sous-ensembles de E.

Axiome 1.2.6 (de l'infini)**.**
Il existe un ensemble infini.

Remarque 1.2.1.
Cet axiome est essentiel pour construire l'ensemble $\mathbb{N}$ des entiers naturels.

Il resterait à dire ce que veut dire « infini ». Parfois, cet axiome est exprimé sous la forme plus forte suivante qui permet d'évacuer cette question : il existe un ensemble W, tel qu'on ait à la fois

(i) l'ensemble vide appartient à W ;

(ii) $\forall x \in W \quad x \cup \{\, x \,\} \in W$.

Axiome 1.2.7 (Schéma de compréhension)**.**
Pour tout ensemble E et tout prédicat P, il existe

un ensemble, noté $\{ x \in E \mid P(x) \}$ dont les éléments sont exactement les éléments de E vérifiant P :

$$x \in \{ x \in E \mid P(x) \} \iff (x \in E \text{ et } P(x))$$

Axiome 1.2.8 (Schéma de remplacement)**.**
Étant donné un ensemble E et un prédicat P à deux arguments ayant la propriété d'être fonctionnel, c'est-à-dire que pour tout x, il existe un et un seul y tel que $P(x, y)$ est vérifié, il existe un ensemble X, noté $\{ y \mid \exists x \in E\ P(x, y) \}$ dont les éléments sont exactement les y tels qu'il existe $x \in E$ vérifiant $P(x, y)$. Autrement dit, pour tout y, on a

$$y \in X \iff \exists x \in E\ P(x, y)$$

En notant, pour tout $x \in E$, $f(x)$ l'unique y tel que $P(x, y)$, on note aussi cet ensemble $\{ f(x) \mid x \in E \}$.

Axiome 1.2.9 (de fondation)**.**
Tout ensemble X non vide contient un élément x tel que X et x sont disjoints.

Axiome 1.2.10 (du choix)**.**
Pour tout ensemble E, en notant $\mathscr{P}(E)^*$ l'ensemble des parties de E non vides[4], il existe une application$\sigma : \mathscr{P}(E)^* \to E$, appelée application de choix, associant à toute partie non vide de E l'un de ses éléments, c'est-à-dire telle que pour tout $X \in \mathscr{P}(E)$, on a $\sigma(X) \in X$.

Remarque 1.2.2.
Cet axiome paraît très naturel. Pour saisir la difficulté, essayez par exemple de construire une application σ de ce type dans le cas où $E = \mathbb{N}$, $E = \mathbb{Z}$, $E = \mathbb{Q}$, $E = \mathbb{R}$.

4. Cet ensemble existe bien d'après l'axiome de l'ensemble des parties et du schéma de compréhension

2 Définitions

Nous développons ici la notion d'ensemble, en partant d'une définition intuitive et peu formelle : un ensemble est une collection d'objets mathématiques. Si un objet x est dans cette collection-ensemble E, on note alors $x \in E$ la phrase « x appartient à E ». Sa négation, « x n'appartient pas à E », s'écrit $x \notin E$.

Remarque 2.0.1.
Traditionnellement, on essaie de noter les ensembles avec des lettres majuscules et leurs éléments avec des lettres minuscules.

2.1 Appartenance, égalité

Proposition 2.1.1 (Extentionnalité)**.**
Deux ensembles E et F sont égaux si et seulement s'ils ont les mêmes éléments :

$$E = F \iff \forall x\ (x \in E \iff x \in F).$$

Remarque 2.1.2.
Intuitivement, cette proposition dit que la caractéristique qui définit un ensemble, ce sont ses éléments. Autrement dit, si on voit les ensembles comme des sacs contenant des objets, le sac n'a aucune caractéristique qui puisse le distinguer d'un autre. Cette caractéristique est très particulière au monde idéalisé des ensembles mathématiques. En informatique on verra par exemple qu'on peut avoir deux tableaux contenant les mêmes éléments dans le même ordre et qui ne sont pas le même objet.

Démonstration.
Le sens direct est une conséquence de ce qu'est l'égalité. E étant égal à F toute proposition est équivalente à cette même proposition dans laquelle E est remplacée par F, en particulier, pour tout x, $x \in E$ est équivalent à $x \in F$.

Le sens indirect est une conséquence de l'axiome d'extentionnalité. □

Remarque 2.1.3.
Au niveau de ce cours, on peut considérer la proposition précédente comme une définition.

Définition 2.1.4 (Ensemble vide)**.**
On note $\varnothing$ l'ensemble vide.

Remarque 2.1.5.
Cet ensemble existe d'après l'axiome de l'ensemble vide. Et d'après l'axiome d'extentionnalité, il est unique.

Démonstration.
Soit $\varnothing$ et $\varnothing'$ deux ensembles sans éléments, soit x un objet. Alors, $x \in \varnothing$ et $x \in \varnothing'$ sont toutes deux fausses, donc équivalentes, donc $\varnothing = \varnothing'$. □

Définition 2.1.6.
Étant donnés des objets x_1, x_2, …, x_n, on note $\{ x_1, \ldots, x_n \}$ l'ensemble contenant exactement x_1, …, x_n.

Pour tout ensemble E et tout prédicat P, on note $\{ x \in E \mid P(x) \}$ l'ensemble dont les éléments sont exactement les éléments de E vérifiant P.

Pour tout ensemble E et toute expression $e[x]$ contenant une variable x, on note $\{ e[x] \mid x \in E \}$ l'ensemble des objets mathématiques qui s'écrivent sous la forme $e[x]$ pour au moins un $x \in E$.

Remarque 2.1.7.
1. Pour le premier point, l'ordre des éléments n'importe pas, ni le nombre de fois où ils apparaissent dans la liste des éléments. $\{ 1, 2 \} = \{ 2, 1 \} = \{ 1, 2, 1 \}$. L'existence d'un tel ensemble peut être justifié à partir de l'axiome de la paire et de la réunion. On parle de définition de l'ensemble en extension.
2. Pour le second point, l'existence de l'ensemble est justifiée par le schéma de compréhension. On parle de donc de définition en compréhension.
3. Pour le troisième point, l'existence de l'ensemble est assurée par l'axiome de compréhension si l'on sait que pour tout $x \in E$, $e[x]$ appartient nécessairement à un ensemble fixé F indépendant de x. C'est par exemple le cas de $\{ 2n \mid n \in \mathbb{N} \}$. Sinon, le schéma de remplacement assure son existence (on prend comme prédicat $P(x, y)$ la proposition $y = e[x]$). C'est par exemple le cas de $\{ \mathscr{P}(x) \mid x \in E \}$ où E est un ensemble.

Exemple 2.1.8.
Un même ensemble peut parfois être défini en extension ou en compréhension :

$$\begin{aligned} E &= \{0; 1; 4; 9\} \\ &= \{n \in \mathbb{N} \mid n \leqslant 15 \text{ et } \exists p \in \mathbb{N} \mid n = p^2\}. \end{aligned}$$

Dans toute la suite, E et F désignent deux ensembles.

2.2 Inclusion, ensemble des parties

Définition 2.2.1 (Inclusion)**.**
On dit que E est *inclus* dans F, ce que l'on note $E \subset F$ si tout élément de E est aussi un élément de F, *i.e.*

$$\forall x \in E \; x \in F.$$

Si $E \subset F$, on dit que E est une *partie* ou un *sous-ensemble* de F.

Exemple 2.2.2.
1. Pour tout ensemble E, on a $\varnothing \subset E$ et $E \subset E$.
2. $\mathbb{N} \subset \mathbb{Z}$.
3. $\{1, \{1; 2\}, \mathbb{R}\} \subset \{\mathbb{Z}, \pi, 1, \{1; 2\}, \mathbb{R}\}$.
4. $\{\{1; 2\}\} \not\subset \{1; 2\}$.

Remarque 2.2.3.
Attention à ne pas confondre. $\in$ et $\subset$. Ainsi $1 \in \{1, 2\}, \{1\} \subset \{1, 2\}$, mais $\{1\} \notin \{1, 2\}$. En revanche on a $\{1, 2\} \in \{1, 2, \{1, 2\}\}$ ainsi que $\{1, 2\} \subset \{1, 2, \{1, 2\}\}$.

En pratique pour démontrer une inclusion, on utilise la définition et la manière usuelle de démontrer une proposition universellement quantifiée.

Exemple 2.2.4.
On note E l'ensemble des entiers relatifs pairs qui sont des multiples de 15 et F l'ensemble des entiers relatifs multiples de 6. Montrer $E \subset F$.

Proposition 2.2.5 (Transitivité)**.**
Soit E, F, G trois ensembles, si $E \subset F$ et $F \subset G$, alors $E \subset G$.

Démonstration.
Soit x un objet. Si $x \in E$, comme $E \subset F$, on a $x \in F$. De même, comme $F \subset G$, on a $x \in G$. □

Théorème 2.2.6 (Double inclusion)**.**
Soit E, F deux ensembles, alors

$$(E = F) \Leftrightarrow (E \subset F \text{ et } F \subset E).$$

Démonstration.
Il est clair que pour tout ensemble A, on a $\forall x \in A \quad x \in A$, donc $A \subset A$. Le sens direct est donc évident.

Montrons l'implication réciproque. Supposons $E \subset F$ et $F \subset E$. Alors soit x un objet mathématique quelconque. Montrons $x \in E \iff x \in F$:

— Supposons $x \in E$, alors comme $E \subset F$, on a $x \in F$.

— Supposons $x \in F$, alors comme $F \subset E$, on a $x \in E$.

donc $x \in E \iff x \in F$.

Donc $\forall x \quad x \in E \iff x \in F$.

Donc (par extentionnalité) $E = F$. □

Remarque 2.2.7.
En pratique, on a deux méthodes pour démontrer l'égalité de deux ensembles E et F :

— ou bien on utilise ce théorème ;

— ou bien on utilise directement la propriété d'extentionnalité, en montrant que pour tout x, $x \in E \iff x \in F$ par équivalences successives.

Axiome 2.2.1 (Ensemble des parties de E)**.**
Pour tout ensemble E, on admet l'existence d'un ensemble, noté $\mathscr{P}(E)$ et appelé *ensemble des parties de* E et dont les éléments sont exactement les sous-ensembles de E. Ainsi pour tout ensemble F, on a

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

Exercice 2.2.8.
Déterminer $\mathscr{P}(\{1, 2, 3\})$. Combien cet ensemble admet-il d'éléments ?

Remarque 2.2.9.
Ne pas oublier $\varnothing$ dans l'ensemble des parties.

Exercice 2.2.10.
Déterminer $\mathscr{P}(\varnothing)$, $\mathscr{P}(\{\varnothing\})$ et $\mathscr{P}(\{\varnothing, \{\varnothing\}\})$.

2.3 Réunion, intersection, complémentaire

Dans cette partie A et B désignent deux ensembles.

Définition 2.3.1. 1. On appelle *réunion de A et B* notée $A \cup B$, l'ensemble dont les éléments sont exactement ceux qui sont dans A ou dans B, autrement dit, pour tout objet x,

$$x \in A \cup B \iff (x \in A \text{ ou } x \in B).$$

2. On appelle *intersection de A et B* notée $A \cap B$ dont les éléments sont exactement ceux qui sont dans A et dans B à la fois, autrement dit, pour tout objet x,

$$x \in A \cap B \iff (x \in A \text{ et } x \in B).$$

Démonstration. 1. L'existence de $A \cup B$ est assurée par l'axiome de la réunion appliqué à la paire $\{ A, B \}$.

2. L'existence de $A \cap B$ est assurée par le schéma de compréhension. Il s'agit en effet simplement de $\{ x \in A \mid x \in B \}$.

□

Exemple 2.3.2.
On pose $E = \{ 0, 1, 2, 4 \}$ et $F = \{ 0, 1, 3, 4, 5, 6 \}$. Que vaut $E \cup F$? $E \cap F$?

Remarque 2.3.3.
On a toujours $A \cap B \subset A \subset A \cup B$.

Remarque 2.3.4.
Si $A \subset B$, on a toujours $X \cap A \subset X \cap B$ et $X \cup A \subset X \cup B$.

Définition 2.3.5.
On peut généraliser cette notion à une famille d'ensembles.

1. Si E est un ensemble d'ensemble, on note $\bigcup_{X\in E} X$ la réunion de tous les éléments de E et, dans le cas où E est non vide, $\bigcap_{X\in E} X$ l'intersection de tous les éléments de E. Pour tout x, on a les propriétés :
$$x \in \bigcup_{X\in E} X \iff \exists X \in E,\ x \in X;$$
$$x \in \bigcap_{X\in E} X \iff \forall X \in E,\ x \in X.$$
2. Plus généralement, si on considère une famille d'ensemble $(A_i)_{i\in I}$, on note $\bigcup_{i\in I} A_i$ la réunion de tous les A_i pour $i \in I$ et $\bigcap_{i\in I} A_i$ l'intersection de tous les A_i. Pour tout x, on a les propriétés :
$$x \in \bigcup_{i\in I} A_i \iff \exists i \in I,\ x \in A_i\ ;$$
$$x \in \bigcap_{i\in I} A_i \iff \forall i \in I,\ x \in A_i.$$

Exercice 2.3.6. 1. On note X l'ensemble des segments $[n, n+1]$, pour $n \in \mathbb{N}$.
Que valent $\bigcup_{n\in\mathbb{N}} [n, n+1]$ et $\bigcap_{n\in\mathbb{N}^*} [n, n+1]$?
2. Quel est l'ensemble de définition de tan ?
3. Que vaut chacun des ensembles ci-dessous ?

$$\bigcup_{\varepsilon\in]0,1]}[\varepsilon,1] \quad \bigcup_{\varepsilon\in]0,1]}]\varepsilon,1] \quad \bigcap_{\varepsilon\in]0,1]}[0,\varepsilon] \quad \bigcap_{\varepsilon\in]0,1]}[0,\varepsilon[$$
$$\bigcap_{\varepsilon\in]0,1]}]0,\varepsilon] \quad \bigcap_{\varepsilon\in]0,1]}]0,\varepsilon[\quad \bigcap_{\varepsilon\in]0,1]\cap\mathbb{Q}}[0,\varepsilon] \quad \bigcap_{\varepsilon\in]0,1]\cap\mathbb{Q}}[0,\varepsilon[$$

Remarque 2.3.7.
- Si, pour tout $i \in I$, $A_i \subset B$, alors $\bigcup_{i\in I} A_i \subset B$.
- Si, pour tout $i \in I$, $B \subset A_i$, alors $B \subset \bigcap_{i\in I} A_i$.
- Si $j \in I$, alors $\bigcap_{i\in I} A_i \subset A_j \subset \bigcup_{i\in I} A_i$.

Définition 2.3.8.
On dit que deux ensembles sont *disjoints* si leur intersection est vide.

Théorème 2.3.9 (Distributivité)**.**
La réunion et l'intersection sont distributives l'une sur l'autre. Plus précisément, soit A, B et C trois ensembles. Alors on a les deux égalités suivantes :
$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C);$$
$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C).$$

Plus généralement, soit $(A_i)_{i\in I}$ une famille d'ensembles et B un ensemble, alors
$$\left(\bigcup_{i\in I} A_i\right) \cap B = \bigcup_{i\in I} (A_i \cap B); \tag{IV.1}$$
$$\left(\bigcap_{i\in I} A_i\right) \cup B = \bigcap_{i\in I} (A_i \cup B). \tag{IV.2}$$

Démonstration.
Faire un dessin pour les deux premières égalités.
Les résultats se montrent aisément par double inclusion. On donne la démonstration de l'égalité (IV.1).
Pour tout x :
$$\begin{aligned} x \in \left(\bigcup_{i\in I} A_i\right) \cap B &\Leftrightarrow x \in B \text{ et } x \in \left(\bigcup_{i\in I} A_i\right) \\ &\Leftrightarrow x \in B \text{ et } \exists i_0 \in I,\ x \in A_{i_0} \\ &\Leftrightarrow \exists i_0 \in I,\ x \in A_{i_0} \cap B \\ &\Leftrightarrow x \in \bigcup_{i\in I} (A_i \cap B). \end{aligned}$$
□

Exercice 2.3.10.
Montrer les propriétés (IV.1) et (**? ?**) en raisonnant par double inclusion et en prenant soin de bien revenir aux définitions des objets manipulés.

Définition 2.3.11.
On appelle A *privé de* B, ou *différence de* A *et* B, ou A *moins* B, l'ensemble noté $A \setminus B$ ou $A - B$, tel

que pour tout objet x, $x \in A \setminus B$ si et seulement si $x \in A$ et $x \notin B$.

Cet ensemble est bien défini d'après le schéma de compréhension.

Exercice 2.3.12.
Montrer que $A \setminus B = A \setminus (A \cap B)$.

Définition 2.3.13.
Si $A \subset E$, on appelle *complémentaire de A dans E* noté $\complement_E A$ ou A^C ou $\overline{A}$ quand il n'y a pas de confusion, l'ensemble $E \setminus A$.

Proposition 2.3.14.
Si A et B sont deux parties de E, on a $A \setminus B = A \cap B^C$.

Démonstration.
Faire un dessin.

Soit x quelconque. On a $A \subset E$ donc $x \in A \iff (x \in A$ et $x \in E)$. On a donc :

$$\begin{aligned} x \in A \setminus B &\iff x \in A \text{ et } x \notin B \\ &\iff x \in A \text{ et } (x \in E \text{ et } (x \notin B)) \\ &\iff x \in A \text{ et } x \in E \setminus B \\ &\iff x \in A \cap B^C. \end{aligned}$$

□

Proposition 2.3.15.
Soit E un ensemble et A une partie de E, alors $\overline{\overline{A}} = A$.

Démonstration.
C'est une conséquence de la propriété de double négation : soit x un élément de E, on a $x \in A \Leftrightarrow \neg(\neg(x \in A))$. □

Proposition 2.3.16.
Soit E un ensemble et A une partie de E, alors $A \cup \bar{A} = E$ et $A \cap \bar{A} = \varnothing$.

Démonstration.
Soit $x \in E$, on a $x \in A$ ou $x \notin A$ (tiers exclu), donc $x \in A \cup \bar{A}$.

De plus, on ne peut avoir simultanément $x \in A$ et $x \notin A$, donc $A \cap \bar{A} = \varnothing$. □

Théorème 2.3.17 (Relations de De Morgan)**.**
Soit $(A_i)_{i \in I}$ une famille de parties d'un ensemble E. Alors on a

$$\left(\bigcap_{i \in I} A_i\right)^C = \bigcup_{i \in I} \left(A_i^C\right);$$
$$\left(\bigcup_{i \in I} A_i\right)^C = \bigcap_{i \in I} \left(A_i^C\right).$$

Démonstration.
On montre le deuxième point. Les deux termes de l'égalité sont évidemment des sous-ensembles de E. Considérons donc un $x \in E$ quelconque et montrons que x appartient au premier ensemble si et seulement s'il appartient au deuxième. On a les équivalences :

$$\begin{aligned} x \in \left(\bigcup_{i \in I} A_i\right)^C &\iff x \notin \bigcup_{i \in I} A_i \\ &\iff \neg(\exists i \in I \; x \in A_i) \\ &\iff \forall i \in I \; x \notin A_i \\ &\iff x \in \bigcap_{i \in I} \left(A_i^C\right). \end{aligned}$$

Le premier se déduit de la seconde en passant au complémentaire pur la famille $(A_i^C)_{i \in I}$. □

2.4 Produit cartésien

Définition 2.4.1.
On admettra qu'étant donné deux objets x et y on peut construire un objet appelé *couple* (x, y) et qu'on a la propriété suivante pour tous objets x_1, x_2, y_1, y_2 :

$$(x_1, x_2) = (y_1, y_2) \iff (x_1 = y_1 \text{ et } x_2 = y_2).$$

Remarque 2.4.2. — La construction des couples ne demande en fait aucun axiome supplémentaire, celle-ci pouvant être construite à partir des paires.

— On peut généraliser cette notion à celle de n-uplets.

Définition 2.4.3.
Soient E et F deux ensembles. On admet qu'on peut construire un ensemble noté $E \times F$, appelé *produit cartésien de E et F*, dont les éléments sont les couples avec $x_1 \in E$ et $x_2 \in F$. On définit de même le produit cartésien de n ensembles $E_1 \dots E_n$, noté $E_1 \times \dots \times E_n$, et formé des n-uplets $(x_1, \dots, x_n)$ avec $x_1 \in E_1, \dots, x_n \in E_n$. Si les E_i sont égaux à un ensemble E, on note ce produit E^n.

Remarque 2.4.4.
Attention à ne pas confondre l'ensemble $\{x, y\}$ avec le couple (x, y).

Exemple 2.4.5.
L'ensemble $\mathbb{R}^2$, le rectangle $[0, 2] \times [-1, 4]$, la bande $[0, 1] \times \{ (x, y) \in \mathbb{R}^2 \mid y = 0 \}$ (faire des dessins).

3 Interprétation logique

Soit E un ensemble, P et Q deux prédicats. On pose

$$A = \{ x \in E \mid P(x) \}\,;$$
$$B = \{ x \in E \mid Q(x) \}\,.$$

Soit $x \in E$. On a alors les équivalences logiques suivantes :

$$\begin{aligned}
x \in A \cap B &\iff P(x) \text{ et } Q(x);\\
x \in A \cup B &\iff P(x) \text{ ou } Q(x);\\
x \notin A &\iff \neg(P(x));\\
A = E &\iff \forall x \in E,\ P(x);\\
A \neq \varnothing &\iff \exists x \in E,\ P(x);\\
A \subset B &\iff \forall x \in E,\ (P(x) \Rightarrow Q(x));\\
A = B &\iff \forall x \in E,\ (P(x) \iff Q(x)).
\end{aligned}$$

Chapitre V

Notion d'application

1 Vocabulaire

• En toute rigueur, une *application* est un objet différent d'une *fonction*, mais la différence est hors programme. On emploiera donc les deux termes indifféremment.
• Une application d'un ensemble E dans un ensemble F est une relation qui, à tout élement de E associe un unique élément de F. Attention : on a forcément unicité de l'image et les ensembles de départ et d'arrivée sont une donnée de l'application.

Exemple 1.0.1.
Les applications qui à x associe x^2, partant respectivement de $\mathbb{R}$ et de $\mathbb{R}_+$, sont différentes : la seconde permet de définir la fonction $\sqrt{.}$, pas la première. Dans les deux cas, on pourra considérer comme ensemble d'arrivée $\mathbb{R}$ ou $\mathbb{R}_+$. Une formule ne définit donc pas à elle seule une application.

Définition 1.0.2.
On appelle *fonction* (ou *application*) tout triplet $f = (E, F, \Gamma)$ où E est un ensemble appelé *ensemble de départ* ou *domaine de définition*, F est un ensemble appelé *ensemble d'arrivée*, et Γ est une partie de $E \times F$ appelée *graphe de* f telle que $\forall x \in E, \exists! y \in F, (x, y) \in \Gamma$. Si $(x, y) \in \Gamma$, on note plus simplement $y = f(x)$. On dit que x est alors **un** antécédent de y, et y **l'**image de x.

Remarque 1.0.3.
Il peut y avoir plusieurs antécédents d'un élément dans l'espace d'arrivée, mais une seule image d'un élément de l'espace de départ : cela se voit sur le graphe, que l'on représente comme suit.

• On note une application f allant d'un ensemble E dans un ensemble F de la manière suivante : $f : E \to F$.
• Si l'application est de plus définie par une formule, on écrit alors :

$$\begin{array}{rccc} f : & E & \to & F, \\ & x & \mapsto & \text{Formule dépendant de } x. \end{array}$$

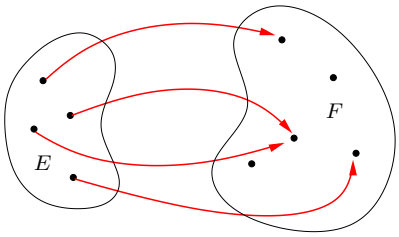


FIGURE V.1 – Exemple d'application – on remarque qu'une image a deux antécédents.

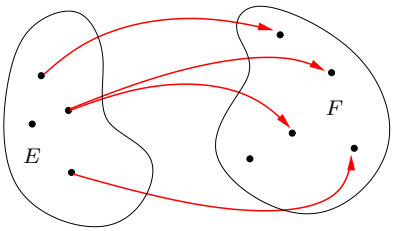


FIGURE V.2 – Cette relation n'est pas une application.

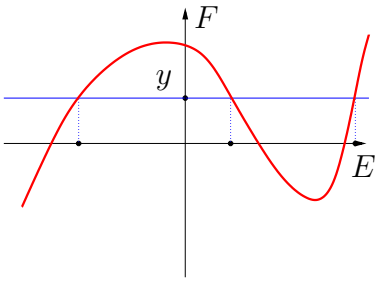


FIGURE V.3 – y a ici trois antécédents représentés.

Remarque 1.0.4.
La notation

$$\begin{array}{rccc} f : & E & \to & F, \\ & x & \mapsto & f(x). \end{array}$$

n'est pas informative.

Remarque 1.0.5.
Si $f, g : E \to F$, alors $f = g$ équivaut à $\forall x \in E$, $f(x) = g(x)$.

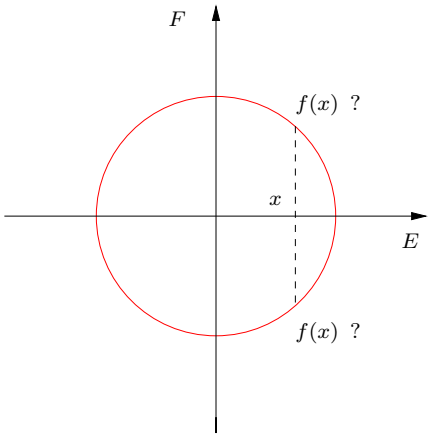


FIGURE V.4 – Cette courbe ne représente pas une application.

Définition 1.0.6.
Soit E, F deux ensembles et $f : E \to F$ une application. On appelle *image* de f le sous-ensemble de F, noté $f(E)$ ou $\mathrm{Im}(f)$, égal à $\{f(x),\ x \in E\}$.

Remarque 1.0.7.
La notation $f(E)$ indique bien l'ensemble de départ, contrairement à la notation $\mathrm{Im}\, f$. Cet ensemble peut aussi s'écrire $\{y \in F \mid \exists x \in E,\ y = f(x)\}$.

Remarque 1.0.8.
Les ensembles de départ et d'arrivée peuvent être n'importe quoi, pas forcément de $\mathbb{R}$ dans $\mathbb{R}$.

• On note $\mathscr{F}(E, F)$, ou F^E, l'ensemble des applications de E dans F. Comment s'en souvenir ? Penser que $\mathrm{Card}\, F^E = \mathrm{Card}\, F^{\mathrm{Card}\, E}$.

Exemple 1.0.9.
L'ensemble des suites réelles est noté $\mathbb{R}^{\mathbb{N}}$. $\{1\}^{\mathbb{N}}$: une seule suite possible.

Définition 1.0.10 (Familles)**.**
Soit I un ensemble. On appelle *famille* d'éléments de E indexée par I toute application de I dans E. Les familles sont notées $(x_i)_{i\in I}$, et rarement, voire jamais, comme des applications.

L'ensemble des familles de E indexées par I est noté E^I.

Exemple 1.0.11.
$\mathbb{R}^{\{1,2\}}$: on peut l'identifier à $\mathbb{R}\times\mathbb{R}$, que l'on note opportunément $\mathbb{R}^2$.

Définition 1.0.12.
Soit E un ensemble et A une partie de E. On appelle *fonction indicatrice de* A la fonction notée $\mathbb{1}_A$ telle que pour tout $x \in A$, $\mathbb{1}_A(x) = 1$, et pour tout $x \in E\backslash A$, $\mathbb{1}_A(x) = 0$.

Exercice 1.0.13.
Soit A et B deux ensembles. Calculer $\mathbb{1}_{A\cap B}$ et $\mathbb{1}_{A\cup B}$ en fonction de $\mathbb{1}_A$ et de $\mathbb{1}_B$.

2 Restriction, prolongement

Définition 2.0.1.
Soit E, E', F, F' quatre ensembles, $f : E \to F$ et $f' : E' \to F'$ deux applications.

(i) Pour toute partie G de E, la restriction de f à G est l'application

$$\begin{array}{rccc} f_{|G} : & G & \to & F, \\ & x & \mapsto & f(x). \end{array}$$

(ii) On dit que f' est un prolongement de f si $E \subset E'$, $F \subset F'$ et $\forall x \in E,\ f(x) = f'(x)$.

 Il y a toujours une infinité de prolongements possibles à une application.
• Une fonction est toujours le prolongement d'une de ses restrictions.

Exemple 2.0.2.
Tout réel strictement positif a deux antécédents par la fonction $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$; mais il n'a qu'un antécédent par la restriction de f à $\mathbb{R}_+$.

3 Composition d'applications

Définition 3.0.1.
Soit E, F, G trois ensembles, $f : E \to F$ et $g : F \to G$ deux applications. On définit alors la *composée* de f par g comme l'application

$$\begin{array}{rccc} g \circ f : & E & \to & G, \\ & x & \mapsto & g(f(x)). \end{array}$$

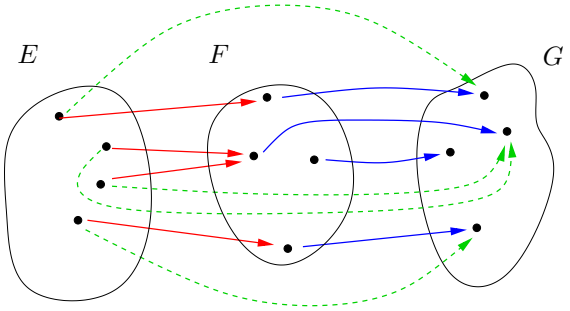


FIGURE V.5 – Exemple de composée.

 On ne peut pas toujours composer deux applications. Par exemple : les fonctions $\mathbb{R}^* \to \mathbb{R}, x \mapsto 1/x$ et $\mathbb{R} \to \mathbb{R}, x \mapsto x^2$.
• Ce n'est pas une opération commutative. Par exemple : $\exists x \in \mathbb{R}_+,\ \ln(x^2) \neq (\ln x)^2$.

Définition 3.0.2.
Soit E un ensemble, on définit dessus l'application *identité sur* E comme $\mathrm{Id}_E : E \to E,\ x \mapsto x$.

Proposition 3.0.3.
Soit E un ensemble, alors $(E^E, \circ)$ est un monoïde de neutre Id_E.

Démonstration.
Soit $x \in E$, f, g et h trois applications de E dans E. On a alors $h(g(f(x)) = h((g \circ f)(x)) = h \circ (g \circ f)(x)$ et $h(g(f(x))) = (h \circ g)(f(x)) = (h \circ g) \circ f(x)$, d'où l'associativité.

On a aussi pour tout $x \in E$, $(\mathrm{Id}_E \circ f)(x) = \mathrm{Id}_E(f(x)) = f(x)$ et $(f \circ \mathrm{Id}_E)(x) = f(\mathrm{Id}_E(x)) = f(x)$, ce qui montre que $f \circ \mathrm{Id}_E = \mathrm{Id}_E \circ f = f$. □

Remarque 3.0.4.
Nous avons vu dans le premier chapitre (et nous reverrons en TD) que certaines fonctions (dans ce cas, $f : \mathbb{N} \to \mathbb{N}$) ne sont pas inversibles (au sens de la structure $(E^E, \circ)$).

4 Injectivité, surjectivité, bijectivité

On comprend vite, en considérant quelques exemples, quelles sont les propriétés qui peuvent empêcher une fonction $f : E \to E$ d'être inversible pour $\circ$.

— Si deux éléments de E ont même image par f, on ne pourra pas « revenir en arrière » et construire g vérifiant $g \circ f = \mathrm{Id}_E$.
— Si un élément de E n'a pas d'antécédent par f, on ne pourra pas construire g vérifiant $f \circ g = \mathrm{Id}_E$.

4.1 Injectivité

Définition 4.1.1.
Soit E, F deux ensembles, $f : E \to F$ une application. On dit que f est *injective* (ou est une *injection*) si $\forall (x, y) \in E^2, f(x) = f(y) \Rightarrow x = y$.

Remarque 4.1.2.
On utilise également la contraposée de cette proposition : $\forall (x, y) \in E^2,\ x \neq y \Rightarrow f(x) \neq f(y)$.

Remarque 4.1.3.
La donnée de l'ensemble de départ est primordiale. Exemple : l'application $[-\pi/2, \pi/2] \to \mathbb{R}, x \mapsto \sin(x)$ est injective alors que $\mathbb{R} \to \mathbb{R}, x \mapsto \sin(x)$ ne l'est pas (*le montrer et tracer les courbes représentatives de ces deux applications*). On peut aussi se demander ce qu'il adviendrait de la figure V.8 si l'on ne précise pas que l'espace de départ est le segment I ici représenté.

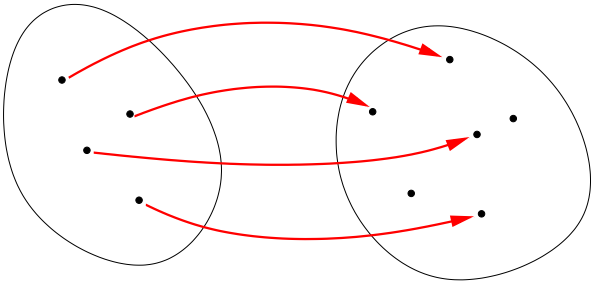


FIGURE V.6 – Exemple d'application injective.

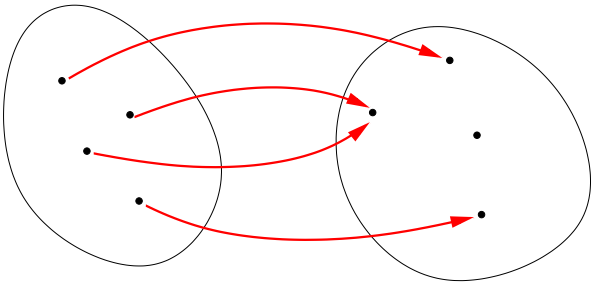


FIGURE V.7 – Exemple d'application non injective : une image a deux antécédents ou plus.

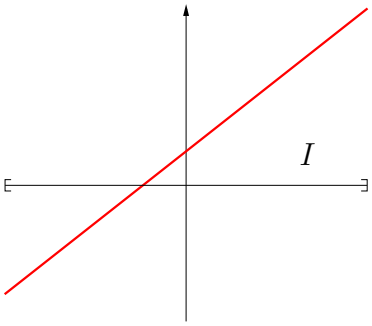


FIGURE V.8 – Graphe d'application injective sur un segment I.

Remarque 4.1.4.
Une application $f : E \to F$ est injective si et seulement si, pour tout $y \in F$, l'équation $y = f(x)$ admet au plus une solution dans E.

Remarque 4.1.5.
Une restriction d'une fonction injective est toujours injective.

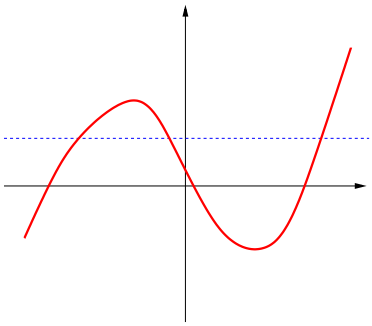


FIGURE V.9 – Graphe d'application non injective : une image a deux antécédents ou plus.

Exercice 4.1.6.
Montrer qu'une fonction réelle strictement croissante est injective.

Théorème 4.1.7 (Composée d'injections.)**.**
Soit E, F et G trois ensembles, $f : E \to F$ et $g : F \to G$ deux applications injectives. Alors $g \circ f$ est injective.

Démonstration.
Soit $(x, y)) \in E^2$, supposons que $g \circ f(x) = g \circ f(y)$. Alors, par injectivité de g puis de f, $f(x) = f(y)$ puis $x = y$. □

4.2 Surjectivité

Définition 4.2.1.
Soit E et F deux ensembles, $f : E \to F$ une application. On dit que f est *surjective* (ou est/réalise une *surjection*) si $\forall y \in F, \exists x \in E, y = f(x)$.

• La donnée de l'espace de départ *et* de l'espace d'arrivée est, là encore, primordiale.

Exemple 4.2.2.
La fonction définie par $x \mapsto \sin x$ est surjective de $[0, 2\pi]$ sur $[-1, 1]$, mais pas de $[0, 2\pi]$ sur $\mathbb{R}$ ni de $[0, \pi]$ sur $[-1, 1]$. Revenir aussi sur les figures V.12 et V.13.

Exercice 4.2.3.
Dans chaque cas, dire si cette application est surjective ou non : $(\mathbb{R}^* \text{ ou } \mathbb{R}_+^*) \to (\mathbb{R} \text{ ou } \mathbb{R}^*)$, $x \mapsto \dfrac{1}{x}$

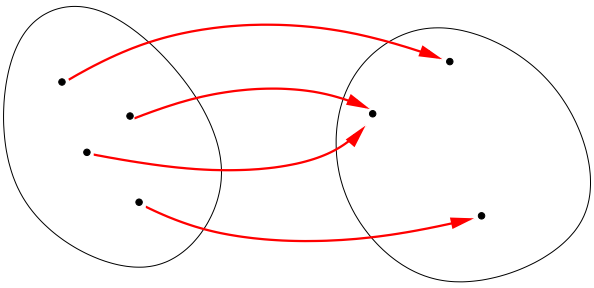


FIGURE V.10 – Exemple d'application surjective.

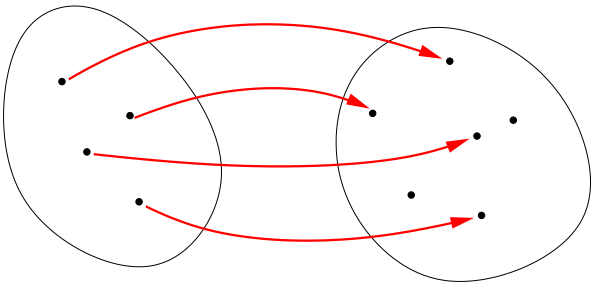


FIGURE V.11 – Exemple d'application non surjective.

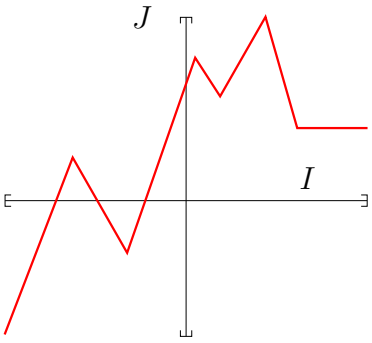


FIGURE V.12 – Graphe d'une application surjective d'un segment I dans un segment J.

Remarque 4.2.4.
Une fonction est toujours surjective sur son image (formellement : la *corestriction* d'une application à son image est toujours surjective).


Une fonction non surjective n'est pas nécessairement injective, et vice-versa.

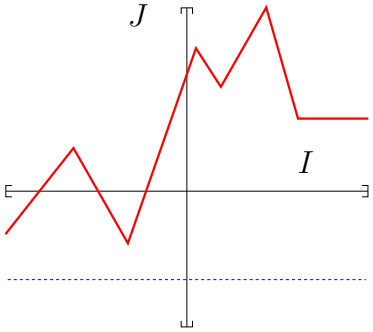


FIGURE V.13 – Graphe d'une application non surjective d'un segment I dans un segment J.

Remarque 4.2.5.
Une application $f : E \to F$ est surjective si et seulement si, pour tout $y \in F$, l'équation $y = f(x)$ admet au moins une solution dans E.

Exercice 4.2.6.
Montrer la surjectivité de $z \mapsto \dfrac{z+i}{z-i}$, définie sur $\mathbb{C}\backslash\{i\}$.

Théorème 4.2.7 (Composée de surjections.)**.**
Soit E, F et G trois ensembles, $f : E \to F$ et $g : F \to G$ deux applications surjectives. Alors $g \circ f$ est surjective.

Démonstration.
Soit $z \in G$, g est surjective : il existe $y \in F$ vérifiant $z = g(y)$. Comme f est surjective, il existe $x \in E$ vérifiant $y = f(x)$ et on a donc $z = g \circ f(x)$. □

4.3 Bijectivité

Définition 4.3.1.
Une application *bijective* (ou qui réalise une *bijection*) est une application injective et surjective.

Soit E et F deux ensembles. Une application $f : E \to F$ est donc bijective si et seulement si $\forall y \in F,\ \exists!\ x \in E,\ y = f(x)$.

Exemple 4.3.2.
Application identité, fonctions affines de la forme $\mathbb{R} \to \mathbb{R}, x \mapsto ax + b$, avec $a \neq 0$, les similitudes ...

Théorème 4.3.3 (Fonction réciproque)**.**
Soit $f : E \to F$ une application.

1. f est bijective si et seulement s'il existe $g : F \to E$ telle que $g \circ f = \mathrm{Id}_E$ et $f \circ g = \mathrm{Id}_F$.
2. Dans ce cas, g est unique et notée f^{-1}, appelée *fonction réciproque de* f, et on a, pour tout $(x, y) \in E \times F$, $f(x) = y$ si et seulement si $x = f^{-1}(y)$.
3. f^{-1} est bijective et $(f^{-1})^{-1} = f$.

Démonstration. 1. Si f bijective, on construit g. Soit $y \in F$. On note $g(y)$ l'unique antécédent de y par f : donc g est une fonction bien définie (tout point a une et une seule image). On vérifie bien que $f \circ g = \mathrm{I}_F$ et que $g \circ f = \mathrm{Id}_E$.
Si g existe, on montre que f est injective et que f est surjective.
2. Unicité : on utilise l'injectivité de f.
Équivalence : facile par double implication.
3. On utilise le point (i) pour la bijectivité et le point (ii) pour l'unicité.

□

 Ne JAMAIS parler de f^{-1} avant d'avoir montré qu'elle existe.

 Dans le cas d'une fonction réelle, il ne faut pas confondre f^{-1} et $1/f$. Ex : $f = 1$ ($1/f$ existe, pas f^{-1}), $f : x \mapsto x$ (f^{-1} existe, pas $1/f$).
• Le graphe de la réciproque d'une fonction est le symétrique par rapport à la première bissectrice du plan du graphe de cette fonction. En effet, si on note Γ le graphe de f et Γ' celui de sa réciproque, on a par définition, pour tous x et y, $(x, y) \in \Gamma$ si et seulement si $(y, x) \in \Gamma'$.

Exemple 4.3.4.
$x \mapsto x^2$ et $x \mapsto \sqrt{x}$, $x \mapsto \ln x$ et $x \mapsto \mathrm{e}^x$, tan et arctan (sur leurs espaces de départ et d'arrivée usuels).

Remarque 4.3.5.
Une application $f : E \to F$ est bijective si et seulement si, pour tout $y \in F$, l'équation $y = f(x)$ admet exactement une solution dans E.

• En pratique, pour montrer que f est bijective, on peut au choix :

1. montrer que f est injective et surjective ;
2. montrer que f a une réciproque en raisonnant par équivalence : $y = f(x)$ ssi $x = f^{-1}(y)$, où f^{-1} est alors à donner (on résout donc $y = f(x)$) ;
3. donner f^{-1} et vérifier que $f \circ f^{-1} = \mathrm{Id}$ **et** $f^{-1} \circ f = \mathrm{Id}$.

Exemple 4.3.6.
Reprendre l'exercice **? ?** et déterminer l'inverse de cette application.

Remarque 4.3.7.
Une injection réalise toujours une bijection sur son image.

Remarque 4.3.8.
Si E est un ensemble et $f : E \to E$ une application bijective, alors f est un élément inversible dans le monoïde $(E^E, \circ)$, d'inverse (au sens algébrique) sa réciproque : f^{-1}.

Théorème 4.3.9 (Composée de bijections.)**.**
Soit E, F et G trois ensembles, $f : E \to F$ et $g : F \to G$ deux bijections. Alors $g \circ f$ est une bijection et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Démonstration.
Utilise les résultats analogues sur injectivité et surjectivité. Ou encore : on donne l'inverse (formule à connaître !) $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$, et surtout ne pas inverser les membres ! □

Exercice 4.3.10.
Trouver deux applications f et g toutes les deux non bijectives, telles que $g \circ f$ est bijective.

4.4 Un peu de vocabulaire anglais ...

• Application : *mapping* ou *map* .
• Injection : *injection* ou *one-to-one mapping* .
• Surjection : *surjection* ou *onto mapping* .
• « non injection » : *many-to-one mapping* .
• Bijection : *bijection* ou *one-to-one correspondance* .

5 Image directe, image reciproque

5.1 Image directe

Définition 5.1.1.
Soit E et F deux ensembles, $f : E \to F$ une application et A une partie de E. On appelle *image directe* de A par f l'ensemble des images des éléments de A, *i.e.* la partie de F :

$$f(A) = \{ f(x) \mid x \in A \}$$
$$= \{ y \in F \mid \exists x \in A,\ y = f(x) \}.$$

Remarque 5.1.2.
La seconde forme de $f(A)$ est la plus pratique à utiliser et est à retenir en priorité.

Remarque 5.1.3.
La notation $f(E)$ utilisée pour l'image de f est bien cohérente.

Remarque 5.1.4.
On a toujours $f(A) \subset \mathrm{Im}(f)$.

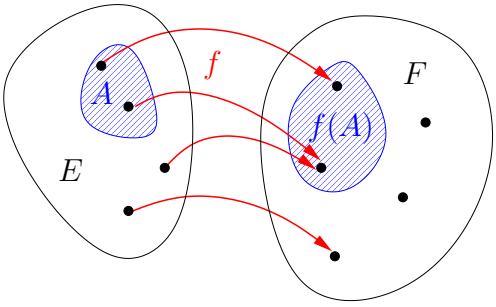


FIGURE V.14 – Image directe d'une partie A par une application f.

• Cela se lit aisément sur un graphe.

Exercice 5.1.5.
Soit E et F deux ensembles, $f : E \to F$ une application, A et B deux parties de E.
• Si $A \subset B$, est-ce que $f(A) \subset f(B)$?
• Comparer $f(A \cup B)$ et $f(A) \cup f(B)$, puis $f(A \cap B)$ et $f(A) \cap f(B)$.

5.2 Image réciproque

Définition 5.2.1.
Soit E et F deux ensembles, $f : E \to F$ une application et B une partie de F. On appelle *image réciproque* de B par f l'ensemble des antécédents des éléments de B, *i.e.* la partie de E :

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

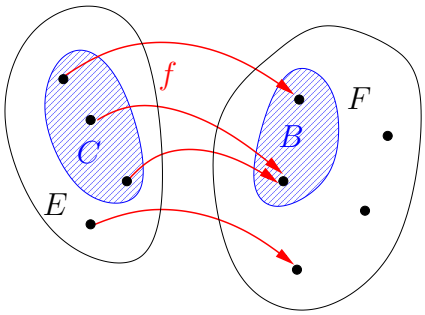


FIGURE V.15 – Image réciproque $C = f^{-1}(B)$ d'une partie B par une application f.

• On lit aussi l'image réciproque d'une partie sur le graphe d'une fonction..


Ne pas confondre avec la réciproque d'une fonction, qui n'existe pas si f n'est pas bijective.
• Notamment, les notations $f^{-1}(\{x\})$ et $f^{-1}(x)$ ne font formellement pas référence au même type d'objet.

Théorème 5.2.2.
Soit E et F deux ensembles. Si $f : E \to F$ est une application bijective et si $B \subset F$, alors on a $f^{-1}(B) = f^{-1}(B)$ pour les deux significations : image réciproque par f et image directe par f^{-1}.

Démonstration.

Soit $x \in E$, alors

$$\begin{aligned} x \in \underbrace{f^{-1}(B)}_{\text{image directe par } f^{-1}} &\Leftrightarrow \exists y \in B,\ x = f^{-1}(y) \\ &\Leftrightarrow \exists y \in B,\ f(x) = y \\ &\Leftrightarrow f(x) \in B \\ &\Leftrightarrow x \in \underbrace{f^{-1}(B)}_{\text{image réciproque par } f} \end{aligned}$$

□

Exercice 5.2.3.
Soit E et F deux ensembles, $f : E \to F$ une application, A et B deux parties de F.
• Si $A \subset B$, est-ce que $f^{-1}(A) \subset f^{-1}(B)$?
• Comparer $f^{-1}(A \cup B)$ et $f^{-1}(A) \cup f^{-1}(B)$, puis $f^{-1}(A \cap B)$ et $f^{-1}(A) \cap f^{-1}(B)$.

Chapitre VI

Fonctions usuelles

Dans tout ce chapitre, A désigne une partie de $\mathbb{R}$ et f une application de A dans $\mathbb{R}$.

1 Vocabulaire usuel des fonctions de $\mathbb{R}$ dans $\mathbb{R}$

On considère une application $f : A \to \mathbb{R}$, dont on veut étudier les propriétés. Notamment, on peut vouloir représenter le graphe de cette fonction : c'est $\{(x, y) \in \mathbb{R}^2 | x \in A \text{ et } y = f(x)\}$ (que l'on représente, lorsque c'est possible, par une « courbe »).

1.1 Transformations usuelles d'une fonction.

Proposition 1.1.1.
Soit $a \in \mathbb{R}_+^*$, on considère des graphes tracés dans le repère orthonormé direct $(O, \overrightarrow{\imath}, \overrightarrow{\jmath})$.

- Le graphe de la fonction $x \mapsto f(x) + a$ s'obtient en translatant le graphe de f du vecteur $a\overrightarrow{\jmath}$ (voir la figure VI.1).
- Le graphe de la fonction $x \mapsto f(x + a)$ s'obtient en translatant le graphe de f du vecteur $-a\overrightarrow{\imath}$ (voir la figure VI.2).
- Le graphe de la fonction $x \mapsto f(ax)$ s'obtient en dilatant le graphe de f suivant le vecteur $\overrightarrow{\imath}$ et par le rapport $\frac{1}{a}$ (voir la figure VI.4).
- Le graphe de la fonction $x \mapsto af(x)$ s'obtient en dilatant le graphe de f suivant le vecteur $\overrightarrow{\jmath}$ et par le rapport a (voir la figure VI.5).
- Le graphe de la fonction $x \mapsto f(-x)$ s'obtient en prenant le symétrique du graphe de f par rapport à l'axe $O\overrightarrow{\jmath}$ (voir la figure **? ?**).
- Le graphe de la fonction $x \mapsto -f(x)$ s'obtient en prenant le symétrique du graphe de f par rapport à l'axe $O\overrightarrow{\imath}$ (voir la figure **? ?**).
- Le graphe de la fonction $x \mapsto -f(-x)$ s'obtient en prenant le symétrique du graphe de f par rapport au point O (voir la figure **? ?**).

Démonstration.
On montre le premier cas, les autres sont similaires. Notons Γ le graphe de f, Γ' celui de $x \mapsto f(x)+a$. Soit $(x, y) \in \mathbb{R}^2$, alors $(x, y) \in \Gamma' \Leftrightarrow (x, y-a) \in \Gamma$, ce qui est bien le résultat demandé. □

Remarque 1.1.2.
Le graphe de la fonction $x \mapsto f(a - x)$ s'obtient donc

- soit en translatant le graphe de f du vecteur $-a\overrightarrow{\imath}$ puis en prenant le symétrique par rapport à $O\overrightarrow{\jmath}$;
- soit en prenant le symétrique du graphe de f par rapport à $O\overrightarrow{\jmath}$ puis en le transtlatant par le vecteur $a\overrightarrow{\imath}$.

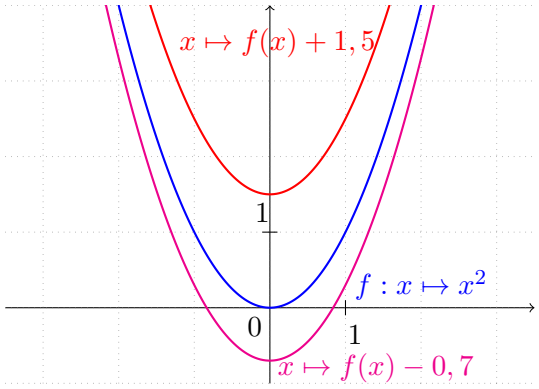


FIGURE VI.1 – Translation verticale du graphe.

1.2 Fonctions paires, impaires et périodiques.

Nous nous intéressons maintenant aux classes de fonctions invariantes par certaines transformations introduites plus haut.

Définition 1.2.1. (i) On dit que f est *paire* si $\forall x \in A$, $-x \in A$ et $f(-x) = f(x)$.

(ii) On dit que f est *impaire* si $\forall x \in A$, $-x \in A$ et $f(-x) = -f(x)$.

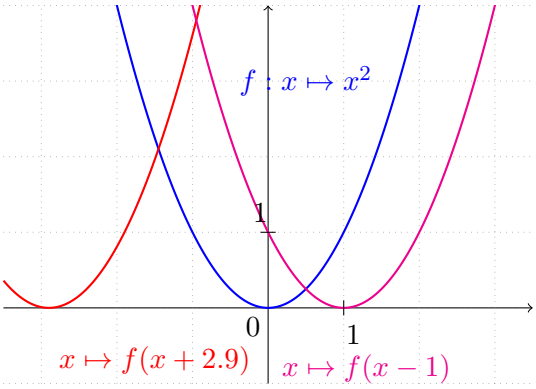


FIGURE VI.2 – Translation horizontale du graphe.

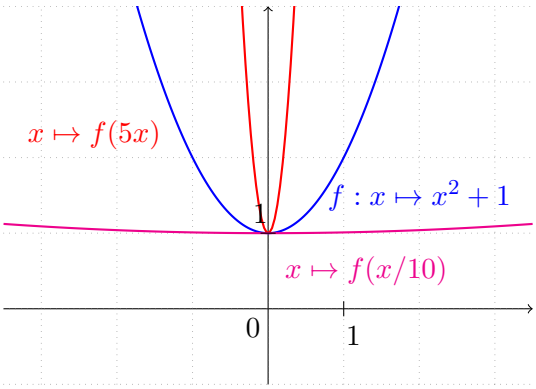


FIGURE VI.3 – Dilatation horizontale du graphe.

• Dessin : les graphes des fonctions paires sont symétriques par rapport à l'axe des ordonnées, ceux des fonctions impaires sont symétriques par rapport à l'origine.
• Réduction du domaine étude : il suffit d'étudier une fonction paire ou impaire sur $\mathbb{R}_+^* \cap A$ pour obtenir toutes les informations nécessaires sur cette fonction.


Une fonction n'est pas toujours paire ou impaire. Le contraire de paire n'est pas impaire.

Exemple 1.2.2.
Sur $\mathbb{R}$, $x \mapsto x^2$ est paire, $x \mapsto x^3$ est impaire et $x \mapsto x^2 + x$ n'est ni paire ni impaire.

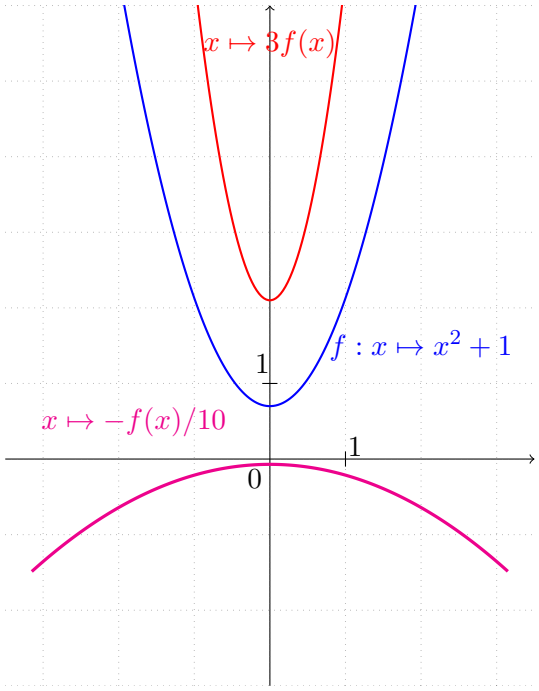


FIGURE VI.4 – Dilatation verticale du graphe.

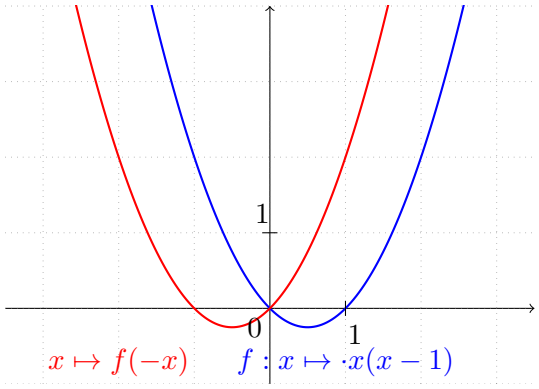


FIGURE VI.5 – Symétrie du graphe par rapport à l'axe vertical.

Proposition 1.2.3.
Soit E, F, G trois parties de $\mathbb{R}$, $f : E \to F$ et $g : F \to G$.

1. Si f est paire, $g \circ f$ est paire.
2. Si f est impaire et g est paire, $g \circ f$ est paire.
3. Si f et g sont impaires, $g \circ f$ est impaire.

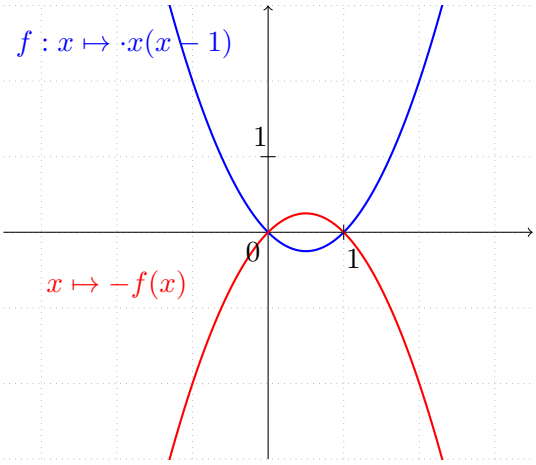


FIGURE VI.6 – Symétrie du graphe par rapport à l'axe horizontal.

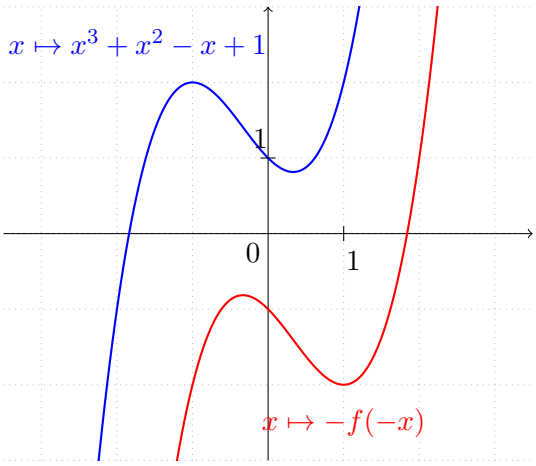


FIGURE VI.7 – Symétrie du graphe par rapport à l'axe horizontal.

Démonstration.
Élémentaire. □

Définition 1.2.4.
Supposons que A est centré ($\forall x \in A, -x \in A$). Alors il existe deux uniques fonctions $g : A \to \mathbb{R}$ et $h : A \to \mathbb{R}$ vérifiant :
— g est paire ;
— h est impaire ;
— $f = g + h$.
On dit que g est la *partie paire* de f et h sa *partie impaire*.

Démonstration.
On raisonne par analyse-synthèse.

Analyse : On suppose que l'on a g et h qui conviennent et l'on essaie d'obtenir des informations dessus. *Indice : si $x \in A$, calculer $f(x) + f(-x)$.*
On a en fait montré l'unicité de g et de h.

Synthèse : On vérifie que les fonctions trouvées dans la phase d'analyse conviennent.
On a alors montré l'existence de g et de h.

□

Exemple 1.2.5.
Les fonctions cosinus et sinus hyperboliques, que nous introduirons bientôt, sont les parties paires et impaires de la fonction exponentielle.

Définition 1.2.6.
Soit $T > 0$. On dit que f est T-périodique si pour tout $x \in A$, $x + T \in A$ et $f(x + T) = f(x)$. Dans ce cas T est appelé ***UNE*** période de f.

• Dessin : on observe un « motif » de longueur T se répétant.
• Réduction du domaine d'étude : si f est T-périodique, il suffit d'étudier f sur tout intervalle de longueur T inclus dans A.

 Il n'y a jamais unicité de la période !

Exemple 1.2.7.
Les fonctions constantes, cos, sin, tan, $x \mapsto x - \lfloor x \rfloor$, $\mathbb{R} \to \mathbb{R}$ sont périodiques.

Exercice 1.2.8.
Déterminer l'allure de la fonction f paire, 4-périodique et telle que $f|_{[0,2]} = \mathrm{Id}$.

1.3 Fonctions monotones

Définition 1.3.1. (i) On dit que f est *croissante* (resp. *strictement croissante*) si :

$$\forall (x,y) \in A^2,\ x \geqslant y \Rightarrow f(x) \geqslant f(y).$$

$$(\text{resp. } \forall (x,y) \in A^2,\ x > y \Rightarrow f(x) > f(y).$$

(ii) On dit que f est *décroissante* (resp. *strictement décroissante*) si :

$$\forall (x,y) \in A^2,\ x \geqslant y \Rightarrow f(x) \leqslant f(y).$$

$$(\text{resp. } \forall (x,y) \in A^2,\ x > y \Rightarrow f(x) < f(y).$$

(iii) On dit que f est *monotone* (resp. *strictement monotone*) si elle croissante ou décroissante (resp. strictement croissante ou strictemement décroissante).

 Une fonction n'est pas toujours croissante ou décroissante. Le contraire de croissant n'est pas décroissant : l'écrire avec des quantificateurs.

Exercice 1.3.2.
Donner un exemple de fonction croissante et décroissante, puis de fonction ni croissante, ni décroissante.

Théorème 1.3.3.
Si f est strictement monotone, alors f est injective.

Démonstration.
Cas strictement croissant (le cas strictement décroissant se traite de la même manière). Soient $x, x' \in A$ tq $f(x) = f(x')$. On ne peut pas avoir $x < x'$ car sinon on aurait $f(x) < f(x')$, ni $x > x'$ car sinon $f(x) > f(x')$. Ainsi $x = x'$. □

Exemple 1.3.4.
cos sur $[\pi, 3\pi/2]$ est strictement croissante.

Proposition 1.3.5.
Soit E, F, G trois parties de $\mathbb{R}$, $f : E \to F$ et $g : F \to G$ monotones.

1. Si f et g sont de même monotonie, $g \circ f$ est croissante.
2. Si f et g sont de monotonies opposées, $g \circ f$ est décroissante.

Démonstration.
Élémentaire, sera vu en TD. □

2 Théorèmes d'analyse admis

Ces résultats seront démontrés plus tard. Soit I un intervalle de $\mathbb{R}$ et $f : I \to \mathbb{R}$. On utilise ici les notions de continuité, de dérivabilité et de primitives comme vues en terminale : nous les définirons proprement plus tard.

Théorème 2.0.1.
Soit $f : I \to \mathbb{R}$ dérivable.

1. f est croissante (resp. décroissante) si et seulement si $f' \geqslant 0$ (resp. $f' \leqslant 0$).
2. La fonction f est constante si et seulement si $\forall x \in I,\ f'(x) = 0$.

Remarque 2.0.2. — On déduit de ce théorème que deux primitives d'une même fonction diffèrent d'une constante.

—  Il est essentiel que I soit un intervalle pour que l'implication de la droite vers la gauche soit vraie (en revanche pour l'autre implication ce n'est pas nécessaire).

— On a aussi que si f' est strictement positive (resp. négative), alors f est strictement croissante (resp. décroissante). Attention, la réciproque est fausse !

Exercice 2.0.3. 1. Trouver une application f non croissante dérivable sur son ensemble de définition, de dérivée positive.

2. Trouver une application g non constante dérivable sur son ensemble de définition, de dérivée nulle.

3. Trouver une application h dérivable non décroissante sur son ensemble de définition, de dérivée négative.

Théorème 2.0.4.
Soient $a < b$, et $f : [a,b] \to \mathbb{R}$ continue strictement monotone. Alors f est bijective de $[a,b]$ sur l'intervalle $f([a,b])$. Et :

(i) Si f croissante : $f([a,b]) = [f(a), f(b)]$;

(ii) Si f décroissante : $f([a,b]) = [f(b), f(a)]$;

(iii) on a des résultats analogues avec un intervalle semi-ouvert, même si a ou $b = \pm\infty$, mais ces résultats font intervenir des limites.

On résume cette information dans un tableau de variation, en indiquant par une flèche continue les intervalles sur lesquels la fonction est continue et strictement croissante.

Exercice 2.0.5.
Déterminer l'intervalle de définition de $x \mapsto \dfrac{(x+1)^2}{\mathrm{e}^x - 1}$ puis tracer son tableau de variations.

Exercice 2.0.6.
Chercher un contre-exemple au Théorème 2.0.8 pour chaque hypothèse que l'on enlève.

Proposition 2.0.7.
Soit $f : I \to \mathbb{R}$ et $g : J \to \mathbb{R}$ deux fonctions dérivables, avec $f(I) \subset J$.

Alors, $g \circ f$ est dérivable et

$$(g \circ f)' = f' \times (g' \circ f).$$

Remarque 2.0.8.
Cela généralise les formules de dérivations de e^u, $\ln(u)$, $\sqrt{u}$ (*etc.*) vues au lycée.

Remarque 2.0.9.
On rappelle que le graphe de la réciproque d'une fonction bijective est le symétrique du graphe de cette fonction par rapport à la première bissectrice du plan.

Théorème 2.0.10.
Soit $f : I \to \mathbb{R}$ bijective.

(i) Si f est strictement monotone, alors f^{-1} l'est aussi et est de même monotonie que f.

(ii) Si f est continue, alors f^{-1} aussi.

(iii) Si f dérivable et si f' ne s'annule pas, alors f^{-1} est aussi dérivable et $(f^{-1})' = \dfrac{1}{f' \circ f^{-1}}$.

• Que se passe-t'il quand f' s'annule pour la tangente de f^{-1} ?

Exemple 2.0.11.
Retrouver ainsi la dérivée de $\sqrt{.}$.

Remarque 2.0.12.
On peut facilement retrouver cette formule en dérivant $(f \circ f^{-1})$.

3 Fonction valeur absolue

Définition 3.0.1.
Soit $x \in \mathbb{R}$ On appelle *valeur absolue* de x le réel $|x| = \sqrt{x^2}$. Il vaut x si $x \geqslant 0$ et $-x$ sinon (voir la figure VI.6).

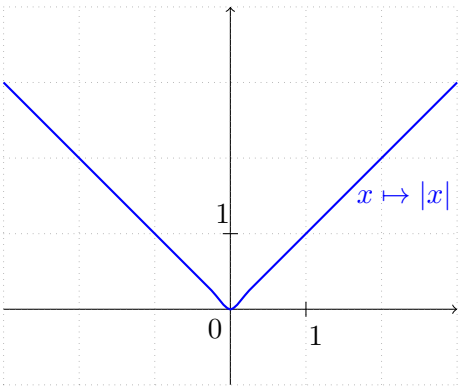


FIGURE VI.8 – Fonction valeur absolue.

Proposition 3.0.2.
C'est une fonction paire, continue sur $\mathbb{R}$ et dérivable sur $\mathbb{R}_-^*$ et $\mathbb{R}_+^*$. Si $x > 0$, on a $\dfrac{\mathrm{d}}{\mathrm{d}x}(|x|) = 1$ et si $x < 0$, $\dfrac{\mathrm{d}}{\mathrm{d}x}(|x|) = -1$.

• Pour tout réel x, $|x|$ est positive, et est nulle ssi $x = 0$.
• $\forall (x, y) \in \mathbb{R}^2$, $|x.y| = |x|.|y|$.
• La valeur absolue coïncide avec le module complexe. L'inégalité triangulaire est toujours vraie. Le cas d'égalité s'exprime alors simplement !
• Interprétation en terme de distance : $|x - y|$ est la distance entre x et y. On peut alors écrire, avec $(x, \varepsilon) \in \mathbb{R}^2$, les intervalles $[x - \varepsilon, x + \varepsilon] = \{y \in \mathbb{R} |\ |y - x| \leqslant \varepsilon\}$ et $]x - \varepsilon, x + \varepsilon[= \{y \in \mathbb{R} |\ |y - x| < \varepsilon\}$.

4 Fonctions puissances entières, polynomiales et rationnelles

4.1 Fonctions puissances entières

Définition 4.1.1.
$x \in \mathbb{R}$, $n \in \mathbb{N}$. On appelle x *puissance* n le réel $x \times \ldots \times x$ (n fois), noté x^n.
Par convention $x^0 = 1$ pour tout $x \in \mathbb{R}$, même 0. Si n est strictement négatif, et si $x \neq 0$, on pose $x^n = \dfrac{1}{x^{-n}}$.

Remarque 4.1.2.
Cela peut se définir rigoureusement par récurrence.

Proposition 4.1.3. (i) $x^{m+n} = x^m x^n$, $x^{mn} = (x^m)^n$, $(xy)^n = x^n y^n$, $\dfrac{x^n}{y^n} = \left(\dfrac{x}{y}\right)^n$.
(ii) $x \mapsto x^n$ a la même parité que n. elle est définie, continue, dérivable de dérivée $x \mapsto nx^{n-1}$.

• Allure des courbes dans tous les cas (n pair, impair, positif, négatif) : voir les figures VI.7 et VI.8.

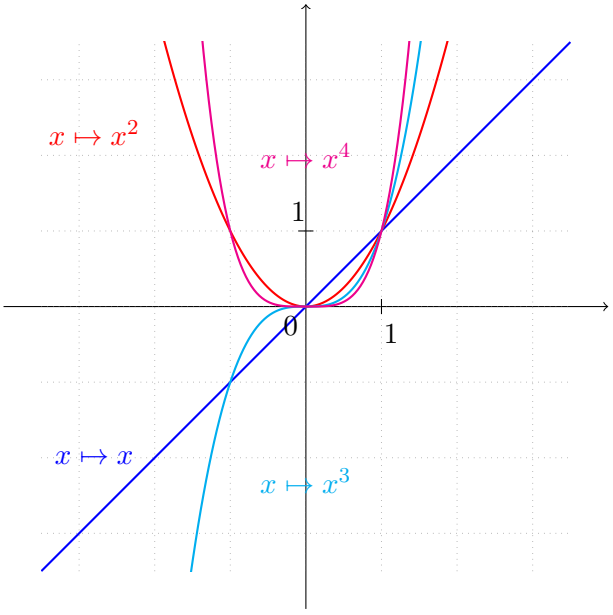


FIGURE VI.9 – Quelques fonctions puissance, exposants positifs.

• Comparaisons : pour $x \in]0, 1]$, $0 \leqslant x^4 \leqslant x^3 \leqslant x^2 \leqslant x \leqslant 1 \leqslant 1/x \leqslant 1/x^2 \ldots$ et l'inverse pour $x \in [1, +\infty[$.

4.2 Fonctions polynomiales et rationnelles

Définition 4.2.1.
On appelle fonction polynomiale toute fonction de la forme $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = \sum_{k=0}^{n} a_k x^k$, où $n \in \mathbb{N}$ et les $a_i \in \mathbb{R}$, $a_n \neq 0$. Dans ce cas, n est appelé le degré de f.

Proposition 4.2.2.
Toute fonction polynomiale est continue et dérivable sur $\mathbb{R}$, et : $\lim\limits_{x \to \pm\infty} f(x) = \lim\limits_{x \to \pm\infty} a_n x^n$.

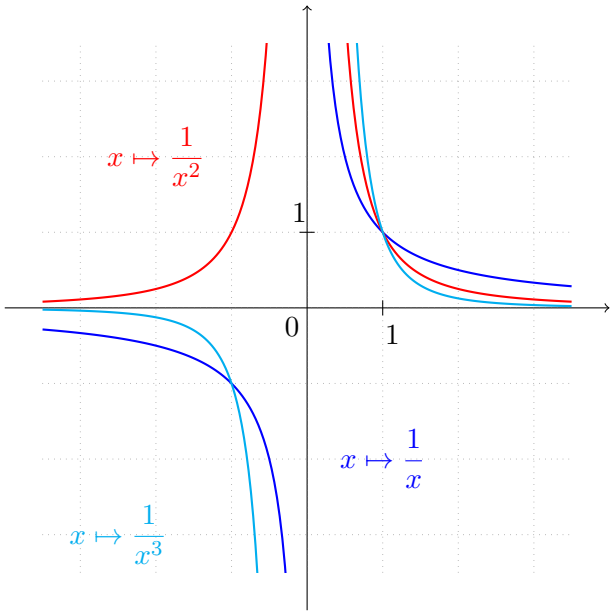


FIGURE VI.10 – Quelques fonctions puissance, exposants négatifs.

Démonstration.
Mettre $a_n x^n$ en facteur. □

Définition 4.2.3.
On appelle *fonction rationnelle* toute fonction de la forme $f : x \mapsto \dfrac{g(x)}{h(x)}$ où g et h sont des fonctions polynomiales. Si $a_n x^n$ et $b_m x^m$ sont les termes dominants de g et h, on a : $\lim\limits_{x\to\pm\infty} f(x) = \lim\limits_{x\to\pm\infty} \dfrac{a_n x^n}{b_m x^m}$.

Remarque 4.2.4.
L'ensemble de définition d'une telle fonction est au moins inclus dans l'ensemble des réels sur lesquels h ne s'annule pas. Nous l'étudierons précisément dans le chapitre dédié aux fractions rationnelles. Sur cet ensemble, toute fraction rationnelle est continue et dérivable.

5 Fonctions exponentielles, logarithmes et puissances quelconques

5.1 Exponentielle et logarithme

Définition 5.1.1.
On appelle *logarithme népérien* la primitive, notée ln, de $x \mapsto \dfrac{1}{x}$ sur $\mathbb{R}_+^*$ valant 0 en 1.

Proposition 5.1.2.
La fonction ln est continue, dérivable sur $\mathbb{R}_+^*$, strictement croissante (donc injective) et bijective de $\mathbb{R}_+^*$ dans $\mathbb{R}$.
Si $x \in \mathbb{R}_+^*$, on a $\ln'(x) = \dfrac{1}{x}$.

Démonstration.
Les outils pour cela seront vus plus tard, mais il suffit de dire que c'est la primitive d'une fonction continue et positive. □

Définition 5.1.3.
On appelle fonction *exponentielle* notée exp la réciproque de ln. On a donc $\exp : \mathbb{R} \to \mathbb{R}_+^*$.

Proposition 5.1.4.
La fonction exp est continue, dérivable sur $\mathbb{R}$, et égale à sa dérivée.

Démonstration.
Utiliser les propriétés de la réciproque. □

• Graphes : voir la figure VI.9.

Proposition 5.1.5.
L'exponentielle est partout strictement positive, elle est trictement croissante et bijective de $\mathbb{R}$ dans $\mathbb{R}_+^*$.

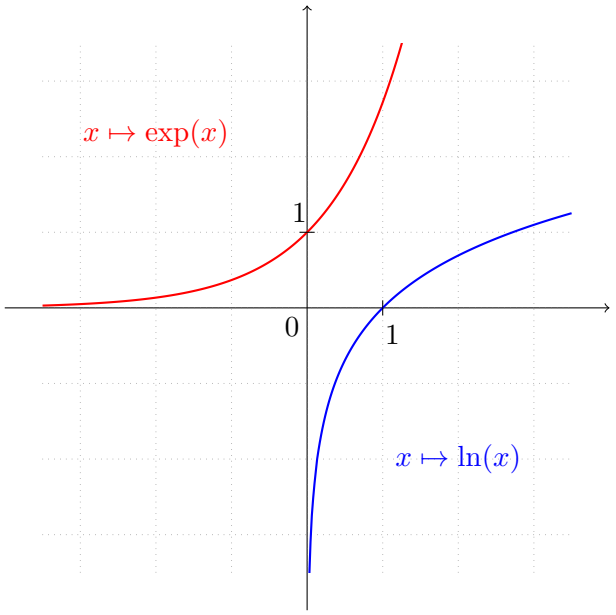


FIGURE VI.11 – Logarithme et exponentielle.

Démonstration.
Utiliser les propriétés de la réciproque. □

Proposition 5.1.6.
On a $\forall (x,y) \in (\mathbb{R}_+^*)^2,\ \ln(xy) = \ln(x) + \ln(y)$ et $\forall (x,y) \in \mathbb{R}^2,\ \exp(x+y) = \exp(x)\exp(y)$.

Démonstration.
Soit $y \in \mathbb{R}_+^*$, étudions $f_y : \mathbb{R}_+^* \to \mathbb{R},\ x \mapsto \ln(xy)$. C'est une fonction dérivable, comme composée de fonctions dérivables, et si $x \in \mathbb{R}_+^*$, $f_y'(x) = y\left(\frac{1}{xy}\right) = \frac{1}{x}$. Ainsi, f_y est une primitive de $x \mapsto \frac{1}{x}$, donc diffère de ln d'une constante. Avec $x = 1$, on obtient cette constante : pour tout $x > 0$, on a bien $\ln(xy) = \ln x + \ln y$.

L'autre identité s'en déduit en observant que exp est la réciproque de ln. □

- En particulier, $\exp(-x) = \dfrac{1}{\exp(x)}$, $\ln(1/x) = -\ln x$ et $\ln(x^n) = n \ln x$.
- $\mathrm{e} = \exp(1) \approx 2,718\ldots$

5.2 Exponentielle de base quelconque

Définition 5.2.1.
Soient $x \in \mathbb{R}_+^*$ et $a \in \mathbb{R}$. On appelle « x puissance a » (ou exponentielle de base x), noté x^a, le réel $x^a = \exp(a \ln x)$.

 x^a n'est qu'une notation pour $\exp(a \ln x)$.

 x^a n'est pas défini avec $x \leqslant 0$, avec cette définition.

Remarque 5.2.2.
- Si $a \in \mathbb{N}$, cette définition coïncide avec la définition donnée précédemment.
- On a alors pour tout $x > 0$, $\exp(x) = \mathrm{e}^x$. La notation e^x est alors utilisée pour tout $x \in \mathbb{R}$ pour désigner $\exp(x)$.
- Cas particuliers :
  1. $a \in \mathbb{N}$: x^a défini sur $\mathbb{R}$.
  2. $a \in \mathbb{Z}$: x^a défini sur $\mathbb{R}^*$.
  3. $a \in \mathbb{R}^+$: prolongeable en 0 par continuité.
  4. $a = \dfrac{p}{q} \in \mathbb{Q}$, $p, q > 0$: définie sur $\mathbb{R}_+$, donc prolongeable en zéro, comme réciproque de la fonction x^q. Et même prolongeable sur $\mathbb{R}$ si q impair.
- Pour traiter un exercice avec des puissances quelconques, il faut quasiment toujours repasser par l'écriture exponentielle.

Proposition 5.2.3.
$\forall x, x' \in \mathbb{R}_+^*$ et $y, y' \in \mathbb{R}$, on a :
1. $(xx')^y = x^y . x'^y$.
2. $x^{y+y'} = x^y . x^{y'}$.
3. $x^{(yy')} = (x^y)^{y'}$.
4. $x^{-y} = \dfrac{1}{x^y} = \left(\dfrac{1}{x}\right)^y$.

Démonstration.
Revenir à la définition via l'exponentielle. □

• On peut dériver x^a en utilisant directement sa définition. On remarquera notamment que

$$\frac{\mathrm{d}}{\mathrm{d}x}(x^a) \neq \frac{\mathrm{d}}{\mathrm{d}a}(x^a).$$


On n'utilisera jamais le symbole $'$ pour dériver une expression, mais plutôt $\frac{\mathrm{d}}{\mathrm{d}\heartsuit}$, où $\heartsuit$ est la variable par rapport à laquelle on dérive l'expression (les autres étant fixées).

Exemple 5.2.4.
Que veut dire $(x^y)'$?

Proposition 5.2.5.
Soit $a \in \mathbb{R}$. On note $f_a : \mathbb{R}_+^* \to \mathbb{R}_+^*, x \mapsto x^a$.

1. f_a est continue, et dérivable et $\forall x \in \mathbb{R}_+^*$, $f_a'(x) = ax^{a-1}$.
2. Si $a \neq 0$, f_a est bijective de $\mathbb{R}_+^*$ sur $\mathbb{R}_+^*$. Sa réciproque est $f_{1/a}$.
3. Si $a < a'$, $\forall x > 1$, $x^a < x^{a'}$, si $x \in]0,1[$, $x^a > x^{a'}$

Démonstration.
1. Il suffit de dériver dans la définition.
2. Il suffit de vérifier que $(x^a)^{1/a} = (x^{1/a})^a = x$.
3. Étude des limites, suivant le signe de a.

□

• Graphes : voir la figure VI.10.

Définition 5.2.6 (Logarithme de base a)**.**
Soit $a \in \mathbb{R}_+^*$. La fonction « puissance en base a », $\mathbb{R} \to \mathbb{R}_+^*, x \mapsto a^x$, est bijective. Sa réciproque est le logarithme de base a

$$\log_a : \left\{ \begin{array}{ccc} \mathbb{R}_+^* & \longrightarrow & \mathbb{R}, \\ x & \longmapsto & \dfrac{\ln(x)}{\ln(a)}. \end{array} \right.$$

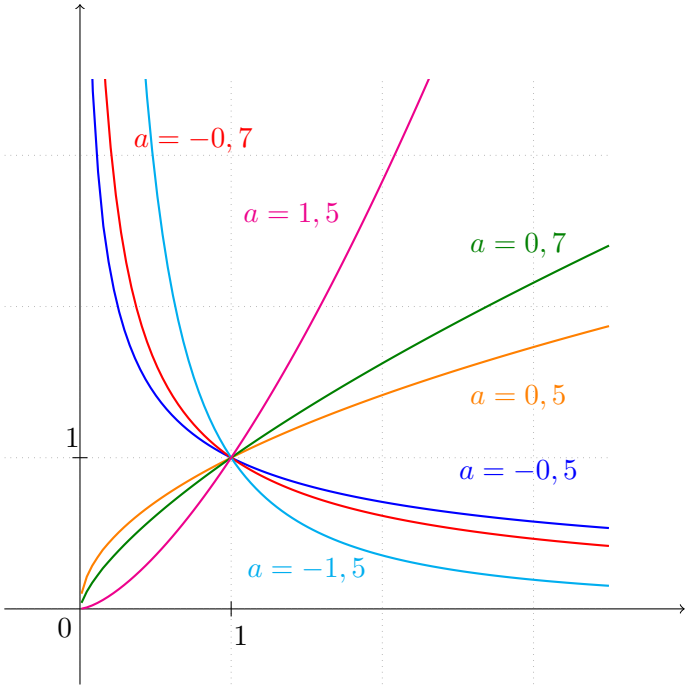
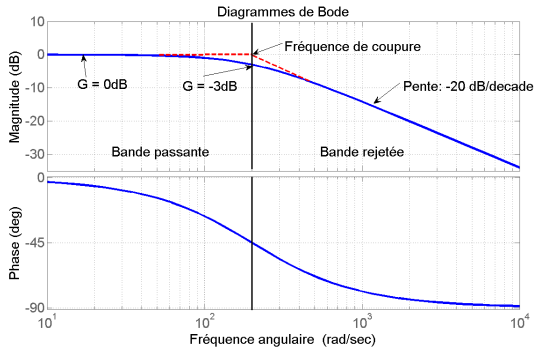


FIGURE VI.12 – Quelques fonctions de la forme $x \mapsto x^a$.

Remarque 5.2.7.
1. Cas particuliers utiles : $\log_{10}$ et $\log_2$. Ils donnent le nombre de chiffres dans l'écriture d'un entier en base 10 ou 2 : si $10^p \leqslant n < 10^{p+1}$, alors n s'écrit avec p chiffres en base 10 et $\lfloor \log_{10} n \rfloor = p$.
2. Propriétés fondamentales : $\log_{10}(10^x) = x$ et $10^{\log_{10} x} = x$.
3. Lien avec les diagrammes de Bode en SI pour représenter une fonction de transfert d'un système électrique (électronique ?). Échelle log/dB, où $dB = 20 \log_{10}$ (autrement dit, 20dB d'augmentation signifie multiplication par 10 du signal) :



5.3 Croissances comparées

Exercice 5.3.1.
Montrer que $\forall x \in \mathbb{R}_+,\ \exp(x) \geqslant 1+x+x^2/2$. En déduire la limite de $\exp(x)/x$ lorsque $x \to +\infty$.

Proposition 5.3.2.
Soient $a, b \in \mathbb{R}_+^*$. Alors :

1. l'exponentielle l'emporte sur les puissances : $\lim\limits_{x\to+\infty} \dfrac{\mathrm{e}^{bx}}{x^a} = +\infty$.
2. les puissances l'emportent sur les logarithmes : $\lim\limits_{x\to 0} x^a.|\ln x|^b = 0$ et $\lim\limits_{x\to+\infty} \dfrac{x^a}{(\ln x)^b} = +\infty$.
3. l'exponentielle l'emporte sur les logarithmes (repasser par les deux premiers points).

Démonstration. 1. On utilise le résultat de l'exercice 5.3.1. Alors, $\dfrac{\mathrm{e}^{bx}}{x^a} = \left(\dfrac{\mathrm{e}^{bx/a}}{x}\right)^a = \left(\dfrac{b}{a}\right)^a \cdot \left(\dfrac{\mathrm{e}^{bx/a}}{bx/a}\right)^a$.

2. Par composition de limites, on a directement $\lim\limits_{x\to+\infty} \dfrac{x}{\ln x} = +\infty$ (et $\lim\limits_{x\to 0} x\ln x = 0$).
Ensuite, $\dfrac{x^a}{(\ln x)^b} = \left(\dfrac{x^{a/b}}{\ln x}\right)^b = \left(\dfrac{a}{b}\right)^b \left(\dfrac{x^{a/b}}{\ln\left(x^{a/b}\right)}\right)^b$.
On obtient l'autre limite par composition.

3. Repasser par les deux premiers points.

□

6 Fonctions circulaires réciproques

6.1 Arccos et Arcsin

Définition 6.1.1.
La fonction cosinus est bijective de $[0,\pi]$ sur $[-1,1]$. Sa fonction réciproque est appelée arccosinus et noté Arccos. Elle est continue sur $[-1,1]$, dérivable sur $]-1,1[$ de dérivée $x \mapsto -\dfrac{1}{\sqrt{1-x^2}}$, décroissante. Son graphe est représenté sur la figure VI.11.

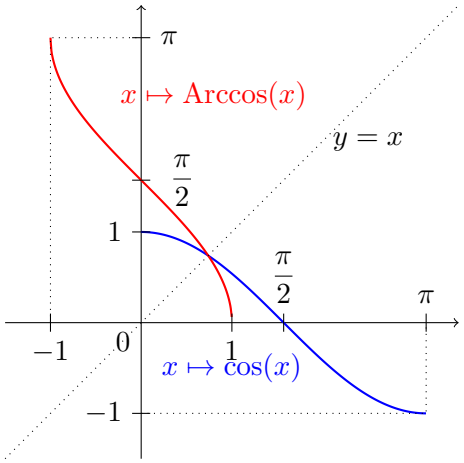


FIGURE VI.13 – Fonctions cos et Arccos.

Définition 6.1.2.
La fonction sinus est bijective de $[-\pi/2,\pi/2]$ sur $[-1,1]$. Sa fonction réciproque est appelée arcsinus et noté Arcsin. Elle est continue sur $[-1,1]$, dérivable sur $]-1,1[$ de dérivée $x \mapsto \dfrac{1}{\sqrt{1-x^2}}$, impaire et croissante. Son graphe est représenté sur la figure VI.12

Démonstration.
Donnons-la pour Arccos ; pour Arcsin on ne montre que l'imparité. □

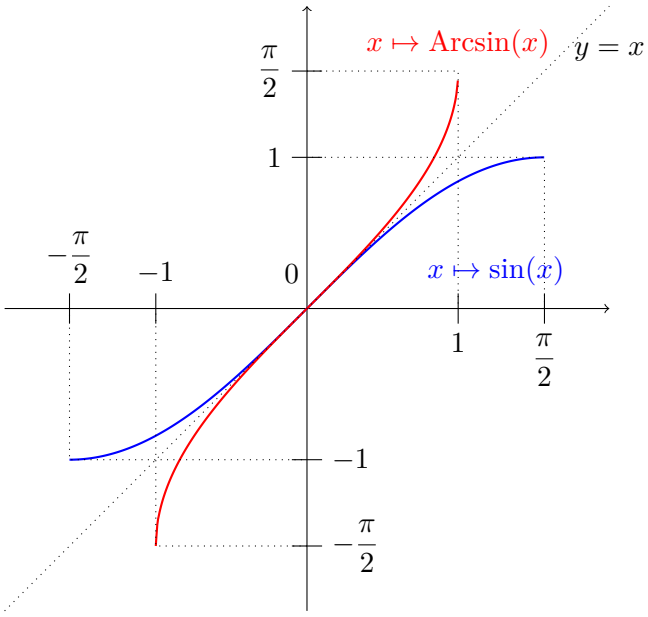


FIGURE VI.14 – Fonctions sin et Arcsin.

Théorème 6.1.3.
$\forall x \in [-1,1]$, $\sin(\mathrm{Arccos}\, x) = \cos(\mathrm{Arcsin}\, x) = \sqrt{1-x^2}$.

Démonstration.

$\cos \circ \mathrm{Arccos} = \mathrm{Id}_{[-1,1]}$, ( $\mathrm{Arccos} \circ \cos \neq \mathrm{Id}_{\mathbb{R}}$, $=$ Id que sur $[0,\pi]$, exemple), donc $\sin^2(\mathrm{Arccos}\, x) = 1 - \cos^2(\mathrm{Arccos}\, x) = 1 - x^2$. Pour finir, on remarque que sur $[0,\pi]$, sin est positif, or $\mathrm{Im}(\mathrm{Arccos}) = [0,\pi]$. □

Exemple 6.1.4.

Très classique : résoudre $\mathrm{Arcsin}\, x = \mathrm{Arccos}\, \frac{4}{5}$, d'inconnue $x \in [-1,1]$.

On a $\frac{4}{5} > 0$, donc $\mathrm{Arccos}\, \frac{4}{5} \in [0, \pi/2]$, donc on doit avoir $\mathrm{Arcsin}\, x \in [0, \pi/2]$, et donc $x \geqslant 0$.

Donc $\mathrm{Arcsin}\, x = \mathrm{Arccos}\, \frac{4}{5}$ ssi $\sin \mathrm{Arcsin}\, x = \sin \mathrm{Arccos}\, \frac{4}{5}$ (car $\mathrm{Arccos}\, \frac{4}{5} \in [-\pi/2, \pi/2]$) ssi $x = \sqrt{1-(4/5)^2} = \frac{3}{5}$ (car $x \geqslant 0$).

 Toujours faire attention aux signes des objets, et aux ensembles auxquels ils appartiennent.

Proposition 6.1.5.
Pour tout $x \in [-1,1]$, on a $\mathrm{Arcsin}\, x + \mathrm{Arccos}\, x = \pi/2$.

Démonstration.
Notons $f : [-1,1] \to \mathbb{R}$, l'application $x \mapsto \mathrm{Arcsin}\, x + \mathrm{Arccos}\, x$. Il suffit de montrer que f est constante sur $[-1,1]$, de valeur $\pi/2$. Pour cela on peut vérifier les trois points suivants :

1. f est constante sur $]-1,1[$. En effet, f est dérivable sur $]-1,1[$ et d'après ce qui précède sa dérivée est nulle. Notons C sa valeur sur $]-1,1[$.
2. f est constante sur $[-1,1]$. En effet, on a $\forall x \in]-1,1[\quad f(x) = C$, donc f admet une limite à droite en -1 et $\lim_{\substack{x \to -1 \\ x > -1}} f(x) = C$. Or f est continue en -1 car Arcsin et Arccos le sont. Donc $\lim_{\substack{x \to -1 \\ x > -1}} f(x) = f(-1)$. Donc $f(-1) = C$. De même $f(1) = C$.
   On a donc $\forall x \in [-1,1] \quad f(x) = C$.
3. La valeur de f sur $[-1,1]$ est $\pi/2$. En effet, en 0, f vaut $\mathrm{Arcsin}\, 0 + \mathrm{Arccos}\, 0$, qui est égal à $0 + \pi/2$.

□

6.2 Arctangente

Remarque 6.2.1.

- La dérivée de tan est $1 + \tan^2 = \frac{1}{\cos^2}$.
- On rappelle le graphe de tan sur $\mathbb{R} \setminus \{\pi/2 + k\pi, k \in \mathbb{Z}\}$ dans la figure VI.13.

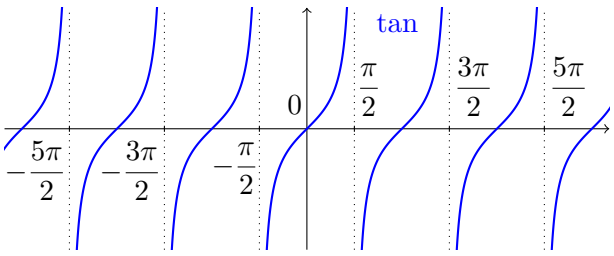


FIGURE VI.15 – Fonction tan.

Définition 6.2.2.
La fonction tangente est bijective de $]-\pi/2, \pi/2[$ sur $\mathbb{R}$. Sa fonction réciproque est appelée arctangente et noté Arctan (parfois atan). Elle est continue sur $\mathbb{R}$, dérivable sur $\mathbb{R}$ de dérivée $x \mapsto \dfrac{1}{1+x^2}$, impaire et strictement croissante. Son graphe est donné figure VI.14 (noter les asymptotes).

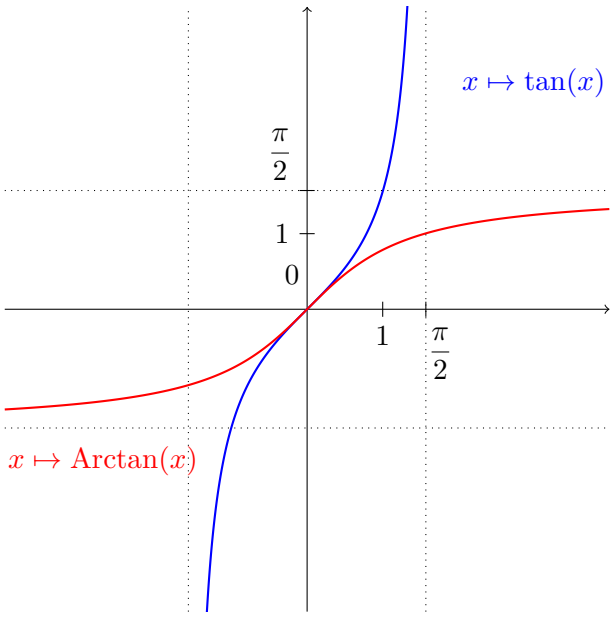


FIGURE VI.16 – Fonctions tan et Arctan.

Proposition 6.2.3.
À nouveau, remarquer que $\tan \circ \mathrm{Arctan} = \mathrm{Id}_{\mathbb{R}}$, mais pas $\mathrm{Arctan} \circ \tan$: ce n'est l'identité que sur $]-\pi/2, \pi/2[$.

Exemple 6.2.4.
Résoudre l'équation $\mathrm{Arctan}(2x) + \mathrm{Arctan}(3x) = \dfrac{\pi}{4}$ (E).

Analyse Soit x une solution de l'équation. On a nécessairement

$$\tan(\mathrm{Arctan}(2x) + \mathrm{Arctan}(3x)) = \tan \pi/4$$

On en déduit successivement

$$\frac{\tan(\mathrm{Arctan}(2x)) + \tan(\mathrm{Arctan}(3x))}{1 - \tan(\mathrm{Arctan}(2x)).\tan(\mathrm{Arctan}(3x))} = 1$$
$$\frac{2x+3x}{1-2x.3x} = 1$$
$$5x = 1 - 6x^2$$

donc $x = -1$ ou $x = \dfrac{-1}{6}$.
Or $\mathrm{Arctan}(-2) + \mathrm{Arctan}(-3) < 0$, donc -1 ne peut pas être solution de (E). Donc il existe au plus une solution : $\dfrac{1}{6}$

Synthèse Posons $x = \dfrac{1}{6}$ et montrons que x est solution de (E).
Posons $v = \tan(\mathrm{Arctan}(2x) + \mathrm{Arctan}(3x))$. On a

$$\begin{aligned} v &= \frac{\tan(\mathrm{Arctan}(2x)) + \tan(\mathrm{Arctan}(3x))}{1 - \tan(\mathrm{Arctan}(2x)).\tan(\mathrm{Arctan}(3x))} \\ &= \frac{1/3 + 1/2}{1 - 1/3 \times 1/2} \\ &= \frac{5/6}{5/6} \\ &= 1 \end{aligned}$$

On a donc

$$\tan(\mathrm{Arctan}(2x) + \mathrm{Arctan}(3x)) = \tan \pi/4 \quad \text{(VI.1)}$$

De plus, $\mathrm{Arctan}(1/3) + \mathrm{Arctan}(1/2) \geqslant 0$. En outre, l'application Arctan étant strictement croissante, on a $\mathrm{Arctan}(1/3) < \mathrm{Arctan}(1/2) < \mathrm{Arctan}(1)$, or $\mathrm{Arctan}(1) = \pi/4$, donc on a $\mathrm{Arctan}(1/3) + \mathrm{Arctan}(1/2) < \pi/2$. Donc on a

$$\mathrm{Arctan}(2x) + \mathrm{Arctan}(3x) \in [0, \pi[\quad \text{(VI.2)}$$

Or la restriction de tan à $[0, \pi[$ est injective donc d'après (VI.1) et (VI.2), on a $\mathrm{Arctan}(2x) + \mathrm{Arctan}(3x) = \dfrac{\pi}{4}$, 1/6 est donc solution de (E).

Conclusion L'équation (E) admet une unique solution : 1/6.

Exercice 6.2.5.
Étudier la fonction

$$f : x \mapsto \operatorname{Arctan}(x) + \operatorname{Arctan}\left(\frac{1}{x}\right).$$

6.3 Coordonnées polaires

Soit (x, y) un couple de coordonnées cartésiennes d'un point M du plan. On veut un couple de coordonnées polaires de M. On cherche un tel couple sous la forme (r, θ) avec $r \geqslant 0$ et $\theta \in]-\pi, \pi[$. On a $r = \sqrt{x^2 + y^2}$. On doit avoir $x = r\cos\theta =$ et $y = r\sin\theta$, donc $\cos\theta = x/r$ et $\sin\theta = y/r$ (on écarte le cas $r = 0$, on dit par convention que toutes les $(0, \theta)$ conviennent).

On distingue deux cas :

Premier cas $y \geqslant 0$. donc M appartient au demi-plan supérieur, donc $\theta \in [0, \pi]$ et donc $\theta = \operatorname{Arccos}(x/r)$.

Second cas $y < 0$, alors $\theta \in]-\pi, 0[$, donc $-\theta \in]0, \pi[$, donc $-\theta = \operatorname{Arccos}(x/r)$, d'où $\theta = -\operatorname{Arccos}(x/r)$.

Remarque 6.3.1.
On aurait aussi pu utiliser Arcsin en distinguant les cas $x \geqslant 0$ ($\theta = \operatorname{Arcsin}(y/r)$) et $x < 0$ ($\theta = \pi - \operatorname{Arcsin}(y/r)$).

Exemple 6.3.2.
Un couple de coordonnées polaires de $(4, -3)$ est $\left(5, -\operatorname{Arccos}\frac{4}{5}\right)$.

7 Fonctions hyperboliques

7.1 ch, sh et th

Définition 7.1.1.
On appelle :

1. *Sinus hyperbolique* et on note sh l'application $\begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \dfrac{\mathrm{e}^{\,x} - \mathrm{e}^{\,-x}}{2} \end{array}$.
2. *Cosinus hyperbolique* et on note ch l'application $\begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \dfrac{\mathrm{e}^{\,x} + \mathrm{e}^{\,-x}}{2} \end{array}$.
3. *Tangente hyperbolique* et on note þ l'application $\begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \dfrac{\operatorname{sh} x}{\operatorname{ch} x} = \dfrac{\mathrm{e}^{\,x} - \mathrm{e}^{\,-x}}{\mathrm{e}^{\,x} + \mathrm{e}^{\,-x}} \end{array}$.

Remarque 7.1.2.
Ces définitions sont les formules d'Euler pour cos, sin et tan, dans lesquelles on a retiré l'imaginaire i, d'où les noms de cosinus, sinus et tangente.

On retrouve aussi les parties paire (ch) et impaire (sh) de l'exponentielle.

Proposition 7.1.3.
1. La fonction ch est continue et dérivable sur $\mathbb{R}$ et sa dérivée est sh. ch est paire.
2. La fonction sh est continue et dérivable sur $\mathbb{R}$ et sa dérivée est ch. sh est impaire.
3. Graphes (cf. figure VI.15).
4. La fonction th est continue et dérivable sur $\mathbb{R}$ et $\text{þ}' = 1 - \text{þ}^2 = \dfrac{1}{\operatorname{ch}^2}$. th est impaire. Voir son graphe figure VI.16.
5. $\operatorname{ch}^2 - \operatorname{sh}^2 = 1$.

Démonstration.
1. On calcule ch′, et $\operatorname{ch}(-x)$.
2. Idem.
3. Tableau de variations. On rajoute : $\lim\limits_{x\to+\infty} \operatorname{ch}(x) - \operatorname{sh}(x) = 0$, donc graphes asymptotiques l'un de l'autre.
4. On dérive þ. Tableau de variations, étude des asymptotes.
5. Simple calcul.

□

Remarque 7.1.4.
Pourquoi fonctions «hyperboliques» et «circulaires» ? Car $x^2 + y^2 = 1$ est l'équation du cercle trigonométrique $\mathscr{C}$, donc $(x, y) \in \mathscr{C}$ ssi $\exists t \in \mathbb{R} \quad x = \cos t$ et $y = \sin t$.

De même, $x^2 - y^2 = 1$ est l'équation de l'hyperbole équilatère $\mathscr{H}$ d'asymptotes $x = \pm y$. Donc $(x, y) \in \mathscr{H}$ ssi $\exists t \in \mathbb{R} \quad x = \operatorname{ch} t$ et $y = \operatorname{sh} t$.

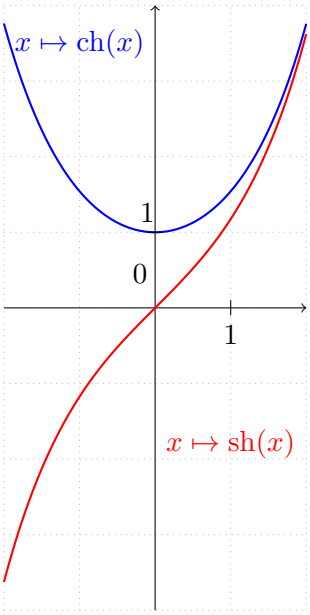


FIGURE VI.17 – Fonctions ch et sh.

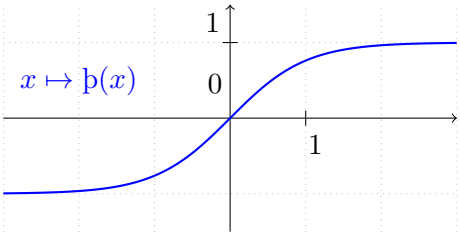


FIGURE VI.18 – Fonction þ.

Remarque 7.1.5.
Toutes les formules trigo circulaires ont une analogue hyperbolique : ex : $\mathrm{ch}(a+b) = \mathrm{ch}\,a\,\mathrm{ch}\,b + \mathrm{sh}\,a\,\mathrm{sh}\,b$, $\mathrm{sh}(a+b) = \mathrm{sh}\,a\,\mathrm{ch}\,b + \mathrm{ch}\,a\,\mathrm{sh}\,b$.

7.2 Fonctions hyperboliques inverses

Elles sont hors-programme. :'(

Mais vous pouvez très bien les retrouver, ainsi que leurs propriétés, en tant qu'exercice ! :)

Chapitre VII

Équations différentielles linéaires

$\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

1 Résultats d'analyse

On se fonde ici sur les notions d'analyse vues en terminale : continuité, dérivabilité, intégrales. Elles seront définies ultérieurement.

1.1 Dérivabilité d'une fonction à valeurs réelles.

Rappel : si une fonction $f : A \to \mathbb{R}$, avec $A \subset \mathbb{R}$, est dérivable en $a \in A$, alors le graphe de f admet une tangente en a, d'équation $y = (x-a)f'(a) + f(a)$.

Proposition 1.1.1.
Soit f et g deux fonctions réelles définies sur $A \subset \mathbb{R}$, dérivables, soit $\lambda \in \mathbb{R}$.

1. La fonction $f + \lambda \cdot g$ est dérivable sur A et $(f + \lambda \cdot g)' = f + \lambda \cdot g'$.
2. La fonction fg est dérivable sur A et $(fg)' = f'g + fg'$.

Proposition 1.1.2.
Soit $f : A \to \mathbb{R}$ et $g : B \to \mathbb{R}$, avec $A \subset \mathbb{R}$, $B \subset \mathbb{R}$ et $f(A) \subset \mathbb{R}$. Si f et g sont dérivables, alors $g \circ f$ est aussi dérivable et $(g \circ f)' = f' \times (g' \circ f)$.

Corollaire 1.1.3.
On retrouve ainsi les résultats usuels

1. Si $f : A \to \mathbb{R}$ est dérivable et ne s'annule pas, alors $1/f$ est dérivable et $\left(\frac{1}{f}\right)' = -\frac{f'}{f^2}$.
2. Si $f : A \to \mathbb{R}$ et $g : A \to \mathbb{R}$ sont dérivables et si g ne s'annule pas, alors f/g est dérivable et $\left(\frac{f}{g}\right)' = \frac{f' \times g - f \times g'}{g^2}$.

Remarque 1.1.4.
On retrouve aussi les formules vues en terminale : dérivée de la puissance, de l'exponentielle et du logarithme d'une fonction.

1.2 Continuité et dérivabilité d'une fonction à valeurs complexes.

I est toujours un intervalle de $\mathbb{R}$ et $f : I \to \mathbb{C}$.

Définition 1.2.1.
On appelle *partie réelle de* f la fonction $\mathrm{Re}(f)$: $I \to \mathbb{R}$, $x \mapsto \mathrm{Re}(f(x))$.
De même on appelle *partie imaginaire de* f la fonction $\mathrm{Im}(f)$: $I \to \mathbb{R}$, $x \mapsto \mathrm{Im}(f(x))$.
On peut alors décomposer f en $\mathrm{Re}(f) + i\,\mathrm{Im}(f)$.

Exemple 1.2.2.
$f : \mathbb{R} \to \mathbb{C},\ x \mapsto (2+i)\mathrm{e}^{(1+i)x}$.

Définition 1.2.3. (i) On dit que f est *continue* (resp. *dérivable*) en a si $\mathrm{Re}(f)$ et $\mathrm{Im}(f)$ le sont. Dans le cas où f est dérivable, on appelle dérivée de f en a notée $f'(a)$ le complexe $f'(a) = (\mathrm{Re}(f))'(a) + i(\mathrm{Im}(f))'(a)$.

(ii) On dit que f est *continue* (resp. *dérivable*) sur un intervalle si elle l'est en tout point de cet intervalle.

(iii) On note (notations non officielles) $\mathscr{C}(I, \mathbb{K})$ et $\mathscr{D}(I, \mathbb{K})$ l'ensemble des fonctions respectivement continues et dérivables de I dans $\mathbb{K}$.

Définition 1.2.4 (Dérivées successives.)**.**
On définit par récurrence les dérivées successives d'une fonction $f : I \to \mathbb{C}$.

— $f^{(0)} = f$.
— Si f est dérivable, $f^{(1)} = f'$.
— Pour tout entier naturel n, si $f^{(n)}$ est définie et est dérivable, alors on définit $f^{(n+1)} = (f^{(n)})'$.

Remarque 1.2.5.
On notera souvent f'' au lieu de $f^{(2)}$, un peu plus rarement f''' au lieu de $f^{(3)}$. Les physiciens utilisent souvent les notations $\dot{f}$, $\ddot{f}$ et $\dddot{f}$ pour indiquer des dérivées successives par rapport à la variable temps.

Définition 1.2.6. (i) On note $\mathscr{C}^1(I,\mathbb{K})$ l'ensemble des fonctions continuement dérivables sur I : $\mathscr{C}^1(I,\mathbb{K}) = \{f \in \mathscr{D}(I,\mathbb{K}) | f' \in \mathscr{C}(I,K)\}$.

(ii) Si $n \in \mathbb{N}$, on note $\mathscr{D}^n(I,\mathbb{K})$ l'ensemble des fonctions n fois dérivables sur I : ce sont les fonctions f telles que $f^{(n)}$ est définie. On note aussi $\mathscr{C}^n(I,\mathbb{K})$ l'ensemble des fonctions n fois continuement dérivables : $\mathscr{C}^n(I,\mathbb{K}) = \left\{f \in \mathscr{D}^n(I,\mathbb{K}) | f^{(n)} \in \mathscr{C}(I,\mathbb{K})\right\}$.

(iii) On note $\mathscr{C}^\infty(I,\mathbb{K})$ l'intersection $\bigcap_{n\in\mathbb{N}} \mathscr{C}^n(I,\mathbb{K})$.

 On ne dérive ici que des fonctions d'une variable réelle.

Remarque 1.2.7.
Si f est dans $\mathscr{C}^n(I,\mathbb{K})$, on dit que f est de *classe* $\mathscr{C}^n$ sur I.

Théorème 1.2.8.
Soit $\varphi \in \mathscr{D}(I,\mathbb{K})$. L'application $x \mapsto \mathrm{e}^{\varphi(x)}$ est dérivable sur I de dérivée l'application $x \mapsto \varphi'(x)\mathrm{e}^{\varphi(x)}$.

Démonstration.
On dérive $\mathrm{e}^{\mathrm{Re}(\varphi)}$ (on obtient $(\mathrm{Re}(\varphi))' \times \mathrm{e}^{\mathrm{Re}(\varphi)}$), puis on dérive d'un côté $\mathrm{Re}(\mathrm{e}^{\varphi(x)}) = \mathrm{e}^{\mathrm{Re}(\varphi)} \cos \mathrm{Im}\,\varphi$ et $\mathrm{Im}(\mathrm{e}^{\varphi(x)}) = \mathrm{e}^{\mathrm{Re}(\varphi)} \sin \mathrm{Im}\,\varphi$ de l'autre. □

Exemple 1.2.9.
Dériver la fonction de l'exemple 1.2.2.

Remarque 1.2.10.
On a les mêmes formules que dans le cas réel pour la dérivée d'une combinaison linéaire, d'un produit ainsi que d'un quotient de fonctions.

1.3 Rappels d'intégration

Définition 1.3.1.
Soit $f : I \to \mathbb{C}$ et $F : I \to \mathbb{C}$. On dit que F est **UNE** *primitive* de f si F est dérivable sur I, de dérivée f.

Théorème 1.3.2.
On rappelle que I est un INTERVALLE.
Soit $f : I \to \mathbb{K}$ dérivable. La fonction f est constante si et seulement si $\forall x \in I,\ f'(x) = 0$.

Exercice 1.3.3.
Proposer un contre-exemple au théorème précédent dans le cas où I n'est pas un intervalle.

Corollaire 1.3.4.
Toutes les primitives d'une même fonction *sur un intervalle* diffèrent d'une constante, et quand cette constante parcourt $\mathbb{K}$, on obtient toutes les primitives. Autrement dit, si F est une primitive de f, $\{F + \lambda,\ \lambda \in \mathbb{K}\}$ est l'ensemble de toutes les primitives de f.

Démonstration.
Soit F et G deux primitives d'une même application sur un intervalle. Alors $F' = G'$, donc $(F-G)'$ est nulle sur cet intervalle, donc $F - G$ est constante sur cet intervalle. Donc toutes les primitives d'une même application diffèrent d'une constante.

Réciproquement, si F est une primitive de f, il est aisé de voir que $F + \lambda$ est une primitive de f pour tout $\lambda \in \mathbb{K}$. □

Exercice 1.3.5.
Déterminer l'ensemble des primitives de la fonction inverse, définie sur $\mathbb{R}^*$.

Il convient de connaître toutes les primitives du formulaire.

Exercice 1.3.6.
Soient a, b, c trois réels. Calculer les primitives de $x \mapsto \dfrac{1}{ax^2 + bx + c}$.
Traiter également le cas $a, b, c \in \mathbb{C}$.

Définition 1.3.7.
Soient $a, b \in I$ et $f \in \mathscr{C}(I, \mathbb{C})$. On appelle *intégrale de f sur $[a,b]$* le complexe $\int_a^b \mathrm{Re}(f)(t)\,\mathrm{d}t + i\int_a^b \mathrm{Im}(f)(t)\,\mathrm{d}t$, noté $\int_a^b f(t)\,\mathrm{d}t$ ou $\int_a^b f$.

 L'interprétation en terme d'aire ne veut rien dire pour une fonction à valeurs complexes.

Exemple 1.3.8.
$\int_0^{2\pi} (1+i)\mathrm{e}^{ix}\,\mathrm{d}x = 0$. (2 méthodes : en séparant parties réelle et imaginaire, ou en primitivant directement).

Théorème 1.3.9 (Le théorème fondamental de l'analyse)**.**
Soit $f \in \mathscr{C}(I, \mathbb{K})$. Soit $a \in I$.

(i) La fonction : $\left\{ \begin{array}{ccc} I & \to & \mathbb{K} \\ x & \mapsto & \int_a^x f(t)\,\mathrm{d}t \end{array} \right.$ est une primitive de f.

(ii) Soit $A \in \mathbb{K}$. La fonction F : $\left\{ \begin{array}{ccc} I & \to & \mathbb{K} \\ x & \mapsto & A + \int_a^x f(t)\,\mathrm{d}t \end{array} \right.$ est la seule primitive de f telle que $F(a) = A$.

Remarque 1.3.10.
C'est ce théorème qui assure que « $\int_a^b f(t)\,\mathrm{d}t = F(b) - F(a)$ ».

Exercice 1.3.11.
Soient a et b deux réels. Calculer les primitives de $x \mapsto \mathrm{e}^{ax}\cos(bx)$ et celles de $x \mapsto \mathrm{e}^{ax}\sin(bx)$.

1.4 Méthodes de calcul

a Intégration par parties

Théorème 1.4.1.
Soient u et $v \in \mathscr{C}^1(I, \mathbb{R})$ et $a, b \in I$. Alors $\int_a^b u'v = [uv]_a^b - \int_a^b uv'$.

Démonstration.
Puisque u, v sont de classe $\mathscr{C}^1$, $u'v + uv'$ est continue, donc admet une primitive F sur I. Or uv est une primitive de $u'v + uv'$, et on finit avec le théorème fondamental. □

Exemple 1.4.2.
Les grands classiques :
• Trouver une primitive de ln. Idem avec Arctan.
• Trouver une primitive du produit d'un polynôme et d'une exponentielle : par exemple $(x^2+1)\mathrm{e}^{x}$.
• Trouver une primitive du produit d'une fonction trigonométrique et d'une exponentielle : par exemple $\cos(x)\mathrm{e}^{2x}$.
• Trouver une primitive du produit d'un polynôme et d'une fonction trigonométrique : par exemple $x^2\cos x$.

b Changement de variable

Théorème 1.4.3.
Soit $\varphi \in \mathscr{C}^1(I, \mathbb{R})$ et $f \in \mathscr{C}^0(J, \mathbb{R})$, où J est un intervalle de $\mathbb{R}$.
On suppose que $\varphi(I) \subset J$. Soient $a, b \in I$.
Alors $\int_{\varphi(a)}^{\varphi(b)} f(t)\,\mathrm{d}t = \int_a^b \varphi'(t)\cdot(f\circ\varphi)(t)\,\mathrm{d}t$.

Remarque 1.4.4.
Moyen mnémotechnique : on écrit "$x = \varphi(t)$" (**au brouillon seulement** !). Alors $\mathrm{d}x = \varphi'(t)\,\mathrm{d}t$, donc $\int f(x)\,\mathrm{d}x = \int f(\varphi(t))\varphi'(t)\,\mathrm{d}t$. Reste le problème des bornes. Quand t va de a à b, $x = \varphi(t)$ va de $\varphi(a)$ à $\varphi(b)$. Et voilà ...

Démonstration.
$\varphi \in \mathscr{C}^1$, $f \in \mathscr{C}^0$, donc $\varphi'.f\circ\varphi \in \mathscr{C}^0$, donc f admet une primitve F, et $\varphi'.f\circ\varphi$ admet $F\circ\varphi$ comme primitive.
On déduit alors le résultat du théorème fondamental :

$$\int_{\varphi(a)}^{\varphi(b)} f(t)\,\mathrm{d}t = [F]_{\varphi(a)}^{\varphi(b)} = F(\varphi(b)) - F(\varphi(a))$$
$$= [F\circ\varphi]_a^b = \int_a^b f(\varphi(t))\varphi'(t)\,\mathrm{d}t$$

□

Remarque 1.4.5.
Les seuls changements de variables que l'on se permettra de ne pas justifier sont ceux affines (on les signalera quand même !).

Exemple 1.4.6.

Calculons l'aire de l'ellipse d'équation $\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$. Le quart supérieur droit de cette ellipse peut être paramétré par $\left(x, b\sqrt{1-\frac{x^2}{a^2}}\right)$, x allant de 0 à a.

On calcule donc $I = \int_0^a b\sqrt{1-\frac{x^2}{a^2}}\,\mathrm{d}x$. On effectue le changement de variable $x = a\cos\theta$ et on obtient : $I = -ab\int_{\pi/2}^0 \sin^2\theta\,\mathrm{d}\theta = ab\int_0^{\pi/2}\frac{1-\cos(2\theta)}{2}\,\mathrm{d}\theta = \frac{1}{4}\pi ab - \frac{ab}{2}\left[\frac{1}{2}\sin(2\theta)\right]_0^{\pi/2} = \frac{1}{4}\pi ab.$

L'aire de l'ellipse est donc πab.

Proposition 1.4.7.
Soit $f : \mathbb{R}\to\mathbb{R}$ une application continue.

1. Si f est paire et $a\in\mathbb{R}$ alors $\int_{-a}^a f(t)\,\mathrm{d}t = 2\int_{-a}^0 f(t)\,\mathrm{d}t = 2\int_0^a f(t)\,\mathrm{d}t$.
2. Si f est impaire et $a\in\mathbb{R}$ alors $\int_{-a}^a f(t)\,\mathrm{d}t = 0$ et $\int_{-a}^0 f(t)\,\mathrm{d}t = -\int_0^a f(t)\,\mathrm{d}t$.
3. Si f est T-périodique ($T>0$) et $a\in\mathbb{R}$ alors $\int_0^T f(t)\,\mathrm{d}t = \int_a^{a+T} f(t)\,\mathrm{d}t$.

Démonstration. 1. On considère $\int_0^a f(t)\,\mathrm{d}t$ et on pose $x=-t$.
Donc $\int_0^a f(t)\,\mathrm{d}t = \int_0^{-a} -f(-x)\,\mathrm{d}x = -\int_0^{-a} f(x)\,\mathrm{d}x = \int_{-a}^0 f(x)\,\mathrm{d}x$.

2. Comme le point précédent avec $\int_0^a f(t)\,\mathrm{d}t = \int_0^{-a} -f(-x)\,\mathrm{d}x = \int_0^{-a} f(x)\,\mathrm{d}x = -\int_{-a}^0 f(x)\,\mathrm{d}x$.

3. *On peut commencer à regarder à partir d'un dessin, dans le cas où $-T<a<0$.*
On a :
$$\int_a^{a+T} f(t)\,\mathrm{d}t = \int_a^0 f(t)\,\mathrm{d}t + \int_0^{a+T} f(t)\,\mathrm{d}t$$
Or par changement de variable $x=t+T$, on obtient
$$\int_a^0 f(t)\,\mathrm{d}t = \int_{a+T}^T f(x)\,\mathrm{d}x.$$
On en déduit que
$$\int_a^{a+T} f(t)\,\mathrm{d}t = \int_{a+T}^T f(t)\,\mathrm{d}t + \int_0^{a+T} f(t)\,\mathrm{d}t = \int_0^T f(t)\,\mathrm{d}t$$
On peut remarquer que l'hypothèse $-T<a<0$ qui a nourri notre intuition ne joue en fait aucun rôle : elle n'est utilisée nulle part dans la démonstration.
Nous avons donc le résultat attendu.

□

2 Généralités

2.1 Cadre

— On s'intéressera à des équations différentielles dont les solutions sont à valeurs dans $\mathbb{K}$, avec $\mathbb{K}=\mathbb{R}$ ou $\mathbb{K}=\mathbb{C}$.
— On considérera I un intervalle ouvert de $\mathbb{R}$.
— On s'intéressera uniquement à des équations différentielles *linéaires*.

Définition 2.1.1 (Équation différentielle linéaire)**.**
Soit n un entier naturel non nul, et $a_0,\ldots,a_{n-1}$ et b des applications continues de I dans $\mathbb{K}$, alors

— On appelle *équation différentielle linéaire d'ordre n* l'équation
$$y^{(n)} + a_{n-1}(t)y^{(n-1)} + \ldots + a_1(t)y' + a_0(t)y = b(t) \qquad (\mathscr{E})$$

— Une *solution* de cette équation est une application $f : I\to\mathbb{K}$ n fois dérivable sur I vérifiant
$$\forall t\in I \quad f^{(n)}(t) + a_{n-1}(t)f^{(n-1)}(t) + \ldots + a_1(t)f'(t) + a_0(t)f(t) = b(t)$$

— L'équation $(\mathscr{E})$ est dite *homogène* si $b = 0_{\mathbb{K}^I}$
— *L'équation homogène associée à* $(\mathscr{E})$ est

$$y^{(n)} + a_{n-1}(t)y^{(n-1)} + \ldots + a_1(t)y' + a_0(t)y = 0 \qquad (\mathscr{H})$$

Remarque 2.1.2.
Nous ne nous intéresserons pas dans le reste de ce chapitre au cas plus général d'une équation

$$a_n(t)y^{(n)} + a_{n-1}(t)y^{(n-1)} + \ldots + a_1(t)y' + a_0(t)y = b(t) \qquad (\mathscr{E})$$

où on a également affecté $y^{(n)}$ d'un coefficient $a_n(t)$.

En effet :
— Si a_n ne s'annule pas, il suffit de diviser cette équation par $a_n(t)$ pour se ramener au cas étudié ici.
— Si a_n s'annule, il est difficile de donner des résultats généraux. En pratique, si on rencontre une telle équation où a_n s'annule, on cherchera en général les solutions sur les intervalles où a_n ne s'annule pas et on regardera au cas par cas comment recoller les solutions aux points où a_n s'annule.

Définition 2.1.3 (Problème de Cauchy)**.**
Soit
— $t_0 \in I$
— $y_0, \ldots, y_{n-1}$ des éléments de $\mathbb{K}$

La recherche des solutions f de $(\mathscr{E})$ vérifiant les *conditions initiales* suivantes :

$$\begin{aligned} & f(t_0) = y_0 \\ \text{et } & f'(t_0) = y_1 \\ & \ldots \\ \text{et } & f^{(n-1)}(t_0) = y_{n-1} \end{aligned}$$

est appelé *problème de Cauchy linéaire d'ordre n*

Exemple 2.1.4.
En physique les déplacement d'un mobile sont régis par l'équation de la dynamique reliant la dérivée seconde de la position et les forces qui s'appliquent au mobile, qui dépendent en général de sa position et ou de sa vitesse. Il s'agit donc d'une équation différentielle d'ordre 2. [1] Il est raisonnable de penser que le problème de Cauchy a alors une unique solution : une position initiale et une vitesse initiale étant données, une seule trajectoire est possible.

2.2 Structure de l'ensemble des solutions

Théorème 2.2.1 (Structure des solutions)**.**
Soit
— $n \in \mathbb{N}$
— $(\mathscr{E})$ une équation différentielle linéaire d'ordre n, d'ensemble de solutions $S_{\mathscr{E}}$
— $(\mathscr{H})$ l'équation homogène associée, d'ensemble de solutions $S_{\mathscr{H}}$

Alors

1. $S_{\mathscr{E}} \subset \mathscr{C}^n(I, \mathbb{K})$
2. $S_{\mathscr{H}}$ est non vide et est stable par combinaisons linéaires.
3. Pour tout $y_0 \in S_{\mathscr{E}}$ fixé, on a
$$S_{\mathscr{E}} = \{\, y_0 + y \mid y \in S_{\mathscr{H}} \,\}$$
4. En particulier, $S_{\mathscr{E}}$ est l'ensemble vide ou un singleton ou un ensemble infini.

Démonstration.
Sous les hypothèses de l'énoncé :

1. Toute solution f est nécessairement n fois dérivable et pour tout $t \in I$,
$$f^{(n)}(t) = b(t) - a_{n-1}(t)f^{(n-1)}(t) - \ldots - a_1(t)f'(t) - a_0(t)f(t)$$
Or b, a_{n-1}, $f^{(n-1)}$, $\ldots$, a_0, f sont des applications continues. Donc $f^{(n)}$ est continue, donc $f \in \mathscr{C}^n(I, \mathbb{K})$.

1. En général linéaire dans les problèmes de prépa mais dans la vraie vie c'est parfois plus compliqué.

2. L'application nulle est une solution triviale de $S_{\mathscr{H}}$, donc $S_{\mathscr{H}}$ est non vide.
   Pour toute application f n fois dérivable et tout $t \in I$, notons $\psi_f(t)$ le scalaire
   $$f^{(n)}(t) + a_{n-1}(t)f^{(n-1)}(t) + \ldots + a_1(t)f'(t) + a_0(t)f(t)$$
   On a alors $f \in S_{\mathscr{H}} \iff \forall t \in I \quad \psi_f(t) = 0$ (ou, de façon plus concise : $f \in S_{\mathscr{H}} \iff \psi_f = 0_{\mathbb{K}^I}$).
   Soit alors f et g deux applications n fois dérivables de I dans $\mathbb{K}$ et λ et μ deux éléments de $\mathbb{K}$. Alors $\lambda f + \mu g$ est évidemment n fois dérivable. Et pour tout $t \in I$, on a $\psi_{\lambda f+\mu g}(t) = \lambda\psi_f(t) + \mu\psi_g(t)$ (autrement dit $\psi_{\lambda f+\mu g} = \lambda\psi_f + \mu\psi_g$).
   En particulier, si f et g sont solutions de l'équation homogène, on a $\psi_f = 0$ et $\psi_g = 0$, donc $\psi_{\lambda f+\mu g} = 0$ donc $\lambda f + \mu g \in S_{\mathscr{H}}$.
3. Soit $y_0 \in S_{\mathscr{E}}$ fixé. On a donc, pour tout $t \in I$, $\psi_{y_0}(t) = b(t)$
   Soit alors $f : I \to \mathbb{K}$ une application n fois dérivable. On a
   $$\begin{aligned} f \in S_{\mathscr{E}} &\iff \psi_f = b \\ &\iff \psi_f = \psi_{y_0} \\ &\iff \psi_{f-y_0} = 0 \\ &\iff f - y_0 \in S_{\mathscr{H}} \end{aligned}$$
   Donc pour tout $f \in S_{\mathscr{E}}$, f s'écrit sous la forme $y_0 + y$ où $y \in S_{\mathscr{H}}$. Donc $S_{\mathscr{E}} \subset \{ y_0 + y \mid y \in S_{\mathscr{H}} \}$.
   Réciproquement, pour tout $y \in S_{cH}$, l'application f définie par $f = y_0 + y$ est n fois dérivable et $f - y_0 \in S_{\mathscr{H}}$, donc $f \in S_{\mathscr{E}}$. Donc $\{ y_0 + y \mid y \in S_{\mathscr{H}} \} \subset S_{\mathscr{E}}$.
   On a donc bien $S_{\mathscr{E}} = \{ y_0 + y \mid y \in S_{\mathscr{H}} \}$.
4. On sait que $S_{\mathscr{H}}$ n'est pas vide puisqu'il contient au moins l'application nulle. Supposons qu'il contienne au moins une autre application f. Alors pour tout $\lambda \in \mathbb{K}$, λf appartient également à $S_{\mathscr{H}}$. Donc ou bien $S_{\mathscr{H}}$ est réduit à un élément, ou bien il est infini.
   D'après le point précédent, si $S_{\mathscr{E}}$ possède au moins un élément y_0, on a $S_{\mathscr{E}} = \{ y_0 + y \mid y \in S_{\mathscr{H}} \}$. Donc $y \mapsto y_0 + y$ est une bijection de $S_{\mathscr{H}}$ sur $S_{\mathscr{E}}$, donc $S_{\mathscr{E}}$ est ou bien réduit à un élément (y_0) ou bien est infini.
   Donc ou bien $S_{\mathscr{E}}$ est vide, ou il est réduit à un élément, ou il est infini.

□

Remarque 2.2.2.
Nous retrouvons ici le même type de structure de l'ensemble des solutions que dans le cas des systèmes linéaires. Ce n'est pas une coïncidence : un même type de structure algébrique se cache derrière (les espaces vectoriels et affines) !

Théorème 2.2.3 (Principe de superposition)**.**
Soit n un entier, $a_0,\ldots,a_{n-1}$, b_1, b_2 des applications continues de I dans $\mathbb{K}$ et $(\lambda_1, \lambda_2) \in \mathbb{K}^2$. Notons a_n la fonction constante égale à 1. On considère les équations

$$\sum_{i=0}^{n} a_i y^{(i)} = b_1 \qquad (\mathscr{E}_1)$$
$$\sum_{i=0}^{n} a_i y^{(i)} = b_2 \qquad (\mathscr{E}_2)$$
$$\sum_{i=0}^{n} a_i y^{(i)} = \lambda_1 b_1 + \lambda_2 b_2 \qquad (\mathscr{E})$$

Alors pour toute solution y_1 de $\mathscr{E}_1$ et toute solution y_2 de $\mathscr{E}_2$, $\lambda_1 y_1 + \lambda_2 y_2$ est une solution de $\mathscr{E}$.

Démonstration.
On reprend les notations de la démonstration de la proposition **? ?**. Soit y_1 et y_2 des solutions respectives de $\mathscr{E}_1$ et $\mathscr{E}_2$. On a $\psi_{y_1} = b_1$ et $\psi_{y_2} = b_2$. Or $\psi_{\lambda_1 y_1+\lambda_2 y_2} = \lambda_1\psi_{y_1} + \lambda_2\psi_{y_2}$. Donc $\psi_{\lambda_1 y_1+\lambda_2 y_2} = \lambda_1 b_1 + \lambda_2 b_2$. □

Théorème 2.2.4 (Solutions du problème de Cauchy linéaire)**.**
Soit n un entier naturel et $\mathscr{E}$ une équation différentielle linéaire d'ordre n. Alors, pour tout choix des conditions initiales, le problème de Cauchy linéaire d'ordre n admet une unique solution.

Remarque 2.2.5.
Ce théorème est hors-programme dans le cas général. Sa démonstration dans le cas général requiert en effet des outils d'analyse que nous n'avons pas encore à notre disposition.

En revanche, dans les cas $n = 1$ et $n = 2$, le résultat est au programme et sera démontré.

3 Équations linéaires du premier ordre

3.1 Résolution de l'équation homogène

Théorème 3.1.1.
Soit A une primitive de a sur I. Soit $a \in \mathscr{C}^0(I, \mathbb{K})$. Alors, l'ensemble des solutions de l'équation homogène $y' + ay = 0$ est

$$S_{\mathscr{H}} = \left\{ \begin{array}{ccc} I & \to & \mathbb{K} \\ t & \mapsto & K\mathrm{e}^{-A(t)} \end{array} \;\middle|\; K \in \mathbb{K} \right\}.$$

Si de plus une condition initiale est fixée, alors la solution est unique. En particulier si y s'annule en un point, elle est identiquement nulle.

Démonstration.
Toute fonction de la forme $t \mapsto K\mathrm{e}^{-A(t)}$ est une solution (c'est évident, il n'y a qu'à dériver).

Réciproquement, soit y une solution. On pose $z(t) = y(t)\mathrm{e}^{A(t)}$ pour $t \in I$. z est dérivable sur I et pour tout t, $z'(t) = y'(t)\mathrm{e}^{A(t)} + y(t)A'(t)\mathrm{e}^{A(t)} = (y'(t) + a(t)y(t))\mathrm{e}^{A(t)} = 0$, donc z est une constante K.

Une condition initiale $y(t_0) = y_0$ étant donnée, elle est vérifiée si et seulement si $K\mathrm{e}^{-A(t_0)} = y_0$, c'est-à-dire si et seulement si $K = y_0\mathrm{e}^{A(t_0)}$. Il y a alors une et une seule solution : $t \mapsto y_0\mathrm{e}^{A(t_0)-A(t)}$. □

Remarque 3.1.2.
On dit que l'ensemble des solutions a une structure de droite vectorielle, de vecteur directeur $t \mapsto \mathrm{e}^{-A(t)}$.

Exercice 3.1.3.
Déterminer les intervalles de résolution puis résoudre les équations différentielles suivantes.

1. $y' + y = 0$
2. $y' + \dfrac{1}{\sqrt{1-x^2}}y = 0$ avec $y(1/2) = 1$.

Corollaire 3.1.4.
Une solution qui s'annule en un point ne peut être que la fonction nulle.

Démonstration.
En effet elle est solution d'un problème de Cauchy de la forme $y(t_0) = 0$. Or il existe une unique solution à ce problème et la fonction nulle est manifestement solution. □

3.2 Résolution d'une équation avec second membre

Remarque 3.2.1.
On a déjà vu que si l'on connaissait une solution $\tilde{y}$ de l'équation avec second membre, alors on pouvait construire toutes les solutions de l'équation avec second membre à partir de l'ensemble des solutions de l'équation homogène.

Dans le cas d'une équation d'ordre un, on dit que l'ensemble des solutions a une structure de droite affine, car l'ensemble des solutions est l'ensemble des $\tilde{y} + y$ pour y parcourant une droite vectorielle.

Théorème 3.2.2.
Soit a et b deux applications continues de I dans $\mathbb{C}$, et A une primitive de a.

Alors le problème de Cauchy $y' + ay = b$ et $y(t_0) = y_0$ admet une unique solution :

$$\left\{ \begin{array}{ccc} I & \to & \mathbb{K} \\ t & \mapsto & \mathrm{e}^{A(t_0)-A(t)}y_0 + \mathrm{e}^{-A(t)} \displaystyle\int_{t_0}^{t} \mathrm{e}^{A(u)}b(u)\,\mathrm{d}u \end{array} \right.$$

Remarque 3.2.3.
L'unicité est aisée à démontrer : si on dispose de deux solutions de ce problème, leur différence est une solution de l'équation homogène du problème s'annulant en t_0, c'est donc l'application nulle.

On peut également assez directement montrer que l'application donnée est solution par calcul.

Nous donnons cependant ci-dessous une autre démonstration qui a l'avantage de permettre de retrouver la formule. Cette méthode est à connaître et s'appelle la *méthode de la variation de la constante*.

Lemme 3.2.4.
Soit $h : I \to \mathbb{C}$ ne s'annulant pas. Alors, pour tout $y : I \to C$, il existe une unique fonction $C : I \to \mathbb{C}$ telle que $y = Ch$.

De plus, si h est dérivable, alors y est dérivable si et seulement si C l'est.

Démonstration.
C'est élémentaire : $y = Ch$ si et seulement si $C = \dfrac{h}{y}$.

On obtient la dérivabilité de C ou de y par opérations usuelles sur les fonctions dérivables. □

Démonstration (Théorème **? ?**).
Notons $\mathscr{E}$ l'équation $y' + ay = b$, $(\mathscr{H})$ l'équation homogène associée, $S_{\mathscr{E}}$ et $S_{\mathscr{H}}$ les ensembles de solutions respectifs de ces deux équations et S l'ensemble des solutions du problème de Cauchy $y' + ay = b$ et $y(t_0) = y_0$.

On sait que $y_{\mathscr{H}} : t \mapsto \mathrm{e}^{-A(t)}$ est une solution de $\mathscr{H}$ qui ne s'annule jamais.

D'après le lemme **? ?**, toute fonction $y : I \to \mathbb{K}$ dérivable est de la forme $Cy_{\mathscr{H}}$, avec $C : I \to \mathbb{K}$ dérivable..

Soit donc une fonction $C : I \to \mathbb{K}$ est une application dérivable, posons $y = Cy_{\mathscr{H}}$. La fonction y est dérivable comme produit de fonctions dérivables.

Soit alors $t \in I$. On a

$$\begin{aligned} y' + ay &= C'y_{\mathscr{H}} + Cy'_{\mathscr{H}} + aCy_{\mathscr{H}} \\ &= C'y_{\mathscr{H}} + C\big(y'_{\mathscr{H}} + ay_{\mathscr{H}}\big). \end{aligned}$$

Or $y_{\mathscr{H}}$ est solution de $(\mathscr{H})$, donc $y'_{\mathscr{H}} + ay_{\mathscr{H}} = 0$. Donc y est solution de $\mathscr{E}$ si et seulement si $C'y_{\mathscr{H}} = b$, c'est-à-dire si et seulement si C' est l'application $t \mapsto \mathrm{e}^{A(t)}b(t)$, c'est-à-dire si et seulement si C est une primitive de $t \mapsto \mathrm{e}^{A(t)}b(t)$, *i.e.* si et seulement s'il existe $\lambda \in \mathbb{K}$ tel que

$$C : t \mapsto \lambda + \int_{t_0}^{t} \mathrm{e}^{A(u)}b(u)\,\mathrm{d}u.$$

Soit $\lambda \in \mathbb{K}$ et

$$y : t \mapsto \lambda \mathrm{e}^{-A(t)} + \mathrm{e}^{-A(t)} \int_{t_0}^{t} \mathrm{e}^{A(u)}b(u)\,\mathrm{d}u.$$

Remarque : On vient donc de prendre une solution quelconque de $(\mathscr{H})$.

Alors, y est solution du problème de Cauchy ($y' + ay = b$ et $y(t_0) = y_0$) si et seulement si $y(t_0) = y_0$, donc si et seulement si $\lambda = y_0 \mathrm{e}^{A(t_0)}$, c'est-à-dire si et seulement si y est l'application

$$t \mapsto \mathrm{e}^{A(t_0)-A(t)}y_0 + \mathrm{e}^{-A(t)} \int_{t_0}^{t} \mathrm{e}^{A(u)}b(u)\,\mathrm{d}u.$$

□

3.3 Résolution pratique

a Schéma de résolution (à connaître !)

On effectuera *toujours* les actions suivantes, dans l'ordre.

1. Déterminer I.
2. Résoudre (E_H).
3. Trouver une solution dite particulière (solution évidente, second membre d'une forme particulière ou méthode de variation de la constante).
4. S'occuper éventuellement des conditions initiales.
5. Donner les solutions.

Remarque 3.3.1.
On ne vous demande jamais que de trouver *une* solution particulière : faites le plus simplement possible ! Si vous ne voyez pas de solution évidente, la méthode de la variation de la constante est assez efficace et vous permet de retrouver la formule générale (une erreur est vite arrivée !). Il est permis de chercher une solution particulière au brouillon puis de l'exhiber sur sa copie, en justifiant qu'elle vérifie bien les conditions imposées.

Exemple 3.3.2.
On résout l'équation $y' + y = \mathrm{e}^{2x}$ sur $\mathbb{R}$. Ses solutions sont les $x \mapsto \dfrac{1}{3}\mathrm{e}^{2x} + K\mathrm{e}^{-x}$, avec $K \in \mathbb{K}$.

b Seconds membres particuliers

On considère l'équations $y' + ay = b$, dans le cas où a est ***une constante***. Si b est d'une des formes suivantes, alors la méthode de la variation de la constante (ainsi que certains arguments que nous développerons un peu plus tard) nous indique qu'il est possible à chaque fois de chercher une solution particulière sous une forme assez simple.

Polynôme - exponentielle Si $b : x \mapsto P(x)\mathrm{e}^{\alpha x}$, où P est un polynôme de degré n, on cherche une solution particulière de la forme $Q(t)\mathrm{e}^{\alpha t}$ avec Q de degré n si $\alpha \neq -a$, $n + 1$ sinon.

Polynôme - fonction trigonométrique Si $b : x \mapsto P(x)\cos(\alpha x)$ (ou $P(x)\sin(\alpha x)$) et si $\mathbb{K} = \mathbb{R}$, on résout d'abord l'équation $y' + ay = P(t)\mathrm{e}^{i\alpha t}$ avec la méthode du point précédent (Q sera alors à coefficients complexes), et on prend les parties réelles et imaginaires (explications).

Polynôme - fonction hyperbolique Si $b : x \mapsto P(x)\,\mathrm{ch}(\alpha x)$ (ou $P(x)\,\mathrm{sh}(\alpha x)$) et si $\mathbb{K} = \mathbb{R}$, on résout d'abord l'équation $y'+ay = P(t)\mathrm{e}^{\alpha t}$ avec la méthode du premier point, on obtient une solution y_+. On résout ensuite l'équation $y' + ay = P(t)\mathrm{e}^{-\alpha t}$ avec la méthode du premier point, on obtient alors une solution y_-. Par superposition, on prend $\frac{y_+ + y_-}{2}$ pour ch et $\frac{y_+ - y_-}{2}$ pour sh.

On remarquera qu'il est souvent tout aussi rapide de procéder par variation de la constante ...

Exemple 3.3.3.
Trouver une solution particulière pour $y' + y = \mathrm{e}^{t}$, pour $y' + y = \sin(t)$ et pour $y' + y = \mathrm{ch}(t)$.

Exemple 3.3.4.
Résoudre $y' + 2y = \mathrm{ch}\, t - (1 + t)\mathrm{e}^{-2t}$. On trouve $t \mapsto \frac{1}{6}\mathrm{e}^{t} + \frac{1}{2}\mathrm{e}^{-t} - (\frac{1}{2}t^2 + t + K)\mathrm{e}^{-2t}$.

4 Équations différentielles du second ordre à coefficients constants

4.1 Définitions

Une équation différentielle linéaire du second ordre est une équation de la forme $y'' + \alpha y' + \beta y = d$ où α, β et f sont des applications continues, d'inconnue $y : I \to \mathbb{K}$ deux fois dérivable sur I.

Dans la suite de ce chapitre, on ne s'intéressera qu'au cas où α et β sont des constantes. Plus généralement, on s'intéressera aux équations de la forme $ay'' + by' + cy = d$, où a, b, c sont des constantes de $\mathbb{K}$ avec $a \neq 0$ et $d \in \mathscr{C}(I, \mathbb{K})$, d'inconnue $y : I \to \mathbb{K}$ deux fois dérivable sur I. d est appelé le *second membre* de cette équation. On dit qu'elle est homogène si son second membre est nul. On appelle *équation homogène* associée à $ay'' + by' + cy = d$ l'équation $ay'' + by' + cy = 0$.

4.2 Résolution d'une équation homogène

On considère ici l'équation homogène définie sur $\mathbb{R}$

$$ay'' + by' + cy = 0. \qquad (\mathscr{H})$$

Lemme 4.2.1.
Soit $r \in \mathbb{K}$, la fonction $y_r : t \mapsto \mathrm{e}^{rt}$ est solution de (**? ?**) si et seulement si $ar^2 + br + c = 0$.

Démonstration.
y_r est dérivable et $y_r' = ry_r$. Donc y_r est deux fois dérivable et $y_r'' = r^2 y_r$. On a donc $ay_r'' + by_r' + cy_r = (ar^2 + br + c)y_r$. On conclut en remarquant que y_r ne s'annule jamais. □

Définition 4.2.2 (Équation et polynôme caractéristique)**.**
L'équation caractéristique de (**? ?**) est l'équation

$$ar^2 + br + c = 0. \qquad \text{(EC)}$$

Le polynôme caractéristique de (**? ?**) est

$$aX^2 + bX + c.$$

Théorème 4.2.3 (Solutions complexes de (**? ?**))**.**
Soit $a, b, c \in \mathbb{C}$, avec $a \neq 0$.

1. Si (**? ?**) a deux solutions complexes distinctes r_1, r_2, alors les solutions complexes de (**? ?**) sont les applications de la forme
$$\left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{C} \\ t & \mapsto & \lambda \mathrm{e}^{r_1 t} + \mu \mathrm{e}^{r_2 t} \end{array} \right.$$
pour $(\lambda, \mu) \in \mathbb{C}^2$.
2. Si (**? ?**) a une unique solution complexe r, alors les solutions complexes de (**? ?**) sont les applications de la forme
$$\left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{C} \\ t & \mapsto & (\lambda t + \mu)\mathrm{e}^{rt} \end{array} \right.$$

pour $(\lambda, \mu) \in \mathbb{C}^2$.

Démonstration.
Soit r une solution complexe de (? ?), on sait d'après le lemme ? ? que $y_r : t \mapsto \mathrm{e}^{rt}$ est une solution de (? ?). De plus, y_r ne s'annule jamais.

On peut donc mettre en œuvre la méthode de la variation de la constante. En effet, pour toute fonction $y : \mathbb{R} \to \mathbb{C}$ deux fois dérivable, il existe $K : \mathbb{R} \to \mathbb{C}$ deux fois dérivable telle que $y = Ky_r$ (poser $K = y/y_r$).

Soit donc $K : \mathbb{R} \to \mathbb{C}$ deux fois dérivable, posons $y = Ky_r$. La fonction y est deux fois dérivable, par produit. On a alors, comme $y_r' = ry_r$.

$$y' = K'y_r + Ky_r' = (K' + rK)y_r.$$

Le même type de calcul donne

$$y'' = (K'' + 2rK' + r^2K)y_r.$$

On a alors

$$ay''+by'+cy = \left[aK'' + (2ar + b)K' + (ar^2 + br + c)K\right] y_r.$$

Ainsi, comme r est solution de (? ?), on a $ar^2 + br + c = 0$, donc

$$ay'' + by' + cy = (aK'' + (2ar + b)K')y_r.$$

Comme y_r ne s'annule jamais, $ay'' + by' + cy = 0$ si et seulement si

$$aK'' + (2ar + b)K' = 0.$$

Remarquons que $2ar + b = 0$ si et seulement si $r = -\dfrac{b}{2a}$, *i.e.* si et seulement si (? ?) possède une unique solution complexe : r.

• Si (? ?) possède une unique solution complexe, alors y est solution de (? ?) si et seulement si $K'' = 0$. En primitivant deux fois, on obtient directement que c'est équivalent à « K est une fonction affine », d'où le résultat dans ce cas là.

• Supposons maintenant que (? ?) possède deux solutions complexes distinctes, notons r' la seconde solution. On peut tout de suite remarquer que $r + r' = -\dfrac{b}{a}$. Remarquons aussi que l'équation $aK'' + (2ar + b)K' = 0$ équivaut à l'équation différentielle linéaire d'ordre 1 portant sur K' :

$$(K')' + \left(2r + \frac{b}{a}\right)K' = 0.$$

Ainsi, y est solution de (? ?) si et seulement s'il existe $\alpha \in \mathbb{C}$ tel que

$$K' : t \mapsto \alpha \exp\left[-\left(2r + \frac{b}{a}\right)t\right].$$

En primitivant ceci, y est solution de (? ?) si et seulement s'il existe $\beta, \gamma \in \mathbb{C}$ tel que

$$K : t \mapsto \beta \exp\left[-\left(2r + \frac{b}{a}\right)t\right] + \gamma.$$

Ainsi, y est solution de (? ?) si et seulement s'il existe $\beta, \gamma \in \mathbb{C}$ tel que

$$y : t \mapsto \left(\beta \exp\left[-\left(2r + \frac{b}{a}\right)t\right] + \gamma\right) \times \mathrm{e}^{rt}.$$

Après simplification, y est solution de (? ?) si et seulement s'il existe $\beta, \gamma \in \mathbb{C}$ tel que

$$y : t \mapsto \beta \mathrm{e}^{r't} + \gamma \mathrm{e}^{rt}.$$

□

Théorème 4.2.4 (Solutions réelles de (? ?))**.**
Soit $a, b, c \in \mathbb{R}$, avec $a \neq 0$.

1. Si (? ?) a deux solutions réelles distinctes r_1, r_2, alors les solutions réelles de (? ?) sont les applications de la forme
$$\begin{cases} \mathbb{R} & \to & \mathbb{R} \\ t & \mapsto & \lambda \mathrm{e}^{r_1 t} + \mu \mathrm{e}^{r_2 t} \end{cases}$$
pour $(\lambda, \mu) \in \mathbb{R}^2$.
2. Si (? ?) a une unique solution réelle r, alors les solutions réelles de (? ?) sont les applications de la forme
$$\begin{cases} \mathbb{R} & \to & \mathbb{R} \\ t & \mapsto & (\lambda t + \mu)\mathrm{e}^{rt} \end{cases}$$
pour $(\lambda, \mu) \in \mathbb{R}^2$.
3. Si (? ?) a deux solutions complexes conjuguées distinctes, que l'on note $\alpha \pm i\omega$ avec $\alpha, \omega \in \mathbb{R}$, alors les solutions réelles de (? ?) sont les applications de la forme
$$\begin{cases} \mathbb{R} & \to & \mathbb{R} \\ t & \mapsto & \lambda \cos(\omega t)\mathrm{e}^{\alpha t} + \mu \sin(\omega t)\mathrm{e}^{\alpha t} \end{cases}$$
pour $(\lambda, \mu) \in \mathbb{R}^2$.
Ce sont aussi exactement les applications de la forme
$$\begin{cases} \mathbb{R} & \to & \mathbb{R} \\ t & \mapsto & A \cos(\omega t + \varphi)\mathrm{e}^{\alpha t} \end{cases}$$
pour $A \in \mathbb{R}_+$ et $\varphi \in]-\pi, \pi]$.

Lemme 4.2.5.
Soit $\alpha, \omega \in \mathbb{R}$, avec $\omega \neq 0$. Les deux ensembles de fonctions exposés au point **? ?**. du théorème **? ?** sont égaux.

Démonstration.
Soit $A \in \mathbb{R}_+$ et $\varphi \in]-\pi, \pi]$, soit

$$f : \left\{ \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ t & \longmapsto & A\cos(\omega t + \varphi)\mathrm{e}^{\alpha t} \end{array} \right. .$$

Par les formules d'addition, si $t \in \mathbb{R}$,

$$f(t) = A\cos(\varphi)\cos(\omega t)\mathrm{e}^{\alpha t} - A\sin(\varphi)\sin(\omega t)\mathrm{e}^{\alpha t},$$

donc f est bien de la première forme.

Réciproquement, soit $\lambda, \mu \in \mathbb{R}$. Si $\lambda = \mu = 0$, il suffit de prendre $A = 0$ et φ quelconque. Sinon, posons $A = \sqrt{\lambda^2 + \mu^2}$ et $\varphi \in]-\pi, \pi]$ tel que $\cos\varphi = \dfrac{\lambda}{\sqrt{\lambda^2+\mu^2}}$ et $\sin\varphi = -\dfrac{\mu}{\sqrt{\lambda^2+\mu^2}}$. Alors,

$$\begin{aligned} &\lambda\cos(\omega t) + \mu\sin(\omega t) \\ =&\sqrt{\lambda^2+\mu^2}\left(\frac{\lambda}{\sqrt{\lambda^2+\mu^2}}\cos(\omega t) + \frac{\mu}{\sqrt{\lambda^2+\mu^2}}\sin(\omega t)\right) \\ =&A(\cos(\omega t)\cos(\varphi) + \sin(\omega t)\sin(\varphi)) \\ =&A\cos(\omega t + \varphi). \end{aligned}$$

□

Démonstration (Théorème **? ?**).
• Les cas où (**? ?**) admet une ou deux solutions réelles se traitent exactement comme le cas complexe.
• Supposons donc que (**? ?**) admette deux solutions complexes conjuguées distinctes $\alpha \pm i\omega$. On raisonne par analyse-synthèse.

Analyse : Soit $y : \mathbb{R} \to \mathbb{R}$ solution de (**? ?**). Alors y est solution complexe de (**? ?**), donc il existe $\lambda, \mu \in \mathbb{C}$ tels que

$$y : t \mapsto \lambda\mathrm{e}^{(\alpha+i\omega)t} + \mu\mathrm{e}^{(\alpha-i\omega)t}$$

Or $y(0) = \lambda + \mu$ est réel donc $\lambda + \mu \in \mathbb{R}$, donc $\mathrm{Im}(\lambda) = -\mathrm{Im}(\mu)$.

De même $y(\pi/(2\omega)) \in \mathbb{R}$, donc

$$y\left(\frac{\pi}{2\omega}\right) = i(\lambda - \mu)\exp\left(\frac{r\pi}{2\omega}\right) \in \mathbb{R},$$

donc $\mathrm{Re}(\lambda) = \mathrm{Re}(\mu)$.

Ainsi, $\mu = \overline{\lambda}$.

Soit $\rho \in \mathbb{R}^+$ et $\varphi \in]-\pi, \pi]$ tels que $\lambda = \rho\mathrm{e}^{i\varphi}$. Si $t \in \mathbb{R}$, alors

$$y(t) = 2\rho\cos(\omega t + \varphi)\mathrm{e}^{\alpha t}.$$

Ainsi, y est de la forme demandée.

Synthèse : Soit $\lambda, \mu \in \mathbb{R}$ et

$$y : \left\{ \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ t & \longmapsto & \lambda\cos(\omega t)\mathrm{e}^{\alpha t} + \mu\sin(\omega t)\mathrm{e}^{\alpha t} \end{array} \right.$$

D'après le théorème de structure des solutions homogène (**? ?** – une combinaison linéaire de solutions homogènes est solution homogène), il suffit de montrer que

$$s_1 : \left\{ \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ t & \longmapsto & \cos(\omega t)\mathrm{e}^{\alpha t} \end{array} \right.$$

et

$$s_2 : \left\{ \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ t & \longmapsto & \sin(\omega t)\mathrm{e}^{\alpha t} \end{array} \right.$$

sont solution de (**? ?**). Or, si $t \in \mathbb{R}$, par les formules d'Euler,

$$s_1(t) = \frac{1}{2}\mathrm{e}^{(\alpha+i\omega)t} + \frac{1}{2}\mathrm{e}^{(\alpha-i\omega)t}.$$

D'après le théorème **? ?**, $t \mapsto \mathrm{e}^{(\alpha+i\omega)t}$ et $t \mapsto \mathrm{e}^{(\alpha-i\omega)t}$ sont solutions de (**? ?**), donc s_1 aussi. On effectue le même raisonnement pour s_2. □

Remarque 4.2.6.
Dans tous les cas, les solutions sont les combinaisons linéaires de deux solutions linéairement indépendantes. On dit que cet ensemble a une structure de plan vectoriel.

Exemple 4.2.7. 1. Solutions complexes et réelles de $y'' + y' + 2y = 0$. On trouve

$$\begin{aligned} t \mapsto &\lambda\mathrm{e}^{\frac{-1-i\sqrt{7}}{2}t} + \mu\mathrm{e}^{\frac{-1+i\sqrt{7}}{2}t} \\ &= \mathrm{e}^{-\frac{1}{2}t}\left(\lambda\mathrm{e}^{\frac{-i\sqrt{7}}{2}t} + \mu\mathrm{e}^{\frac{i\sqrt{7}}{2}t}\right) \end{aligned}$$

2. $y'' + 2y' + y = 0$, avec $y(1) = 1$, $y'(1) = 0$ alors $\lambda = e$, $\mu = 0$.

Théorème 4.2.8.
Le problème de Cauchy $ay'' + by' + cy = 0$ et $y(t_0) = y_0$ et $y'(t_0) = y'_0$, admet une unique solution.

Démonstration.
(*hors programme*) Nous traitons ici le cas où on cherche une solution à valeurs complexes et où le polynôme caractéristique a deux racines distinctes r_1 et r_2. Alors les solutions de l'équation différentielle considérées sont les applications y de la forme $t \mapsto \lambda\mathrm{e}^{r_1 t} + \mu\mathrm{e}^{r_2 t}$ où λ et μ sont deux complexes. On a $y(t_0) = \lambda\mathrm{e}^{r_1 t_0} + \mu\mathrm{e}^{r_2 t_0}$ et $y'(t_0) = \lambda r_1\mathrm{e}^{r_1 0} + \mu r_2\mathrm{e}^{r_2 t_0}$.

Pour montrer que le problème de Cauchy admet une unique solution, il suffit de montrer que le système

$$\begin{cases} \lambda \mathrm{e}^{r_1 t_0} + \mu \mathrm{e}^{r_2 t_0} = y_0 \\ \lambda r_1 \mathrm{e}^{r_1 t_0} + \mu r_2 \mathrm{e}^{r_2 t_0} = y_0' \end{cases}$$

d'inconnues λ et μ admet une unique solution.

On peut s'en assurer par le calcul, ou on peut simplement remarquer que pour que ce système admette une unique solution, il suffit que l'équation

$$\lambda \begin{pmatrix} \mathrm{e}^{r_1 t_0} \\ r_1 \mathrm{e}^{r_1 t_0} \end{pmatrix} + \mu \begin{pmatrix} \mathrm{e}^{r_2 t_0} \\ r_2 \mathrm{e}^{r_2 t_0} \end{pmatrix} = \begin{pmatrix} y_0 \\ y_0' \end{pmatrix}$$

admette une unique solution.

Pour cela, il suffit de montrer que les vecteurs $\begin{pmatrix} \mathrm{e}^{r_1 t_0} \\ r_1 \mathrm{e}^{r_1 t_0} \end{pmatrix}$ et $\begin{pmatrix} \mathrm{e}^{r_2 t_0} \\ r_2 \mathrm{e}^{r_2 t_0} \end{pmatrix}$ forment une base de $\mathbb{R}^2$. Il suffit de vérifier qu'ils sont linéairement indépendants, ce qui est le cas puisque leur déterminant vaut $\mathrm{e}^{r_1 t_0} r_2 \mathrm{e}^{r_2 t_0} - r_1 \mathrm{e}^{r_1 t_0} \mathrm{e}^{r_2 t_0}$, qui est égal à $(r_2 - r_1)\mathrm{e}^{(r_1+r_2)t_0}$, qui est non nul puisque $r_1 \neq r_2$. □

4.3 Résolution d'une équation avec second membre

Théorème 4.3.1.
Si l'on connaît une solution $\tilde{y}$ de l'équation avec second membre alors on en connaît toutes les solutions : l'ensemble S des solutions de l'équation avec second membre est $S = \{ y_H + \tilde{y} \mid y_H \in S_H \}$.

Remarque 4.3.2.
On a déjà vu que si l'on connaissait une solution de l'équation $\tilde{y}$ avec second membre, alors on pouvait construire toutes les solutions de l'équation avec second membre à partir de l'ensemble des solutions de l'équation homogène.

Dans le cas d'une équation d'ordre deux à coefficients constants, on dit que l'ensemble des solutions a une structure de plan affine, car l'ensemble des solutions est l'ensemble des $\tilde{y} + y$ pour y parcourant un plan vectoriel.

• Cas particulier de seconds membres (le seul au programme) : $P(t)\mathrm{e}^{\alpha t}$: P polynôme de degré n. on cherche une solution particulière de la forme $Q(t)\mathrm{e}^{\alpha t}$ avec Q de degré :

(i) $\leqslant n$ si α n'est pas racine du poly. carac.

(ii) $\leqslant n+1$ si α est racine simple (i.e. $\Delta \neq 0$).

(iii) $\leqslant n+2$ si α est double.

Exemple 4.3.3. 1. Résoudre $y'' - y = 2 + \mathrm{e}^{2t}$. Solutions homogène : $t \mapsto \lambda \mathrm{e}^{t} + \mu \mathrm{e}^{-t}$, solutions particulières : -2 (second membre 2), et $\frac{1}{3}\mathrm{e}^{2t}$.

2. Résoudre $y'' + 2y' + y = (1+x)\mathrm{e}^{-x}$. Solutions homogène : $x \mapsto (\lambda x + \mu)\mathrm{e}^{-x}$, solution particulière : $y(x) = \left(\frac{1}{2}x^2 + \frac{1}{6}x^3\right)\mathrm{e}^{-x}$.

5 Un peu de physique : circuits RL et RLC

Des équations différentielles apparaissent fréquemment en physique. Par exemple les oscillateurs, qu'ils soient mécaniques ou électriques mènent à des équations différentielle du second ordre. Ainsi l'étude du pendule simple conduit à une équation du second ordre, avec ou sans terme de degré 1, suivant que les frottements sont pris en compte ou non.
Nous étudierons ici des circuits électriques.

Remarque : on adopte exceptionnellement les notations des physiciens : i pour l'intensité et j pour le complexe correspondant au point $(0,1)$, et donc $j^2 = -1$.

5.1 Circuit RL

• On place en série : un générateur fournissant une tension constante U, une résistance R et une inductance L, et enfin un interrupteur, ouvert aux temps $t < 0$. Au temps $t = 0$ on ferme l'interrupteur, et on veut déterminer l'évolution de l'intensité : pour $t < 0$ on a évidemment $i = 0$.
On sait que la tension aux bornes de la résistance est Ri, celle aux bornes de l'inductance est $L\frac{\mathrm{d}i}{\mathrm{d}t} = Li'(t)$. Avec la loi des mailles : $Li' + Ri = U$. On pose : $\tau = \frac{L}{R}$, appelée

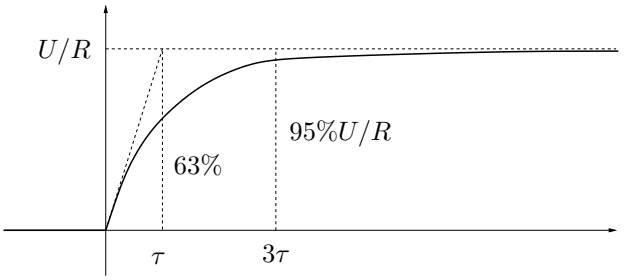
constante de temps du circuit. On va donc résoudre l'équation diff $i' + \frac{i}{\tau} = \frac{U}{L}$, sur $\mathbb{R}_+$.

• On commence par résoudre l'équation homogène : $t \mapsto K\mathrm{e}^{-t/\tau}$, $K \in \mathbb{R}$.

• On cherche une solution particulière : le second membre est une constante, on cherche donc une solution constante : ici $i = \frac{\tau U}{L} = \frac{U}{R}$ convient.

• Pour finir, on détermine K pour satisfaire la condition initiale : $i(0) = 0$. On obtient $K = -\frac{U}{R}$.

• Traçons le graphe de i.



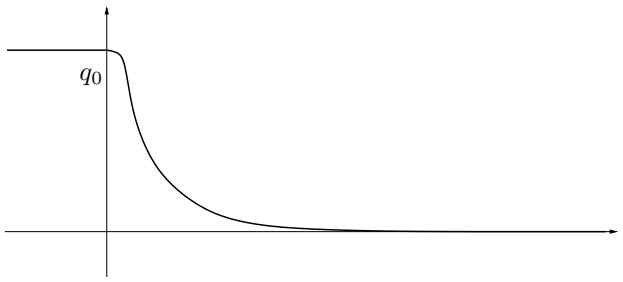
On observe un régime *transitoire* (pour t proche de 0) et un régime *permanent* (pour t proche de $+\infty$). On peut déterminer graphiquement τ, en traçant l'asymptote horizontale, puis la tangente en 0, qui a pour équation $y = i'(0)t + i(0)$, soit $y = \frac{U}{R\tau}t$. Pour $t = \tau$, ces droites se coupent. On considère que le régime permanent est atteint à partir de $t = 3\tau$. On a les approximations suivantes : $i(\tau) = \frac{U}{R}(1 - 1/e) \approx 0.63\frac{U}{R}$ et $i(3\tau) = \frac{U}{R}(1 - \mathrm{e}^{-3}) \approx 0.95\frac{U}{R}$.

5.2 Circuit RLC

• Cette fois-ci on enlève le générateur de tension, mais on rajoute un condensateur de capacité C en série, et on veut étudier l'évolution de la charge q du condensateur. On sait que : $q = Cu_C$ et $i = \frac{\mathrm{d}q}{\mathrm{d}t} = q'$. On a donc : $Li' + Ri + q/C = 0$, mais on pose $\omega_0 = \frac{1}{\sqrt{LC}}$, appelée *pulsation propre* du circuit, et $Q = \frac{1}{R}\sqrt{\frac{L}{C}}$, appelée *facteur de qualité*. Avec ces deux constantes, on obtient : $\frac{\mathrm{d}^2q}{\mathrm{d}t^2} + \frac{\omega_0}{Q}\frac{\mathrm{d}q}{\mathrm{d}t} + \omega_0^2 q = 0$.

• Résolvons l'équation homogène : Le discriminant du poly car est $\Delta = \frac{\omega_0^2}{Q^2} - 4\omega_0^2 = \left(\frac{\omega_0}{Q}\right)^2(1 - 4Q^2)$. Il faut distinguer trois cas suivant la valeur de Q.

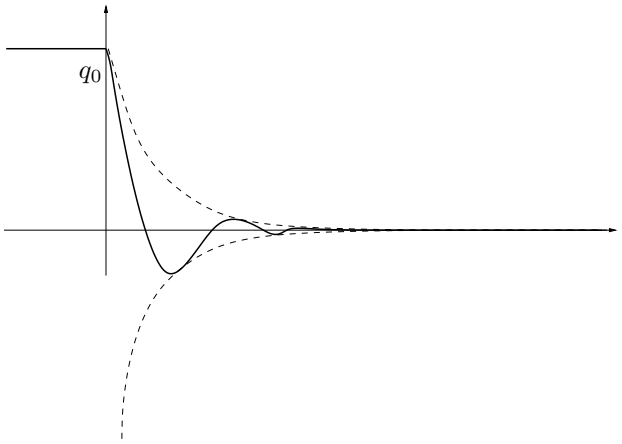
1. Régime apériodique ($Q < 1/2$ i.e. $\Delta > 0$) : les racines du poly car sont $-\frac{\omega_0}{2Q} \pm \frac{\omega_0}{2Q}\sqrt{1 - 4Q^2}$, toutes les deux strictement négatives, et appelées ω_1 et ω_2. Forme des solutions. On a : $q(0) = q_0$ et $q'(0) = 0$, car la charge q est constante pour $t \leqslant 0$, et q est continue. On a donc le graphe suivant :



2. Régime critique ($Q = 1/2$ i.e. $\Delta = 0$) : une racine double, $-\omega_0$. Forme des solutions. Même graphe qu'avant.

3. Régime pseudo-périodique ($Q > 1/2$ i.e. $\Delta < 0$) : les racines du polynôme caractéristique sont $-\frac{\omega_0}{2Q} \pm j\frac{\omega_0}{2Q}\sqrt{4Q^2 - 1}$. Forme des solutions, avec un cos et un déphasage. Une solution est comprise entre $|\lambda|\mathrm{e}^{-\frac{\omega_0 t}{2Q}}$ et $-|\lambda|\mathrm{e}^{-\frac{\omega_0 t}{2Q}}$. Graphe :

Dans tous les cas, la décroissance de q vers 0 est très rapide : exponentielle. Pendant le régime permanent, il ne se passe rien.



6 Méthode d'Euler

Comme on l'a vu, résoudre une équation différentielle revient à calculer une primitive d'une certaine fonction. Or il n'existe pas toujours de fonction élémentaire qui soit une primitive d'une fonction élémentaire donnée, ou alors on ne sait pas la trouver. Dans ce cas il est utile de savoir construire une approximation de la solution d'une équation différentielle de premier ordre. La méthode d'Euler est l'une des méthodes simples et classiques pour faire cela. Elle sera étudiée au second semestre en informatique.

Chapitre VIII

Relations d'ordre

Dans tout ce chapitre, E est un ensemble.

1 Relations binaires

Définition 1.0.1.
On appelle *relation binaire* sur E tout triplet $\mathscr{R} = (E, E, \Gamma)$ où Γ est une partie de $E \times E$. Au lieu de noter $(x, y) \in \Gamma$, on note $x\mathscr{R}y$ ce qui se lit : x est en relation avec y.

Exemple 1.0.2.
— « Aimer » est une relation binaire : Brandon aime Sue Ellen mais Sue Ellen n'aime pas Brandon. On voit sur cet exemple qu'en général $x\mathscr{R}y$ n'implique pas $y\mathscr{R}x$.
— L'égalité est l'exemple le plus courant de relation binaire.
— Soit $f : \mathbb{R} \to \mathbb{R}$. On peut définir pour tous $x, y \in \mathbb{R}$, $x\mathscr{R}y$ ssi $y = f(x)$ (on a en fait défini ainsi une application via son graphe).
— Sur $\mathbb{R}$, $\leqslant$ et $<$ (autre exemple où $x\mathscr{R}y$ est vrai mais $y\mathscr{R}x$ est faux).
— $\subset$ est une relation binaire sur $\mathscr{P}(E)$.
— les divisibilités sur $\mathbb{N}$ et $\mathbb{Z}$.

Remarque 1.0.3.
Une relation binaire sur un ensemble E fini peut être représentée au moyen d'un graphe dont les sommets sont les éléments de E et dont les arêtes sont orientées d'un sommet à l'autre : une flèche allant de x à y signifie $x\mathscr{R}y$.

Définition 1.0.4.
Soit $\mathscr{R}$ une relation binaire sur E. On dit que $\mathscr{R}$ est :

(i) *réflexive* si $\forall x \in E$, $x\mathscr{R}x$.

(ii) *transitive* si $\forall x, y, z \in E$, $(x\mathscr{R}y$ et $y\mathscr{R}z) \Rightarrow x\mathscr{R}z$.

(iii) *symétrique* si $\forall x, y \in E$, $x\mathscr{R}y \Rightarrow y\mathscr{R}x$.

(iv) *antisymétrique* si $\forall x, y \in E$, $(x\mathscr{R}y$ et $y\mathscr{R}x) \Rightarrow x = y$.

Remarque 1.0.5.
Ces propriétés peuvent être décelées sur un graphe de la relation binaire, défini en 1.0.3.

Exemple 1.0.6.
— « Aimer » ne vérifie aucune de ces propriétés.
— L'égalité est réflexive, symétrique, antisymétrique et transitive.
— Soit $f : \mathbb{R} \to \mathbb{R}$ et $x\mathscr{R}y$ ssi $y = f(x)$: les propriétés de cette relation dépendent du choix de f mais ne vérifie aucune de ces propriétés en général (considérer par exemple $f : x \mapsto x + 1$ et $f : x \mapsto x$).
— $\leqslant$ est réflexive, transitive et antisymétrique sur $\mathbb{R}$.
— $<$ est transitive et antisymétrique sur $\mathbb{R}$.
— $\subset$ est réflexive, transitive et antisymétrique sur $\mathscr{P}(E)$.
— la divisibilité sur $\mathbb{N}$ est réflexive, transitive et antisymétrique.
— la divisibilité sur $\mathbb{Z}$ est réflexive et transitive mais pas antisymétrique.

Démonstration.
— Montrons le résultat pour $\subset$: Soient $A, B, C \in \mathscr{P}(E)$.
• On a bien entendu $A \subset A$, donc $\subset$ est réflexive.
• On suppose $A \subset B$ et $B \subset C$. Alors $A \subset C$ et donc $\subset$ est transitive.
• On suppose $A \subset B$ et $B \subset A$. Alors $A = B$, et $\subset$ est antisymétrique.
— Montrons le résultat pour la divisibilité sur $\mathbb{N}$: soient $n, p, q \in \mathbb{N}$.
• On a $n = 1 \times n$ donc $n|n$.
• Si $n|p$ et $p|q$, alors il existe $k, \ell \in \mathbb{N}$ tels que $p = kn$ et $q = \ell p$, donc $q = (\ell k)n$ et ainsi $n|q$.
• Si $n|p$ et $p|n$, alors il existe $k, \ell \in \mathbb{N}$ tels que $p = kn$ et $n = \ell p$, donc $n = (\ell k)n$ et ainsi $\ell k = 1$. Mais ℓ et k sont deux entiers naturels et sont donc égaux à 1, donc $n = p$.
Dans le cas de la divisibilité dans $\mathbb{Z}$, on aurait pour ce point $k, \ell \in \mathbb{Z}$, et donc $\ell k = 1$ serait aussi vérifié si $k = \ell = -1$, et en effet si $n = -p$ on a bien $n|p$ et $p|n$, mais $n \neq p$!
□

2 Relations d'équivalence

Définition 2.0.1.
On appelle *relation d'équivalence* toute relation

binaire réflexive, transitive et symétrique.

Exemple 2.0.2.
• L'égalité sur E est l'exemple le plus classique de relation d'équivalence.
• La relation de congruence modulo n sur $\mathbb{Z}$ en est aussi une : on fixe $n \in \mathbb{Z}$ non nul, et on dit que deux entiers p et q sont *congrus modulo* n s'il existe $k \in \mathbb{Z}$ tel que $p = q + kn$, ce qui se note $p = q[n]$ ou $p \equiv q[n]$.
• Sur $\mathbb{R}^n$, on a la relation d'équivalence : $M \mathscr{R} N$ si $\overrightarrow{OM}$ et $\overrightarrow{ON}$ sont colinéaires. C'est le point de départ de la *géométrie projective*.
• Sur $\mathscr{M}_n(\mathbb{K})$, deux matrices M et N sont dites semblables si $\exists P \in GL_n(\mathbb{K}), M = P^{-1}NP$. Cela définit une relation d'équivalence.
• Sur $\mathscr{M}_n(\mathbb{K})$, deux matrices M et N sont dites équivalentes si $\exists (P,Q) \in GL_n(\mathbb{K})^2, M = Q^{-1}NP$. Cela définit une relation d'équivalence.

Définition 2.0.3.
Soit E un ensemble et $\mathscr{R}$ une relation d'équivalence sur E. Alors, pour tout élément x de E, on appelle *classe d'équivalence* de x l'ensemble $\{ y \in E \mid x \mathscr{R} y \}$, que l'on note parfois $\overline{x}$.

Proposition 2.0.4.
Soit E un ensemble et $\mathscr{R}$ une relation d'équivalence sur E. Soit $(x,y) \in E^2$. Alors,

1. $x \in \overline{x}$.
2. $x \mathscr{R} y \iff x \in \overline{y}$.
3. $x \mathscr{R} y \iff \overline{x} = \overline{y}$.

Démonstration.
Le premier point découle de la réflexivité. Le second découle de la définition de $\overline{y}$. Pour le troisième, il s'agit de montrer l'équivalence. Le sens direct se fait en montrant une double inclusion, qui découle de la transitivité. Le sens indirect découle du premier point et du second. □

Définition 2.0.5.
Soit E un ensemble, $(A_i)_{i \in I}$ une famille de parties de E indexée par un ensemble I. On dit que $(A_i)_{i \in I}$ est une *partition* de E si les éléments de cette famille sont tous non vides, sont disjoints et si leur réunion vaut E.

Proposition 2.0.6. 1. Si $\mathscr{R}$ est une relation d'équivalence sur E, alors l'ensemble des classes d'équivalences de $\mathscr{R}$ forme une partition de E.
2. Réciproquement, si $(A_i)_{i \in I}$ est une partition de E, alors la relation binaire définie sur E par $x \mathscr{R} y$ si $\exists i \in I, (x \in A_i) \wedge (y \in A_i)$ est une relation d'équivalence.

Nous introduisons maintenant dans un but culturel l'ensemble quotient (hors programme).

Définition 2.0.7.
Si $\mathscr{R}$ est une relation d'équivalence sur E, on appelle ensemble quotient de E par $\mathscr{R}$ l'ensemble des classes d'équivalences, noté $E/\mathscr{R}$.

Exemple 2.0.8.
Si $f : E \to F$ est une application, la relation binaire sur E définie par $x \mathscr{R} y$ si $f(x) = f(y)$ est une relation d'équivalence. Quelle est alors la partition qui lui est naturellement associée ? On pourra alors se poser la question suivante : y a-t-il un moyen naturel de construire une injection $\tilde{f} : E/\mathscr{R} \to F$?

Exemple 2.0.9.
On manipule naturellement certains ensembles quotients : les vecteurs de $\mathbb{R}^n$ et les fractions, par exemple.

3 Relations d'ordre

Définition 3.0.1.
On appelle *relation d'ordre* toute relation binaire réflexive, transitive et antisymétrique.

Remarque 3.0.2.
L'usage est de noter $\preccurlyeq$, parfois $\leqslant$, les relations d'ordre.

Exemple 3.0.3.
Reprendre tous les exemples précédents et repérer les relations d'ordre.

Définition 3.0.4.
Soit $\preccurlyeq$ une relation d'ordre sur E.

1. On dit que $x, y \in E$ sont des *éléments comparables* si $x \preccurlyeq y$ ou $y \preccurlyeq x$.
2. On dit que $\preccurlyeq$ est une *relation d'ordre totale* (ou que cet ordre est total) si tous les éléments de E sont comparables deux à deux. Sinon la relation est dite *partielle* (ou l'ordre est dit partiel).

Exemple 3.0.5. — On définit la relation d'ordre usuelle sur $\mathbb{N}$, notée $\leqslant$ par : $a \leqslant b$ si $\exists k \in \mathbb{N}, b = a+k$. C'est une relation d'ordre totale.
— La relation d'ordre usuelle $\leqslant$ sur $\mathbb{R}$ est totale : quand on choisit deux réels, il y en a toujours un des deux qui est inférieur ou égal à l'autre.
— La relation d'ordre $\subset$ sur $\mathscr{P}(E)$ est partielle (si $\operatorname{Card} E \geqslant 2$) : en effet, quand on choisit deux parties de E, il n'y a aucune raison pour que l'une soit incluse dans l'autre.
— La relation de divisibilité sur $\mathbb{N}$ est une relation d'ordre partielle : quand on choisit deux entiers positifs, l'un n'est pas forcément multiple ou diviseur de l'autre.

4 Majorants, minorants et compagnie

Dans toute cette section, $\preccurlyeq$ est une relation d'ordre sur E et A est une partie de E.

4.1 Majorants, minorants

Définition 4.1.1. (i) On dit que A est *majorée* (resp. *minorée*) pour $\preccurlyeq$ s'il existe un élément $M \in E$ tel que pour tout $a \in A$, $a \preccurlyeq M$ (resp. $M \preccurlyeq a$) ; on dit alors que M est **UN** *majorant* (resp. *minorant*) de A ou que M majore (resp. minore) A.
(ii) on dit que A est *bornée* si elle est à la fois majorée et minorée.

 En général, une partie majorée a plusieurs majorants, et peut même en avoir une infinité !

Exemple 4.1.2.
• $[1, 2]$ dans $\mathbb{R}$ est majoré par tout réel x tel que $2 \leqslant x$, et minoré par tout réel y tel que $y \leqslant 1$.
• $]-\infty, 2[$ est majoré mais non minoré.
• Pour la relation $\subset$, $\mathscr{P}(E)$ est minorée par $\varnothing$ et majorée par E.

4.2 Plus grand et plus petit éléments

Définition 4.2.1.
On dit que $x \in E$ est un *plus grand élément* ou *maximum* (resp. *plus petit élément* ou *minimum*) de A si x est un majorant (resp. minorant de A) **ET** $x \in A$.

Exemple 4.2.2.
• $I = [-1, 2[$ a un plus petit élément, mais pas de plus grand élément. En effet, -1 est un minorant de I et $-1 \in I$. Mais supposons par l'absurde que I ait un plus grand élément M. Alors $M \in I$, donc $M < 2$. Ainsi il existe $a \in]M, 2[$, donc $a \in I$ et $M < a$, ce qui est en contradiction avec le fait que M majore I.
• $\mathbb{R}$ n'est ni majoré ni minoré, donc n'a ni plus grand ni plus petit élément.

Théorème 4.2.3.
Si A a un plus grand élément, ce dernier est unique. Il en est de même pour un petit élément, s'il existe. Dans le cas d'existence, le plus grand élément de A est alors noté $\max A$, et le plus petit élément de A est noté $\min A$.

Démonstration.
On suppose que A a deux maxima : ils sont alors réciproquement plus grand l'un que l'autre, et par antisymétrie ils sont égaux. □

Exemple 4.2.4.
Dans $\mathbb{N}$ muni de la relation d'ordre $|$: 0 est le plus grand élément et 1 est le plus petit. En effet tout entier divise 0, et 1 divise tout entier.

4.3 Bornes supérieure et inférieure

Définition 4.3.1. (i) **S'il existe**, le plus petit élément de l'ensemble des majorants de A est appelé la borne supérieure de A et noté $\sup A$.

(ii) **S'il existe**, le plus grand élément de l'ensemble des minorants de A est appelé la borne inférieure de A et noté $\inf A$.

 Il y a un grosse différence entre max et sup : le premier doit appartenir à A, pas le deuxième.

Exemple 4.3.2.
$I = [-1, 2[$ a une borne inférieure et une borne supérieure : l'ensemble des minorants de I est $]-\infty, -1]$, qui admet -1 comme maximum, et donc -1 est la borne inférieure de I. De même $[2, +\infty[$ est l'ensemble des majorants de I, et il admet 2 comme minimum, donc 2 est la borne supérieure de I.

Proposition 4.3.3.
Soit $A \subset E$ et $M \in E$. Si A admet une borne supérieure, alors $\sup A \preccurlyeq M \Leftrightarrow \forall x \in A \quad x \preccurlyeq M$.

Remarque 4.3.4.
L'idée est la suivante : si on peut « caser » un élément de E entre M et A, ce qui revient en fait à trouver un majorant de A plus petit que M, alors M n'est pas la borne supérieure de A : la borne supérieure « colle » à A.

Démonstration.
$\Rightarrow$: car $\sup A$ est un majorant de A.
$\Leftarrow$: car $\sup A$ est le plus petit majorant de A. □

Théorème 4.3.5.
Si A possède un maximum (resp. minimum), alors A a une borne supérieure (resp. inférieure) et cette borne est justement le maximum (resp. le minimum) de A : $\sup A = \max A$ (resp. $\inf A = \min A$).

Démonstration.
On ne donne la démonstration que pour la borne supérieure (c'est la même pour la borne inférieure) : soit $\mathscr{E}$ l'ensemble des majorants de A. Il faut montrer que $\mathscr{E}$ a un plus petit élément. Par définition $\max A$ est un majorant de A, donc $\max A \in \mathscr{E}$. Soit $M \in \mathscr{E}$. M est plus grand que tout élément de A, or $\max A$ appartient à A donc $A \preccurlyeq M$, et ce pour tout M de $\mathscr{E}$: $\max A$ est donc un minorant de $\mathscr{E}$. De ces deux points on tire $\max A = \min \mathscr{E}$, et donc $\max A = \sup A$. □

4.4 Application aux fonctions réelles

Définition 4.4.1.
Soient A une partie de $\mathbb{R}$ et $f : A \to \mathbb{R}$.

(i) On dit que f est *majorée* (resp. *minorée*) sur A si $f(A)$ l'est pour la relation naturelle sur $\mathbb{R}$, i.e. : $\exists M \in \mathbb{R} \quad \forall x \in A \quad f(x) \leqslant M$ (resp. $M \leqslant f(x)$). Dans ce cas on dit que M est un *majorant* (resp. *minorant*) de f, ou que M *majore* (resp. *minore*) f.

(ii) On dit que f est *bornée* si elle est majorée et minorée. Ceci est équivalent à : $|f|$ est majorée.

 Un majorant ou minorant ne doit pas dépendre de la variable de la fonction ! Ainsi sur

$\mathbb{R}_+$, $x \mapsto x$ n'est pas un majorant de sin, bien que $\forall x \in \mathbb{R}_+,\ \sin x \leqslant x$. Un majorant est une **CONSTANTE**.

Définition 4.4.2.
Si l'ensemble $f(A)$ a un maximum (resp. un minimum), alors ce dernier est appelé le *maximum* (resp. *minimum*) *de f sur A*, et noté $\max_A f$ ou $\max_{x\in A} f(x)$ (resp. $\min_A f$ ou $\min_{x\in A} f(x)$). Ainsi $\max f(A) = \max_A f$. Un maximum ou minimum d'une fonction est donc un majorant ou minorant **ATTEINT**.
On appelle *extremum* de f tout minimum ou maximum de f.

 Les extrema sont uniques mais peuvent être atteints plusieurs fois. Considérer pas exemple les fonctions continues périodiques comme sin ou cos.

Exemple 4.4.3.
• $x \mapsto x^2$ admet un minimum mais pas de majorant sur $\mathbb{R}$.
• Arctan est majorée et minorée sur $\mathbb{R}$, mais n'admet ni minimum ni maximum.

Définition 4.4.4.
Si l'ensemble $f(A)$ admet une borne supérieure (resp. une borne inférieure), alors cette dernière est appelée la *borne supérieure* (resp. *inférieure*) *de f sur A*. On la note $\sup_A f$ ou $\sup_{x\in A}\{f(x)\}$ (resp.$\inf_A f$ ou $\inf_{x\in A}\{f(x)\}$). Ainsi $\sup f(A) = \sup_A f$.

Théorème 4.4.5.
Si f admet un maximum (resp. un minimum) sur A, alors f admet également une borne supérieure (resp. une borne inférieure) sur A, et $\sup_A f = \max_A f$ (resp. $\inf_A f = \min_A f$).

5 Relation d'ordre naturelle sur $\mathbb{N}$

La relation naturelle est la relation usuelle $\leqslant$.

Théorème 5.0.1.
Toute partie non vide de $\mathbb{N}$ possède un plus petit élément.

On donne ici deux démonstrations de cette propriété. On remarquera que l'on utilise ici des récurrences et que l'on a montré le principe de récurrence en utilisant cette propriété : cette dernière est donc équivalente au principe de récurrence.

Démonstration.
Soit $A \subset \mathbb{N}$, tq $A \neq \varnothing$, et soit $a_0 \in A$. On suppose que A n'a pas de plus petit élément. Puisque $a_0 \in A$, a_0 ne peut pas être un minorant de A, sinon ce serait un minimum. Donc il existe $a_1 < a_0$ dans A. Mais de même, a_1 ne peut pas être un minorant, donc il existe $a_< a_1$ dans A. Par récurrence, on construit une suite d'éléments de A (a_n) tq pour tout n, $a_{n+1} < a_n$, ou encore $a_{n+1} \leqslant a_n - 1$, donc à nouveau par récurrence on a :

$$\forall n \in \mathbb{N} \quad a_n \leqslant a_0 - n$$

Cette proposition est en particulier vraie pour l'entier a_0+1, c'est-à-dire : $a_{a_0+1} \leqslant a_0 - a_0 - 1$. Mais ceci est absurde car $a_{a_0+1} \in \mathbb{N}$. □

Démonstration.
Notons, pour $n \in \mathbb{N}$, $P(n)$ l'assertion «toute partie de $\mathbb{N}$ contenant l'entier n possède un plus petit élément». Montrons $\forall n \in \mathbb{N} \quad P(n)$ par récurrence forte.

- Toute partie de $\mathbb{N}$ contenant l'entier 0 possède 0 pour plus petit élément. Donc on a clairement $P(0)$.
- Soit $n \in \mathbb{N}$. Supposons que pour tout $k \leqslant n$, on a $P(k)$ et montrons $P(n+1)$.
  Soit A une partie de $\mathbb{N}$ contenant l'entier $n+1$. Alors ou bien A contient un entier k strictement inférieur à $n+1$, ou bien elle n'en contient pas.
  - Dans le premier cas, on sait qu'on a $P(k)$, donc A admet un plus petit élément.
  - Dans le second, cela signifie que $n+1$ est le plus petit élément de A. A admet donc un plus petit élément.

  On a donc $P(n+1)$.
  Donc P est héréditaire.

On a donc

$$\forall n \in \mathbb{N} \quad P(n)$$

On en déduit le résultat :
Soit A une partie non vide de $\mathbb{N}$. Alors A possède un élément n, or on a $P(n)$, donc A possède un plus petit élément n. □

Corollaire 5.0.2.
Toute partie non vide minorée (resp majorée) de $\mathbb{Z}$ possède un plus petit (resp. grand) élément.

Démonstration.
Soit $A \subset \mathbb{Z}$ avec $A \neq \varnothing$ et m un minorant de A (resp. M un majorant de A). On pose $B = \{ n - m \mid n \in A \}$ (resp. $B = \{ M - n \mid n \in A \}$).

Alors B est une partie non vide de $\mathbb{N}$.

Donc B possède un plus petit (resp. plus grand) élément. On en déduit le résultat. □

6 Relation d'ordre naturelle sur $\mathbb{R}$

On admettra l'existence de $\mathbb{R}$ et les propriétés usuelles sur $\mathbb{R}$.

6.1 Opérations usuelles

Théorème 6.1.1 (Compatibilité de la relation d'ordre avec l'addition et la multiplication)**.**
On a, $\forall x, y, z \in \mathbb{R}$,

$$x \leqslant y \Rightarrow x + z \leqslant y + z$$

et

$$(x \leqslant y \text{ et } 0 \leqslant z) \Rightarrow xz \leqslant yz.$$

On en déduit les règles usuelles de manipulation des inégalités, pour tous $x, y, x', y' \in \mathbb{R}$:

$$(x \leqslant y \text{ et } x' \leqslant y') \Rightarrow x + x' \leqslant y + y'$$

$$(0 \leqslant x \leqslant y \text{ et } 0 \leqslant x' \leqslant y') \Rightarrow xx' \leqslant yy'$$

$$x \leqslant y \Rightarrow -y \leqslant -x$$

$$0 < x \leqslant y \Rightarrow 0 < \frac{1}{y} \leqslant \frac{1}{x}.$$

Tout cela reste vrai avec des inégalités strictes.

Définition 6.1.2.
On appelle droite achevée l'ensemble $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$, où $-\infty$ et $+\infty$ sont deux éléments distincts n'appartenant pas à $\mathbb{R}$. De plus, on prolonge l'ordre sur $\mathbb{R}$, l'addition et la multiplication de façon à avoir les propriétés suivantes :

(i) Prolongement de l'ordre : $\forall x \in \mathbb{R} \quad -\infty < x < +\infty$.

(ii) Prolongement de l'addition : pour tout $x \in \mathbb{R}$, on a $x + +\infty = +\infty$, $x + (-\infty) = -\infty$, $+\infty + +\infty = +\infty$, $-\infty + (-\infty) = -\infty$.

(iii) Prolongement de l'opposé : $-(+\infty) = -\infty$, $-(-\infty) = +\infty$.

(iv) Prolongement de la multiplication : pour tout $x \in \bar{\mathbb{R}} \setminus \{ 0 \}$, $+\infty \times x = +\infty$ si $x > 0$, $+\infty \times x = -\infty$ si $x < 0$ et $(-\infty) \times x = -(+\infty \times x)$.

(v) Prolongement de l'inverse : $\dfrac{1}{+\infty} = 0$ et $\dfrac{1}{-\infty} = 0$.

 Il y a des formes indéterminées : $+$ et $\times$ ne sont pas des lois de composition interne sur $\overline{\mathbb{R}}$.

6.2 Caractère archimédien de $\mathbb{R}$ et partie entière

a Propriété d'Archimède

Proposition 6.2.1.
Soient deux réels x et y tels que $x > 0$. Alors il existe un entier N tel que $Nx \geqslant y$.

• Slogan : « quelle que soit la taille de nos enjambées, on peut aller au bout du monde si on fait assez de pas ».

Démonstration.
C'est une conséquence simple du Théorème 6.3.1, que l'on admet. Il suffit de considérer $A = \{nx | n \in \mathbb{N}\}$ et de raisonner par l'absurde. □

b Partie entière

Définition 6.2.2.
Soit $x \in \mathbb{R}$, il existe un unique entier, noté $\lfloor x \rfloor$ (parfois $E(x)$ ou $\mathbb{E}(x)$) et que l'on appelle *partie entière* de x, vérifiant : $\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1$.

Démonstration.
Soit $A = \{k \in \mathbb{Z} \mid k \leqslant x\}$.

La propriété d'Archimède implique qu'il existe $k \in \mathbb{N}$ tel que $k \times 1 \geqslant -x$, donc $-k \leqslant x$, donc $-k \in A$. Ainsi, A est non vide.

Une seconde fois, la propriété d'Archimède implique qu'il existe $\ell \in \mathbb{N}$ tel que $\ell \times 1 \geqslant x$. Ainsi, si $k \in A$, alors $k \leqslant x \leqslant \ell$, donc A est majorée par ℓ.

Ainsi, A est une partie non vide et majorée de $\mathbb{Z}$, donc A possède un plus grand élément, noté n. On a alors $n \geqslant x$ et comme $n + 1 > n$, $n + 1 \notin A$ donc $n + 1 > x$, d'où l'existence.

Soit N un entier vérifiant $N \leqslant x < N + 1$. Alors $N \in A$. De plus, si $k \in A$, alors $k \leqslant x < N + 1$ donc $k < N + 1$ donc $k \leqslant N$. N est donc bien le plus grand élément de A, d'où l'unicité. □

Remarque 6.2.3.
On vient de montrer que $\lfloor x \rfloor$ est le plus grand entier relatif inférieur ou égal à n. On peut très bien définir $\lfloor x \rfloor$ de cette manière, et voir la définition **??** comme une caractérisation de $\lfloor x \rfloor$.

Remarque 6.2.4.
Ce résultat permet de montrer que si deux réels x et y vérifient $y - x > 1$, il existe un entier n tel que $x < n < y$: il suffit de prendre $n = \lfloor x \rfloor + 1$. On a alors $x < n$ et aussi $n \leqslant x + 1 < x + (y - x) = y$.

 Ne pas confondre la partie entière avec la troncature. Ainsi $\lfloor -3,2 \rfloor = -4$ et non -3 !

c Densité de $\mathbb{Q}$ dans $\mathbb{R}$

Théorème 6.2.5.
Tout intervalle ouvert non vide rencontre $\mathbb{Q}$. Autrement dit, soient x, y des réels tels que $x < y$; alors il existe un nombre rationnel q tel que $x < q < y$.

Démonstration.
D'après la propriété d'Archimède, on peut trouver un entier naturel non nul r tel que $r(y-x) > 1$. D'après la remarque précédente, il existe un entier $p \in \mathbb{Z}$ tel que $rx < p < ry$. En posant $q = p/r$ on a le résultat. □

Corollaire 6.2.6.
Tout intervalle ouvert non vide rencontre $\mathbb{R} \setminus \mathbb{Q}$. Autrement dit, soient x, y des réels tels que $x < y$; alors il existe un nombre irrationnel q tel que $x < q < y$.

Démonstration.
En vertu du théorème précédent, il existe un rationnel r **non nul** entre $x\sqrt{2}$ et $y\sqrt{2}$. En effet, si $0 \leqslant x < y$, on a $r > x\sqrt{2}$ donc $r \neq 0$, si $x < y \geqslant 0$, même raisonnement, et si $x < 0 < y$, on applique le théorème précédent à 0 et y par exemple pour obtenir r. Il suffit alors de prendre $q = \dfrac{r}{\sqrt{2}}$. q est forcément irrationnel, sinon $\sqrt{2}$ serait rationnel. □

d Approximations décimales

Définition 6.2.7.
Soit x un réel et ε un réel strictement positif. On appelle *valeur approchée de x à la précision ε* tout réel y tel que $|x - y| \leqslant \varepsilon$. Si $y \leqslant x$ on dit que y est une valeur approchée *par défaut*, si $y \geqslant x$, on dit que y est une valeur approchée *par excès*.

• Souvent on cherche des valeurs approchées qui soient des décimaux.

Théorème 6.2.8.
Soit $a \in \mathbb{R}$. Pour tout entier n on note $a_n = \dfrac{\lfloor 10^n a \rfloor}{10^n}$ et $a'_n = \dfrac{\lfloor 10^n a \rfloor + 1}{10^n}$. Alors a_n et a'_n sont respectivement des valeurs approchées par défaut et excès de a à 10^{-n} près, qui de plus sont des décimaux.

Démonstration.
Évident par propriété de la partie entière. □

Ce dernier résultat a pour corollaire le résultat fondamental suivant :

Corollaire 6.2.9.
Tout réel est limite d'une suite de rationnels.

Exemple 6.2.10.
Calculer une approximation décimale de $1/7$ à 10^{-5} près.

6.3 Propriété de la borne supérieure

Cette propriété fait partie des propriétés inhérentes à $\mathbb{R}$ de par sa construction.

Théorème 6.3.1.
Toute partie non vide majorée (resp. minorée) de $\mathbb{R}$ admet une borne supérieure (resp. inférieure) dans $\mathbb{R}$.

Remarque 6.3.2.
C'est un résultat d'existence : il assure l'existence d'un objet sans donner sa valeur. Ce théorème est tout à fait inutile pour calculer une borne sup. Au mieux, il permet de montrer que la borne sup d'un ensemble existe, et donc on peut en parler (ce qui est interdit sinon).
Il est cependant fondamental dans un grand nombre de résultats théoriques qui servent tous les jours : TVI, théorèmes de la limite monotone, de Rolle, TAF, construction de l'intégrale ...

Corollaire 6.3.3.
Toute partie de $\bar{\mathbb{R}}$ admet une borne supérieure (resp. inférieure) dans $\bar{\mathbb{R}}$.

Démonstration.
Soit A une partie de $\bar{\mathbb{R}}$. Et posons $A' = A \cap \mathbb{R}$.
- Si $+\infty \in A$, alors A admet $+\infty$ pour maximum.
- Dans le cas contraire, on a les possibilités suivantes :
  - Si A' est vide, alors A admet $-\infty$ pour borne supérieure.
  - Si A' est non vide alors on a deux possibilités :
    - Si A' est non-majorée dans $\mathbb{R}$, alors A admet $+\infty$ comme borne supérieure.
    - Si A' est majorée dans $\mathbb{R}$, alors d'après la propriété de la borne supérieure, elle admet une borne supérieure M dans $\mathbb{R}$. Cette borne supérieure est aussi une borne supérieure de A dans $\bar{\mathbb{R}}$.

□

On a aussi une caractérisation fort utile des bornes supérieures et inférieures.

Proposition 6.3.4.
1. Soit A une partie non vide, majorée de $\mathbb{R}$. Alors, $a \in \mathbb{R}$ est la borne supérieure de A si et seulement si $\forall x \in A, x \leqslant a$ et $\forall \varepsilon > 0, \exists x \in A \cap]a-\varepsilon, a]$.
2. Soit A une partie non vide, minorée de $\mathbb{R}$. Alors, $a \in \mathbb{R}$ est la borne inférieure de A si et seulement si $\forall x \in A, x \geqslant a$ et $\forall \varepsilon > 0, \exists x \in A \cap [a, a+\varepsilon[$.

Démonstration.
On ne démontre que la partie concernant les bornes supérieures, l'autre en découle immédiatement.

Supposons d'abord que a est la borne supérieure de A. Alors, a majore A et donc $\forall x \in A, x \leqslant a$. Soit $\varepsilon > 0$, $a-\varepsilon < a$ et $a-\varepsilon$ n'est donc pas un majorant de A. Il existe donc $x \in A$ vérifiant $a - \varepsilon < x$ et, comme a majore A, on a $x \leqslant a$, ce qui permet de conclure pour cette implication.

Réciproquement, si a vérifie : $\forall x \in A, x \geqslant a$ et $\forall \varepsilon > 0, \exists x \in A \cap]a-\varepsilon, a]$. Ainsi, a est bien un majorant de A. Montrons que c'en est le plus petit. Sinon, il existerait $b \in \mathbb{R}$ majorant A, avec $b < a$. Alors, $]b, a[\cap A = \varnothing$, ce qui contredit l'hypothèse. a est donc la borne supérieure de A. □

6.4 Intervalles de $\mathbb{R}$

Il existe neuf types d'intervalles dans $\mathbb{R}$ (avec $a, b \in \mathbb{R}$) :

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

Les intervalles de types 1 à 4 sont dits *bornés*. Ceux de types 1, 5, 7 et 9 sont dits *fermés*. Ceux de types 4, 6 et 8 et 9 sont dits *ouverts*. Ceux de type 2 et 3 sont dits *semi-ouverts* ou *semi-fermés*. Seuls les intervalles de type 1 sont à la fois fermés et bornés : on dit que ce sont des *segments*.
Un intervalle peut être *vide* ou *réduit à un point* (dans le cas 1 si $a = b$). Un intervalle qui n'est ni vide ni réduit à un point est dit *non trivial*.
Énoncer tous ces intervalles est fastidieux : on préfère une définition unifiée d'intervalle qui les définit tous d'un coup :

Théorème 6.4.1.
Soit I une partie de $\mathbb{R}$. Alors les deux propositions suivantes sont équivalentes :

(i) I est un intervalle de $\mathbb{R}$;

(ii) Pour tous $u, v \in I$ et pour tout $t \in \mathbb{R}$, on a : $u \leqslant t \leqslant v \Rightarrow t \in I$.

Démonstration.
C'est trivial si $I = \varnothing$ (on a alors (ii) et (i) car $I = [0, -1]$).

(i)⇒(ii) Facile et connu.

(ii)⇒(i) On distingue plusieurs cas :

— Supposons d'abord que I majoré et minoré. On pose $a = \inf I$ et $b = \sup I$. Alors pour tout $x \in I$, on a $x \leqslant b$ et $x \geqslant a$, donc $x \in [a, b]$, et donc $I \subset [a, b]$ (1).
• Si $a = b$, alors $I = \{a\} = [a, a]$ (car I non vide).
• Si $a < b$, alors soit $x \in]a, b[$. Par définition de la borne inf il existe $u \in I$ tel que $a \leqslant u < x$. De même il existe $v \in I$ tel que $x < v \leqslant b$. Alors $x \in [u, v]$ et donc $x \in I$. Donc $]a, b[\subset I$ (2)
Ainsi on a la chaîne d'inégalité : $]a, b[\subset I \subset [a, b]$, donc I est de de l'un des types précédents. On détermine précisément lequel en regardant juste si a et b appartiennent ou pas à I.

— Si I n'est pas majoré mais est minoré, alors I n'a pas de sup, donc $I \subset [a, +\infty[$, et comme toute à l'heure, $]a, +\infty[\subset I$. On finit comme précédemment.

— Si I n'est pas minoré mais majoré : idem avec $]-\infty, b[$.

— Si I n'est ni majoré ni minoré, alors $I = \mathbb{R}$.

□

Chapitre IX

Entiers relatifs et arithmétique de $\mathbb{Z}$

Dans tout ce chapitre, a, b, c, d, m, n, p, q et r sont des entiers relatifs, sauf mention contraire.

1 Divisibilité

1.1 Définition

Définition 1.1.1.
On dit que n *divise* m, que n *est un diviseur de* m ou que m *est un multiple de* n et on note $n|m$ si et seulement s'il existe $k \in \mathbb{Z}$ vérifiant $m = kn$.

Proposition 1.1.2. (i) La relation $|$ est réflexive, transitive, mais pas symétrique (sur $\mathbb{Z}$ comme sur $\mathbb{N}$). Elle n'est pas antisymétrique sur $\mathbb{Z}$ mais l'est sur $\mathbb{N}$: plus précisément on a sur $\mathbb{Z}$:

$$a|b \text{ et } b|a \iff |a| = |b| \iff a = \pm b$$

(ii) Si a divise b et c, il divise toute combinaison linéaire à coefficients entiers de b et c :

$$a|b \text{ et } a|c \Rightarrow a|bn + cm$$

(iii) La relation $|$ est compatible avec le produit :

$$a|b \text{ et } c|d \Rightarrow ac|bd$$

En particulier, pour tout $k \in \mathbb{N}$, $a|b$ implique $a^k|b^k$;

(iv) Si $c \neq 0$, $a|b \Leftrightarrow ac|bc$.

Démonstration. (i) on ne montre que la dernière partie (le reste a déjà été fait dans le chapitre VIII). Soient $a, b \in \mathbb{Z}$ tels que $a|b$ et $b|a$. Alors il existe $k, \ell \in \mathbb{Z}$ tels que $a = kb$ et $b = a\ell$, donc $b = bk\ell$. Si $b = 0$, alors $a = 0$ également, car $b|a$. Si $b \neq 0$, alors $k\ell = 1$, et donc $k \neq 0$, $\ell \neq 0$, et $|k| \leqslant 1$, ainsi que $|\ell| \leqslant 1$. Par conséquent $k = \ell = 1$ ou $k = \ell = -1$, et donc $a = b$ ou $a = -b$.

(ii) Élémentaire.

(iii) Élémentaire.

(iv) Élémentaire.

□

Exercice 1.1.3.
Montrer que si $a \in \mathbb{Z}$ vérifie $a|1$, alors $a = \pm 1$.

Définition 1.1.4.
On dit que a *est congru à* b *modulo* n et on note $a \equiv b \quad [n]$ (voire $a = b \quad [n]$) si et seulement si n divise $a - b$:

$$a \equiv b \quad [n] \iff n|a - b.$$

Remarque 1.1.5.
Pour tout entier n, la relation de congruence modulo n est une relation d'équivalence.

Proposition 1.1.6.
La relation de congruence modulo n est compatible avec l'addition et la multiplication : si $a \equiv b[n]$ et $c \equiv d[n]$, alors $a + c \equiv b + d[n]$ et $ac \equiv bd[n]$.

Démonstration.
On sait qu'il existe $(k, \ell) \in \mathbb{Z}^2$ vérifiant $a = b + nk$ et $c = d + n\ell$. On a alors $a + c = b + d + n(k + \ell)$, donc $a + c \equiv b + d[n]$, et $ac = bd + n(b\ell + dk + nk\ell)$, donc $ac \equiv bd[n]$. □

Remarque 1.1.7.
Attention, ce n'est pas le cas de la relation usuelle de congruence modulo 2π. Ainsi, $2\pi \equiv 0 \quad [2\pi]$ mais $4\pi^2 \not\equiv 0 \quad [2\pi]$.

Remarque 1.1.8.
On a $n|a$ si et seulement si $a \equiv 0[n]$.

Exercice 1.1.9.
Retrouver les critères de divisibilité énoncés au collège.

1.2 Division euclidienne

Théorème 1.2.1.
Soient $a \in \mathbb{Z}$, et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que $a = bq + r$ et $0 \leqslant r < b$. q et r sont respectivement appelés le quotient et le reste de la division euclidienne de a par b. b

est appelé le diviseur et a le dividende de cette division.

Démonstration.
On montre l'existence puis l'unicité.

Existence : On note $A = \{ k \in \mathbb{Z} \mid kb \leqslant a \}$. Alors :
- A est non vide car si $a \geqslant 0$, $0 \in A$, et si $a < 0$ on a $a \in A$ car $b \geqslant 1$.
- De plus A est majoré, par 0 si $a \leqslant 0$ et par a si $a > 0$.

A a donc un plus grand élément noté q. Alors par construction $qb \leqslant a < (q+1)b$, d'où le résultat en posant $r = a - qb$.

Unicité : Soit (q, r) et (q', r') deux couples vérifiant les conditions considérées.
Alors $a = qb + r = q'b + r'$, donc $b(q - q') = r' - r$ et ainsi $b|q - q'| = |r - r'|$. Or on a $0 \leqslant r < b$ et $-b < -r' \leqslant 0$, donc $|r - r'| < b$, donc $|q - q'| < 1$, or $q - q'$ est un entier donc $q = q'$, donc $r = r'$.

□

Remarque 1.2.2.
On a donc $r \equiv a[b]$.

Exemple 1.2.3.
Poser une division à la main. Par exemple 360 divisé par 7.

Remarque 1.2.4.
Dans la pratique, pour $a \geqslant 0$, un algorithme naïf de calcul consiste à soustraire b de a autant de fois que nécessaire pour qu'il reste un nombre plus petit que b. Ainsi :
- Si $a < b$, le quotient est 0 et le reste est a. Sinon on calcule $a_1 = a - b$
- Si $a_1 < b$, le quotient est 0 et le reste est a_1. Sinon on calcule $a_2 = a_1 - b$.
- Si $a_2 < b$, le quotient est 0 et le reste est a_2. Sinon on calcule $a_3 = a_2 - b$.

Et ainsi de suite par récurrence : on s'arrête dès que $a_n < b$. On a alors soustrait n fois b, et il reste a_n : $a = nb + a_n$.

Dans le cas où $a < 0$, on ajoute b jusqu'à obtenir un nombre positif ou nul.

Théorème 1.2.5 (Fonction Python)**.**

```
def diveuclide (a, b) :
    """Précondition : b > 0"""
    q = 0
    r = a
    while r >= b :
        # Invariant : a = b*q + r
        # Variant : r
        r = r-b
        q = q+1
    # Invariant : r < b
    while r < 0 :
        # Invariants :
        # a = b*q + r
        # r < b
        # Variant : -r
        r = r+b
        q = q+1
    # Invariants :
    # 0 <= r < b
    # a = b*q + r
    return(q,r)


def quotient (a, b) :
    """Précondition b > 0"""
    (q, r) = diveuclide (a, b)
    return q


def reste (a, b) :
    """Précondition b > 0"""
    (q, r) = diveuclide (a, b);
    return r

print(reste(11**42424244,7))
```

Démonstration.
- Les boucles `while` terminent : dans la première, la valeur de `r` est un entier qui décroît strictement à chaque itération et sera donc strictement inférieure à celle de b à partir d'un certain moment ; dans la seconde, la valeur de `r` est toujours entière et croît strictement à chaque itération et sera donc strictement positive à partir d'un certain moment.
- Le premier invariant de boucle est vrai à l'arrivée dans la boucle et est préservé au cours de son exécution.

— En sortie de la première boucle, la condition de boucle est fausse donc on a nécessairement `r < b`.
— À l'entrée de la seconde, l'invariant annoncé est vrai, il est également préservé. De plus, au début de chaque itération, on a `r < 0` donc à la fin de chaque itération, on a `r < b`.
— À la sortie de la seconde boucle, la condition de boucle est fausse donc on a nécessairement `r ⩾ 0`. De plus l'invariant de boucle est encore vrai et `r < b`. □

Remarque 1.2.6.
Dans la pratique, au lieu d'enlever b un par un, on peut l'enlever paquets par paquets : c'est ce que l'on fait en posant la division usuelle.

Exemple 1.2.7.
$2356 = 18 \times 125 + 106$.

Proposition 1.2.8.
Soit $n \in \mathbb{N}^*$, alors $a \equiv b[n]$ si et seulement si a et b ont le même reste dans la division euclidienne par n.

Démonstration.
Si a et b ont le même reste dans la division euclidienne par n, on écrit $a = nq_1 + r$ et $b = nq_2 + r$, avec $(q_1, q_2) \in \mathbb{Z}^2$ et $0 \leqslant r < n$. On a donc bien $a - b = n(q_1 - q_2)$, donc $n|(a-b)$.

Réciproquement, si $a \equiv b[n]$, on écrit les divisions euclidiennes de a et b par n : $a = nq_1 + r_1$ et $b = nq_2 + r_2$, avec $(q_1, q_2) \in \mathbb{Z}^2$ et $(r_1, r_2) \in \mathbb{N}^2$ vérifiant, pour tout $i \in \{1, 2\}$, $0 \leqslant r_i < n$. On a alors $a - b - n(q_1 - q_2) = r_1 - r_2$, donc $n|(r_1 - r_2)$. Or, $-n < r_1 - r_2 < n$ et il existe un seul entier dans $[\![-n+1, n-1]\!]$ divisible par n (le montrer !) : c'est 0. Ainsi, $r_1 = r_2$. □

Exemple 1.2.9.
Exercice classique : calculer à la main le reste de la division euclidienne de $11^{42424244}$ par 7.

2 PGCD, PPCM

Soit $a \in \mathbb{Z}$. L'ensemble des multiples de a est noté $a\mathbb{Z}$. C'est donc $\{ak | k \in \mathbb{Z}\}$. Remarquons que, si $a \neq 0$, $|a|$ est le plus petit entier strictement positif de $a\mathbb{Z}$.

On notera aussi $\mathscr{D}(a)$ l'ensemble des diviseurs de a : c'est donc $\{k \in \mathbb{Z} \mid \exists \ell \in \mathbb{Z}, a = k\ell\}$. On remarquera que, si $a \neq 0$, $\mathscr{D}(a)$ est borné par $|a|$.

2.1 PGCD de deux entiers

Dans cette partie, pour tout couple $(a, b) \in \mathbb{Z}$, on note $\mathscr{D}(a, b)$ l'ensemble des diviseurs communs à a et b. Ainsi, $\mathscr{D}(a, b) = \mathscr{D}(a) \cap \mathscr{D}(b)$.

Remarque 2.1.1.
Si $b = 0$, alors $\mathscr{D}(a, b) = \mathscr{D}(a)$.

Définition 2.1.2.
Soit a et b deux entiers avec $(a, b) \neq (0, 0)$, alors on appelle plus grand diviseur commun de a et b (pgcd de a et b) et on note $\mathrm{PGCD}(a, b)$ ou $a \wedge b$ le plus grand élément de $\mathscr{D}(a, b)$.

Remarque 2.1.3.
L'un des deux entiers est non nul, donc $\mathscr{D}(a, b)$ est majoré par la valeur absolue de cet entier. Par ailleurs, $1 \in \mathscr{D}(a, b)$. Donc $\mathscr{D}(a, b)$ est un ensemble d'entiers non vide majoré, donc il admet un plus grand élément, ce qui justifie la définition.

Lemme 2.1.4 (Lemme d'Euclide)**.**
Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$, r le reste de la division euclidienne de a par b. Alors $\mathscr{D}(a, b) = \mathscr{D}(b, r)$.

Démonstration.
Soit $d \in \mathscr{D}(a, b)$. Alors a s'écrit sous la forme $bq + r$ donc $r = a - bq$, or $d|a$ et $d|b$, donc d divise toute combinaison linéaire de a et b, donc divise r. Donc $\mathscr{D}(a, b) \subset \mathscr{D}(b, r)$.

Réciproquement, soit $d \in \mathscr{D}(b, r)$, alors a s'écrit sous la forme $bq + r$ or $d|b$ et $d|r$ donc $d|a$, donc $\mathscr{D}(b, r) \subset \mathscr{D}(a, b)$. □

Théorème 2.1.5.
Soit $(a, b) \in \mathbb{Z}^2$ avec $(a, b) \neq (0, 0)$. Alors il existe un unique entier $d > 0$ tel que $\mathscr{D}(a, b)$ soit l'ensemble des diviseurs de d. Cet entier est $a \wedge b$.

Démonstration.
Montrons tout d'abord l'unicité sous réserve d'existence. Soit d et d' deux entiers strictement positifs tels que $\mathscr{D}(a, b)$ soit l'ensemble des diviseurs de d et soit également l'ensemble des diviseurs de d'. Alors on a $d \in \mathscr{D}(a, b)$. Or $\mathscr{D}(a, b)$ est l'ensemble des diviseurs de d', donc $d|d'$. De même $d'|d$. Or $d > 0$ et $d' > 0$ donc $d = d'$.

L'existence repose sur un algorithme, appelé algorithme d'Euclide. En Python, il s'écrit :

```
def euclide (a,b) :
    """Précondition (a,b) != (0,0)"""
    R0 = abs(a)
    R1 = abs(b)
    while R1 > 0 :
        # Invariant : D(R0,R1) = D(a,b)
        # et R0 >= 0 et R1 >= 0
        # et (R0, R1) != (0,0)
        # Variant : R1
        (q, R2) = diveuclide (R0,R1)
        R0 = R1
        R1 = R2
    # Sortie de boucle : R1 == 0
    return R0
```

Soit a et b deux entiers relatifs non tous les deux nuls. Il est clair que l'appel `euclide(a,b)` termine. La valeur d retournée vérifie $\mathscr{D}(a,b) = \mathscr{D}(d,0)$, $d \geqslant 0$ et $(d,0) \neq (0,0)$. Or $\mathscr{D}(d,0)$ est l'ensemble des diviseurs de d donc $\mathscr{D}(a,b)$ est bien l'ensemble des diviseurs d'un entier $d > 0$.

Un autre point de vue sur cet algorithme est la suite r définie de la façon suivante :

$$\begin{cases} r_0 = |a| \\ r_1 = |b| \\ \forall n \in \mathbb{N} \quad r_{n+2} = \begin{cases} \texttt{reste}(r_n, r_{n+1}) & \text{si } r_{n+1} \neq 0 \\ 0 & \texttt{sinon} \end{cases} \end{cases}$$

Il est clair que cette suite est à valeurs positives ou nulles. À partir d'un certain rang, cette suite est nulle, sinon r serait strictement décroissante (du moins à partir du rang 1), ce qui serait absurde. Par ailleurs, pour toutes les valeurs de n pour lesquelles $(r_n, r_{n+1}) \neq (0,0)$, on a $\mathscr{D}(r_n, r_{n+1}) = \mathscr{D}(a,b)$. En particulier, pour la dernière valeur non-nulle r_n, on a $\mathscr{D}(r_n, 0) = \mathscr{D}(a,b)$.

L'algorithme d'Euclide n'est rien d'autre que le calcul des termes successifs de la suite (r_n) : en numérotant les tours de boucle (à partir de 0) dans l'algorithme précédent, on peut d'ailleurs noter qu'au n^{e} tour de boucle, R_0 contient la valeur de r_n, et R_1 celle de r_{n+1}. □

Remarque 2.1.6. — Sur $(\mathbb{N}^*)^2$, le pgcd de deux nombres a et b est donc la borne inférieure de $\{a,b\}$ pour l'ordre $|$. C'est donc aussi le maximum de $\mathscr{D}(a,b) \cap \mathbb{N}^*$ pour l'ordre $|$ et pour l'ordre $\leqslant$.

— Sur $\mathbb{Z}^*$, la relation $|$ n'est pas un ordre car elle n'est pas antisymétrique : on a à la fois $1|-1$ et $-1|1$ (on dit qu'on à affaire à un préordre). L'ensemble des diviseurs de a et b a alors deux «plus grands» éléments pour la relation de divisibilité : $a \wedge b$ et $-(a \wedge b)$. On peut donc en fait considérer que a et b ont deux pgcd : $a \wedge b$ et $-(a \wedge b)$; lorsqu'on parle *du* pgcd, on considère alors qu'il s'agit du pgcd positif.

On peut donner la caractérisation suivante :

Proposition 2.1.7.
Soient $a, b, d \in \mathbb{Z}$, avec $(a,b) \neq (0,0)$. On a l'équivalence :

$$\Big(d \text{ est le PGCD de } a \text{ et } b\Big)$$
$$\Leftrightarrow \Big(d|a,\ d|b,\ d \geqslant 0 \text{ et } \forall n \in \mathbb{Z},\ (n|a \text{ et } n|b) \Rightarrow n|d\Big)$$

Démonstration.
Le sens $\Rightarrow$ découle du théorème précédent.

Réciproquement, si $d \in \mathbb{N}$ vérifie $d|a$, $d|b$ et $\forall n \in \mathbb{N}$, $n|a$ et $n|b \Rightarrow n|d$. Alors d'après les deux premiers points $d|a \wedge b$ et d'après le dernier, $a \wedge b|d$. On conclut avec $d \geqslant 0$ et $a \wedge b \geqslant 0$. □

Théorème 2.1.8 (Théorème de Bézout, première partie)**.**
Soient $a, b \in \mathbb{Z}^2 \setminus \{(0,0)\}$. Il existe deux entiers u, v tels que $au + bv = a \wedge b$. Un tel couple est appelé un couple de Bézout de a et b.

Démonstration.
L'idée de la démonstration est de regarder ce qui se passe dans l'algorithme d'Euclide. On constate qu'à chaque étape, les variables R_0 et R_1 sont des combinaisons linéaires de a et b. À la fin de l'algorithme, le pgcd R_0 est donc une combinaison linéaire de a et b.

Pour calculer les coefficients de Bézout, on aura recours à l'algorithme d'Euclide étendu. Celui-ci est un simple ajout à l'algorithme vu précédemment ; on introduit en effet des variables U_i et V_i pour $i = 0, 1$ qu'on va modifier au fur et à mesure de l'exécution de façon à garantir $R_0 = U_0 a + V_0 b$ et $R_1 = U_1 a + V_1 b$.

```
def euclide_etendu (a, b) :
    """Précondition (a,b) != (0,0)"""
    R0 = abs(a)
    if a < 0 :
        U0 = -1
    else :
        U0 = 1
    V0 = 0
    # Invariant : R0 == U0*a + V0*b
```

```
R1 = abs(b)
U1 = 0
if b < 0 :
    V1 = -1
else :
    V1 = 1
# Invariant : R1 == U1*a + V1*b
# Invariant : D(R0,R1) == D(a,b)
while R1 > 0 :
    # Invariants :
    # D(R0,R1) == D(a,b)
    # R1>=0 et R2>=0
    # (R1,R2) != (0,0)
    # R0 == U0*a + V0*b
    # R1 == U1*a + V1*b
    # Variant : R1
    (q,R2) = diveuclide(R0,R1)
    # donc R2 = R0 - q*R1
    U2 = U0-q*U1
    V2 = V0-q*V1
    # R2 = U2*a + V2*b
    R0, U0, V0 = R1, U1, V1
    R1, U1, V1 = R2, U2, V2
# R1 == 0
return (R0,U0,V0)
```

Là encore, une autre façon de considérer cet algorithme est de regarder les suites r, u et v, où r est la suite considérée précédemment, où u et v vérifient $r_i = u_i a + v_i b$ pour $i = 0, 1$ et pour n tel que r_{n+1} soit non nul, $u_{n+2} = u_n - aq_{n+1}$ et $v_{n+2} = v_n - qv_{n+1}$, où q est le quotient de la division euclidienne de r_n par r_{n+1}. Là encore, il n'est pas difficile de montrer par récurrence double que tant que $(r_n, r_{n+1}) \neq (0,0)$, on a $r_n = u_n a + v_n b$. □

 Le couple des coefficients de Bézout n'est pas unique. Par exemple on a $-1 \times 2 + 1 \times 3 = 1$ et $2 \times 2 + (-1) \times 3 = 1$.

Exemple 2.1.9.
Calcul d'un couple de Bézout pour 1750 et 644.

On peut alors faire la remarque suivante :

Corollaire 2.1.10.
Soit $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$. Alors

$$a\mathbb{Z} + b\mathbb{Z} = \left\{ au + bv \;\middle|\; (u,v) \in \mathbb{Z}^2 \right\} = (a \wedge b)\mathbb{Z}$$

Démonstration.
L'inclusion gauche-droite découle du fait que, a et b étant des multiples de $a \wedge b$, toute combinaison linéaire de a et b est également un multiple de $a \wedge b$.

L'inclusion droite-gauche découle du fait que $a \wedge b$ s'écrit comme combinaison linéaire à coefficients entiers de a et b (d'après le théorème de Bézout) et que tout multiple d'une combinaison linéaire de a et b à coefficients entiers est encore une combinaison linéaire à coefficients entiers. □

Corollaire 2.1.11.
Soient $a, b, c \in \mathbb{Z}$. Alors $(ac) \wedge (bc) = |c|(a \wedge b)$.

Démonstration.
Posons $p = (ac) \wedge (bc)$ et $q = |c|(a \wedge b)$. On a $p > 0$ et $q > 0$ donc p et q sont respectivement les plus petits éléments strictement positifs de $p\mathbb{Z}$ et $q\mathbb{Z}$.

Il suffit donc de montrer $p\mathbb{Z} = q\mathbb{Z}$.

Or d'après ce qui précède, on a successivement :

$$\begin{aligned}(a \wedge b)\mathbb{Z} &= \left\{ au + bv \;\middle|\; (u,v) \in \mathbb{Z}^2 \right\} \\ q\mathbb{Z} &= \left\{ |c|(au + bv) \;\middle|\; (u,v) \in \mathbb{Z}^2 \right\} \\ &= \left\{ cau + cbv \;\middle|\; (u,v) \in \mathbb{Z}^2 \right\} \\ &= p\mathbb{Z}\end{aligned}$$

□

2.2 PGCD d'une famille finie d'entiers

Les définitions et résultats de la section précédente se généralisent à une famille finie d'entiers.

Ainsi, si $a_1, \ldots, a_p$ sont p entiers non tous nuls, on note $\mathscr{D}(a_1, \ldots, a_p)$ l'ensemble des diviseurs communs à tous les entiers $a_1, \ldots, a_p$. Cet ensemble étant non vide (il contient 1) et fini, il admet un plus grand élément, appelé *plus grand commun diviseur* des entiers $a_1, \ldots, a_p$ et noté $\bigwedge_{i=1}^{p} a_i$, ou $a_1 \wedge \ldots \wedge a_p$.

Proposition 2.2.1.
Soient $(a_1, \ldots, a_p) \in \mathbb{Z}^p$, avec $a_1 \neq 0$ et $p \in \mathbb{N}^*$.

(i) Soit $k \in \mathscr{D}(a_1, \ldots, a_p)$, alors $k | a_1 \wedge \ldots \wedge a_p$.

(ii) $a_1 \wedge \ldots \wedge a_p = (a_1 \wedge \ldots \wedge a_{p-1}) \wedge a_p$.

Démonstration.
Démontrons les deux résultats en une récurrence, en posant pour chaque $p \in \mathbb{N}^*$:

(H_p) : pour tout $(a_1, \dots, a_p) \in \mathbb{Z}^p$, avec $a_1 \neq 0$, on a (i) et (ii).

Le résultat est connu pour $p = 1$ et $p = 2$.
Soit $p \in \mathbb{N}^*$ tel (H_p) soit vraie.
Soient $a_1, \dots, a_{p+1} \in \mathbb{N}$ tels que $a_1 \neq 0$.
Notons $d = a_1 \wedge \dots \wedge a_p$, $D = a_1 \wedge \dots \wedge a_p \wedge a_{p+1}$ et $D' = d \wedge a_{p+1}$.
Par définition, D divise $a_1, \dots, a_p$: par hypothèse de récurrence (i), D divise donc d. De plus, D divise a_{p+1}, donc $D|D'$.
Par définition, D' divise d et a_{p+1}, et d divise $a_1, \dots, a_p$. Par transitivité de la relation de divisibilité, D' est donc un diviseur de $a_1, \dots, a_{p+1}$. Par définition de D', on a donc $D' \leqslant D$: il vient donc $D = D'$.
Soit k un autre diviseur de $a_1, \dots, a_{p+1}$. En particulier, k est un diviseur de $a_1, \dots, a_p$, donc $k|d$. Et comme $k|a_{p+1}$, alors $k|D'$, et donc $k|D$: (H_{p+1}) est bien démontrée. □

Remarque 2.2.2.
La proposition précédente assure que l'on peut calculer le PGCD d'une famille $a_1, \dots, a_p$ d'entiers en plusieurs étapes : on calcule d'abord $a_1 \wedge a_2$ puis $(a_1 \wedge a_2) \wedge a_3$, et ainsi de suite. Par commutativité du PGCD, on peut aussi choisir les entiers dans un autre ordre, et tout ceci prouve l'associativité du PGCD et assure que la notation $a_1 \wedge \dots \wedge a_p$ est sans ambiguïté.

Le théorème de Bézout peut alors se généraliser par récurrence :

Théorème 2.2.3.
Soient $a_1, \dots, a_p$ des entiers non tous nuls. Alors il existe des entiers $u_1, \dots, u_p$ tels que

$$u_1 a_1 + \dots + u_p a_p = a_1 \wedge \dots \wedge a_p.$$

Démonstration.
Montrons-le par récurrence sur p.
On sait déjà que la propriété est vraie pour $p = 2$.
Soit $p \geqslant 2$ tel que la propriété soit vraie, et soient $a_1, \dots, a_p, a_{p+1}$ des entiers, avec par exemple $a_1 \neq 0$.

Si $a_1 = \dots = a_p = 0$, alors $a_1 \wedge \dots \wedge a_{p+1} = a_{p+1}$, ce qui est bien une relation de Bézout.

Sinon, par hypothèse de récurrence, il existe des entiers $u_1, \dots, u_p$ tels que $u_1 a_1 + \dots + u_p a_p = a_1 \wedge \dots \wedge a_p$. Mais $a_1 \wedge \dots \wedge a_p \wedge a_{p+1} = (a_1 \wedge \dots \wedge a_p) \wedge a_{p+1}$ et d'après le théorème de Bézout pour deux entiers, il existe $b, c \in \mathbb{Z}$ tels que $b.a_1 \wedge \dots \wedge a_p + c.a_{p+1} = a_1 \wedge \dots \wedge a_{p+1}$. D'où $a_1 \wedge \dots \wedge a_{p+1} = bu_1 a_1 + \dots + bu_p a_p + ca_{p+1}$, et l'hérédité est démontrée. □

Exemple 2.2.4.
Trouver trois entiers a, b, c tels que $72a + 180b + 120c = 12$.

Remarque 2.2.5.
Le corollaire 2.1.10 se généralise : soient $a_1, \dots, a_n$ une famille finie d'entiers et $c \in \mathbb{Z}$. Alors $\bigwedge_{i=1}^{n} (ca_i) = |c| \bigwedge_{i=1}^{n} a_i$.

2.3 Nombres premiers entre eux

Définition 2.3.1.
Deux entiers relatifs a et b sont dit premiers entre eux si et seulement si $(a, b) \neq (0, 0)$ et $a \wedge b = 1$.

Remarque 2.3.2.
Deux entier a et b sont premiers entre eux si et seulement si leurs seuls diviseurs communs sont 1 et -1, en d'autres termes si et seulement si $\mathscr{D}(a, b) \subset \{ -1, 1 \}$ (ce qui est équivalent à $\mathscr{D}(a, b) = \{ -1, 1 \}$).

Théorème 2.3.3 (Théorème de Bézout, seconde partie)**.**
Soient $a, b \in \mathbb{Z}$. Alors, a et b sont premiers entre eux si et seulement s'il existe deux entiers u et v tels que $au + bv = 1$.

Démonstration.
Le cas $(a, b) = (0, 0)$ est direct : les deux propositions sont fausses, donc équivalentes. Considérons donc $(a, b) \in \mathbb{Z}^2 \setminus \{ (0, 0) \}$.

Supposons a et b premiers entre eux. Alors, d'après le théorème de Bézout (première partie), on a le résultat.

Réciproquement, supposons qu'il existe deux entiers u et v vérifiant $au + bv = 1$. Soit alors $d \in \mathscr{D}(a, b)$. On a $d|a$ et $d|b$, donc $d|(au + bv)$, donc $d|1$, donc $d = \pm 1$. Donc $\mathscr{D}(a, b) \subset \{ -1, +1 \}$. □

Remarque 2.3.4.
On a donc $a \wedge b = 1$ si et seulement si a est inversible modulo b (*i.e.* il existe $k \in \mathbb{Z}$ vérifiant $ak = 1[b]$).

 $au + bv = 1$ implique $a \wedge b = 1$, mais $au + bv = d$ n'implique pas $a \wedge b = d$, mais simplement $(a \wedge b)|d$.

Corollaire 2.3.5.
Soit $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$. Alors en posant $d = a \wedge b$, $a' = a/d$ et $b' = b/d$, on a

$$a' \wedge b' = 1$$

Démonstration.
On utilise les deux versions du théorème de Bézout : On sait qu'il existe u et v vérifiant $d = au + bv$, d'où $1 = a'u + b'v$, d'où a' et b' sont premiers entre eux. □

Remarque 2.3.6.
Ce corollaire est très fréquemment utilisé.

Corollaire 2.3.7. (i) Soient a premier avec k entiers relatifs b_1, b_2, ..., b_k. Alors a est premier avec $b_1 \times b_2 \times \ldots \times b_k$.

(ii) Si a et b sont premiers entre eux, alors pour tous $m, n \in \mathbb{N}^*$, a^m et b^n sont également premiers entre eux.

Démonstration. (i) On traite le cas $k = 2$, le cas général s'en déduit immédiatement par récurrence. Il existe u_i et v_i vérifiant $au_i + b_i v_i = 1$ pour $i = 1, 2$. En multipliant ces deux relations, il vient successivement

$$1 = (au_1 + b_1 v_1)(au_2 + b_2 v_2)$$
$$1 = a^2 u_1 u_2 + a u_1 b_2 v_2 + b_1 v_1 a u_2 + b_1 v_1 b_2 v_2$$
$$1 = a(a u_1 u_2 + u_1 b_2 v_2 + b_1 v_1 u_2) + b_1 b_2 (v_1 v_2)$$

D'où le résultat.

(ii) On applique (i) à a et $b \times b \times b \times \ldots \times b$, puis (i) à b^n et $a \times a \times a \times \ldots \times a$.

□

Théorème 2.3.8 (Lemme de Gauss)**.**
Soient $a, b, c \in \mathbb{Z}$. On suppose $a|bc$ et $a \wedge b = 1$. Alors $a|c$.

Démonstration.
Ce résultat est une généralisation d'un lemme d'Euclide . On a $a \wedge b = 1$ donc 1 s'écrit comme combinaison linéaire $au + bv$ de a et b. Donc $c = c \times 1 = a(cu) + (bc)v$. Donc c est combinaison linéaire de a et bc. Or bc est un multiple de a donc c est un multiple de a.

On peut aussi le voir d'un point de vue plus algébrique : le théorème de Bézout (2e partie) nous indique que $a \wedge b = 1$ si et seulement si b est inversible modulo a (*i.e*, il existe $k \in \mathbb{Z}$ tel que $kb = 1[a]$). On a alors $bc = 0[a]$, donc $kbc = c = 0[a]$. □

Corollaire 2.3.9 (Forme irréductible d'un rationnel)**.**
Soit $r \in \mathbb{Q}$. Il existe un unique couple $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \dfrac{p}{q}$ et $p \wedge q = 1$. Ce couple est appelé *la forme irréductible de* r.

Démonstration.Existence C'est une conséquence directe du corollaire 4.2.4.

Unicité Soit (p,q) et (p',q') deux formes irréductibles d'un même rationnel r. Alors $p/q = p'/q'$ donc $pq' = p'q$. Donc $q|pq'$ et $p \wedge q = 1$. Donc d'après le théorème de Gauss, on a $q|q'$. De même $q'|q$. Donc $q = q'$ ou $q = -q'$. Or q et q' sont tous deux positifs, donc $q = q'$, donc $p = p'$.

□

Définition 2.3.10.
On dit que des entiers $a_1, \ldots, a_p$ sont *premiers entre eux dans leur ensemble* si leur PGCD vaut 1.

Remarque 2.3.11.
Ne pas confondre « premiers entre eux dans leur ensemble » et « premiers deux à deux ».

Remarque 2.3.12.
La deuxième partie du théorème de Bézout se généralise sans problème à une famille finie d'entiers : soient $a_1, \ldots, a_p$ des entiers. Ces entiers sont premiers entre eux dans leur ensemble si et seulement si il existe des entiers $u_1, \ldots, u_p$ tels que $u_1 a_1 + \ldots + u_p a_p = 1$.

2.4 PPCM

Définition 2.4.1.
Soit a et b deux entiers relatifs. L'ensemble de leurs multiples communs est $a\mathbb{Z} \cap b\mathbb{Z}$. Si a et b sont tous deux non nuls, alors cet ensemble possède un plus petit élément strictement positif. Celui-ci est appelé ppcm de a et b et est noté $\mathrm{PPCM}(a,b)$ ou $a \vee b$.

Remarque 2.4.2.
$|ab|$ est un multiple commun à a et b. De plus, comme a et b sont non nuls, c'est un nombre strictement positif. L'ensemble des multiples communs de a et de b strictement positifs est donc non vide. Il est évidemment minoré (par 0), donc il admet un plus petit élément.

Théorème 2.4.3.
Soit a et b deux entiers relatifs. Alors il existe un unique $m \geqslant 0$ vérifiant $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. Dans le cas où a et b sont non-nuls, cet entier m est le ppcm de a et b et vaut $\frac{|ab|}{a \wedge b}$

Démonstration.
Le cas ou a ou b est nul est trivial : on a alors $a\mathbb{Z} \cap b\mathbb{Z} = \{0\} = 0\mathbb{Z}$. On suppose donc dans la suite de cette démonstration que a et b sont non nuls. Posons $d = a \wedge b$, $a' = a/d$ et $b' = b/d$. a' et b' sont premiers entre eux.

Posons $m = |ab/d| = |a'b'd|$. m est un multiple de a et de b, donc tout multiple de m est un multiple commun de a et b : $m\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$.

Soit alors p un multiple de a et de b. Alors p s'écrit à la fois sous la forme au et sous la forme bv. On a donc $p = au = bv$, donc $a'du = b'dv$, donc $a'u = b'v$. Donc $a'|b'v$, or $a' \wedge b' = 1$ donc $a'|v$. Donc il existe k vérifiant $v = ka'$. On a alors $p = bv = bka' = ka'b'd$, donc p est un multiple de m. Donc $a\mathbb{Z} \cap b\mathbb{Z} \subset m\mathbb{Z}$.

On a donc $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. De plus, m est le plus petit élément strictement positif de $a\mathbb{Z} \cap b\mathbb{Z}$ et pour tout $m' \geqslant 0$ vérifiant $m'\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$, m' est également le plus petit élément strictement positif de $a\mathbb{Z} \cap b\mathbb{Z}$, donc $m' = m$. □

Remarque 2.4.4. — Sur $(\mathbb{N}^*)^2$, le ppcm de deux nombres a et b est donc la borne supérieure de $\{a, b\}$ pour l'ordre $|$. C'est donc aussi le minimum de $a\mathbb{N} \cap b\mathbb{N}$ pour l'ordre $|$ et pour l'ordre $\leqslant$.
— De même que pour le pgcd, sur $\mathbb{Z}^*$, l'ensemble des diviseurs de a et b a deux «plus petits» éléments pour la relation de divisibilité : $a \vee b$ et $-(a \vee b)$. On peut donc en fait considérer que a et b ont deux ppcm : $a \vee b$ et $-(a \vee b)$; lorsqu'on parle *du* ppcm, on considère alors qu'il s'agit du ppcm positif.

On peut donner la caractérisation suivante :

Proposition 2.4.5.
Soient $a, b, m \in \mathbb{Z}$. On a l'équivalence :

$$\Big(m \text{ est le PPCM de } a \text{ et } b\Big)$$
$$\Leftrightarrow \Big(a|m,\ b|m,\ m \geqslant 0$$
$$\text{et : } \forall n \in \mathbb{Z},\ (a|n \text{ et } b|n) \Rightarrow m|n\Big)$$

Et également (le point (ii) a d'ailleurs été démontré au cours de la démonstration du théorème 2.4.3) :

Proposition 2.4.6.
Soient $a, b, c \in \mathbb{Z}$. Alors :
(i) $(ac) \vee (bc) = |c|(a \vee b)$.
(ii) si $(a, b) \neq (0, 0)$, alors $|ab| = (a \wedge b).(a \vee b)$.

Exemple 2.4.7.
Calculer $1750 \vee 644$.

Remarque 2.4.8.
Là encore, si $a_1, \ldots, a_n$ est une famille finie d'entiers et $c \in \mathbb{Z}$, alors $\bigvee_{i=1}^{n} (ca_i) = |c| \bigvee_{i=1}^{n} a_i$.

3 Nombres premiers

Définition 3.0.1.
Soit $p \in \mathbb{N}^*$. On dit que p est *premier* si $p \neq 1$ et si ses seuls diviseurs positifs sont 1 et p. On dit que p est *composé* si $p \neq 1$ et p est non premier.

Exemple 3.0.2.
Les premiers nombres premiers : $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \ldots$. 2 est le seul nombre premier pair.

Remarque 3.0.3.
On appelle *diviseur strict* de n tout entier naturel diviseur de n différent de n. Un nombre premier est donc un entier autre que 1 sans diviseur strict autre que 1.

Remarque 3.0.4.
Soit p et q sont deux nombres premiers distincts. Alors p et q sont premiers entre eux.

Démonstration.
Par l'absurde, supposons $p \wedge q \neq 1$. Alors $p \wedge q$ est un diviseur de p et de q autre que 1. p et q étant premiers, ce ne peut être un diviseur strict, donc $p = p \wedge q = q$. Or $p \neq q$, donc c'est absurde. □

Le résultat suivant, fondamental, ainsi que la démonstration donnée, sont connus depuis Euclide :

Théorème 3.0.5.
L'ensemble des nombres premiers est infini.

Démonstration.
En effet, soient $p_1, \ldots, p_n$ n nombres premiers, avec $n \geqslant 1$. Montrons qu'il en existe nécessairement un autre.

On considère la quantité $p_1.p_2.\ldots.p_n+1$. Cette quantité est un entier strictement supérieur à 1. L'ensemble de ses diviseurs (positifs) différents de 1 est donc non vide et possède donc un plus petit élément q, différent de 1, qui ne peut posséder aucun diviseur strict autre que 1 : q est donc premier.

Alors q est nécessairement différent de tous les p_i. Car si $q = p_i$ pour un certain $i \in [\![1, n]\!]$, q divise $p_1.p_2.\ldots.p_n$ d'une part, et divise $p_1.p_2.\ldots.p_n + 1$ d'autre part, donc divise la différence qui vaut 1, ce qui est impossible.

q est donc un $(n+1)$ème nombre premier. □

Théorème 3.0.6.
Tout entier naturel supérieur ou égal à 1 se décompose de manière unique (à l'ordre des facteurs près) en un produit de nombres premiers (ce produit est éventuellement réduit à zéro ou un terme, et peut avoir plusieurs facteurs égaux). Plus précisément, pour tout $n \in \mathbb{N}\backslash\{0, 1\}$, il existe $k \in \mathbb{N}^*$, des entiers premiers $p_1, \ldots, p_k$ distincts et $\alpha_1, \ldots, \alpha_k \in \mathbb{N}^*$ tels que

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} = p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_k^{\alpha_k}.$$

Démonstration.Existence on en donne trois démonstrations

Principe de la descente infinie de Fermat Si n est un nombre ne se décomposant pas en facteurs premiers, alors n n'est lui-même pas premier (sinon, $n = n$ est une décomposition). Donc, n s'écrit $n = ab$, avec $1 < a < n$ et $1 < b < n$. n ne se décomposant pas en facteurs premiers, nécessairement, a ou b ne se décompose pas en facteurs premiers. On trouve donc, pour tout entier ne se décomposant pas en facteurs premiers, un entier strictement plus petit ne se décomposant pas en facteurs premiers. Ce qui est impossible, car en itérant le procédé, on construirait une suite strictement décroissante d'entiers.

Principe du bon ordre Soit A l'ensemble des entiers n'admettant pas de décomposition. Nous voulons montrer que A est vide. S'il était non vide, il y aurait un plus petit élément a. Si a n'admet pour diviseur que 1 et lui-même, a est premier. $a = a$ est une décomposition de a en facteurs premiers, ce qui est contraire à l'hypothèse. Donc a s'écrit $b \times c$ où b et c sont des entiers différents de a et de 1. a étant le minimum de A, b et c ne sont pas éléments de A et se décomposent donc en produit de facteurs premiers. Il en est donc de même de a.

Principe de récurrence On suppose que tout entier inférieur ou égal à n se décompose en produits de facteurs premiers (ce qui est vrai pour $n \leqslant 2$). Considérons $n + 1$:

- Si $n + 1$ est premier, alors $n + 1 = n + 1$ est une décomposition.
- Sinon, $n + 1 = ab$, avec $1 < a < n + 1$, et $1 < b < n + 1$. L'hypothèse de récurrence s'applique sur a et b, qui se décomposent donc en produits de facteurs premiers. Il en est donc de même de $n + 1$.

Unicité Commençons par remarquer que pour tout entier non nul p, $p^0 = 1$. Ainsi si $n = p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_k^{\alpha_k}$ et si p_{k+1} est un nombre premier distinct des k précédents, on peut écrire $n = p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_k^{\alpha_k}.p_{k+1}^{\alpha_{k+1}}$, avec $\alpha_{k+1} = 0$.
On suppose que n a deux décompositions en facteurs premiers, que l'on peut donc écrire $n = p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_k^{\alpha_k} = p_1^{\beta_1}.p_2^{\beta_2}.\ldots.p_k^{\beta_k}$, les deux membres étant éventuellement complétés par p^0 pour avoir les mêmes facteurs premiers dans les deux membres. Le théorème de Gauss permet de dire que $p_1^{\alpha_1}$ divise le membre de droite, mais puisqu'il est premier avec $p_2, \ldots, p_k$ car tous ces nombres premiers sont distincts, il divise $p_1^{\beta_1}$, et donc $\alpha_1 \leqslant \beta_1$. Symétriquement, $\alpha_1 \geqslant \beta_1$, et ainsi $\alpha_1 = \beta_1$. Il en est de même pour les autres puissances.

□

Définition 3.0.7.
Pour un nombre premier p on définit l'application

$$\begin{array}{rccl} \nu_p & : & \mathbb{Z} & \to & \mathbb{N} \cup \{ +\infty \} \\ & & n & \mapsto & \left\{ \begin{array}{l} +\infty \text{ si } n = 0 \\ \max \left\{ k \in \mathbb{N} \;\middle|\; p^k | n \right\} \quad \text{sinon} \end{array} \right. \end{array}$$

qui à un entier n associe l'exposant de p dans la décomposition de n en facteurs premiers, avec la convention $\nu_p(0) = +\infty$. Cette fonction est appelée *valuation p-adique sur* $\mathbb{Z}$.

Démonstration.
Il faut démontrer que $\max \left\{ k \in \mathbb{N} \;\middle|\; p^k | n \right\}$ existe bien. L'ensemble $\left\{ k \in \mathbb{N} \;\middle|\; p^k | n \right\}$ est non vide car il contient 0 ; de plus $p^k \xrightarrow[k \to +\infty]{} +\infty$, donc il existe $K \in \mathbb{N}$ tel que $p^K > n$, donc cet ensemble est majoré. Comme c'est une partie de $\mathbb{N}$, il admet bien un maximum. □

Exemple 3.0.8.
$\nu_5(50) = 2$, $\nu_3(50) = 0$.

Proposition 3.0.9.
Soient $a, b \in \mathbb{Z}$. On note $\mathscr{P}$ l'ensemble des nombres premiers.

(i) Pour tout entier p premier, p divise a si et seulement si $\nu_p(a) > 0$.

(ii) Si $a \neq 0$, $|a| = \prod_{p \in \mathscr{P}} p^{\nu_p(a)}$.

(iii) On a $a|b$ si et seulement si, pour tout $p \in \mathscr{P}$, $\nu_p(a) \leqslant \nu_p(b)$.

(iv) Si $(a, b) \neq (0, 0)$, $a \wedge b = \prod_{p \in \mathscr{P}} p^{\min(\nu_p(a), \nu_p(b))}$.

(v) si $a \neq 0$ et $b \neq 0$, $a \vee b = \prod_{p \in \mathscr{P}} p^{\max(\nu_p(a), \nu_p(b))}$

(vi) Les entiers a et b sont premiers entre eux si et seulement si ils n'ont aucun facteur premier en commun (*i.e.* pour tout p, $\nu_p(a) = 0$ ou $\nu_p(b) = 0$).

Démonstration. (i) Évident.

(ii) C'est une simple réécriture de la décomposition de a en facteurs premiers.

(iii) Si $a|b$, soit $p \in \mathscr{P}$. Alors, $p^{\nu_p(a)}$ divise a donc p, donc $\nu_p(b) \geqslant \nu_p(a)$.
Réciproquement, supposons que pour tout $p \in \mathscr{P}$, $\nu_p(a) \leqslant \nu_p(b)$. On voit alors dans la décomposition en facteurs premiers de b que l'on peut factoriser a dans b, donc $a|b$.

(iv) Commençons par remarquer que le produit considéré est bien défini : c'est un produit faisant intervenir une infinité de termes car $\mathscr{P}$ est infini, mais en fait seul un nombre fini de ces termes sont différents de 1. En effet, les diviseurs premiers de a sont en nombre fini, donc la valuation de a n'est non nulle que pour un nombre fini d'entiers premiers. Il en est de même pour b, et donc $\min(\nu_p(a), \nu_p(b))$ n'est non nulle que pour un nombre fini d'entiers premiers p.
On note $d = \prod_{p \in \mathscr{P}} p^{\min(\nu_p(a), \nu_p(b))}$. Alors :

$$d \times \prod_{p \in \mathscr{P}} p^{\nu_p(a) - \min(\nu_p(a), \nu_p(b))} = \prod_{p \in \mathscr{P}} p^{\nu_p(a)} = a$$
$$\text{et } d \times \prod_{p \in \mathscr{P}} p^{\nu_p(b) - \min(\nu_p(a), \nu_p(b))} = \prod_{p \in \mathscr{P}} p^{\nu_p(b)} = b$$

donc d est un diviseur commun à a et b.
Soit d' un autre diviseur commun à a et b. Alors d' s'écrit nécessairement : $d' = \prod_{p \in \mathscr{P}} p^{\delta(p)}$, avec pour tout p, $\delta(p) \in \mathbb{N}$, et il n'y a qu'un nombre fini d'entiers premiers p tels que $\delta(p) > 0$. Mais si $d'|a$, on doit avoir pour tout $p \in \mathscr{P}$, $\delta(p) \leqslant \nu_p(a)$. De même, $d'|b$ donc pour tout $p \in \mathscr{P}$, $\delta(p) \leqslant \nu_p(b)$. On a donc pour tout $p \in \mathscr{P}$, $\delta(p) \leqslant \min(\nu_p(a), \nu_p(b))$, et par conséquent $d'|d$, et d est bien le pgcd de a et b.

(v) S'inspirer de la démonstration du point précédent.

(vi)
$$\begin{array}{ll} & a \text{ et } b \text{ sont premiers entre eux} \\ \Leftrightarrow & a \wedge b = 1 \\ \Leftrightarrow & \text{pour tout entier premier } p, \\ & \nu_p(a \wedge b) = 0 \\ \Leftrightarrow & \text{pour tout entier premier } p, \\ & \min(\nu_p(a), \nu_p(b)) = 0 \\ \Leftrightarrow & \text{pour tout entier premier } p, \\ & \nu_p(a) = 0 \text{ ou } \nu_p(b) = 0 \\ \Leftrightarrow & \text{pour tout entier premier } p, \; p \text{ ne} \\ & \text{divise pas } a \text{ ou } p \text{ ne divise pas } b \\ \Leftrightarrow & \text{ils n'ont aucun facteur premier} \\ & \text{en commun.} \end{array}$$

□

Finissons par un dernier résultat classique, le petit théorème de Fermat (Pierre de, Beaumont-de-Lomagne, première décennie du XVIIe siècle - Castres, 1665) (le grand n'est malheureusement pas à notre portée), qui a deux formulations équivalentes :

Théorème 3.0.10 (Petit théorème de Fermat, 1640)**.**
Soit p un nombre premier. Alors on a :

(i) pour tout $a \in \mathbb{Z}$, p divise $a^p - a$.

(ii) pour tout $a \in \mathbb{Z}$ qui n'est pas un multiple de p, p divise $a^{p-1} - 1$.

Démonstration.
Ce théorème admet plus de 100 démonstrations. Fermat disait en connaître une mais ne l'a jamais publiée et elle n'est pas parvenue jusqu'à nous. La première démonstration est dûe à Leibniz en 1683, dans un manuscrit qui lui non plus n'a pas été publié. Il faut attendre 1736 pour qu'Euler donne la première démonstration publique, qui est essentiellement la même que celle de Leibniz.
Un petit nombre de ces démonstrations ainsi qu'une introduction historique peuvent être lus à l'adresse suivante, sur le site de l'ENS :

http ://preview.tinyurl.com/pm49tb4

Donnons-en encore une autre :

Commençons par montrer l'équivalence des deux énoncés [1] :
Si (i) est vrai et que a n'est pas un multiple de p, alors puisque p est premier, a et p sont premiers entre eux. Par conséquent, grâce au théorème de Gauss, $p|a(a^{p-1} - 1)$ donc $p|a^{p-1} - 1$.
Si (ii) est vrai, soit $a \in \mathbb{Z}$. Si a est un multiple de p, $p|a$ donc $p|a(a^{p-1} - 1)$. Et si a n'est pas un multiple de p, alors avec (ii) $p|a^{p-1} - 1$ donc $p|a(a^{p-1} - 1)$. Dans tous les cas, (i) est vrai.

Montrons maintenant le point (ii).
Soit a un entier non multiple de p. Posons $N = a(2a)(3a)...((p-1)a)$. Nous allons calculer N modulo p de deux manières.

Tout d'abord, réécrivons $N = a^{p-1} \times (p-1)!$.

Ensuite, pour tout $i \in [\![1, p-1]\!]$, appelons r_i le reste de la division euclidienne de ia par p. Alors $N \equiv r_1 r_2 \dots r_{p-1}\ [p]$. Supposons qu'il existe $i, j \in [\![1, p-1]\!]$ tels que $r_i = r_j$. Alors $ia \equiv ja\ [p]$ donc $p|(i-j)a$. Or $a \wedge p = 1$ donc avec le théorème de Gauss, $p|(i-j)$. Mais $|i-j| < p$ donc nécessairement $i - j = 0$, donc $i = j$. Ainsi les $r_1, \dots, r_{p-1}$ sont deux à deux distincts. Mais comme ils sont tous dans l'intervalle $[\![1, p-1]\!]$, qui contient exactement $p-1$ éléments, $\{r_1, \dots, r_{p-1}\} = [\![1, p-1]\!]$, et donc $r_1 r_2 \dots r_{p-1} = (p-1)!$.

Finalement, $N = a^{p-1} \times (p-1)! \equiv (p-1)!\ [p]$, donc $p|(p-1)!(a^{p-1} - 1)$. Or p est premier avec tous les entiers de 1 à $p-1$, donc il est premier avec $(p-1)!$, et à nouveau avec le théorème de Gauss, il vient bien $p|a^{p-1} - 1$. □

Le Petit théorème de Fermat donne donc une condition nécessaire pour qu'un nombre entier soit premier. Il est d'ailleurs très largement utilisé dans les tests de primalité, comme celui de Rabin-Miller. Mais, sa réciproque étant fausse, il n'est pas possible de savoir de manière certaine qu'un nombre est premier en n'utilisant que ce théorème. Ainsi, on appelle *nombres de Carmichael* ou *menteurs de Fermat* les nombres entiers qui ne sont pas premiers mais vérifient tout de même le Petit théorème de Fermat. Le plus petit nombre de Carmichael est 561, et a été découvert par Carmichael en 1910, bien que les propriétés de tels nombres aient déjà été énoncées en 1899 par Korselt. Les nombres de Carmichael étant relativement rares par rapport aux nombres premiers, un test de primalité basé sur le petit théorème de Fermat aura peu de chances de donner un résultat erroné, mais il n'est cependant pas considéré comme un test suffisament fiable. C'est pourquoi on le combine avec d'autres tests pour obtenir des tests de primalité probabilistes plus fiables.

1. Ici, nous n'avons besoin que de montrer que (ii) implique (i) puisque nous allons montrer (i) par la suite.

Chapitre X

Suites réelles et complexes

1 Vocabulaire

Définition 1.0.1 (Suite réelle)**.**
• Une *suite à valeurs réelles* ou *suite réelle* u est une application de $\mathbb{N}$ dans $\mathbb{R}$, u. On note en général u_n au lieu de $u(n)$ l'image de n par u.
• Étant donnée une expression e contenant la variable n, on note $(e)_{n\in\mathbb{N}}$ la suite $\begin{array}{ccc} \mathbb{N} & \to & \mathbb{R} \\ n & \mapsto & e \end{array}$.
Ainsi, la suite u est souvent notée $(u_n)_{n\in\mathbb{N}}$.
• La suite $(u_n)_{n\in\mathbb{N}}$ est aussi appelée *la suite de terme général* u_n.
• On note $\mathbb{R}^{\mathbb{N}}$ l'ensemble des suites réelles.

Remarque 1.0.2 (Représentation graphique des termes d'une suite)**.**
Cela peut se faire en plaçant les termes sur la droite des réels (représentation unidimensionnelle) ou en traçant le "graphe" de la suite (représentation bidimensionnelle). Chacune présente des avantages et des inconvénients.

Définition 1.0.3 (Opérations sur les suites)**.**
• Étant donné deux suites u et v on peut former leur somme $u+v$, définie comme $(u_n+v_n)_{n\in\mathbb{N}}$.
• Étant donnéune suite u et un scalaire λ, on peut former la suite λu définie comme $(\lambda u_n)_{n\in\mathbb{N}}$.
• On dit que $\mathbb{R}^{\mathbb{N}}$ muni de ces deux opérations est un *espace vectoriel*.
• Étant donné deux suites u et v on peut former leur produit uv, définie comme $(u_nv_n)_{n\in\mathbb{N}}$.
• Étant donné deux suites u et v telles que v ne s'annule pas, on peut former leur quotient $\dfrac{u}{v}$, définie comme $\left(\dfrac{u_n}{v_n}\right)_{n\in\mathbb{N}}$.
• Étant donné une suite u , on peut former la suite $|u|$ définie comme $(|u_n|)_{n\in\mathbb{N}}$.

Définition 1.0.4.
• Étant donné une propriété P sur les suites réelles et un entier n_0 et une suite réelle u, on dit que P est *vraie à partir du rang* n_0 si la propriété P est vraie pour la suite des termes u_{n_0}, u_{n_0+1}, u_{n_0+2}, ... autrement dit pour la suite v où v est définie par $\forall n\in\mathbb{N}\ v_n = u_{n_0+n}$.
• On dit que P est *vraie à partir d'un certain rang* s'il existe un entier n_0 tel que la propriété P est vraie à partir du rang n_0.

Remarque 1.0.5.
En général, seul le comportement des suites quand n tend vers l'infini nous intéresse, et non les premiers termes de la suite, d'où l'intérêt de la notion de propriété vraie à partir d'un certain rang.

Exemple 1.0.6.
• La suite $(n(n-5))_{n\in\mathbb{N}}$ n'est pas à valeurs positives ou nulles mais elle est à valeurs positives ou nulles à partir du rang 5 (ainsi d'ailleurs qu'à partir du rang 10, du rang 2389, ...).
• La suite u définie par

$$\forall n\in\mathbb{N}\ u_n = \begin{cases} n & \text{si } n<735 \\ 735 & \text{sinon} \end{cases}$$

n'est pas constante mais est constante à partir du rang 735.

Exemple 1.0.7.
Dire qu'une suite est positive ou nulle à partir d'un certain rang est équivalent à

$$\exists n_0\in\mathbb{N},\ \forall n\in\mathbb{N},\quad u_{n+n_0}\geqslant 0,$$

autrement dit :

$$\exists n_0\in\mathbb{N},\ \forall k\in\mathbb{N},\ k\geqslant n_0\Rightarrow u_k\geqslant 0.$$

Définition 1.0.8.
Une suite réelle u est dite :

(i) *constante* si $\forall n\in\mathbb{N},\ u_n = u_0$;

(ii) *stationnaire* si elle est constante à partir d'un certain rang, c'est-à-dire si

$$\exists n_0\in\mathbb{N}\ \forall n\in\mathbb{N},\ n\geqslant n_0\Rightarrow u_n = u_{n_0}.$$

Remarque 1.0.9.
Jusque là, toutes les définitions données sur les suites à valeurs réelles s'étendent directement aux suites à valeurs complexes. Ce n'est plus le cas pour ce qui suit.

Définition 1.0.10.
Une suite réelle u est dite :

(i) *croissante* (resp. *stric. croissante*) si pour tout $n \in \mathbb{N}$, $u_n \leqslant u_{n+1}$ (resp. $u_n < u_{n+1}$) ;

(ii) *décroissante* (resp. *stric. décroissante*) si pour tout $n \in \mathbb{N}$, $u_n \geqslant u_{n+1}$ (resp. $u_n > u_{n+1}$) ;

(iii) *monotone* si la suite est croissante ou décroissante ;

(iv) *strictement monotone* si la suite est strictement croissante ou strictement décroissante ;

(v) *majorée* (resp. *minorée*) s'il existe $M \in \mathbb{R}$ tel que pour tout $n \in \mathbb{N}$, $u_n \leqslant M$ (resp. $u_n \geqslant M$) ;

(vi) *bornée* si elle est majorée et minorée.

Remarque 1.0.11.
• Toutes ces propriétés peuvent s'énoncer « à partir d'un certain rang ».
• « (u_n) est bornée » s'écrit aussi : $\exists M \in \mathbb{R}$, $\forall n \in \mathbb{N}$, $|u_n| \leqslant M$.
• Pour montrer qu'une suite est croissante, on peut utiliser plusieurs méthodes : la plus classique consiste à étudier le signe de $u_{n+1} - u_n$. On peut aussi comparer $\dfrac{u_{n+1}}{u_n}$ à 1, **à condition de connaître le signe de** u_n.

2 Limite d'une suite réelle

2.1 Définition et premières propriétés

Définition 2.1.1.
Soit $(u_n) \in \mathbb{R}^{\mathbb{N}}$, soit $\ell \in \mathbb{R}$. On dit que (u_n) tend (ou converge) vers ℓ si

$$\forall \varepsilon \in \mathbb{R}_+^*,\ \exists n_0 \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geqslant n_0 \Rightarrow |u_n - \ell| \leqslant \varepsilon.$$

On note ceci $u_n \xrightarrow[n\to+\infty]{} \ell$, ou plus simplement $u \to \ell$.

Remarque 2.1.2.
Ceci est équivalent à

$$\forall \varepsilon \in \mathbb{R}_+^*,\ \exists n_0 \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geqslant n_0 \Rightarrow |u_n - \ell| < \varepsilon.$$

En pratique, on préférera souvent (mais pas toujours) utiliser des inégalités larges.

Remarque 2.1.3.
On utilise souvent les abus de notation suivant :

$$\forall \varepsilon > 0,\ \exists n_0 \in \mathbb{N},\ \forall n \geqslant n_0,\ |u_n - \ell| \leqslant \varepsilon.$$

Exemple 2.1.4.
Montrer que la suite de terme général $u_n = \dfrac{n-1}{n+1}$ converge vers 1.

Définition 2.1.5.
Soit $(u_n) \in \mathbb{R}^{\mathbb{N}}$. On dit que (u_n) est convergente s'il existe $\ell \in \mathbb{R}$ tel que $u_n \xrightarrow[n\to+\infty]{} \ell$. Si (u_n) n'est pas convergente, on dit qu'elle est divergente (ou diverge).

Théorème 2.1.6.
Toute suite convergente est bornée.

Démonstration.
Soit (u_n) convergeant vers $\ell \in \mathbb{R}$. Alors d'après la proposition précédente, il existe $n_0 \in \mathbb{N}$ tel que pour tout $n \geqslant n_0$, $|u_n - \ell| \leqslant 1$, et donc $\ell - 1 \leqslant u_n \leqslant \ell + 1$. Par conséquent, (u_n) est bornée à partir du rang n_0. Mais les n_0 premiers termes de la suite étant en nombre fini, ils forment un ensemble borné. L'ensemble des termes de la suite (u_n) étant la réunion de deux ensembles bornées, il est borné également, et donc la suite (u_n) est bornée. □

Définition 2.1.7.
Soit $(u_n) \in \mathbb{R}^{\mathbb{N}}$. On dit que (u_n) tend vers $+\infty$ si

$$\forall A \in \mathbb{R},\ \exists n_0 \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geqslant n_0 \Rightarrow u_n \geqslant A.$$

On note ceci $u_n \xrightarrow[n\to+\infty]{} +\infty$, ou plus simplement $u \to +\infty$.

Définition 2.1.8.
Soit $(u_n) \in \mathbb{R}^{\mathbb{N}}$. On dit que (u_n) tend vers $-\infty$ si

$$\forall A \in \mathbb{R},\ \exists n_0 \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geqslant n_0 \Rightarrow u_n \leqslant A.$$

On note ceci $u_n \xrightarrow[n\to+\infty]{} -\infty$, ou plus simplement $u \to -\infty$.

Remarque 2.1.9.
Une suite qui tend vers $+\infty$ (ou vers $-\infty$) diverge.

On peut cependant introduire l'ensemble $\overline{\mathbb{R}} = \mathbb{R} \cup \{+\infty, -\infty\}$, que l'on appelle *droite numérique achevée*. Dans $\overline{\mathbb{R}}$, une suite tendant vers $+\infty$ (ou moins $-\infty$) converge. Le théorème **??** est toujours valable : toute suite à valeurs dans $\overline{\mathbb{R}}$ est bornée (par $-\infty$ et $+\infty$) !

Par défaut, la notion de convergence s'entendra dans $\mathbb{R}$. Le lecteur intéressé pourra consulter la partie **??** pour obtenir une présentation succinte unifiant ces points de vues.

Théorème 2.1.10 (Unicité de la limite)**.**
Soit (u_n) une suite réelle, soit $\ell_1, \ell_2 \in \overline{\mathbb{R}}$ tels que $u_n \xrightarrow[n\to+\infty]{} \ell_1$ et $u_n \xrightarrow[n\to+\infty]{} \ell_2$. Alors, $\ell_1 = \ell_2$.

Démonstration.
Il convient *a priori* de distinguer 9 cas. Par symétrie, et en supposant $\ell_1 \neq \ell_2$, il suffit de considérer les cas :
- $\ell_1 \in \mathbb{R}$ et $\ell_2 \in \mathbb{R}$;
- $\ell_1 \in \mathbb{R}$ et $\ell_2 = -\infty$;
- $\ell_1 \in \mathbb{R}$ et $\ell_2 = +\infty$;
- $\ell_1 = -\infty$ et $\ell_2 = +\infty$.

Nous ne détaillerons ici que les deux premiers, les deux derniers sont laissés au lecteur.

Si $\ell_1 \in \mathbb{R}$ et $\ell_2 \in \mathbb{R}$, posons $\varepsilon = \frac{1}{3}|\ell_1 - \ell_2| > 0$. Alors, il existe $n_1, n_2 \in \mathbb{N}$ tels que, pour tout $n \in \mathbb{N}$:
- si $n \geqslant n_1$, $|u_n - \ell_1| \leqslant \varepsilon$;
- si $n \geqslant n_2$, $|u_n - \ell_2| \leqslant \varepsilon$.

Alors, pour $n \geqslant \max(n_1, n_2)$, on a par l'inégalité triangulaire

$$\begin{aligned} |\ell_1 - \ell_2| &= |\ell_1 - u_n - (\ell_2 - u_n)| \\ &\leqslant |\ell_1 - u_n| + |\ell_2 - u_n| \\ &\leqslant \frac{2}{3}|\ell_1 - \ell_2|. \end{aligned}$$

C'est impossible !

Si $\ell_1 \in \mathbb{R}$ et $\ell_2 = -\infty$, posons $A = \ell_1 - 1$ et $\varepsilon = \frac{1}{2}$. Alors, il existe $n_1, n_2 \in \mathbb{N}$ tels que, pour tout $n \in \mathbb{N}$:
- si $n \geqslant n_1$, $|u_n - \ell_1| \leqslant \varepsilon$;
- si $n \geqslant n_2$, $u_n \leqslant A$.

Alors, pour $n \geqslant \max(n_1, n_2)$, on a $u_n \leqslant A < \ell_1 - \frac{1}{2} \leqslant u_n$.
C'est impossible ! □

Définition 2.1.11 (Limite)**.**
Soit $u \in \mathbb{R}^{\mathbb{N}}$. Lorsqu'il existe un élément $\ell \in \overline{\mathbb{R}}$ vérifiant $u_n \xrightarrow[n\to+\infty]{} \ell$, on l'appelle **la** *limite* de u, et on le note $\lim u$ ou $\lim\limits_{n\to+\infty} u_n$.


Le symbole $\lim\limits_{n\to+\infty}$ ne peut s'utiliser qu'après avoir montré l'existence de ladite limite. L'utiliser avant est une erreur grave. On préfèrera *systématiquement* utiliser l'écriture $u_n \xrightarrow[n\to+\infty]{} \ell$.

Proposition 2.1.12.
Soit $u \in \mathbb{R}^{\mathbb{N}}$ et $\ell \in \mathbb{R}$. On a les propriétés suivantes :

$$u_n \xrightarrow[n\to+\infty]{} \ell \iff u_n - \ell \xrightarrow[n\to+\infty]{} 0$$
$$u_n \xrightarrow[n\to+\infty]{} 0 \iff |u_n| \xrightarrow[n\to+\infty]{} 0$$

Remarque 2.1.13.
En particulier pour tout $\ell \in \mathbb{R}$ et tout $u \in \mathbb{R}^{\mathbb{N}}$, $u \xrightarrow[+\infty]{} \ell$ si et seulement si u s'écrit comme somme de ℓ et d'une suite tendant vers 0.

Corollaire 2.1.14.
Soit $u \in \mathbb{R}^{\mathbb{N}}$ et $\ell \in \mathbb{R}$.

$$u_n \xrightarrow[n\to+\infty]{} \ell \iff |u_n - \ell| \xrightarrow[n\to+\infty]{} 0$$

Corollaire 2.1.15.
Soit $u \in \mathbb{R}^{\mathbb{N}}$, $\ell \in \mathbb{R}$. Alors u tend vers ℓ si et seulement s'il existe $v \in \mathbb{R}^{\mathbb{N}}$ tendant vers 0 telle que $u = \ell + v$.

Proposition 2.1.16.
Soit u une suite convergeant vers 0 et v une suite bornée. Alors uv converge vers 0.

Démonstration.
Soit $M > 0$ un majorant de $|v|$. Soit $\varepsilon > 0$, il existe donc un rang $N \in \mathbb{N}$ tel que pour, tout entier naturel $n \geqslant N$, $|u_n| \leqslant \dfrac{\varepsilon}{M}$. Ainsi, si $n \geqslant N$, $|u_n v_n| \leqslant \varepsilon$, d'où le résultat. □

Exemple 2.1.17.
Étudier la convergence de la suite $\left(\frac{\cos n}{n}\right)_{n\in\mathbb{N}^*}$

Proposition 2.1.18.
L'ensemble des suites convergeant vers 0 est stable par addition et par multiplication par un scalaire. On dit que l'ensemble des suites convergeant vers 0 est *un sous-espace vectoriel de l'espace vectoriel des suites à valeur réelles.*

Démonstration.
Comme un scalaire peut-être vu comme une suite constante, donc bornée, il suffit de montrer que la somme de deux suites convergeant vers 0 converge vers 0.

Soit u et v tendant vers 0, soit $\varepsilon > 0$. Il existe deux rangs $N \in \mathbb{N}$ et $N' \in \mathbb{N}$ tels que, pour tout entier n,

— si $n \geqslant N$, $|u_n| \leqslant \dfrac{\varepsilon}{2}$;

— si $n \geqslant N'$, $|v_n| \leqslant \dfrac{\varepsilon}{2}$.

Ainsi, si $n \geqslant \max(N, N')$, alors $|u_n + v_n| \leqslant |u_n| + |v_n| \leqslant \varepsilon$, d'où le résultat. □

2.2 Opérations sur les limites

Soit u et v deux suites qui admettent chacune pour limite $\ell, \ell' \in \overline{\mathbb{R}}$.

a Étude de $(u_n + v_n)_{n\in\mathbb{N}}$

u_n \ v_n	$\ell' \in \mathbb{R}$	$+\infty$	$-\infty$
$\ell \in \mathbb{R}$			
$+\infty$			
$-\infty$			

b Étude de $(u_n v_n)_{n\in\mathbb{N}}$

u_n \ v_n	$\ell' \in \mathbb{R}_+^*$	$\ell' \in \mathbb{R}_-^*$	0	$+\infty$	$-\infty$
$\ell \in \mathbb{R}_+^*$					
$\ell \in \mathbb{R}_-^*$					
0					
$+\infty$					
$-\infty$					

c Étude de $\left(\frac{1}{u_n}\right)_{n\in\mathbb{N}}$

Si la suite u ne s'annule pas.

Remarque 2.2.1.
Si v tend vers 0, alors $\dfrac{1}{1+v}$ tend vers 1.

$u_n \to$	$\ell \in \mathbb{R}\setminus\{0\}$	0	$+\infty$	$-\infty$
$1/u_n \to$				

On obtient alors le comportement de $\left(\dfrac{u_n}{v_n}\right)_{n\in\mathbb{N}}$ en utilisant les deux tableaux précédents.

d Étude de $(|u_n|)_{n\in\mathbb{N}}$

$u_n \to$	$\ell \in \mathbb{R}$	$+\infty$	$-\infty$
$\lvert u_n\rvert \to$			

e Étude de $(\max(u_n, v_n))_{n\in\mathbb{N}}$

Proposition 2.2.2.
Si $u_n \xrightarrow[n\to+\infty]{} \ell \in \overline{\mathbb{R}}$ et $v_n \xrightarrow[n\to+\infty]{} \ell' \in \overline{\mathbb{R}}$, alors $\max(u_n, v_n) \xrightarrow[n\to+\infty]{} \max(\ell, \ell')$.

Démonstration.
Il suffit d'écrire $\max(u_n, v_n) = \dfrac{|u_n - v_n| + u_n + v_n}{2}$. □

Remarque 2.2.3.
On a bien sûr le même résultat avec le minimum.

f Exemples de formes indéterminées

Exemple 2.2.4.
Déterminer les limites (si elles existent) des suites de termes généraux suivants :

1. $u_n = \frac{3n^2+n+15}{n^2+\sin n}$
2. $u_n = \frac{\mathrm{e}^n-3^n}{n^2-2^n}$
3. $u_n = \left(1+\dfrac{1}{n}\right)^n$.

2.3 Limites et suites extraites

Définition 2.3.1.
On appelle *suite extraite ou sous-suite de la suite* u toute suite $(u_{\varphi(n)})_{n\in\mathbb{N}}$ où φ est une application strictement croissante de $\mathbb{N}$ dans $\mathbb{N}$. La fonction φ est une *extraction*, ou *extractrice*.

Remarque 2.3.2.
On ne conserve que les termes de rang $\varphi(n)$ pour $n \in \mathbb{N}$, d'où la dénomination suite extraite.

Exemple 2.3.3.
$(u_{n+1})_{n\in\mathbb{N}}$, $(u_{2n})_{n\in\mathbb{N}}$ et $(u_{2n+1})_{n\in\mathbb{N}}$ sont des suites extraites de $(u_n)_{n\in\mathbb{N}}$.

Exercice 2.3.4.
Soit u une suite, φ et ψ deux extractrices. Quelle est la suite extraite de $(u_{\varphi(n)})_{n\in\mathbb{N}}$ par ψ ?

Lemme 2.3.5.
Soit φ une fonction strictement croissante de $\mathbb{N}$ dans $\mathbb{N}$. Alors pour tout $n \in \mathbb{N}$, $\varphi(n) \geqslant n$.

Théorème 2.3.6.
Soit $u \in \mathbb{R}^{\mathbb{N}}$ et $\ell \in \overline{\mathbb{R}}$. Si $u \xrightarrow[+\infty]{} \ell$ alors toute suite extraite de u tend aussi vers ℓ.

Démonstration.
On traite le cas $\ell \in \mathbb{R}$, les deux autres cas sont laissés au lecteur.

Soit φ une extractrice, soit $\varepsilon > 0$. Il existe donc un rang $n_0 \in \mathbb{N}$ tel que , pour tout $n \geqslant n_0$, $|u_n - \ell| \leqslant \varepsilon$. Soit $n \geqslant n_0$, on a alors $\varphi(n) \geqslant n \geqslant n_0$ et donc $\left|u_{\varphi(n)} - \ell\right| \leqslant \varepsilon$. □

Corollaire 2.3.7.
• Si une suite admet deux suites extraites ne convergeant pas vers la même limite alors cette suite n'a pas de limite.
• Si une suite admet une suite extraite n'ayant pas de limite, alors cette suite n'a pas de limite.

Exemple 2.3.8.
Montrer que les suites $((-1)^n)_{n\in\mathbb{N}}$ et $\left(\cos\frac{n\pi}{3}\right)_{n\in\mathbb{N}}$ ne convergent pas.

Théorème 2.3.9.
Soit u une suite à valeurs réelles et $\ell \in \overline{\mathbb{R}}$. Si on a $u_{2n} \xrightarrow[n\to+\infty]{} \ell$ et $u_{2n+1} \xrightarrow[n\to+\infty]{} \ell$, alors $u_n \xrightarrow[n\to+\infty]{} \ell$.

Démonstration.
On traite le cas $\ell \in \mathbb{R}$, les deux autres cas sont laissés au lecteur.

Soit $\varepsilon > 0$ un voisinage de ℓ. Il existe donc deux rangs N et N' tels que, pour tout entier naturel n,
— si $n \geqslant N$, $|u_{2n} - \ell| \leqslant \varepsilon$;
— si $n \geqslant N'$, $|u_{2n+1} - \ell| \leqslant \varepsilon$.
Ainsi, si $n \geqslant \max(2N, 2N'+1)$, on a $|u_n - \ell| \leqslant \varepsilon$ (il suffit de distinguer selon la parité de N), d'où le résultat. □

2.4 Limites et inégalités

Proposition 2.4.1.
Soit $u \in \mathbb{R}^N$ et $(a, b, \ell) \in \mathbb{R}$. Supposons $u \xrightarrow[+\infty]{} \ell$ et $a < \ell < b$. Alors à partir d'un certain rang, les

valeurs de u sont comprises strictement entre a et b. Autrement dit :

$$\exists n_0 \in \mathbb{N} \ \forall n \in \mathbb{N} \ n \geqslant n_0 \Rightarrow a < u_n < b$$

Démonstration.
On pose $\varepsilon = \frac{1}{2}\min(\ell - a; b - \ell) > 0$. Soit $n_0 \in \mathbb{N}$ tel que, pour tout $n \geqslant n_0$, $|u_n - \ell| \leqslant \varepsilon$. On a $a < \ell - \varepsilon < \ell + \varepsilon < b$,
Alors, si $n \geqslant n_0$, on a $\ell - \varepsilon \leqslant u_n \leqslant \ell + \varepsilon$, donc $a < u_n < b$. □

Corollaire 2.4.2.
En particulier toute suite convergeant vers une limite strictement positive (resp. strictement négative) est strictement positive (resp. strictement négative) à partir d'un certain rang.

Corollaire 2.4.3.
Soit $u \in \mathbb{R}^{\mathbb{N}}$ et $(a, \ell) \in \mathbb{R}^2$. Supposons $u \xrightarrow[n\to+\infty]{} \ell$.
- Si à partir d'un certain rang $u_n \leqslant a$, alors $\ell \leqslant a$.
- Si à partir d'un certain rang $a \leqslant u_n$, alors $a \leqslant \ell$.

 Ne pas croire que si à partir d'un certain rang $u_n < a$, alors $\ell < a$. En passant à la limite dans une inégalité, les inégalités strictes deviennent des inégalités larges. (Par exemple : la suite $\left(\frac{1}{n}\right)_{n\in\mathbb{N}^*}$ converge vers 0, et pourtant tous les termes sont strictement positifs).

Corollaire 2.4.4.
Soient u et v deux suites réelles telles que, à partir d'un certain rang, $u_n \leqslant v_n$. Si les suites u et v convergent respectivement vers ℓ et ℓ', alors $\ell \leqslant \ell'$.

 Là encore, même si à partir d'un certain rang, $u_n < v_n$, il se peut que $\ell = \ell'$.

Exemple 2.4.5.
$\forall n \in \mathbb{N}^*,\ 1 - \frac{1}{n} < 1 + \frac{1}{n}$, pourtant $1 - \frac{1}{n} \xrightarrow[n\to+\infty]{} 1$ et $1 + \frac{1}{n} \xrightarrow[n\to+\infty]{} 1$.

Exercice 2.4.6.
Montrer que la suite $(H_n) = \left(\sum_{k=1}^{n} \frac{1}{k}\right)_{n\in\mathbb{N}^*}$ ne converge pas. On pourra commencer par montrer que pour tout $n \geqslant 1$, $H_{2n} - H_n \geqslant \frac{1}{2}$.

Proposition 2.4.7.
Si une suite $(u_n)_{n\in\mathbb{N}}$ est croissante (resp. décroissante) et converge vers un réel ℓ, alors $\forall n \in \mathbb{N},\ u_n \leqslant \ell$ (resp. $\forall n \in \mathbb{N},\ u_n \geqslant \ell$).

Si une suite $(u_n)_{n\in\mathbb{N}}$ est strict. croissante (resp. strict. décroissante) et converge vers un réel ℓ alors $\forall n \in \mathbb{N},\ u_n < \ell$ (resp. $\forall n \in \mathbb{N},\ u_n > \ell$).

Démonstration.
On ne traite que le premier cas. S'il existe $N \in \mathbb{N}$ tel que $u_n > \ell$ alors, si $n \geqslant N$, $u_n - \ell \geqslant u_N - \ell > 0$, ce qui est impossible. □

Remarque 2.4.8.
Ces propriétés ne permettent pas de montrer la convergence d'une suite. Elles se contentent de donner des renseignements sur la suite ou sa limite, *en cas de convergence.*

3 Résultats de convergence

3.1 Composition

Théorème 3.1.1.
Soient a et b deux éléments de $\overline{\mathbb{R}}$ et f une fonction à valeurs réelles définie sur une partie D de $\mathbb{R}$ vérifiant

$$f(x) \xrightarrow[x\to a]{} b$$

et u une suite réelle telle que la suite $(f(u_n))_{n\in\mathbb{N}}$ soit bien définie (c'est-à-dire vérifiant $\forall n \in \mathbb{N}\ u_n \in D$) et vérifiant

$$u_n \xrightarrow[n\to+\infty]{} a.$$

Alors,
$$f(u_n) \xrightarrow[n\to+\infty]{} b.$$

Remarque 3.1.2.
Ce théorème est temporairement admis, la définition de convergence pour les fonctions n'ayant pas encore été donnée.

Exemple 3.1.3.
Si u est une suite qui converge vers 0, alors la suite $(\mathrm{e}^{u_n})_{n\in\mathbb{N}}$ est une suite convergeant vers 1.

3.2 Utilisation d'inégalités

a Techniques d'encadrement

Théorème 3.2.1.
Soient u, v et w trois suites à valeurs réelles et $\ell \in \mathbb{R}$.

(i) **Th. de minoration :** Si $u_n \xrightarrow[n\to+\infty]{} +\infty$ et $u_n \leqslant v_n$ à partir d'un certain rang, alors $v_n \xrightarrow[n\to+\infty]{} +\infty$.

(ii) **Th. de majoration :** Si $u_n \xrightarrow[n\to+\infty]{} -\infty$ et $v_n \leqslant u_n$ à partir d'un certain rang, alors $v_n \xrightarrow[n\to+\infty]{} -\infty$.

(iii) **Th. d'encadrement :** Si $u_n \xrightarrow[n\to+\infty]{} \ell$ et $w_n \xrightarrow[n\to+\infty]{} \ell$ et $u_n \leqslant v_n \leqslant w_n$ à partir d'un certain rang, alors $v_n \xrightarrow[n\to+\infty]{} \ell$.

Remarque 3.2.2.
Le troisième résultat est souvent appelé « Théorème des gendarmes » dans les petites classes. Vous pouvez utiliser cette dénomination, ou tout simplement dire « par encadrement » quand vous l'utilisez.

Démonstration.
Ces trois résultats se démontrent aisément. □

Corollaire 3.2.3.
Soient u et v deux suites à valeurs réelles.
Si $v_n \xrightarrow[n\to+\infty]{} 0$ et $|u_n| \leqslant v_n$ à partir d'un certain rang, alors $u_n \xrightarrow[n\to+\infty]{} 0$.

b Suites monotones

Théorème 3.2.4 (de la limite monotone)**.**
Soit u une suite réelle.

1. Si u est croissante, elle admet une limite (dans $\overline{\mathbb{R}}$) et
$$u_n \xrightarrow[n\to+\infty]{} \sup_{n\in\mathbb{N}} u_n.$$
   (a) Dans le cas où u est majorée par un réel, cette limite est réelle et est le plus petit majorant de u.
   (b) Dans le cas où u n'est pas majorée, cette limite vaut $+\infty$.
2. Même résultat, dans le cas d'une suite u décroissante *mutatis mutandis* (sup en inf, «majorée» en «minorée», $+\infty$ en $-\infty$).

Démonstration. 1. (a) Notons $\ell = \sup_{n\in\mathbb{N}} u_n$. Soit $\varepsilon > 0$, il existe donc un entier naturel n_0 tel que $\ell - \varepsilon < u_{n_0} \leqslant \ell$. Par croissance de u et majoration de u par ℓ, on a, pour tout $n \geqslant n_0$, $\ell - \varepsilon \leqslant u_n \leqslant \ell$. Cela montre donc bien la convergence de u vers ℓ.
(b) Soit $A \in \mathbb{R}$, A ne majore pas u : il existe donc $n_0 \in \mathbb{N}$ tel que $u_{n_0} \geqslant A$. Ainsi, par croissance de u, on a, pour tout $n \geqslant n_0$, $u_n \geqslant A$. Ainsi, u tend vers $+\infty$.
2. Idem
□

Exemple 3.2.5.
On exprime souvent le premier point du théorème en disant que «toute suite croissante majorée converge». Soit u et v les suites définies par
$$\forall n \in \mathbb{N} \quad u_n = n \text{ et } v_n = n + n^2$$
La suite u est croissante, majorée par la suite v : c'est donc une suite croissante majorée. Donc u converge ?

 Une suite croissante majorée converge vers le plus petit de tous ses majorants. Le plus petit de ses majorants n'est **pas** nécessairement le plus petit de ceux que vous avez déjà trouvés ! Retenir :

Corollaire 3.2.6.
Si u est croissante et majorée par $M \in \mathbb{R}$, alors u converge et sa limite est inférieure ou égale à M.

c Suites adjacentes

Définition 3.2.7.
Deux suites u et v sont dites *adjacentes* si l'une est croissante, l'autre est décroissante et leur différence tend vers 0.

Théorème 3.2.8.
Soit u et v deux suites adjacentes. Alors u et v convergent, et ont la même limite.

Démonstration.
Si u et v convergent, $u - v$ converge vers la différence de leurs limites, soit 0 : u et v ont donc même limite.

On peut supposer, sans perte de généralité, que u est croissante et que v est décroissante. Montrons maintenant que u converge (il suffit ensuite d'écrire $v = v - u + u$ pour conclure à la convergence de v). Il suffit de montrer que u est majorée par un réel, par exemple v_0. Sinon, il existe $n_0 \in \mathbb{N}$ vérifiant $u_{n_0} > v_0$ et l'on aurait, par croissance de u et décroissance de v ainsi que pour tout entier $n \geqslant n_0$, $u_n - v_n > u_{n_0} - v_0$, ce qui contredit la convergence de $u - v$ vers 0. Ainsi, u converge. □

 La définition et le théorème des suites adjacentes sont fondamentaux. Le fait qu'ils s'écrivent de façon très concise n'en réduit pas l'importance mais rend en revanche inexcusable les confusions entre ce qui relève de la définition et ce qui relève du théorème.

Remarque 3.2.9.
Soient $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ deux suites réelles adjacentes, avec $(u_n)_{n\in\mathbb{N}}$ croissante.

Notons ℓ leur limite commune. Alors, $\forall n \in \mathbb{N},\ u_n \leqslant \ell \leqslant v_n \quad \text{et} \quad \forall (p,q) \in \mathbb{N}^2,\ u_p \leqslant \ell \leqslant v_q$.

Exemple 3.2.10.
Les suites $(u_n)_{n\in\mathbb{N}^*}$ et $(v_n)_{n\in\mathbb{N}^*}$ définies par $u_n = \sum_{k=0}^{n} \frac{1}{k!}$ et $v_n = u_n + \frac{1}{n.n!}$ sont adjacentes.

Exemple 3.2.11 (Moyenne arithmetico - géométrique)**.**
Soient $u_0, v_0 \in \mathbb{R}_+^*$. On définit deux suites en posant, pour tout $n \in \mathbb{N}$, $u_{n+1} = \frac{u_n + v_n}{2}$ et $v_{n+1} = \sqrt{u_n.v_n}$. Alors ces deux suites sont adjacentes et leur limite commune est appelée *moyenne arithmetico - géométrique de u_0 et v_0*.

Exercice 3.2.12 (Algorithme des Babyloniens)**.**
On pose $v_0 = 2$. On définit deux suites en posant, pour tout $n \in \mathbb{N}$, $u_n = \frac{2}{v_n}$ et $v_{n+1} = \frac{u_n + v_n}{2}$. Montrer que ces deux suites sont adjacentes. Quelle est leur limite ?

Définition 3.2.13.
Étant donné I un intervalle de $\mathbb{R}$, on appelle diamètre de I et on note $\delta(I)$ la valeur de $b - a$ où a et b sont les extrémités gauche et droite de I si celles-ci sont réelles et $+\infty$ si l'une au moins n'est pas réelle.

Théorème 3.2.14 (Des segments emboîtés)**.**
Soit $(I_n)_{n\in\mathbb{N}}$ une suite décroissante de segments non vides emboîtés, c'est-à-dire vérifiant $I_0 \supset I_1 \supset I_2 \supset \dots$ (autrement dit, pour tout $n \in \mathbb{N}$, $I_{n+1} \subset I_n$) et vérifiant $\delta(I_n) \xrightarrow[n\to+\infty]{} 0$. Alors l'ensemble

$$\bigcap_{n\in\mathbb{N}} I_n$$

est un singleton. Autrement dit, il existe un unique réel appartenant à I_n pour tout $n \in \mathbb{N}$.

De plus, tout suite u à valeur réelle telle que pour tout $n \in \mathbb{N}$, $u_n \in I_n$ converge vers ce réel.

Démonstration.
Il suffit de noter, pour tout $n \in \mathbb{N}$, a_n et b_n respectivement

les extrémités gauche et droite de I_n. Les conditions sur les segments entraînent que a et b sont deux suites adjacentes. Elles ont dont une limite commune ℓ. De plus pour tout n, $a_n \leqslant \ell \leqslant b_n$. Donc $\{\ell\} \subset \bigcap_{n\in\mathbb{N}} I_n$. Réciproquement, si $x \in \bigcap_{n\in\mathbb{N}} I_n$, alors pour tout $n \in \mathbb{N}$, $a_n \leqslant x \leqslant b_n$ donc, par encadrement, $x = \ell$.

Tout suite u vérifiant les conditions données est alors encadrée par a et b donc converge vers ℓ. □

Corollaire 3.2.15 (Méthode de la dichotomie)**.** Soit $(I_n)_{n\in\mathbb{N}}$ une suite de segments telle que pour tout $n \in \mathbb{N}$, I_{n+1} est soit la moitié gauche du segment I_n, soit la moitié droite du segment I_n.

Alors la suite $(I_n)_{n\in\mathbb{N}}$ est une suite décroissante de segments emboîtés, dont le diamètre tend vers 0.

Les extrémités gauche et droite de ces segments constituent donc des suites adjacentes.

3.3 Théorème de Bolzano-Weierstrass

Définition 3.3.1.
On dit qu'un sous-ensemble K de $\mathbb{R}$ est compact si et seulement si toute suite à valeurs dans K admet une suite extraite qui converge vers une valeur de K.

Exemple 3.3.2.
1. La suite $(n)_{n\in\mathbb{N}}$ n'admet aucune suite extraite convergente, donc ni $\mathbb{R}$, ni $\mathbb{R}^+$, ni $\mathbb{N}$ ne sont compacts.
2. Tout intervalle ouvert n'est pas compact.
3. Tout singleton est compact.
4. Tout ensemble fini est compact.

Nous avons déjà vu que toute suite convergente est bornée. La réciproque est évidemment fausse, par exemple la suite $((-1)^n)_{n\in\mathbb{N}}$ est bornée et divergente. Mais une version plus faible est vraie : c'est l'objet du théorème suivant, et cela apparaît plus clairement dans la formulation donnée en 3.3.4.

Théorème 3.3.3 (Bolzano-Weierstrass)**.**
Tout segment de $\mathbb{R}$ est compact.

Démonstration (Principe de la dichotomie à connaître, formalisation non exigible)**.**
Le cas où le segment est réduit à un point est trivial. Considérons donc un segment $[a, b]$ de $\mathbb{R}$ avec $a < b$ et une suite u à valeurs dans $[a, b]$ et montrons que u admet une suite extraite qui converge.

Définissons tout d'abord par dichotomie une suite $(I_n)_{n\in\mathbb{N}}$ de segments comme suit :

1. $I_0 = [a, b]$
2. Pour tout n, on définit I_{n+1} comme étant la moitié gauche de I_n si u prend une infinité de fois ses valeurs dans cette moitié gauche. Sinon, on définit I_{n+1} comme étant la moitié droite de I_n.

   Il est clair que la suite $(I_n)_{n\in\mathbb{N}}$ est une suite de segments emboîtés de diamètre tendant vers 0, d'intersection réduite à un singleton l.

   On peut démontrer par récurrence que pour tout $n \in \mathbb{N}$, u prend une infinité de fois ses valeurs dans $I(n)$.

   On va maintenant extraire une suite $\left(u_{\varphi(n)}\right)_{n\in\mathbb{N}}$ de u telle que pour tout $n \in \mathbb{N}$, $u_n \in I_n$.

   Le principe est relativement simple : on prend u_0 pour premier terme de cette suite extraite. On a $u_0 \in I_0$. On prend alors pour terme suivant le premier terme suivant de u appartenant à I_1. Un tel terme existe puisque u prend une infinité de fois ses valeurs dans I_1. On prend alors pour terme suivant le premier terme suivant de u appartenant à I_2. Etc.

   Plus formellement, on définit par récurrence l'application φ comme suit :

   (a) $\varphi(0) = 0$.

   (b) pour tout $n \in \mathbb{N}$, $\varphi(n+1)$ est le plus petit entier k strictement supérieur à $\varphi(n)$ vérifiant $u_n \in I_{n+1}$. La suite u prenant une infinité de fois ses valeurs dans $I(n+1)$, un tel k existe.

   Posons alors, pour $n \in \mathbb{N}$, $v_n = u_{\varphi(n)}$.

   On a pour tout $n \in \mathbb{N}$, $v_n \in I_n$. Donc v converge.

   La suite u admet donc bien une suite extraite convergente, $[a, b]$ est donc compact.

□

Corollaire 3.3.4.
On peut extraire de toute suite réelle bornée une suite convergente.

Remarque 3.3.5.
C'est ce dernier corollaire qui est aussi parfois appelé « Théorème de Bolzano-Weierstrass ».

4 Traduction séquentielle de certaines propriétés

Définition 4.0.1.
On dit qu'une partie de $\mathbb{R}$ est dense dans $\mathbb{R}$ si elle rencontre tout intervalle ouvert non vide de $\mathbb{R}$.

Remarque 4.0.2.
On a déjà vu que l'ensemble des décimaux, $\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$ étaient denses dans $\mathbb{R}$.

Proposition 4.0.3.
Soit $X \subset \mathbb{R}$. X est dense dans $\mathbb{R}$ si et seulement si pour tout $\ell \in \mathbb{R}$ il existe une suite u à valeurs dans X convergeant vers ℓ.

Démonstration.
Supposons que X est dense dans $\mathbb{R}$, soit $\ell \in \mathbb{R}$. Alors, pour tout entier naturel n, $X \cap]\ell - \frac{1}{n+1}, \ell + \frac{1}{n+1}[$ est non vide et l'on peut donc construire une suite u d'éléments de X telle que, pour tout entier naturel n, $\ell - \frac{1}{n+1} \leqslant u_n \leqslant \ell + \frac{1}{n+1}$. Par encadrement, u converge vers ℓ.

Réciproquement, soit une telle partie X, montrons que X est dense dans $\mathbb{R}$. Soit I un intervalle ouvert non vide de $\mathbb{R}$. Si $I \cap X = \varnothing$, il suffit de prendre ℓ comme étant le milieu de I : aucune suite à valeurs dans X ne peut converger vers ℓ. En effet, en considérant ε le quart du diamètre de I, on a, pour tout $x \in X$, $|x - \ell| > r$. Ainsi, X rencontre I. □

Proposition 4.0.4.
Soit X une partie non vide de $\mathbb{R}$. Alors il existe une suite u à valeurs dans X de limite $\sup X$.

1. Si X est majorée, $\sup X \in \mathbb{R}$ et u converge.
2. Si X n'est pas majorée, alors $\sup X = +\infty$ et u tend vers $+\infty$.

Démonstration.
Si X n'est pas majorée, c'est facile : pour tout $n \in \mathbb{N}$, il existe $x \in X$ vérifiant $x \geqslant n$. On construit donc une suite u à valeurs dans X vérifiant $\forall n \in \mathbb{N}, u_n \geqslant n$.

Si X est majorée, revenir à la caractérisation de la borne supérieure dans le cas réel donnée dans le chapitre VIII. □

5 Suites particulières

5.1 Suites arithmétiques

Définition 5.1.1.
Soit α et r deux complexes. On appelle *suite arithmétique* de premier terme α et de *raison* r la suite u définie par

$$\begin{cases} u_0 = \alpha, \\ \forall n \in \mathbb{N},\ u_{n+1} = r + u_n. \end{cases}$$

Remarque 5.1.2.
Une suite arithmétique est à valeurs réelles si et seulement si son premier terme et sa raison sont réels.

Proposition 5.1.3.
Soit $r \in \mathbb{C}$ et u une suite arithmétique de raison r. Alors $\forall n \in \mathbb{N},\ u_n = nr + u_0$. De plus

$$\forall n \in \mathbb{N} \qquad \sum_{k=0}^{n} u_k = (n+1)\frac{u_0 + u_n}{2}.$$

Démonstration.
Revenir à la formule donnant $\sum_{k=0}^{n} k$. □

Remarque 5.1.4.
Cette dernière formule est assez peu utile, il vaut souvent mieux revenir à la formule donnant $\sum_{k=0}^{n} k$.

Proposition 5.1.5.
Soit $r \in \mathbb{R}$ et u une suite arithmétique à valeurs réelles de raison r. Alors,

— si $r > 0$, $u_n \xrightarrow[n\to+\infty]{} +\infty$;
— si $r = 0$, u est la suite constante de valeur u_0 donc $u_n \xrightarrow[n\to+\infty]{} u_0$;
— si $r < 0$, $u_n \xrightarrow[n\to+\infty]{} -\infty$.

5.2 Suites géométriques

Définition 5.2.1.
Soit α et r deux complexes. On appelle *suite géométrique* de premier terme α et de *raison* r la suite u définie par

$$\begin{cases} u_0 = \alpha, \\ \forall n \in \mathbb{N},\ u_{n+1} = r \cdot u_n. \end{cases}$$

Remarque 5.2.2.
Une suite géométrique est à valeurs réelles si et seulement si son premier terme est nul ou son premier terme et sa raison sont réels.

Proposition 5.2.3.
Soit $r \in \mathbb{C}$ et u une suite géométrique de raison r. Alors $\forall n \in \mathbb{N},\ u_n = r^n u_0$. De plus

— si $r \neq 1$, alors

$$\forall n \in \mathbb{N} \qquad \sum_{k=0}^{n} u_k = u_0 \frac{1 - r^{n+1}}{1 - r};$$

— si $r = 1$, alors

$$\forall n \in \mathbb{N} \qquad \sum_{k=0}^{n} u_k = (n+1)u_0.$$

Démonstration.
Revenir à la formule donnant $\sum_{k=0}^{n} q^k$. □

Proposition 5.2.4.
Soit $r \in \mathbb{R}$ et u une suite réelle géométrique de raison r, avec $u_0 \neq 0$.

— Si $r \in]-\infty, -1]$, alors u n'a pas de limite (ni finie, ni infinie).
— Si $r \in]-1, 1[$ (*i.e.* $|r| < 1$), alors u converge vers 0.
— Si $r = 1$, alors u est la suite constante, de valeur u_0 (elle converge donc vers u_0).
— Si $r \in]1, +\infty[$, alors u diverge vers $+\infty$ si $u_0 > 0$ et vers $-\infty$ sinon.
— La suite u converge si et seulement si $r \in]-1, 1]$ (c'est-à-dire $|r| < 1$ ou $r = 1$).

Démonstration.
Direct d'après la question précédente. □

5.3 Suites arithmético-géométriques

Définition 5.3.1.
Une suite u est dite suite *arithmético-géométrique* s'il existe deux nombres complexes a et b vérifiant :

$$\forall n \in \mathbb{N},\ u_{n+1} = au_n + b.$$

Remarque 5.3.2.
Il s'agit d'une généralisation des notions de suites arithmétiques et géométriques :

— Si $a = 1$, alors u est une suite arithmétique.
— Si $b = 0$, alors u est une suite géométrique.

Remarque 5.3.3.
Ces suites interviennent fréquemment dans des problèmes concrets :

— évolution du capital restant à rembourser en fonction du temps dans le cas d'un emprunt à mensualités constantes ;
— modélisation de l'évolution d'une population ;
— dans le jeu du «devinez le nombre que j'ai choisi».

Soit a et b deux complexes. On s'intéresse maintenant à l'ensemble des suites u solutions de l'équation

$$\forall n \in \mathbb{N},\ u_{n+1} = au_n + b. \qquad \textbf{(AG)}$$

Proposition 5.3.4.
Soit u et v deux solutions de (**? ?**). Alors $u - v$ (*i.e.* la suite de terme général $u_n - v_n$ pour $n \in \mathbb{N}$) est une suite géométrique de raison a.

Démonstration.
Très facile. □

Proposition 5.3.5.
Soit v une suite solution de (? ?). Alors, pour toute suite géométrique u de raison a, la suite $u+v$ (*i.e.* la suite de terme général u_n+v_n pour $n\in\mathbb{N}$) est aussi solution de (? ?).

Démonstration.
Très facile. □

Corollaire 5.3.6.
Soit v une solution particulière de (? ?). Soit $u\in\mathbb{C}^{\mathbb{N}}$. On a l'équivalence suivante : u est solution de (? ?) si et seulement si $u-v$ est une suite géométrique de raison a.

Démonstration.
v est solution de (? ?), donc d'après la proposition 5.3.4 si u est solution de (? ?), $u-v$ est une suite géométrique de raison a.

Montrons la réciproque : supposons que $u-v$ est une suite géométrique de raison a. Alors d'après la proposition 5.3.5, $v+(u-v)$ est solution de (? ?). Or $v+(u-v)=u$, d'où le résultat. □

Proposition 5.3.7.
Si $a\neq 1$, alors il existe une unique suite constante solution de (? ?).

Démonstration.
Très facile. □

Méthode de résolution de (? ?)

1. Si $a=1$, les solutions de (? ?) sont les suites arithmétiques de raison b (*i.e.* pour tout $u\in\mathbb{C}^{\mathbb{N}}$, u est solution de E si et seulement si $\forall n\in\mathbb{N},\ u_n=u_0+nb$).
2. Si $a\neq 1$, on cherche une solution constante. Pour cela, on détermine l'unique α vérifiant
$$\alpha=a\alpha+b.$$
3. Les solutions de (? ?) sont alors les suites $u\in\mathbb{C}^{\mathbb{N}}$ telles que la suite $u-\alpha$ (c'est-à-dire $(u_n-\alpha)_{n\in\mathbb{N}}$) soit une suite géométrique de raison a. Autrement dit, les solutions de (? ?) sont les suites $u\in\mathbb{C}^{\mathbb{N}}$ vérifiant :
$$\forall n\in\mathbb{N}\ u_n=\alpha+a^n(u_0-\alpha).$$

Remarque 5.3.8.
L'ensemble des solutions de (? ?) a ici la même structure que dans les cas des systèmes linéaires et des équations différentielles linéaires (espace affine). Ce n'est pas une coïncidence ! On remarquera que l'on résout $(u_{n+1}-au_n)_{n\in\mathbb{N}}=(b)_{n\in\mathbb{N}}$ et que $(u_{n+1}-u_n)_{n\in\mathbb{N}}$ dépend *linéairement* de u.

Exemple 5.3.9.
Donner le terme général de la suite u définie par :
$$\begin{cases} u_0=0,\\ \forall n\in\mathbb{N}\ u_{n+1}=2u_n+1.\end{cases}$$

Exemple 5.3.10.
Votre banquier vous propose un prêt à la consommation de 10 000 € «à un taux de 18% annuel» sur 5 ans, à mensualités fixes (soit 60 mensualités). Après avoir signé le contrat, vous constatez que le taux est de $1,5\%$ par mois. Quel est le montant des mensualités ? Quel est le coût total du crédit ? Que pensez-vous de la manière dont le prêt est présenté ?

5.4 Suites récurrentes linéaires doubles

Définition 5.4.1.
On appelle *équation de récurrence linéaire double* ou *équation de récurrence linéaire d'ordre deux* toute équation de la forme
$$\forall n\in\mathbb{N}\qquad u_{n+2}+au_{n+1}+bu_n=0.$$
où a et b sont des complexes fixés et où la suite u (réelle ou complexe) est l'inconnue.

Toute solution de cette équation est appelée suite *récurrente linéaire double* (ou *d'ordre deux*).

On appelle *équation caractéristique* de cette équation de récurrence linéaire double, l'équation

$$r^2 + ar + b = 0.$$

On appelle *polynôme caractéristique* de cette équation de récurrence linéaire double, le polynôme

$$X^2 + aX + b.$$

Remarque 5.4.2.
Si $r \in \mathbb{C}$, alors r est solution de l'équation caractéristique si et seulement si $(r^n)_{n\in\mathbb{N}}$ est solution de l'équation de récurrence linéaire double.

Soit $(a, b) \in \mathbb{C}^2$, avec $b \neq 0$. On s'intéresse maintenant à l'ensemble des suites u solution de

$$\forall n \in \mathbb{N} \qquad u_{n+2} + au_{n+1} + bu_n = 0. \qquad \textbf{(E)}$$

On note alors l'équation caractéristique de (**? ?**) :

$$r^2 + ar + b = 0. \qquad \textbf{(C)}$$

Théorème 5.4.3 (Solutions complexes de (**? ?**))**.**
On considère l'équation (**? ?**).

(i) Si (**? ?**) admet deux solutions distinctes r_1 et r_2, les solutions de (**? ?**) sont les suites de la forme $(\lambda r_1^n + \mu r_2^n)_{n\in\mathbb{N}}$, où λ et μ sont des complexes.

(ii) Si (**? ?**) admet une unique solution, r_0, alors les solutions de (**? ?**) sont les suites de la forme $(\lambda r_0^n + \mu n r_0^n)_{n\in\mathbb{N}}$, où λ et μ sont des complexes.

Dans les deux cas, il existe une unique solution à (**? ?**) pour u_0 et u_1 fixés.

Démonstration.
La preuve n'est pas exigible, en voici un schéma.

1. Montrer que s'il existe une solution, elle est entièrement déterminée par la donnée de u_0 et u_1.
2. Montrer selon les cas que les suites données dans l'énoncé du théorème sont effectivement *des* solutions.
3. Montrer, selon les cas, que pour tout choix de u_0 et u_1, une de ces suites est solution.
4. En déduire selon les cas que les suites données dans l'énoncé du théorème sont effectivement *les* solutions.

□

Dans tout ce qui suit, on ne s'intéressera qu'au cas où les coefficients a et b sont réels.

Théorème 5.4.4 (Solutions réelles de (**? ?**))**.**
On considère l'équation (**? ?**), avec $(a, b) \in \mathbb{R} \times \mathbb{R}^*$.

(i) Si (**? ?**) admet deux solutions (réelles) distinctes r_1 et r_2, alors les solutions réelles de (**? ?**) sont les suites de la forme $(\lambda r_1^n + \mu r_2^n)_{n\in\mathbb{N}}$, où λ et μ sont des réels.

(ii) Si (**? ?**) admet une unique solution (réelle) r_0, alors les solutions réelles de (**? ?**) sont les suites de la forme $(\lambda r_0^n + \mu n r_0^n)_{n\in\mathbb{N}}$, où λ et μ sont des réels.

(iii) Si (**? ?**) admet deux solutions complexes conjuguées, $re^{\,i\theta}$ et $re^{\,-i\theta}$, alors les solutions réelles de (**? ?**) sont les suites de la forme $(r^n(\lambda\cos(n\theta) + \mu\sin(n\theta)))_{(n\in\mathbb{N})}$ où λ et μ sont des réels fixés.

Dans tous les cas, il existe une unique solution à (**? ?**) pour u_0 et u_1 fixés.

Remarque 5.4.5.
En pratique, on rencontrera des suites définies par la valeur de u_0 et u_1 et une équation linéaire de récurrence d'ordre deux. On détermine alors les solutions générales de l'équation en utilisant le théorème ci-dessus, puis on détermine les constantes λ et μ avec les valeurs de u_0 et u_1.

Démonstration.
La preuve n'est pas exigible, en voici un schéma.

1. Montrer, en étudiant les différents cas que les suites données ci-dessus sont effectivement des solutions.
2. Montrer en étudiant les différents cas, que toute solution est une suite donnée ci-dessus (astuce bien pratique : si u est une solution à valeurs réelles de (**? ?**), alors, pour tout $n \in \mathbb{N}$, $u_n = \mathrm{Re}(u_n)$) et u est aussi une solution complexe de (**? ?**)).
3. En déduire que les suites données dans l'énoncé du théorème sont effectivement *les* solutions.

□

Exemple 5.4.6 (Application pratique)**.**
On considère la suite $(u_n)_{n\in\mathbb{N}}$ définie par

$$\begin{cases} u_0 = 0 \text{ et } u_1 = 1 \\ \forall n \in \mathbb{N},\ u_{n+2} = u_{n+1} + u_n \end{cases}$$

Déterminer une expression de u_n en fonction de n.

Remarque 5.4.7.
La méthode vue ici est très proche de celle utilisée pour résoudre les équations différentielles linéaires de degré deux à coefficients constants. Ce n'est d'ailleurs pas une coïncidence ...

6 Suites définies par une relation de récurrence d'ordre 1

On étudie dans cette partie *les suites (réelles) récurrentes d'ordre 1*, c'est-à-dire les suites réelles u vérifiant une relation du type : $\forall n \in \mathbb{N},\ u_{n+1} = f(u_n)$, où f est une fonction définie sur une partie D de $\mathbb{R}$ et à valeur dans $\mathbb{R}$.

6.1 Définition de la suite

On se donne donc une partie D de $\mathbb{R}$, $f : D \to \mathbb{R}$, et $a \in \mathbb{R}$. On veut définir la suite u par récurrence de la façon suivante

$$\begin{cases} u_0 = a \\ \text{et } \forall n \in \mathbb{N},\ u_{n+1} = f(u_n) \end{cases}$$

Une telle définition n'est pas nécessairement légitime : par exemple, si $a \notin D$, alors u_1 est mal défini donc la suite est mal définie. Autre exemple : on prend pour f l'application $x \mapsto \sqrt{x} - 1$ et pour a la valeur 4. On a bien $a \in \mathbb{R}^+$ mais $u_1 = 1$, $u_2 = 0$, $u_3 = -1 < 0$ et u_4 est mal défini.

Une condition suffisante [1] pour que la suite soit bien définie est de trouver une partie A de D (*i.e.* une partie A de $\mathbb{R}$ sur laquelle f est bien définie) *stable par* f (*i.e.* $\forall x \in A,\ f(x) \in A$) et contenant le premier terme de la suite ($a \in A$).

En notant, pour $n \in \mathbb{N}$, $P(n)$ la propriété «u_n est bien définie et $u_n \in A$», on peut alors montrer par récurrence que pour tout $n \in \mathbb{N}$, on a $P(n)$; on en déduit que pour tout $n \in \mathbb{N}$, u_n est bien définie, donc que u est bien définie.

Exemple 6.1.1. 1. Soit $a \in [-1, +\infty[$, et notons u la suite définie par

$$\begin{cases} u_0 = a \\ \text{et } \forall n \in \mathbb{N}\ u_{n+1} = \sqrt{1 + u_n} \end{cases}$$

Notons f la fonction $x \mapsto \sqrt{1+x}$. Alors l'ensemble de définition $[-1, +\infty[$ est stable par f. Donc la suite $(u_n)_{n\in\mathbb{N}}$ est bien définie.

2. Notons v la suite définie par

$$\begin{cases} v_0 = 5 \\ \text{et } \forall n \in \mathbb{N}\ v_{n+1} = v_n^{\frac{3}{2}} - 1 \end{cases}$$

Posons

$$\begin{array}{rccc} f: & \mathbb{R}^+ & \to & \mathbb{R} \\ & x & \mapsto & x^{\frac{3}{2}} - 1 \end{array}$$

L'ensemble de définition de f est $\mathbb{R}^+$, qui n'est pas stable par f puisque $f(0) \notin \mathbb{R}^+$. En revanche, en posant $A = [4, +\infty[$, on peut remarquer que A est une partie de l'ensemble de définition de f stable par f : en effet, f est croissante sur $\mathbb{R}^+$ et $f(4) = 7 \geqslant 4$ donc pour tout $x \in A$, on a $f(x) \geqslant f(4) \geqslant 4$ donc $f(x) \in A$. Or 5 appartient à A donc on peut montrer que v est bien définie.

Dans toute la suite, A désigne une partie de $\mathbb{R}$, et f une application définie (au moins) sur A et telle que $f(A) \subset A$ et a un élément de A.

6.2 Recherche d'une limite éventuelle

Proposition 6.2.1.
Si la suite $(u_n)_{n\in\mathbb{N}}$ converge vers un réel ℓ et f est continue en ℓ, alors $f(\ell) = \ell$. On dit que ℓ est *un point fixe de* f.

1. Cette condition est aussi nécessaire (pourquoi ?) mais en pratique, c'est le fait qu'elle soit suffisante qui nous intéressera.

Remarque 6.2.2.
Cette proposition sert à déterminer les limites *éventuelles* de la suite $(u_n)_{n\in\mathbb{N}}$ ou à montrer qu'elle n'admet pas de limite.

 En aucun cas, elle ne permet de montrer que u a une limite.

Exemple 6.2.3. — Étudier la convergence de la suite $(u_n)_{n\in\mathbb{N}}$ définie par

$$\begin{cases} u_0 = 1 \\ \forall n \in \mathbb{N},\ u_{n+1} = u_n^2 + 1 \end{cases}$$

— Étudier la convergence de la suite $(u_n)_{n\in\mathbb{N}}$ définie par

$$\begin{cases} u_0 = 1 \\ \forall n \in \mathbb{N},\ u_{n+1} = u_n^2 + \frac{1}{4} \end{cases}$$

6.3 Cas où f est croissante sur A

Proposition 6.3.1.
Si f est une fonction *croissante* sur A : alors la suite u est *monotone*. Plus précisément :
— si $u_0 \leqslant u_1$, alors u est croissante ;
— si $u_0 \geqslant u_1$, alors u est décroissante.

Démonstration.
Montrons le premier point (le second est similaire). Supposons f croissante sur A et $u_0 \leqslant u_1$. Alors, pour $n \in \mathbb{N}$, notons $P(n)$ l'assertion «$u_n \leqslant u_{n+1}$».
— On a $u_0 \leqslant u_1$ donc on a $P(0)$.
— Soit $n \in \mathbb{N}$, supposons $P(n)$. Alors on a $u_n \leqslant u_{n+1}$. Or f est croissante sur A, donc $f(u_n) \leqslant f(u_{n+1})$, donc $u_{n+1} \leqslant u_{n+2}$, donc on a $P(n+1)$.
On a donc, d'après le principe de récurrence, $\forall n \in \mathbb{N}\ u_n \leqslant u_{n+1}$. □

Remarque 6.3.2.
Vous n'avez pas besoin de retenir cette proposition. En revanche, vous devez retenir la technique de démonstration pour être en mesure de l'adapter à un cas concret.

Exemple 6.3.3.
Étudier, pour $a = 0$ et pour $a = 2$, la suite u définie par

$$\begin{cases} u_0 = a, \\ \forall n \in \mathbb{N},\ u_{n+1} = \sqrt{1+u_n}. \end{cases}$$

Exemple 6.3.4.
Étudier la suite u définie par

$$\begin{cases} u_0 = 0, \\ \forall n \in \mathbb{N},\ u_{n+1} = u_n^2 + 2u_n + 1. \end{cases}$$

La suite u admet-elle une limite ? laquelle ?

Exercice 6.3.5.
Montrer qu'une fonction croissante $f : I \to I$, où I est un segment, possède un point fixe.

6.4 Cas où f est décroissante sur A

Proposition 6.4.1.
Si f est une fonction décroissante sur A, alors les suites $(u_{2n})_{n\in\mathbb{N}}$ et $(u_{2n+1})_{n\in\mathbb{N}}$ sont monotones et de sens contraire. Plus précisément :
— si $u_0 \leqslant u_2$, alors $(u_{2n})_{n\in\mathbb{N}}$ est croissante et $(u_{2n+1})_{n\in\mathbb{N}}$ est décroissante ;
— si $u_0 \geqslant u_2$, alors $(u_{2n})_{n\in\mathbb{N}}$ est décroissante et $(u_{2n+1})_{n\in\mathbb{N}}$ est croissante.

Démonstration.
Montrons le premier point (le second se montre de la même façon).
Supposons f décroissante. Alors $f \circ f$ est croissante.
Supposons de plus $u_0 \leqslant u_2$.
Montrons alors que $(u_{2n})_{n\in\mathbb{N}}$ est croissante et $(u_{2n+1})_{n\in\mathbb{N}}$ est décroissante.
En posant $v = (u_{2n})_{n\in\mathbb{N}}$, on a $\forall n \in \mathbb{N},\ v_{n+1} = (f\circ f)(v_n)$ et $v_0 \leqslant v_1$.
Donc v est croissante, d'après la proposition 6.3.1.
On a donc $\forall n \in \mathbb{N},\ u_{2n} \leqslant u_{2n+2}$.
f étant décroissante, on en déduit $\forall n \in \mathbb{N},\ f(u_{2n}) \geqslant f(u_{2n+2})$.
Donc $\forall n \in \mathbb{N},\ u_{2n+1} \geqslant u_{2n+3}$. □

Remarque 6.4.2.
Même remarque que pour la proposition 6.4.1.

Exemple 6.4.3.
Étudier la suite u définie par

$$\begin{cases} u_0 = 10, \\ \forall n \in \mathbb{N},\ u_{n+1} = 10 - \sqrt{u_n}. \end{cases}$$

7 Suites à valeurs complexes

Nous allons définir la notion de convergence de suites à valeurs complexes en s'appuyant sur les

convergences des suites (réelles) des parties réelles et imaginaires associées.

On pourrait définir de manière intrinsèque cette convergence, le lecteur intéressé se rapportera à la partie **? ?**.

Soit $u \in \mathbb{C}^{\mathbb{N}}$ une suite à valeurs complexes. Notons $\mathrm{Re}(u)$ la suite $\mathrm{Re}(u_n)_{n\in\mathbb{N}}$, $\mathrm{Im}(u)$ la suite $\mathrm{Im}(u_n)_{n\in\mathbb{N}}$ et $|u|$ la suite $|u_n|_{n\in\mathbb{N}}$.

Soit alors ℓ un complexe.

Remarque 7.0.1. 1. On rappelle que pour tout complexe z, on a

$$\begin{aligned} |z| &\leqslant |\mathrm{Re}(z)| + |\mathrm{Im}(z)| \\ |\mathrm{Re}(z)| &\leqslant |z| \\ |\mathrm{Im}(z)| &\leqslant |z| \end{aligned}$$

2. En particulier, pour tout $n \in \mathbb{N}$:

$$\begin{aligned} |u_n - \ell| &\leqslant |\mathrm{Re}(u_n) - \mathrm{Re}(\ell)| \\ &\quad + |\mathrm{Im}(u_n) - \mathrm{Im}(\ell)| \\ |\mathrm{Re}(u_n) - \mathrm{Re}(\ell)| &\leqslant |u_n - \ell| \\ |\mathrm{Im}(u_n) - \mathrm{Im}(\ell)| &\leqslant |u_n - \ell| \end{aligned}$$

Proposition 7.0.2.
On a

$$|u_n - \ell| \xrightarrow[n\to+\infty]{} 0$$

si et seulement si

$$\mathrm{Re}(u_n) \xrightarrow[n\to+\infty]{} \mathrm{Re}(\ell) \text{ et } \mathrm{Im}(u_n) \xrightarrow[n\to+\infty]{} \mathrm{Im}(\ell).$$

Définition 7.0.3.
On dit que u converge vers ℓ si

$$|u_n - \ell| \xrightarrow[n\to+\infty]{} 0.$$

Démonstration.
C'est une conséquence directe de la remarque précédente. □

Remarque 7.0.4. 1. Cette définition étend la définition de la convergence pour les suites à valeurs réelles.

2. Il n'y a pas de notion similaire à $+\infty$ et $-\infty$ sur $\mathbb{C}$, donc pas de notion de limite infinie pour les suites à valeurs complexes (mais on peut regarder si $|u|$ tend vers $+\infty$).
3. Les résultats usuels sur les suites à valeurs réelles s'étendent naturellement aux suites à valeurs complexes... sauf ceux qui font appel à l'ordre sur $\mathbb{R}$ vu qu'il n'y a pas d'ordre «raisonnable» sur $\mathbb{C}$.

La proposition suivante peut être utile.

Proposition 7.0.5.

$$u \xrightarrow[+\infty]{} \ell \Rightarrow |u_n| \xrightarrow[n\to+\infty]{} |\ell|$$

Démonstration.
De la définition 7.0.6 et de l'inégalité triangulaire :

$$\forall n \in \mathbb{N} \quad ||u_n| - |\ell|| \leqslant |u_n - \ell|$$

on déduit immédiatement $|u_n| \xrightarrow[n\to+\infty]{} |\ell|$, d'où le résultat. □

Proposition 7.0.6.
Soit u, v deux suites complexes convergeant respectivement vers ℓ et ℓ', soit $\lambda, \mu \in \mathbb{C}$. Alors $\lambda u + \mu v$ converge, vers $\lambda\ell + \mu\ell'$.

Remarque 7.0.7. 1. La réciproque est évidemment fausse

2. Cette proposition permet notamment d'assurer que si u a une limite ℓ non nulle alors, à partir d'un certain rang, $|u|$ est compris entre $\frac{1}{2}|\ell|$ et $\frac{3}{2}|\ell|$.

Définition 7.0.8.
On dit que u est bornée si son module l'est.

Remarque 7.0.9.
C'est équivalent au fait que $\mathrm{Re}(u)$ et $\mathrm{Im}(u)$ soient bornées.

Théorème 7.0.10 (Bolzano-Weierstrass)**.**
De toute suite à valeurs complexes bornée, on peut extraire une sous-suite convergente.

Démonstration (non exigible)**.**
Considérons une suite u à valeurs complexes bornées. Notons r et j respectivement les suites $\mathrm{Re}(u)$ et $\mathrm{Im}(u)$.

r et j sont bornées et à valeurs réelles. D'après le théorème de Bolzano-Weierstrass sur les suites à valeurs réelles, on peut donc extraire de chacune une sous-suite convergente. Pourtant cela ne suffit pas à montrer le résultat. Pourquoi ?

Considérons φ une extraction de r telle que $r \circ \varphi$ converge.

Alors $j \circ \varphi$ est bornée. On peut donc en trouver une extraction ψ telle que $j \circ \varphi \circ \psi$ converge.

$r \circ \varphi$ converge donc $r \circ \varphi \circ \psi$ converge vers la même valeur.

Or $r \circ \varphi \circ \psi = \mathrm{Re}(u \circ \varphi \circ \psi)$ et $j \circ \varphi \circ \psi = \mathrm{Im}(u \circ \varphi \circ \psi)$.

Donc $u \circ \varphi \circ \psi$ converge. □

8 Premiers exemples de séries numériques

Les séries numériques sont des cas particuliers de suites, que nous étudierons en fin d'année. Nous pouvons cependant commencer à étudier quelques exemples significatifs.

8.1 Séries télescopiques.

Soit $(u_n)_{n\in\mathbb{N}}$ une suite à valeurs complexes.

Proposition 8.1.1.
Les suites $(u_n)_{n\in\mathbb{N}}$ et $\left(\sum_{n=0}^{N}(u_{n+1}-u_n)\right)_{N\in\mathbb{N}}$ ont même nature.
Dans le cas de convergence, si $u_n \xrightarrow[n\to+\infty]{} \ell$, alors

$$\sum_{n=0}^{N} u_n \xrightarrow[N\to+\infty]{} \ell - u_0.$$

Démonstration.
Nous savons déjà que les suites $(u_n)_{n\in\mathbb{N}}$ et $(u_{n+1})_{n\in\mathbb{N}}$ ont même nature.
De plus la somme $\sum_{n=0}^{N}(u_{n+1}-u_n)$ vaut $u_{N+1}-u_0$ par sommation télescopique. Elle est donc égale au terme u_{N+1}, à une constante près, et a donc la même nature que la suite $(u_{n+1})_{n\in\mathbb{N}}$.
Dans le cas de convergence, il reste à passer à la limite dans la relation $\sum_{n=0}^{N}(u_{n+1}-u_n) = u_{N+1}-u_0$. □

8.2 Séries géométriques.

Soit z un nombre complexe, p un entier naturel.

Proposition 8.2.1.
La suite $\left(\sum_{n=p}^{N} z^n\right)_{N\in\mathbb{N}}$ converge si et seulement si $|z|<1$. Le cas échéant,

$$\sum_{n=p}^{N} z^n \xrightarrow[N\to+\infty]{} \frac{z^p}{1-z}.$$

Démonstration.
C'est une conséquence directe de la formule de sommation géométrique :

$$\sum_{n=p}^{N} z^n = \frac{z^p}{1-z} - \frac{z^{N+1}}{1-z} \text{ si } z \neq 1 \text{ et } N+1-p \text{ sinon.}$$

Il suffit donc de voir que si $z \neq 1$, (z^{N+1}) converge si et seulement si $|z|<1$ et, dans le cas de convergence, converge vers 0.

Le cas $|z| \neq 1$ s'obtient aisément en considérant le module. Le cas $|z|=1$ est un exercice classique et sera traité en TD. □

9 Annexe : unification des notions de limites.

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

Remarque 9.0.1.
Nous avons étudié trois types de limites différents : vers un point réel, vers $+\infty$ et vers $-\infty$. Vous avez remarqué que les définitions « naïves » de ces trois notions de limites ont une structure en commun. Afin d'éviter des répétitions fastidieuses et de mettre en avant les idées pertinentes, nous

sommes ammenés à développer un vocabulaire permettant de traiter simultanément ces trois notions : c'est le début de la *topologie*, qui fait intervenir la notion de voisinage. Il convient de bien savoir utiliser de manière pertinent les deux visions, :

— dans les cas où l'on sait si la limite étudiée est finie, vaut $+\infty$ ou $-\infty$, on utilisera les définitions naïves des limites (propositions 2.1.8, 2.1.11 et 2.1.12) ;

— dans les autres cas, il peut être judicieux de raisonner en termes de voisinages.

9.1 Voisinages

Définition 9.1.1.
Soit a un réel. Soit ε un réel *strictement* positif.

(i) On appelle *boule ouverte de centre a et de rayon ε*, et on note $\mathcal{B}(a,\varepsilon)$ l'ensemble des réels situés à une distance de a strictement inférieure à ε :

$$\begin{aligned}\mathcal{B}(a,\varepsilon) &= \{\, x \in \mathbb{R} \mid |x-a| < \varepsilon \,\} \\ &=]a-\varepsilon, a+\varepsilon[\end{aligned}$$

(ii) On appelle *boule fermée de centre a et de rayon ε*, et on note $\mathcal{B}_f(a,\varepsilon)$ l'ensemble des réels situés à une distance de a inférieure ou égale à ε :

$$\begin{aligned}\mathcal{B}_f(a,\varepsilon) &= \{\, x \in \mathbb{R} \mid |x-a| \leqslant \varepsilon \,\} \\ &= [a-\varepsilon, a+\varepsilon]\end{aligned}$$

(iii) On appelle *voisinage* de a toute partie de $\mathbb{R}$ contenant au moins une boule ouverte de centre a. L'ensemble des voisinages de a est noté $\mathcal{V}(a)$.

$$\mathcal{V}(a) = \left\{ E \in \mathscr{P}(\mathbb{R}) \;\middle|\; \exists \varepsilon \in \mathbb{R}^{+*} \quad \mathcal{B}(a,\varepsilon) \subset E \right\}$$

(iv) On appelle *voisinage de $+\infty$* toute partie de $\mathbb{R}$ contenant au moins un intervalle de la forme $]A,+\infty[$, où A est un réel. L'ensemble des voisinages de $+\infty$ est noté $\mathcal{V}(+\infty)$.

$$\mathcal{V}(+\infty) = \{\, E \mid \exists A \in \mathbb{R} \quad]A,+\infty[\subset E \,\}$$

(v) On appelle *voisinage de $-\infty$* toute partie de $\mathbb{R}$ contenant au moins un intervalle de la forme $]-\infty, A[$, où A est un réel. L'ensemble des voisinages de $-\infty$ est noté $\mathcal{V}(-\infty)$.

$$\mathcal{V}(-\infty) = \{\, E \mid \exists A \in \mathbb{R} \quad]-\infty, A[\subset E \,\}$$

Proposition 9.1.2.
Soit $V \subset \mathbb{R}$ et $a \in \mathbb{R}$. Les conditions suivantes sont équivalentes :

(i) V est un voisinage de a

(ii) V contient au moins un intervalle ouvert (non vide) contenant a

(iii) V contient au moins un intervalle fermé (non réduit à un point) contenant a dont a n'est pas une extrémité.

Démonstration.
Simple, une fois que l'on a remarqué que si $a \in \mathbb{R}$ et $\varepsilon > 0$,

$$\mathcal{B}\left(a, \frac{\varepsilon}{2}\right) \subset \mathcal{B}_f\left(a, \frac{\varepsilon}{2}\right) \subset \mathcal{B}(a,\varepsilon).$$

□

Définition 9.1.3.
Soit $a \in \overline{\mathbb{R}}$ et P un prédicat sur les réels. On dit que P est vraie *au voisinage de a* si l'ensemble $\{\, x \in \mathbb{R} \mid P(x) \,\}$ est un voisinage de a.

Exemple 9.1.4.
Soit $f : \mathbb{R} \to \mathbb{R}$. Traduire l'expression « f est à valeurs positives au voisinage de a » :

1. pour $a \in \mathbb{R}$?
2. pour $a = +\infty$?
3. pour $a = -\infty$?

Mêmes questions pour

1. « f est nulle au voisinage de a»
2. « f est non-nulle au voisinage de a»

Au voisinage de quels points les fonctions $\mathbb{1}_{\mathbb{Z}}$ et $\mathbb{1}_{\mathbb{R}\setminus\mathbb{Z}}$ sont-elles nulles ?

9.2 Convergence de suite dans $\overline{\mathbb{R}}$

Définition 9.2.1.
Soit $u \in \mathbb{R}^{\mathbb{N}}$ et $\ell \in \overline{\mathbb{R}}$.

(i) On dit que u *tend vers* ℓ, ou que u_n *tend vers* ℓ quand n tend vers $+\infty$ (noté $u \xrightarrow[+\infty]{} \ell$ ou $u_n \xrightarrow[n\to+\infty]{} \ell$), si, pour tout voisinage V de ℓ, les valeurs prises par u appartiennent toutes à V à partir d'un certain rang. Autrement dit, si l'on a

$$\forall V \in \mathcal{V}(\ell)\ \exists n_0 \in \mathbb{N}\ \forall n \in \mathbb{N}\ n \geqslant n_0 \Rightarrow u_n \in V$$

(ii) Si $\ell \in \mathbb{R}$, on dit alors que u *converge vers* ℓ.

(iii) On dit que u *converge* ou est *convergente* si et seulement s'il existe un réel vers lequel elle converge.

(iv) On dit que la suite u *diverge* (ou *est divergente*) si et seulement si elle ne converge pas.

Remarque 9.2.2.
Si $u \xrightarrow[+\infty]{} \ell$, on dit que ℓ est une limite de u. Nous montrerons bientôt l'unicité de cette limite.

Remarque 9.2.3.
Une suite qui tend vers $+\infty$ (ou vers $-\infty$) diverge.

Proposition 9.2.4.
Soit $u \in \mathbb{R}^{\mathbb{N}}$ et $\ell \in \mathbb{R}$. Alors u converge vers ℓ si et seulement si

$$\forall \varepsilon \in \mathbb{R}_+^*,\ \exists n_0 \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geqslant n_0 \Rightarrow |u_n - \ell| \leqslant \varepsilon.$$

Démonstration.
Si u tend vers $\ell \in \mathbb{R}$, soit $\varepsilon > 0$. Alors $\mathcal{B}(\ell, \varepsilon)$ est un voisinage de ℓ donc il existe un rang $N \in \mathbb{N}$ à partir duquel toutes les valeurs de u sont dans ce voisinage : $\forall n \geqslant N,\ |u_n - \ell| \leqslant \varepsilon$.

Réciproquement, soit V un voisinage de ℓ. Il existe donc $\varepsilon > 0$ tel que $\mathcal{B}(\ell, \varepsilon) \subset V$. Il existe alors un $N \in \mathbb{N}$ tel que $\forall n \geqslant N,\ |u_n - \ell| \leqslant \varepsilon$. Soit $n \geqslant N$, on a donc $u_n \in \mathcal{B}(\ell, \varepsilon) \subset V$, d'où le résultat. □

Proposition 9.2.5.
Soit $u \in \mathbb{R}^{\mathbb{N}}$. Alors on a $u_n \xrightarrow[n\to+\infty]{} +\infty$ si et seulement si on a

$$\forall A \in \mathbb{R},\ \exists n_0 \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geqslant n_0 \Rightarrow u_n \geqslant A.$$

Démonstration.
À faire en exercice. □

Proposition 9.2.6.
Soit $u \in \mathbb{R}^{\mathbb{N}}$. Alors on a $u_n \xrightarrow[n\to+\infty]{} -\infty$ si et seulement si on a

$$\forall A \in \mathbb{R},\ \exists n_0 \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geqslant n_0 \Rightarrow u_n \leqslant A.$$

Démonstration.
À faire en exercice. □

9.3 Démonstrations des résultats précédemment obtenus

Les propriétés énoncées auparavant peuvent maintenant se prouver plus rapidement !

Lemme 9.3.1 (Propriété de Hausdorff)**.**
Soit ℓ_1 et ℓ_2 deux éléments distincts de $\overline{\mathbb{R}}$. Alors il existe V_1 et V_2 des voisinages respectifs de ℓ_1 et ℓ_2, tels que V_1 et V_2 soient disjoints.

Démonstration.
— Supposons que ℓ_1 et ℓ_2 sont deux réels, alors il suffit de prendre pour V_1 et V_2 les boules de centre respectifs ℓ_1 et ℓ_2 et de rayon $\frac{1}{3}|\ell_1 - \ell_2|$
— Supposons $\ell_1 = +\infty$ et $\ell_2 = -\infty$. Alors, il suffit de prendre respectivement $[1, +\infty[$ et $]-\infty, -1]$.
— Supposons $\ell_1 \in \mathbb{R}$ et $\ell_2 = +\infty$. Alors, il suffit de prendre pour V_1 la boule de centre ℓ_1 et de rayon 1, et pour V_2 l'intervalle $[\ell_1 + 2, +\infty[$.
— Le cas $\ell_1 \in \mathbb{R}$, $\ell_2 = -\infty$ est similaire.
On a donc le résultat. □

Théorème 9.3.2 (Unicité de la limite)**.**
Soit u une suite réelle. Alors si u admet une limite, celle-ci est unique.

Démonstration.
Il suffit de démontrer que u ne peut admettre deux limites distinctes. Par l'absurde, supposons que u admette deux limites ℓ_1 et ℓ_2 distinctes. D'après le lemme précédent, on peut choisir des voisinages V_1 et V_2 respectivement de ℓ_1 et ℓ_2 qui soient disjoints. u ayant pour limite ℓ_1 (resp. ℓ_2), choisissons un rang n_1 (resp. n_2) tel que les termes de u appartiennent à V_1 (resp. V_2) à partir du rang n_1 (resp. n_2). Notons n_0 le plus grand de ces deux rangs. Alors u_{n_0} appartient à la fois à V_1 et à V_2, ce qui est absurde puisque $V_1 \cap V_2 = \varnothing$. □

Définition 9.3.3 (Limite)**.**
Soit $u \in \mathbb{R}^{\mathbb{N}}$. Lorsqu'il existe un élément ℓ de $\overline{\mathbb{R}}$ vérifiant $u_n \xrightarrow[n\to+\infty]{} \ell$, on l'appelle **la** *limite* de u, et on le note $\lim\limits_{+\infty} u$ ou $\lim\limits_{n\to+\infty} u_n$.

Démonstration.
Il suffit de démontrer que u ne peut admettre deux limites distinctes. Par l'absurde, supposons que u admette deux limites ℓ_1 et ℓ_2 distinctes. D'après le lemme précédent, on peut choisir des voisinages V_1 et V_2 respectivement de ℓ_1 et ℓ_2 qui soient disjoints. u ayant pour limite ℓ_1 (resp. ℓ_2), choisissons un rang n_1 (resp. n_2) tel que les termes de u appartiennent à V_1 (resp. V_2) à partir du rang n_1 (resp. n_2). Notons n_0 le plus grand de ces deux rangs. Alors u_{n_0} appartient à la fois à V_1 et à V_2, ce qui est absurde puisque $V_1 \cap V_2 = \varnothing$. □

Théorème 9.3.4.
Soit $u \in \mathbb{R}^{\mathbb{N}}$ et $\ell \in \overline{\mathbb{R}}$. Si $u \xrightarrow[+\infty]{} \ell$ alors toute suite extraite de u tend aussi vers ℓ.

Démonstration.
Soit φ une extractrice, soit V un voisinage de ℓ. Il existe donc un rang $n_0 \in \mathbb{N}$ tel que , pour tout $n \geqslant n_0$, $u_n \in V$. Soit $n \geqslant n_0$, on a alors $\varphi(n) \geqslant n \geqslant n_0$ et donc $u_{\varphi(n)} \in V$. □

Théorème 9.3.5.
Soit u une suite à valeurs réelles et $\ell \in \overline{\mathbb{R}}$. Si on a $u_{2n} \xrightarrow[n\to+\infty]{} \ell$ et $u_{2n+1} \xrightarrow[n\to+\infty]{} \ell$, alors $u_n \xrightarrow[n\to+\infty]{} \ell$.

Démonstration.
Soit V un voisinage de ℓ. Il existe donc deux rangs N et N' tels que, pour tout entier naturel n,
— si $n \geqslant N$, $u_{2n} \in V$;
— si $n \geqslant N'$, $u_{2n+1} \in V$.
Ainsi, si $n \geqslant \max(2N, 2N'+1)$, on a $u_n \in V$ (il suffit de distinguer selon la parité de N), d'où le résultat. □

Proposition 9.3.6.
Soit $u \in \mathbb{R}^N$ et $(a, b, \ell) \in \mathbb{R}$. Supposons $u \xrightarrow[+\infty]{} \ell$ et $a < \ell < b$. Alors à partir d'un certain rang, les valeurs de u sont comprises strictement entre a et b. Autrement dit :

$$\exists n_0 \in \mathbb{N} \ \forall n \in \mathbb{N} \ \ n \geqslant n_0 \Rightarrow a < u_n < b$$

Démonstration.
$]a, b[$ est un voisinage de ℓ. □

9.4 Suites complexes

Il est possible de définir la notion de limite d'une suite complexe de la même manière que pour les suites réelles, en utilisant les voisinages. Ainsi, si l'on définit ce qu'est une *boule ouverte* dans $\mathbb{C}$ (ce qui a été fait dans le chapitre sur les complexes), on dira qu'un *voisinage* d'un complexe ℓ est toute partie de $\mathbb{C}$ contenant une boule ouverte contenant ℓ. La définition **? ?** peut alors être répétée dans le cas d'une suite complexe. Faisons le bilan : dans la définition **? ?**, on change les valeurs absolues en modules et on ne parle plus d'intervalle, on exclut le cas des limites infinies qui n'ont pas de sens dans $\mathbb{C}$, et le reste est commun aux suites réelles et complexes.

De manière générale, dans tout ensemble sur lequel on peut construire une *distance* on peut donner les définitions de boule ouverte, voisinage et limite d'une suite de cette manière.

Chapitre XI

Groupes, anneaux, corps

On remarque que dans des domaines a priori distincts, des similitudes apparaissent, notamment concernant les structures. Pour avoir une théorie générale, on définit des structures algébriques abstraites, on en démontre les propriétés, puis on les applique dans les exemples mathématiques qui vérifient ces structures.
Dans ce chapitre on s'intéresse aux structures algébriques de base : groupes, anneaux et corps. Plus tard on verra une structure fondamentale : celle d'espace vectoriel.

1 Lois de composition internes

Dans tout ce chapitre, E est un ensemble.

1.1 Définition

Définition 1.1.1.
On appelle *loi de composition interne sur E* (lci) toute application de $E \times E$ dans E.

• Cette définition a déjà été vue, ainsi que des exemples, dans le chapitre I sur les complexes.

Définition 1.1.2.
On appelle *magma* tout couple constitué d'un ensemble et d'une lci.

Exemple 1.1.3.
$(\mathbb{Z}, -)$ est un magma, mais pas $(\mathbb{N}, -)$, car $-4 \notin \mathbb{N}$.

Dans toute la suite, $*$ est une lci sur E.

1.2 Propriétés

Définition 1.2.1.
Soit $(E, *)$ un magma.

1. On dit que E est *associatif* si pour tous $x, y, z \in E$, on a : $x * (y * z) = (x * y) * z$. L'élément $x * (y * z) = (x * y) * z$ est alors noté $x * y * z$.
2. On dit que E est *commutatif* si pour tous $x, y \in E$, on a : $x * y = y * x$.
3. Soit $\#$ une seconde lci sur E. On dit que dans E $*$ est *distributive à gauche* par rapport à $\#$ si pour tous $x, y, z \in E$, on a : $x * (y \# z) = (x * y) \# (x * z)$.

Exemple 1.2.2.
• $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$ avec $+$ ou $\times$ sont associatifs, mais pas $(\mathbb{Z}, -)$ car $1-(2-3) \neq (1-2)-3$, ni $(\mathbb{R}^3, \wedge)$.
• $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$ avec $+$ ou $\times$ sont commutatifs, mais pas $(\mathbb{Z}, -)$ ni $(\mathbb{R}^3, \wedge)$, ni $(\mathscr{F}(\mathbb{R}, \mathbb{R}), \circ)$.
• Sur $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$ $\times$ est distributive par rapport à $+$, et sur $\mathscr{P}(E)$, $\cap$ et $\cup$ sont distributives l'une par rapport à l'autre.

Définition 1.2.3. 1. Soit $e \in E$. on dit que e est un *élément neutre à gauche* (resp. *à droite*) pour $*$ si pour tout $x \in E$ on a $e * x = x$ (resp. $x * e = x$). On dit que e est un *élément neutre* pour $*$ si c'est un élément neutre à gauche et à droite, i.e. pour tout $x \in E$, $e * x = x * e = x$.

2. Soit e un neutre pour $*$ et soit $x \in E$. On dit que x est *inversible à gauche* (resp. *à droite*) s'il existe un élément $y \in E$ tel que $y * x = e$ (resp. $x * y = e$). Un tel élément y s'appelle *UN inverse à gauche* (resp. *à droite*) de x. On dit que x est *inversible* s'il est inversible à gauche et à droite, *i.e.* il existe $y \in E$ tel que $y * x = x * y = e$. Dans ce cas y est *UN inverse de x*.

Exemple 1.2.4.
• 0 est un élément neutre pour $+$ dans $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$.
• 1 est un élément neutre pour $\times$ dans $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$.
• Id est un élément neutre pour $\circ$ dans $\mathscr{F}(E, E)$, et les bijections sont tous les éléments inversibles de cet ensemble.
• Par contre $(\mathbb{R}^3, \wedge)$ n'a pas de neutre. S'il y avait un neutre u, on devrait avoir $u \wedge u = u$, mais $u \wedge u = 0$, donc $u = 0$. Mais pour tout $v \neq 0$, on a $u \wedge v = 0$, et non $u \wedge v = v$.

 Être inversible d'un seul côté ne suffit pas pour être inversible tout court : un exemple a été vu dans le TD du chapitre sur les applications (ensemble des applications de $\mathbb{N}$ dans $\mathbb{N}$ muni de $\circ$).

Remarque 1.2.5.
Un neutre est toujours inversible et est son propre inverse.

Proposition 1.2.6.
Si $*$ admet un neutre, alors ce neutre est unique

Démonstration.
Soient e et e' deux neutres.[1] Alors $e * e' = e$ et $e * e' = e'$, donc $e = e'$. □

Proposition 1.2.7.
On suppose la loi $*$ associative, et admettant un neutre e. Si un élément est inversible, alors il a un seul inverse.

Démonstration.
Soient y et y' deux inverses[2] de $x \in E$. Alors $y * x = e$ et $x * y' = e$. Donc $y * (x * y') = y * e = y$ et $(y * x) * y' = e * y' = y'$, d'où $y = y'$. □

Remarque 1.2.8.
On utilise souvent les *notations additives et multiplicatives*.

- En notation additive, $*$ est en général notée $+$, $\underbrace{x + x + \ldots + x}_{n \text{ fois}}$ se note nx, et si x est inversible, son inverse se note $-x$. On l'appelle alors plutôt *l'opposé de* x. De même, on notera le neutre d'une telle structure 0, ou 0_E.
- En notation multiplicative, $*$ est en général remplacée par $\times$ (et ce symbole est même souvent omis), $\underbrace{x \times x \times \ldots \times x}_{n \text{ fois}}$ se note x^n et si x est inversible, son inverse se note x^{-1}. De même, on notera le neutre d'une telle structure 1, ou 1_E.

Pour éviter toute erreur, on essaiera au maximum de n'utiliser la notation additive que pour des lois qui ont les mêmes propriétés que la loi $+$ sur $\mathbb{R}$. Par exemple, noter $+$ une lci non commutative peut-être déroutant, ainsi que pour une lci pour laquelle tous les éléments ne sont pas inversibles. La notation $+$ est en général réservée à des lci commutatives et pour lesquelles les éléments sont tous inversibles..

Ce n'est pas le cas pour la notation multiplicative, qui est la plus couramment utilisée pour des lois associatives, mais sans plus. Par exemple il est fréquent d'utiliser $\times$ même pour une lci non commutative et pour laquelle les éléments ne sont pas tous inversibles. Donc faites attention, par défaut on aura $xy \neq yx$, et x^{-1} n'existera pas forcément !

Dans toute la suite, on adoptera la notation multiplicative, et on suppose que E a un neutre noté 1.

Proposition 1.2.9.
On suppose la loi $*$ associative. Soient $x, y, z \in E$.

(i) Simplification par un inversible : si x est inversible, alors $x * y = x * z \Leftrightarrow y = z$.

(ii) Inverse d'un produit : si x et y sont inversibles alors $x * y$ l'est aussi et $(x * y)^{-1} = y^{-1} * x^{-1}$. **Attention :** l'inverse de $x * y$ n'a aucune raison d'être $x^{-1} * y^{-1}$.

1. On pourra remarquer que dans cette démonstration on utilise uniquement le fait que e est neutre à gauche et e' neutre à droite. Donc en fait tout neutre à gauche est égal à tout neutre à droite, d'où l'on déduit d'une part que l'existence d'un neutre à gauche et d'un neutre à droite suffit à assurer l'existence d'un neutre et d'autre part que ce neutre est alors le seul neutre à gauche et le seul neutre à droite. Pour qu'un élément ait plusieurs neutres à gauche, il est donc nécessaire (mais pas suffisant) qu'il n'ait aucun neutre à droite et *vice-versa*.

2. On pourra remarquer que dans cette démonstration on utilise uniquement le fait que y est inverse à gauche et y' inverse à droite. Donc en fait tout inverse à gauche est égal à tout inverse à droite, d'où l'on déduit d'une part que l'existence d'un inverse à gauche et d'un inverse à droite pour x suffit à assurer l'existence d'un inverse et d'autre part que cet inverse est alors le seul inverse à gauche et le seul inverse à droite de x. Pour qu'un élément ait plusieurs inverses à gauche, il est donc nécessaire qu'il n'ait aucun inverse à droite et *vice-versa*

(iii) Puissances négatives : si x est inversible, on pose pour $n \in \mathbb{N}^*$, $x^{-n} = (x^{-1})^n$. Alors $x^{-n} = (x^n)^{-1}$.

(iv) Inverse d'un inverse : si x est inversible, x^{-1} l'est aussi et $(x^{-1})^{-1} = x$.

Démonstration. (iii) Par récurrence. Vrai si $n = 0$ ou 1. Si vrai pour n, alors $x^{n+1} * x^{-n-1} = x^n * x * x^{-1} * x^{-n} = x^n * e * x^{-n} = x^n * x^{-n} = e$.

(iv) Vrai par unicité de l'inverse. □

Définition 1.2.10.
Soit $(E, *)$ un magma et F une partie de E. On dit que F est une *partie stable* (de E par $*$) si pour tous $x, y \in F$, $x * y \in F$.

Exemple 1.2.11.
$\{-1, 1\}$ est une partie stable de $(\mathbb{R}, \times)$, mais pas $\{-2, 2\}$.

2 Structure de groupe

2.1 Groupe

Définition 2.1.1.
On appelle *groupe* tout magma associatif, ayant un neutre, et dont tout élément est inversible.
Si un groupe est *commutatif* (ce qui signifie en fait que sa loi est commutative), il est dit *abélien*.

Par défaut on utilise la notation multiplicative pour un groupe, sauf pour les groupes abéliens pour lesquels on utilise la notation additive.

Exemple 2.1.2.
• $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ sont des groupes avec la loi $+$, mais pas avec la loi $\times$.
• Pour $n \in \mathbb{N}^*$, $\mathbb{C}^n$, $\mathbb{R}^n$, $\mathbb{Q}^n$, $\mathbb{Z}^n$ sont des groupes avec la loi $+$.
• $\mathbb{C}\setminus\{0\}$, $\mathbb{R}\setminus\{0\}$, $\mathbb{Q}\setminus\{0\}$, sont des groupes avec la loi $\times$.
• $\mathbb{N}$ n'est un groupe ni avec la loi $+$ ni avec la loi $\times$.

Exemple 2.1.3.
En spé, vous manipulerez le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, que l'on peut voir comme « l'ensemble des congruences modulo n », avec $n \in \mathbb{N}^*$.

Définition 2.1.4.
Soit X un ensemble non vide. On appelle *groupe des permutations de X* l'ensemble des bijections de X dans X. Comme son nom l'indique, c'est un groupe, si on le munit de la loi de composition $\circ$. On le note S_X (on trouvera parfois la notation $\mathfrak{S}(X)$).

Démonstration.
L'application identité, $\mathrm{Id} : X \to X$, $x \mapsto x$, est évidemment une bijection de X, donc S_X est non vide.
On sait déjà que la composée de deux bijections est une bijection, donc $\circ$ est une lci sur S_X. Il est évident que Id en est le neutre. On sait également que cette loi est associative, et que la réciproque d'une bijection est encore une bijection. Cela assure que $(S_X, \circ)$ est un groupe. □

2.2 Sous-groupe

Dans toute la suite, $(G, *)$ est un groupe de neutre e. On adopte la notation multiplicative.

Définition 2.2.1.
On appelle *sous-groupe* de G tout ensemble H vérifiant les propriétés suivantes :

(i) $H \subset G$;

(ii) $e \in H$;

(iii) Stabilité par produit : $\forall x, y \in H, x*y \in H$;

(iv) Stabilité par passage à l'inverse : $\forall x \in H$, on a $x^{-1} \in H$.

En vertu des points (ii) et (iii), le premier point peut être remplacé par $H \neq \varnothing$.

Exemple 2.2.2.
Sont des sous-groupes :
- $\{e\}$ et G dans $(G, *)$.
- $\mathbb{U}$ dans $(\mathbb{C}^*, \times)$.
- $n\mathbb{Z}$ dans $(\mathbb{Z}, +)$.
- $H = \{f \in S_{\mathbb{R}} \mid f(0) = 0\}$ dans $(S_{\mathbb{R}}, \circ)$.

Proposition 2.2.3.
Un ensemble H est un sous groupe de G si et seulement si H est un sous-ensemble non vide de G et pour tout $(x, y) \in H^2$, on a $x^{-1} * y \in H$.

Démonstration.
Montrons l'implication et sa réciproque :

— Supposons que H est un sous-groupe de G. Alors H contient e et n'est donc pas vide. De plus, soit $(x, y) \in H$. H étant stable par passage à l'inverse, on a alors $x^{-1} \in H$ et par stabilité par produit, on a donc $x^{-1} * y \in H$.

— Réciproquement, supposons que H est non vide et que pour tout $(x, y) \in H^2$, on a $x^{-1} * y \in H$. Montrons que H possède les trois propriétés énumérées dans sa définition :

(i) H étant non vide, il possède au moins un élément x_0. On a alors $e = x_0^{-1} x_0 \in H$.

(iii) Soit $x \in H$. On a alors $(x, e) \in H^2$, donc $x^{-1} * e \in H$.

(ii) Soit $(x, y) \in H$. D'après ce qui précède, on a alors $x^{-1} \in H$, donc $(x^{-1}, y) \in H^2$, donc $x * y = \left(x^{-1}\right)^{-1} * y \in H$.

□

Remarque 2.2.4.
On obtient une proposition vraie également en remplaçant ci-dessus la condition $x^{-1}y \in H$ par $xy^{-1} \in H$.

Théorème 2.2.5.
Un sous-groupe muni de la loi induite du groupe est lui-même un groupe.

Démonstration.
Soit $(G, *)$ un groupe de neutre e et H un sous-groupe de G.

1. Montrons qu'on peut restreindre $* : G \times G \to G$ au départ à $H \times H$ et à l'arrivée à H. On appellera alors loi induite par $*$ sur H cette restriction de $*$. On a $H \times H \subset G \times G$, donc la restriction au départ est légitime, pour effectuer la restriction à l'arrivée, il suffit de montrer que pour tout $(x, y) \in H^2$, on a $x * y \in H$, c'est-à-dire que H est stable par $*$. Or H est un sous-groupe de G donc c'est évident.
2. H muni de la loi induite par $*$ est un magma associatif. En effet $(G, *)$ est un magma associatif, on a donc
$$\forall (x, y, z) \in G^3 \quad (x * y) * z = x * (y * z)$$
Or $H \subset G$ donc
$$\forall (x, y, z) \in H^3 \quad (x * y) * z = x * (y * z)$$
Donc la restriction de $*$ à H est associative, d'où le résultat.
3. e est neutre pour la loi induite par $*$ sur H. En effet, e est le neutre de $*$, donc
$$\forall x \in G \quad e * x = x * e = x$$
D'où le résultat.
4. Tout élément de H admet un inverse pour la loi induite par $*$. En effet tout élément x de H admet un inverse x^{-1} dans G pour la loi $*$ et par stabilité de l'inverse sur le sous-groupe H, on a $x^{-1} \in H$. Donc tout élément de H admet un inverse dans H pour la loi induite par $*$.
5. On déduit des points précédents que H muni de la loi induite par $*$ est un groupe.

□

Remarque 2.2.6.
Il est plus facile de montrer qu'un ensemble est un sous-groupe que de montrer que c'est un groupe (pas besoin de redémontrer l'associativité, etc.). Par exemple $(\mathbb{U}, \times)$ est un groupe, vu comme sous-groupe de $(\mathbb{C}^*, \times)$.
À chaque fois que l'on essaiera de montrer qu'un ensemble est muni d'une structure de groupe, on tentera de le voir comme un sous-groupe d'un groupe bien connu.

Remarque 2.2.7.
La réciproque de ce théorème est également vraie (bien que moins utilisée) : si H est un sous-ensemble de G tel que, muni de la loi induite par celle de G, H soit un groupe, alors H est un sous-groupe de G.

Exemple 2.2.8.
Si $n \in \mathbb{N}^*$, $\mathbb{U}_n$ est un sous-groupe de $(\mathbb{U}, \times)$, donc $(\mathbb{U}_n, \times)$ est un groupe.

2.3 Morphismes de groupes

Cette partie est officiellement hors-programme. Nous l'incluons cependant dans ce cours car ces résultats doivent de toute façon être connus pour le chapitre d'algèbre linéaire.

Définition 2.3.1.
Soient $(G,*)$ et $(G',\#)$ deux groupes et $\varphi : G \to G'$.

1. On dit que φ est un *morphisme du groupe* $(G,*)$ *dans le groupe* $(G',\#)$ ou, par abus de langage, un *morphisme du groupe* G *dans le groupe* G', si pour tous $x,y \in G$, $\varphi(x*y) = \varphi(x)\#\varphi(y)$.
2. Tout morphisme d'un groupe dans lui-même est appelé *endomorphisme*.
3. Tout morphisme de G dans G' qui est une bijection est appelé *isomorphisme de* G *sur* G'. Dans ce cas on dit que G et G' sont *isomorphes*. Un morphisme qui est à la fois un isomorphisme et un endomorphisme est appelé *automorphisme*.

Remarque 2.3.2.
• « Morphisme » signifie « forme » en grec.
• Avec la même définition, on peut définir un morphisme de magmas. Dans la suite, « morphisme » sous-entendra toujours « morphisme de groupes ».

Exemple 2.3.3.
• $\begin{array}{ccc} (\mathbb{Z},+) & \to & (\mathbb{Z},+) \\ x & \mapsto & 2x \end{array}$, est un morphisme, mais pas un isomorphisme.
• $\begin{array}{ccc} (\mathbb{C}^*,\times) & \to & (\mathbb{R}^*,\times) \\ z & \mapsto & |z| \end{array}$, est un morphisme, mais pas un isomorphisme.
• $\begin{array}{ccc} (\mathbb{R},+) & \to & (\mathbb{C}^*,\times) \\ x & \mapsto & \mathrm{e}^{ix} \end{array}$, est un morphisme, mais pas un isomorphisme.
• $\begin{array}{ccc} (\mathbb{R},+) & \to & (\mathbb{R}_+^*,\times) \\ x & \mapsto & \mathrm{e}^{x} \end{array}$ est un isomorphisme de réciproque ln, qui est aussi un isomorphisme.

Exemple 2.3.4.
On a déjà manipulé les morphismes suivants, lors des chapitres précédents.
• Si $n \in \mathbb{N}^*$, $\begin{array}{ccc} (\mathbb{C}^*,\times) & \to & (\mathbb{C}^*,\times) \\ z & \mapsto & z^n \end{array}$.
• Si $n \in \mathbb{N}^*$ et $a_1,\dots,a_n \in \mathbb{K}^n$, l'application $\begin{array}{ccc} (\mathbb{K}^n,+) & \to & (\mathbb{K},+) \\ (x_1,\dots,x_n) & \mapsto & a_1x_1+\dots a_nx_n \end{array}$.
• Si I est un intervalle de $\mathbb{R}$, si $a : I \to \mathbb{K}$ est continue, l'application $\begin{array}{ccc} (\mathscr{D}(I,\mathbb{K}),+) & \to & (\mathscr{C}(I,\mathbb{K}),+) \\ f & \mapsto & f'+af \end{array}$.
• Si $a,b \in \mathbb{Z}$, l'application $\begin{array}{ccc} (\mathbb{Z}^2,+) & \to & (\mathbb{Z},+) \\ (x,y) & \mapsto & ax+by \end{array}$.
• Si $a \in \mathbb{C}$, l'application $\begin{array}{ccc} (\mathbb{K}^{\mathbb{N}},+) & \to & (\mathbb{K}^{\mathbb{N}},+) \\ u & \mapsto & (u_{n+1}-au_n)_{n\in\mathbb{N}} \end{array}$.

Dans toute la suite, $(G,*)$ et $(G',\#)$ sont deux groupes de neutres e et e', on adopte une notation muliplicative, et $\varphi : G \to G'$ est un morphisme.

Théorème 2.3.5.
Soit φ un morphisme de G sur G', on a, e et e' désignant les neutres de G et G' :

1. $\varphi(e) = e'$;
2. $\forall x \in G \quad \varphi(x^{-1}) = (\varphi(x))^{-1}$.

Démonstration. 1. On a $\varphi(e)\#\varphi(e) = \varphi(e*e) = \varphi(e) = \varphi(e)\#e'$, donc en simplifiant par $\varphi(e)$, on en déduit $\varphi(e) = e'$.
2. Soit $x \in G$. Alors $\varphi(x^{-1})\varphi(x) = \varphi(x^{-1}x) = \varphi(e) = e'$.

□

Corollaire 2.3.6.
Sous les mêmes hypothèses, on a

$$\forall x \in G \quad \forall k \in \mathbb{Z} \quad \varphi(x^k) = \varphi(x)^k$$

Démonstration.
Soit $x \in G$. D'après le théorème ci-dessus, on a

$$\varphi(x^0) = \varphi(e) = e' = \varphi(x)^0$$

On peut alors démontrer par récurrence que pour tout $n \in \mathbb{N}$, on a $\varphi(x^n) = \varphi(x)^n$ (l'hérédité résulte directement de la définition de morphisme).

D'après le théorème ci-dessus, pour tout $n \in \mathbb{N}$, $\varphi(x^{-n}) = \varphi(x^n)^{-1}$, d'où $\varphi(x^{-n}) = \varphi(x)^{-n}$.

On en déduit le résultat. □

Exemple 2.3.7. 1. $\begin{array}{ccc}\mathbb{C}^* & \to & \mathbb{R}^* \\ z & \mapsto & |z|\end{array}$ est un morphisme de $(\mathbb{C}^*, \times)$ dans $(\mathbb{R}^*, \times)$, donc pour tout $z \in \mathbb{C}^*$, on a

$$\left|\frac{1}{z}\right| = \frac{1}{|z|}$$

2. exp est un morphisme de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \times)$, donc pour tout $z \in \mathbb{C}$, $e^{-z} = \frac{1}{e^z}$
3. ln est un morphisme de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$, donc pour tout $x \in \mathbb{R}_+^*$, on a $\ln(1/x) = -\ln x$.

Remarque 2.3.8.
On peut adapter le théorème 2.3.4 dans le cas où on sait seulement que $(G, *)$ est un groupe, G' est un ensemble muni d'une loi de composition interne $\#$ et où φ est une application $G \to G'$ vérifiant $\forall (x, y) \in G^2\ \varphi(x * y) = \varphi(x)\#\varphi(y)$. Dans ce cas, on ne peut pas déduire que $(G', \#)$ est un groupe mais seulement que $(\varphi(G), \#)$ est un groupe. Voir aussi le théorème disant que «l'image d'un sous-groupe par un morphisme est un sous-groupe».

Théorème 2.3.9. (i) La composée de deux morphismes de groupes est un morphisme de groupe. Plus précisément, soit $(G_1, *_1)$, $(G_2, *_2)$ et $(G_3, *_3)$ trois groupes, φ un morphisme de G_1 dans G_2 et ψ un morphisme de G_2 dans G_3. Alors $\psi \circ \varphi$ est un morphisme de G_1 dans G_3.

(ii) La fonction réciproque d'un isomorphisme (en tant qu'application bijective) est un isomorphisme. Plus précisément, soit $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes et φ un isomorphisme de G_1 sur G_2. Alors φ^{-1} est un isomorphisme de G_2 sur G_1.

Démonstration.
Les démonstrations pour montrer qu'une application est un morphisme ont TOUJOURS la même structure.

1. $\psi \circ \varphi$ est clairement une application de G_1 dans G_3. Soit $(x, y) \in G_1^2$, montrons qu'on a $\psi \circ \varphi(x *_1 y) = (\psi \circ \varphi)(x) *_3 (\psi \circ \varphi)(y)$.
   φ est un morphisme de groupes donc on a $\varphi(x *_1 y) = \varphi(x) *_2 \varphi(y)$. Or ψ est un morphisme de groupes donc on a $\psi(\varphi(x) *_2 \varphi(y)) = (\psi(\varphi(x)) *_3 \psi(\varphi(y))$.
   D'où $(\psi \circ \varphi)(x *_1 y) = (\psi \circ \varphi)(x) *_3 (\psi \circ \varphi)(y)$.
2. φ^{-1} est évidemment une bijection de G_2 sur G_1. Il suffit donc de montrer que φ^{-1} est un morphisme de G_2 dans G_1.
   Soit $(x, y)^2 \in G_2$. Montrons $\varphi^{-1}(x *_2 y) = \varphi^{-1}(x) *_1 \varphi^{-1}(y)$.
   On a d'une part $\varphi(\varphi^{-1}(x *_2 y)) = x *_2 y$ et d'autre part, comme φ est un morphisme, $\varphi(\varphi^{-1}(x) *_1 \varphi^{-1}(y)) = \varphi(\varphi^{-1}(x)) *_2 \varphi(\varphi^{-1})(y)$, d'où $\varphi(\varphi^{-1}(x *_2 y)) = \varphi(\varphi^{-1}(x) *_1 \varphi^{-1}(y))$.
   Or φ est injective donc $\varphi^{-1}(x *_2 y) = \varphi^{-1}(x) *_1 \varphi^{-1}(y)$.
   Donc φ^{-1} est un morphisme, donc un isomorphisme.

□

Remarque 2.3.10.
L'ensemble des automorphismes d'un groupe G est donc un sous-groupe de $(S_G, \circ)$.

Exemple 2.3.11.
On a vu que exp et ln sont des isomorphismes réciproques.

Théorème 2.3.12. (i) L'image d'un sous-groupe par un morphisme de groupes est un sous-groupe.

(ii) L'image réciproque d'un sous-groupe par un morphisme est un sous-groupe.

Démonstration.
Les démonstrations pour montrer qu'un ensemble est un sous-groupe ont TOUJOURS la même structure.

(i) Soient $(G, *)$ et $(G', \#)$ deux groupes de neutres respectifs e et e', et $\varphi : G \to G'$ un morphisme de groupes. Soit H un sous-groupe de G. Montrons que $\varphi(H)$ est un sous-groupe de G'.

1. On a évidemment $\varphi(H) \subset G'$ et de plus $e \in H$ et $e' = \varphi(e) \in \varphi(H)$.
2. Soit $x, y \in \varphi(H)$. Alors x possède un antécédent $x' \in H$ et y un antécédent $y' \in H$ par φ. On a alors successivement

$$\begin{aligned} x\#y^{-1} &= \varphi(x')\#\varphi(y')^{-1} && \text{par définition de } x' \text{ et } y' \\ &= \varphi(x')\#\varphi(y'^{-1}) && \text{car } \varphi \text{ est un morphisme} \\ &= \varphi(x' * y'^{-1}) && \text{car } \varphi \text{ est un morphisme} \end{aligned}$$

Donc $x\#y^{-1} \in \varphi(H)$.

$\varphi(H)$ est donc un sous-groupe de G'.

(ii) Gardons les même notations que dans le premier point, et notons H' un sous-groupe de G'.

1. On a évidemment $\varphi^{-1}(H') \subset G$ et de plus $e' \in H'$ et $e' = \varphi(e) \in H'$ donc $e \in \varphi^{-1}(H')$.
2. Soit $x, y \in \varphi^{-1}(H')$. Alors $\varphi(x), \varphi(y) \in H'$ et donc $\varphi(x * y^{-1}) = \varphi(x)\#(\varphi(y))^{-1} \in H'$ donc $x * y^{-1} \in \varphi^{-1}(H')$.

$\varphi^{-1}(H')$ est donc un sous-groupe de G.

□

Remarque 2.3.13.
On complète la remarque **??** comme suit : lorsque l'on veut montrer qu'un ensemble est muni d'une structure de groupe, on commence toujours par essayer de l'identifier comme image réciproque (ou directe) d'un sous-groupe d'un groupe bien connu par un morphisme.

Définition 2.3.14. (i) On appelle *noyau* de φ, noté $\operatorname{Ker}\varphi$, l'image réciproque de $\{ e' \}$ par φ, autrement dit l'ensemble des antécédents de e' par φ : $\operatorname{Ker}\varphi = \{ x \in G \mid \varphi(x) = e' \}$.

(ii) On appelle *image* de φ notée $\operatorname{Im}\varphi$, l'image directe de G par φ. Autrement dit $\operatorname{Im}\varphi = \{ \varphi(x) \mid x \in G \}$.

Exemple 2.3.15.
Déterminer les images et noyaux des exemples de 2.3.3.

Théorème 2.3.16.
Les noyaux et les images sont des sous-groupes respectivement de G et G'.

Démonstration.
Ceci découle directement du théorème 2.3.11. Néanmoins, redémontrons-le dans le cas particulier du noyau :

Montrons que $\operatorname{Ker}\varphi$ est un sous-groupe de G :

1. On a évidemment $\operatorname{Ker}\varphi \subset G$ et de plus $\varphi(e) = e'$ donc $\operatorname{Ker}\varphi$ est un sous-ensemble non vide de G.
2. Soit $x, y \in \operatorname{Ker}\varphi$. Alors on a successivement
$$\begin{aligned}\varphi(x * y^{-1}) &= \varphi(x)\#\varphi(y)^{-1} \\ &= e'\#e'^{-1} \\ &= e'\end{aligned}$$

Donc $x * y^{-1} \in \operatorname{Ker}\varphi$.

Donc $\operatorname{Ker}\varphi$ est un sous-groupe de G. □

Exemple 2.3.17.
Constatation avec les Im et Ker tirés des exemples de 2.3.3.

Remarque 2.3.18.
On complète la remarque **??** comme suit : lorsque l'on veut montrer qu'un ensemble est muni d'une structure de groupe, on commence toujours par essayer de l'identifier comme noyau ou image d'un morphisme.

Exemple 2.3.19.
$\mathbb{U}$ est le noyau du morphisme « module », de $(\mathbb{C}^*, \times)$ dans $(\mathbb{R}^*, \times)$.

La proposition suivante est primordiale.

Proposition 2.3.20.
Soit $\varphi : G \to G'$ un morphisme de groupes, soit $x, y \in G$. Alors $\varphi(x) = \varphi(y)$ si et seulement si $xy^{-1} \in \operatorname{Ker}\varphi$.

Démonstration.
$\varphi(x) = \varphi(y)$ si et seulement si $\varphi(x)\varphi(y)^{-1} = 1_G$ si et seulement si $\varphi(xy^{-1}) = 1_G$. □

Remarque 2.3.21.
Avec les mêmes notations, si on a $a \in \mathscr{G}$ et $y \in G'$ vérifiant $y = \varphi(a)$, l'ensemble des solutions sur G de l'équation $y = \varphi(x)$ est $\{ ax \mid x \in \operatorname{Ker}(\varphi) \}$.

Exemple 2.3.22.
Reprendre les exemples exposés en **??**.

On retrouve ainsi la structure des racines n^{es} d'un nombre complexe, la structure des solutions d'un système linéaire, la structure des solutions d'une équation différentielle linéaire, les solutions d'une relation de Bézout et la structure des suites vérifiant une relation de récurrence arithmético-géométrique.

Théorème 2.3.23. (i) φ injectif si et seulement si $\operatorname{Ker}\varphi = \{e\}$.

(ii) φ surjectif si et seulement si $\operatorname{Im}\varphi = G'$.

Démonstration. (ii) Rien de nouveau.

(i) On montre l'implication et sa réciproque :
— Supposons φ injectif. Alors e' a au plus un antécédent par φ. Or $\varphi(e) = e'$ donc il en a au moins un : e. Donc $\operatorname{Ker}\varphi = \{ e \}$.
— Réciproquement, supposons $\operatorname{Ker}\varphi = \{ e \}$ et montrons que φ est injectif.
Soit $(x, y) \in G^2$ vérifiant $\varphi(x) = \varphi(y)$. Alors on a succesivement

$$\begin{aligned}\varphi(x * y^{-1}) &= \varphi(x)\#\varphi(y)^{-1} \quad \text{car } \varphi \text{ est un morphisme}\\ &= \varphi(x)\#\varphi(x)^{-1}\\ &= e'\end{aligned}$$

Donc $x * y^{-1} \in \operatorname{Ker}\varphi$, donc $x * y^{-1} = e$, donc $x = y$.

□

Remarque 2.3.24.
Pour montrer qu'un morphisme est injectif, on utilisera **TOUJOURS** le noyau et **JAMAIS** (ou presque) la méthode classique pour des fonctions quelconques : c'est beaucoup plus rapide !

Exemple 2.3.25.
Reprendre les exemples de exp et ln, ainsi que les morphismes vus en **? ?**.

3 Structure d'anneau

Définition 3.0.1.
On appelle *anneau* tout triplet $(A, +, \times)$ constitué d'un ensemble A et de deux lois internes sur A, une loi $+$ appelée *addition* et une loi $\times$ appelée *multiplication*, vérifiant :

1. $(A, +)$ est un groupe abélien dont l'élément neutre est noté 0 (ou 0_A si ambiguïté) ;
2. $(A, \times)$ est un magma associatif possédant un neutre noté 1 (ou 1_A si ambiguïté) ;
3. La multiplication est distributive par rapport à l'addition.

Si la loi $\times$ est commutative, on dit que l'anneau A est commutatif.

Exemple 3.0.2.
• $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ et $\mathscr{F}(\mathbb{R}, \mathbb{R})$ avec $+$ et $\times$ sont des anneaux.
• $(\mathbb{R}^3, +, \wedge)$ et $(\mathscr{F}(\mathbb{R}, \mathbb{R}), +, \circ)$ n'en sont pas.
• $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ en est un.
• $(\mathscr{M}_n(\mathbb{R}), +, \times)$ est un anneau.
• On note $\mathscr{L}(\mathbb{R}^2)$ l'ensemble des endomorphismes de $\mathbb{R}^2$. Alors $(\mathscr{L}(\mathbb{R}^2), +, \circ)$ est un anneau.

Remarque 3.0.3.
Quand il n'y a pas d'ambiguïté, on dit juste que A est un anneau sans préciser les lois. Pour la multiplication, on utilise les mêmes raccourcis de notation que dans $\mathbb{R}$ (omission du $\times$, etc).

 Tous les éléments de A ne sont pas inversibles pour $\times$. Les éléments inversibles sont parfois appelés *éléments unités* de A et leur ensemble est noté $U(A)$, $A^\times$, A^*, voire $E(A)$ (*Einheit*).

 Avec cette notation, A^* n'est pas nécessairement $A \setminus \{ 0 \}$.

Théorème 3.0.4 (Règles de calcul dans un anneau)**.**
Soit A un anneau, $a, b \in A$ et $n \in \mathbb{Z}$.

1. $a \times 0 = 0 \times a = 0$.
2. $-(a \times b) = (-a) \times b = a \times (-b)$. Cas particuliers : $(-a)(-b) = ab$, $(-a)^2 = a^2$, $(-1)^2 = 1$.
3. $n(ab) = (na)b = a(nb)$.

Démonstration. 1. Il suffit de remarquer $a\times 0 + a\times 0 = a \times (0 + 0) = a \times 0$ et de simplifier par $a \times 0$ (ce qui est légitime car il est inversible pour la loi $+$).

2. On a successivement :

$$\begin{aligned}a \times b + (-a) \times b &= (a - a) \times b \quad \text{par distributivité}\\ &= 0 \times b\\ &= 0 \qquad\qquad \text{d'après (1)}\end{aligned}$$

Donc $(-a) \times b$ est l'opposé de $a \times b$, donc $(-a) \times b = -(a \times b)$.
On montre de même $a \times (-b) = -(a \times b)$.

3. **Cas où $n \in \mathbb{N}$:** On peut s'en convaincre par récurrence. Le cas $n = 0$ se déduit du (1), l'hérédité se montre par application de la distributivité.

Cas où $n < 0$: alors $-n \in \mathbb{N}$, et on a

$$\begin{aligned} n(a \times b) =& (-n)(-(a \times b)) \text{ par définition de} \\ & \text{la multiplication par un entier} \\ =& (-n)((-a)b) \text{ d'après 2} \\ =& ((-n)(-a))b \\ & \text{d'après le cas précédent} \end{aligned}$$

L'autre égalité se démontre de la même façon. □

Remarque 3.0.5.
On voit ainsi que l'anneau A possède au moins deux éléments, $1_A \neq 0_A$ et donc que 0_A n'est pas inversible.

Exercice 3.0.6.
Étant donné un anneau $(A, +, \times)$, la notation $n \times a$ peut désigner d'une part le produit dans A de n par a si n et a sont deux éléments de A, d'autre part si $a \in A$ et $n \in \mathbb{Z}$, la valeur $a + \ldots + a$ où a est répété n fois dans le cas où $n \geqslant 0$ et l'opposé de $a + \ldots + a$ où a est répété $-n$ fois si $n < 0$.

Dans le cas où A et $\mathbb{Z}$ sont disjoints, cette ambiguïté n'est évidemment pas gênante si on sait auquel des deux ensembles A et n appartient.

Dans le cas contraire, cette ambiguïté n'est pas gênante non plus. Pourquoi ?

Théorème 3.0.7.
Soient $n \in \mathbb{N}$, $(A, +, \times)$ un anneau et $a, b \in A$ tels que a et b commutent (i.e. $a \times b = b \times a$). Alors :

(i) Formule du binôme de Newton :

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

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

Démonstration.
On remarque d'abord que si a, b commutent, alors toutes les puissances de a et de b commutent (le faire par récurrence).

Recopier la démonstration concernant des complexes ou des matrices carrées, à nouveau en étant conscient de l'importance de l'hypothèse "a et b commutent". □

Proposition 3.0.8 (Groupe des inversibles)**.**
Soit $(A, +, \times)$ un anneau. Alors $(A^*, \times)$ est un groupe, autrement dit l'ensemble des éléments inversibles de A, muni de (la loi induite par) la multiplication de A est un groupe.

Démonstration.
— Remarquons tout d'abord que $\times$ induit une lci sur A^*. Soit x et y deux éléments de A^*. x et y sont donc deux éléments inversibles du magma $(A, \times)$ donc, d'après la proposition 1.2.9, $x \times y$ est inversible.
— $\times$ étant une loi associative sur A, elle l'est aussi sur A^*.
— 1_A est inversible car $1_A \times 1_A = 1_A$. Donc $1_A \in A^*$. De plus 1_A est élément neutre pour la multiplication sur A, donc est élément neutre pour la multiplication sur A^*.
— Pour tout $x \in A^*$, x possède un inverse y dans A. On remarque immédiatement que y est lui-même inversible (d'inverse x), donc $y \in A^*$. Tout élément du magma $(A^*, \times)$ est donc inversible dans A^*.
$(A^*, \times)$ est donc un groupe, de neutre 1_A. □

Exemple 3.0.9.
Quel est le groupe des inversibles des anneaux $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$?

Définition 3.0.10.
1. On appelle *anneau nul* tout anneau $(\{0\}, +, \times)$ (0 est alors le neutre pour les deux lois !).
2. Dans un anneau A, on appelle diviseur de 0 tout élément *a non nul*, tel qu'il existe *b non nul* vérifiant $a \times b = 0_A$ ou $b \times a = 0_A$.
3. On appelle *anneau intègre* tout anneau commutatif non nul *ne possédant aucun diviseur de 0, c'est-à-dire vérifiant*

$$\forall (a, b) \in A^2 \quad ab = 0 \Rightarrow (a = 0 \text{ ou } b = 0)$$

Remarque 3.0.11.
Pour tout anneau A, on a $0_A = 1_A$ si et seulement si A est un anneau nul. En effet, supposons $0_A = 1_A$, alors pour tout $x \in A$, on a $x = 1_A \times x = 0_A \times x = 0_A$, donc tout élément de A est nul, donc A est l'anneau nul. Réciproquement si A est un anneau nul, tous les éléments de A sont égaux (puisqu'il n'y en a qu'un !) donc $0_A = 1_A$.

Remarque 3.0.12.
Un élément inversible a n'est jamais un diviseur de 0. En effet, pour tout b vérifiant $ab = 0$, on a nécessairement $a^{-1}ab = 0$, donc $b = 0$.

Exemple 3.0.13.
• Les anneaux usuels $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ sont intègres.
• $(\mathscr{F}(\mathbb{R}, \mathbb{R}), +, \times)$ n'est pas intègre : ex : considérer $f, g : \mathbb{R} \to \mathbb{R}$, $f(x) = 0$ si $x \geqslant 0$ et $g(x) = 0$ si $x \leqslant 1$.
• $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre : $2 \times 3 = 0$. De manière générale, $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre quand n est composé.
• $(\mathscr{M}(\mathbb{R}^2), +, \circ)$ n'est pas intègre. Par exemple avec $f(x, y) = (x, 0)$ et $g(x, y) = (0, y)$ nous avons $f \circ g = 0$.
• $\mathscr{M}_n(\mathbb{K})$ n'est pas intègre non plus, comme nous l'avons déjà vu en début d'année.

Remarque 3.0.14.
Attention donc aux simplifications de produits dans les anneaux : si l'anneau est intègre, tout fonctionne comme dans $\mathbb{R}$: $ab = ac \Rightarrow a(b-c) = 0 \Rightarrow (a = 0$ ou $b = c)$.

Sinon, on sait qu'on peut simplifier par des éléments inversibles mais on a du mal à en dire plus (quand un élément est non-inversible, il se peut qu'il soit simplifiable ou non [3]).

4 Structure de corps

Définition 4.0.1.
On appelle *corps tout anneau commutatif non nul dans lequel tout élément non nul est inversible pour* $\times$.

Exemple 4.0.2.
• $\mathbb{C}$, $\mathbb{R}$ et $\mathbb{Q}$ sont des corps. $\mathbb{N}$ et $\mathbb{Z}$ n'en sont pas.
• $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier.

Proposition 4.0.3. (i) Un corps est intègre.

(ii) Si $\mathbb{K}$ est un corps, on a $\mathbb{K}^* = \mathbb{K}\backslash\{0\}$ (qui est un groupe pour la loi induite par $\times$).

Démonstration. (i) Soit $(\mathbb{K}, +, \times)$ un corps. Soit $(a, b) \in \mathbb{K}^2$ vérifiant $ab = 0$. Supposons que a est non-nul. Alors a est inversible donc $a^{-1} \times ab = a^{-1} \times 0$, donc $b = 0$.
On a donc $a = 0$ ou $b = 0$.

(ii) Tout élément non-nul est inversible pour $\times$ d'après la définition, d'où $\mathbb{K}^* = \mathbb{K} \setminus \{ 0 \}$ et on sait d'après la proposition 3.0.25 que $(\mathbb{K}^*, \times)$ est un groupe. □

Remarque 4.0.4.
Un corps est un anneau qui est intègre, par contre un anneau intègre n'est pas forcément un corps ! Trouvez un exemple ...

3. Regarder l'ensemble des suites à valeurs entières muni de l'addition et de la multiplication terme à terme

Chapitre XII

Limite d'une fonction

Dans tout ce chapitre, sauf mention expresse du contraire, I et J sont des intervalles de $\mathbb{R}$, et $f : I \to \mathbb{R}$.

1 Préliminaires

Comme pour la notion de limite d'une suite, nous allons définir la notion de limite de fonction de manière naïve. Cela va nous ammener à répéter de nombreuses fois certains énoncés. Vous unifierez cela en spé, avec la notion de voisinage.

Nous nous permettons cependant de définir quelques raccourcis de langages qui simplifieront les énoncés.

Définition 1.0.1.
On dit qu'une propriété est vraie *au voisinage* d'un point $a \in \mathbb{R}$ s'il existe un intervalle ouvert contenant a sur lequel la propriété est vérifiée.

On dit qu'une propriété est vraie *au voisinage* de $+\infty$ (resp. de $-\infty$) s'il existe un intervalle de la forme $[A, +\infty[$ (resp. $]-\infty, A]$) sur lequel la propriété est vérifiée.

Remarque 1.0.2.
On pourrait (voire même devrait) donner ces définitions avec des intervalles ouvert : c'est équivalent.

Exemple 1.0.3.
• La fonction sinus est strictement positive au voisinage de $\pi/2$.
• La fonction Arctan est supérieure à $\pi/4$ au voisinage de $+\infty$.

Remarque 1.0.4.
Si $a \in \mathbb{R}$, si P est un prédicat portant sur les réels, P est vrai au voisinage de a si et seulement si

$$\exists \varepsilon > 0,\ \forall t \in [a-\varepsilon, a+\varepsilon],\ P(t).$$

Si P n'est défini que sur un ensemble $I \subset \mathbb{R}$, la définition **??** doit alors être modifiée en remplaçant tous les intervalles par leurs intersections avec I, *i.e*

$$\exists \varepsilon > 0,\ \forall t \in I \cap [a-\varepsilon, a+\varepsilon],\ P(t),$$

ou encore

$$\exists \varepsilon > 0,\ \forall t \in I,\ t \in [a-\varepsilon, a+\varepsilon] \Rightarrow P(t),$$

On a les mêmes écritures au voisinage de $\pm\infty$.

Exemple 1.0.5.
Si on s'intéresse à la propriété « $\frac{1}{x^2} - 1 \geqslant 0$», celle-ci n'a de sens que sur $D = \mathbb{R}^*$.

Dire que « $\frac{1}{x^2} - 1 \geqslant 0$ au voisinage de 0 » signifie qu'il existe $\varepsilon > 0$ tel que

$$\forall t \in [-\varepsilon, \varepsilon] \cap \mathbb{R}^*,\ \frac{1}{t^2} - 1 \geqslant 0.$$

Proposition 1.0.6.
Si P et Q sont vraies au voisinage de a, alors « P et Q » est vraie au voisinage de a.

Démonstration.
Montrons le dans le cas $a \in \mathbb{R}$ (les autres sont laissés au lecteur).

Soit $\alpha, \beta > 0$ tels que, pour tout $x \in \mathbb{R}$:
— si $|x-a| \leqslant \alpha$, alors $P(x)$;
— si $|x-a| \leqslant \beta$, alors $Q(x)$.

Alors, avec $\gamma = \min(\alpha, \beta) > 0$, pour tout $x \in \mathbb{R}$, si $|x-a| \leqslant \gamma$, on a bien simultanément $|x-a| \leqslant \alpha$ et $|x-a| \leqslant \beta$, donc $P(x)$ et $Q(x)$ sont vraies. □

Remarque 1.0.7.
Dire qu'une propriété est vraie au voisinage de a est vague car on ne précise pas sur quel ensemble elle est vraie mais très pratique car on ne précise pas sur quel ensemble elle est vraie !

C'est l'exact analogue du « à partir d'un certain rang » utilisé sur les suites.

Remarque 1.0.8.
Quand on parle de plusieurs propriétés vraies «au voisinage d'un point a», il faut bien comprendre que tous ces « voisinages » ne sont pas nécessairement les mêmes.

Par exemple, pour tout $\varepsilon > 0$, la propriété «$|x| \leqslant \varepsilon$» est vraie pour x au voisinage de 0 mais le « voisinage » en question dépend de ε (il s'agit de $[-\varepsilon, \varepsilon]$).

On peut remarquer d'ailleurs que, bien que pour tout $\varepsilon > 0$, la propriété «$|x| \leqslant \varepsilon$» soit vraie pour x au voisinage de 0, il est faux d'affirmer que la propriété «pour tout $\varepsilon > 0$, $|x| \leqslant \varepsilon$» est vraie

pour x au voisinage de 0 (elle n'est vraie qu'en 0).

On va s'intéresser dans la suite à la notion de limite de fonction. Étant donné une partie E de $\mathbb{R}$, une fonction f définie sur E et $a \in \overline{\mathbb{R}}$, sans même connaître f, il est intuitivement clair que la notion de limite de f n'a pas de sens dans certains cas. Par exemple si $E = \mathbb{R}^-$, se questionner sur la limite de f en $+\infty$ ou en 1 n'a aucun sens. La définition ci-dessous va nous permettre, étant donné E, de définir précisément en quels points chercher si f admet une limite a un sens. Cet ensemble de points est appelé l'adhérence de E.

Exercice 1.0.9.
Pour les ensembles E suivants, quelles sont les valeurs sur lesquelles chercher si f admet une limite a un sens ?

1. $\mathbb{R}$
2. $[0, +\infty[$
3. $]0, +\infty[$
4. $]\pi, 42[$
5. $]\pi, 42]$
6. $\mathbb{R}^*$
7. $]-\infty, -7] \cup]6, 42]$
8. $\{0\}$

Définition 1.0.10 (HP – sera vu en MP)**.**
Soit E un sous-ensemble de $\mathbb{R}$.

1. On appelle *intérieur de E* et l'on note $\mathring{E}$ l'ensemble des $x \in \mathbb{R}$ tels que E soit un voisinage de x, c'est-à-dire l'ensemble des x appartenant à E tels que E contienne un intervalle ouvert centré en x.
2. On appelle *adhérence de E* et l'on note $\overline{E}$ l'ensemble des éléments de $\overline{\mathbb{R}}$ limites de suites d'éléments de E.
3. On appelle *frontière de E* l'ensemble $\overline{E} \setminus \mathring{E}$

Exercice 1.0.11.
Vérifier que pour les exemples de l'exercice 1.0.44, cette définition donne bien la même chose.

En pratique, on pourra essentiellement se contenter de la définition suivante, en se rappelant que l'adhérence (resp. l'intérieur) de l'union d'un nombre fini d'intervalles disjoints est l'union de leurs adhérences (resp. leurs intérieurs).

Remarque 1.0.12.
E est dense dans $\mathbb{R}$ si et seulement si $\overline{E} = \overline{\mathbb{R}}$.

Définition 1.0.13.
Soit I un intervalle de la forme (a, b), avec $a, b \in \overline{\mathbb{R}}$, tels que $a \leqslant b$, et où les symboles (et) peuvent prendre la valeurs [ou].

1. On appelle *intérieur* de I, noté $\mathsf{Int}(I)$ ou $\mathring{I}$, l'intervalle $]a, b[$, c'est-à-dire I privé de ses extrémités. C'est le plus grand intervalle ouvert contenu dans I.
2. On appelle *fermeture* ou *adhérence* de I, noté $\overline{I}$, l'intervalle $[a, b]$, c'est-à-dire I augmenté de ses extrémités. C'est le plus petit intervalle fermé de $\overline{\mathbb{R}}$ contenant I.

Définition 1.0.14.
Soit I un intervalle de $\mathbb{R}$, soit $a \in \overline{\mathbb{R}}$. Si $a \in \overline{I}$, on dit que a *adhère* à I.

2 Définitions de la limite d'une fonction

Comme pour les suites, nous allons donner différentes définitions naïves de limites de fonctions : on peut considérer la limite d'une fonction en un point réel, en $+\infty$ et en $-\infty$; on peut considérer une limite réelle ou infinie. On traite donc séparément neuf cas différents.

La notion topologique de *voisinage*, que vous verrez l'année prochaine, permet d'unifier tout cela en un seul vocabulaire : quel gain en efficacité et en élégance !

2.1 Limite en un point

Définition 2.1.1 (Limite en un point réel)**.**
Soit $a \in \overline{I} \cap \mathbb{R}$, soit $\ell \in \mathbb{R}$.

• On dit que f *tend vers* ℓ *en* a et l'on note $f \underset{a}{\to} \ell$ ou $f(x) \xrightarrow[x\to a]{} \ell$ si

$$\forall \varepsilon > 0, \exists \alpha > 0, \forall x \in I, |x-a| \leqslant \alpha \Rightarrow |f(x)-\ell| \leqslant \varepsilon.$$

• On dit que f *tend vers* $+\infty$ *en* a et l'on note $f \underset{a}{\to} +\infty$ ou $f(x) \xrightarrow[x\to a]{} +\infty$ si

$$\forall A \in \mathbb{R}, \exists \alpha > 0, \forall x \in I, |x-a| \leqslant \alpha \Rightarrow f(x) \geqslant A.$$

• On dit que f *tend vers* $-\infty$ *en* a et l'on note $f \underset{a}{\to} -\infty$ ou $f(x) \xrightarrow[x\to a]{} -\infty$ si

$$\forall A \in \mathbb{R}, \exists \alpha > 0, \forall x \in I, |x-a| \leqslant \alpha \Rightarrow f(x) \leqslant A.$$

Remarque 2.1.2.
On préférera parfois écrire $|x-a| \leqslant \alpha$ sous la forme $x \in [a-\alpha, a+\alpha]$.

Le bloc $\forall x \in I, |x-a| \leqslant \alpha \Rightarrow [...]$ s'écrit alors $\forall x \in I \cap [a-\alpha, a+\alpha]\,,\ [...]$.

On remarquera la structure commune :

$$\forall [...], \exists \alpha > 0, \forall x \in I, |x-a| \leqslant \alpha \Rightarrow f(x) \in [...].$$

Définition 2.1.3 (Limite en $+\infty$)**.**
Supposons que $\sup I = +\infty$, soit $\ell \in \mathbb{R}$.
• On dit que f *tend vers* ℓ *en* $+\infty$ et l'on note $f \xrightarrow[+\infty]{} \ell$ ou $f(x) \xrightarrow[x\to+\infty]{} \ell$ si

$$\forall \varepsilon > 0, \exists B \in \mathbb{R}, \forall x \in I, x \geqslant B \Rightarrow |f(x)-\ell| \leqslant \varepsilon.$$

• On dit que f *tend vers* $+\infty$ *en* $+\infty$ et l'on note $f \xrightarrow[+\infty]{} +\infty$ ou $f(x) \xrightarrow[x\to+\infty]{} +\infty$ si

$$\forall A \in \mathbb{R}, \exists B \in \mathbb{R}, \forall x \in I, x \geqslant B \Rightarrow f(x) \geqslant A.$$

• On dit que f *tend vers* $-\infty$ *en* $+\infty$ et l'on note $f \xrightarrow[-\infty]{} -\infty$ ou $f(x) \xrightarrow[x\to-\infty]{} -\infty$ si

$$\forall A \in \mathbb{R}, \exists B \in \mathbb{R}, \forall x \in I, x \geqslant B \Rightarrow f(x) \leqslant A.$$

Remarque 2.1.4.
On préférera parfois écrire $x \geqslant B$ sous la forme $x \in [B, +\infty[$.

Le bloc $\forall x \in I, x \geqslant B \Rightarrow [...]$ s'écrit alors $\forall x \in I \cap [B, +\infty[,\ [...]$.

On remarquera la structure commune :

$$\forall [...], \exists B \in \mathbb{R}, \forall x \in I, x \geqslant B \Rightarrow f(x) \in [...].$$

Définition 2.1.5 (Limite en $-\infty$)**.**
Supposons que $\inf I = -\infty$, soit $\ell \in \mathbb{R}$.
• On dit que f *tend vers* ℓ *en* $-\infty$ et l'on note $f \xrightarrow[-\infty]{} \ell$ ou $f(x) \xrightarrow[x\to-\infty]{} \ell$ si

$$\forall \varepsilon > 0, \exists B \in \mathbb{R}, \forall x \in I, x \leqslant B \Rightarrow |f(x)-\ell| \leqslant \varepsilon.$$

• On dit que f *tend vers* $+\infty$ *en* $-\infty$ et l'on note $f \xrightarrow[-\infty]{} +\infty$ ou $f(x) \xrightarrow[x\to-\infty]{} +\infty$ si

$$\forall A \in \mathbb{R}, \exists B \in \mathbb{R}, \forall x \in I, x \leqslant B \Rightarrow f(x) \geqslant A.$$

• On dit que f *tend vers* $-\infty$ *en* $-\infty$ et l'on note $f \xrightarrow[-\infty]{} -\infty$ ou $f(x) \xrightarrow[x\to-\infty]{} -\infty$ si

$$\forall A \in \mathbb{R}, \exists B \in \mathbb{R}, \forall x \in I, x \leqslant B \Rightarrow f(x) \leqslant A.$$

Remarque 2.1.6.
On préférera parfois écrire $x \leqslant B$ sous la forme $x \in]-\infty, B]$.

Le bloc $\forall x \in I, x \leqslant B \Rightarrow [...]$ s'écrit alors $\forall x \in I \cap]-\infty, B],\ [...]$.

On remarquera la structure commune :

$$\forall [...], \exists B \in \mathbb{R}, \forall x \in I, x \leqslant B \Rightarrow f(x) \in [...].$$

Remarque 2.1.7.
On peut aussi remarquer que les trois définitions de « f tend vers $\ell \in \mathbb{R}$ » ont en commun la structure suivante.

$$\forall \varepsilon > 0, \exists [...], \forall x \in I,\ x \in [...] \Rightarrow |f(x)-\ell| \leqslant \varepsilon$$

Exercice 2.1.8.
Dégager la structure commune des trois définitions de « f tend vers $+\infty$ ». Faire de même pour $-\infty$.

Remarque 2.1.9.
Comme dans le cas des suites, on obtient des propositions équivalents en remplaçant les inégalités

larges (ou certaines d'entre elles) par des inégalités strictes. En revanche, attention aux inégalités $\varepsilon > 0$ et $\alpha > 0$ qui doivent être conservées strictes.

Remarque 2.1.10.
On peut également remplacer les conditions $A \in \mathbb{R}$ par $A \in \mathbb{R}_+^*$ ou $A \in \mathbb{R}_-^*$ suivant les cas.

Remarque 2.1.11.
L'ordre des quantificateurs dans ces définitions est évidemment essentiel.

Remarque 2.1.12.
Sur les suites, le «$\forall n \geqslant n_0$» devait être compris comme portant sur un n entier, de façon à ce que u_n ait un sens.

C'est le «$\forall x \in I$» qui ici remplit ce rôle, de façon à ce que $f(x)$ soit bien défini.

Attention à ne pas l'oublier !

Remarque 2.1.13.
Remarquez que la caractérisation de la convergence d'une suite à l'aide de «$\forall \varepsilon \exists n_0 \ldots$» est très similaire à celle de l'existence d'une limite finie pour une fonction en $+\infty$, de même la caractérisation de la divergence vers $+\infty$ d'une suite est très similaire à celle du fait qu'une fonction tend vers $+\infty$ en $+\infty$.

Cette similarité n'est pas un hasard : regardez ce que donne la définition de limite de fonction (utilisant les voisinages) pour une fonction définie sur $\mathbb{N}$. Que constatez-vous ?

Remarque 2.1.14.
Pour donner la défition de limite en un point, nous avons dû traiter neuf cas différents, ce qui est assez fastidieux. Comme dans le cas des suites, la notion de voisinage permet de donner une définition unifiée, regroupant tous les cas en une seule définition. Cette défintion unifiée est la suivante :

Soit $a \in \overline{I}$ et $\ell \in \overline{\mathbb{R}}$. On dit que f *admet* ℓ *pour limite en* a et on note $f \underset{a}{\to} \ell$ ou $f(x) \xrightarrow[x \to a]{} \ell$ si pour tout voisinage $V \in \mathscr{V}(\ell)$, il existe un voisinage $W \in \mathscr{V}(a)$ tel que $\forall x \in W \cap I \quad f(x) \in V$.

Cette définition étant plus abstraite et hors-programme, nous ne l'utiliserons pas en priorité dans ce cours, même si elle peut systématiquement être employée. Cependant, certaines démonstrations seront données sans la notion de voisinage, puis une seconde fois avec la notion de voisinage. Vous pourrez voir les simplifications que ces voisinages apportent et vous entraîner à réécrire d'autres démonstrations grâce aux voisinages.

Théorème 2.1.15.
Soit $a \in \overline{I}$, soit $\ell_1, \ell_2 \in \mathbb{R}$. Si $f(x) \xrightarrow[x \to a]{} \ell_1$ et $f(x) \xrightarrow[x \to a]{} \ell_2$, alors $\ell_1 = \ell_2$.

Démonstration.
Par symétrie et en supposant que $\ell_1 \neq \ell_2$, on a trois cas possibles pour a ($a \in \mathbb{R}$, $a = +\infty$ et $a = -\infty$), et pour chaque choix de a on a quatre cas possibles :
- $\ell_1 \in \mathbb{R}$ et $\ell_2 \in \mathbb{R}$;
- $\ell_1 \in \mathbb{R}$ et $\ell_2 = -\infty$;
- $\ell_1 \in \mathbb{R}$ et $\ell_2 = +\infty$;
- $\ell_1 = -\infty$ et $\ell_2 = +\infty$.

Cela donne donc douze cas à traiter. Nous ne les détaillerons pas tous, le lecteur saura les retrouver sans difficulté.

Supposons $a \in \mathbb{R}$, $\ell_1 \in \mathbb{R}$ et $\ell_2 \in \mathbb{R}$. Posons $\varepsilon = \frac{1}{3}|\ell_1 - \ell_2| > 0$. Il existe donc $\alpha_1, \alpha_2 > 0$ tels que, pour tout $x \in I$,
- si $|x - a| \leqslant \alpha_1$, alors $|f(x) - \ell_1| \leqslant \varepsilon$;
- si $|x - a| \leqslant \alpha_2$, alors $|f(x) - \ell_2| \leqslant \varepsilon$.

Soit $\alpha = \min(\alpha_1, \alpha_2) > 0$. Comme a adhère à I, il existe $x \in I$ tel que $|x - a| \leqslant \alpha$. Les deux conditions précédentes sont donc vérifiées, et

$$\begin{aligned} |\ell_1 - \ell_2| &= |\ell_1 - f(x) - (\ell_2 - f(x))| \\ &\leqslant |\ell_1 - f(x)| + |(\ell_2 - f(x))| \\ &\leqslant \frac{2}{3}|\ell_1 - \ell_2|. \end{aligned}$$

Cela contredit le fait que $\ell_1 \neq \ell_2$.

Supposons $a = +\infty$, $\ell_1 \in \mathbb{R}$ et $\ell_2 = -\infty$. Soit $A = \ell_1 - 1$ et $\varepsilon = \frac{1}{2}$. Il existe donc $B_1, B_2 \in \mathbb{R}$ tels que, pour tout $x \in I$,
- si $x \geqslant B_1$, alors $|f(x) - \ell_1| \leqslant \varepsilon$, notamment $f(x) \leqslant \ell_1 + \frac{1}{2} < A$;
- si $x \geqslant B_2$, alors $f(x) \geqslant A$.

Soit $B = \max(B_1, B_2)$. Comme $\sup I = +\infty$, il existe $x \in I$ tel que $x \geqslant B$. On a alors simultanément $f(x) < A$ et $f(x) \geqslant A$, ce qui est absurde. □

Définition 2.1.16.
Soit $a \in \overline{I}$. S'il existe $\ell \in \overline{\mathbb{R}}$ tel que $f(x) \xrightarrow[x\to a]{} \ell$, alors cet élément est appelé « limite de f en a » et est noté $\lim\limits_{a} f$ ou $\lim\limits_{t\to a} f(t)$.

 Le symbole $\lim\limits_{x\to a}$ ne peut s'utiliser qu'après avoir montré l'existence de ladite limite. L'utiliser avant est une erreur grave. On préfèrera *systématiquement* utiliser l'écriture $f(x) \xrightarrow[x\to a]{} \ell$.

Théorème 2.1.17.
Toute fonction possédant une limite ***finie*** en $a \in \overline{\mathbb{R}}$ est bornée au **voisinage** de a.

Démonstration.
Comme pour les suites. □

Remarque 2.1.18.
Si f admet une limite infinie en $a \in \overline{\mathbb{R}}$, alors f n'est pas bornée au voisinage de a.

Proposition 2.1.19.
Si $a \in I$ et si f tend vers $\ell \in \overline{\mathbb{R}}$ en a, alors $\ell = f(a)$.

 Il s'agit bien d'être certain que a appartient à I (et pas seulement à $\overline{I}$!).

Démonstration.
Supposons $\ell = +\infty$. soit $A = f(a) + 1$. Il existe $\alpha > 0$ tel que, pour tout $x \in I \cap [a-\alpha, a+\alpha]$, $f(x) \geqslant A$. Or, $a \in I \cap [a-\alpha, a+\alpha]$, donc $f(a) \geqslant f(a) + 1$, ce qui est absurde. De même, $\ell = -\infty$ est absurde, donc $\ell \in \mathbb{R}$.

Soit $\varepsilon > 0$, soit $\alpha > 0$ tel que, pour tout $x \in I \cap [a-\alpha, a+\alpha]$, $|f(x) - \ell| \leqslant \varepsilon$. Or, on a toujours $a \in I \cap [a-\alpha, a+\alpha]$, car $a \in I$. Ainsi, $|f(a) - \ell| \leqslant \varepsilon$.

On a donc : pour tout $\varepsilon > 0$, $|f(a) - \ell| \leqslant \varepsilon$. Cela implique bien que $f(a) = \ell$ (sinon, prendre $\varepsilon = \frac{1}{2}|f(a) - \ell|$). □

Remarque 2.1.20.
Pour tous a et ℓ réels, on montre facilement que les assertions suivantes sont équivalentes.

(i) $f \underset{a}{\to} \ell$

(ii) $f - \ell \underset{a}{\to} 0$

(iii) $|f - \ell| \underset{a}{\to} 0$

(iv) $f(a+h) \xrightarrow[h\to 0]{} \ell$

Exemple 2.1.21.
Pour s'entraîner à manipuler la définition (mais ce n'est pas la meilleure méthode dans la pratique), considérons la fonction $f : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^3 + x \end{array}$ Montrons $f(x) \xrightarrow[x\to 1]{} 2$.

On a, pour tout $x \in \mathbb{R}$, $f(x) - 2 = (x-1)(x^2 + x + 2)$.

Si $x \in [0, 2]$, alors $|x| \leqslant 2$ et donc (inégalité triangulaire) $|x^2 + x + 2| \leqslant 8$.

Soit $\varepsilon > 0$. Si $x \in \left[1 - \frac{\varepsilon}{8}; 1 + \frac{\varepsilon}{8}\right]$, alors $|x - 1| \leqslant \frac{\varepsilon}{8}$.

Ainsi, avec $\alpha = \min\left(1; \frac{\varepsilon}{8}\right)$, si $|x-1| \leqslant \alpha$, on a simultanément $|x^2 + x + 2| \leqslant 8$ et $|x - 1| \leqslant \frac{\varepsilon}{8}$.

On a alors $|f(x) - 2| \leqslant \varepsilon$.

Donc on a bien

$$\forall \varepsilon > 0, \exists \alpha > 0, \forall x \in \mathbb{R}, |x-1| \leqslant \alpha \Rightarrow |f(x) - 2| \leqslant \varepsilon.$$

Donc $f(x) \xrightarrow[x\to 1]{} 2$.

2.2 Limites à gauche et à droite en un point

Définition 2.2.1.
Soient $a \in \mathbb{R}$ et $\ell \in \overline{\mathbb{R}}$.

(i) Si f est définie au voisinage de a à gauche, c'est-à-dire si $a \in \overline{I \cap]-\infty, a[}$, on dit que f *admet ℓ pour limite à gauche en a* (ou *tend vers ℓ à gauche en a*) si $f|_{I\cap]-\infty,a[}$ admet ℓ pour limite en a.
On note alors $f(x) \xrightarrow[x\to a^-]{} \ell$, $f(x) \xrightarrow[\substack{x\to a \\ x<a}]{} \ell$ ou encore $f \underset{a^-}{\longrightarrow} \ell$.
Si elle existe, la limite à gauche est unique (puisque c'est une limite) et dans ce cas elle est notée $\lim\limits_{a^-} f$, $\lim\limits_{x\to a^-} f(x)$ ou $\lim\limits_{\substack{x\to a \\ x<a}} f(x)$.

(ii) On définit de la même manière la notion de *limite à droite*.

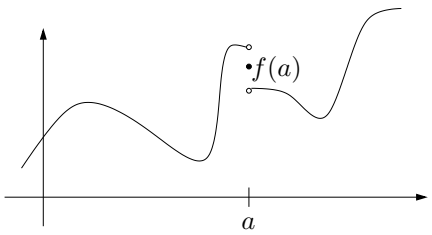


FIGURE XII.1 – Fonction f sans limite en a, ayant des limites à droite et à gauche en a différentes.

Dans la définition de limite à gauche, c'est la fonction $f|_{I\cap]-\infty,a[}$ qu'il faut considérer, et non la fonction $f|_{I\cap]-\infty,a]}$ (intervalle fermé en a). En effet, on veut que la fonction de la figure XII.1 ait une limite à gauche, ce qui n'est le cas qu'avec une restriction à un intervalle ouvert en a.

Remarque 2.2.2.
Comme pour les limites, l'existence d'une limite à gauche / droite s'écrit avec des ε. Par exemple, dans le cas où $a, \ell \in \mathbb{R}$, f admet ℓ pour limite à gauche en a si et seulement si on a

$$\forall \varepsilon > 0 \quad \exists \alpha > 0 \quad \forall x \in I \\ a - \alpha \leqslant x < a \Rightarrow |f(x) - \ell| \leqslant \varepsilon$$

On a le même genre de proposition pour les 5 autres cas (il y a au total 6 cas suivant qu'il s'agit d'une limite à gauche ou à droite d'une part et que la limite est réelle, égale à $+\infty$ ou $-\infty$ d'autre part).

Exemple 2.2.3.
On a $\dfrac{1}{x} \underset{\substack{x\to 0\\ x>0}}{\longrightarrow} +\infty$ et $\dfrac{1}{x} \underset{\substack{x\to 0\\ x<0}}{\longrightarrow} -\infty$.

Théorème 2.2.4.
Soit a un réel appartenant à I, à $\overline{I\cap]-\infty, a[}$ et à $\overline{I\cap]a, +\infty[}$. Soit $\ell \in \overline{\mathbb{R}}$. Alors $f \underset{a}{\to} \ell$ si et seulement si on a simultanément

(i) $f \underset{a^-}{\longrightarrow} \ell$
(ii) $f \underset{a^+}{\longrightarrow} \ell$
(iii) $f(a) = \ell$.

Le point (iii) est indispensable, sinon la fonction de la figure XII.2 aurait une limite en a.

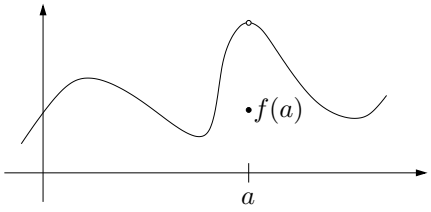


FIGURE XII.2 – Fonction f ayant des limites à gauche et à droite en a égales, mais pas de limite en a.

Démonstration. ($\Rightarrow$) Supposons d'abord $f \underset{a}{\to} \ell$. Nous avons déjà observé que $f(a) = \ell$ est nécessaire. Il est alors immédiat d'après les définitions que $f \underset{a^-}{\longrightarrow} \ell$ et $f \underset{a^+}{\longrightarrow} \ell$.

($\Leftarrow$) Réciproquement, supposons qu'on ait les trois conditions (i), (ii) et (iii). On a $f(a) = \ell$, donc $\ell \in \mathbb{R}$. Soit $\varepsilon > 0$. Il existe $\alpha^-, \alpha^+ \in \mathbb{R}_+^*$ vérifiant

$$\begin{cases} \forall x \in I \quad a - \alpha^- \leqslant x < a \quad \Rightarrow \quad |f(x) - \ell| \leqslant \varepsilon \\ \forall x \in I \quad a < x \leqslant a + \alpha^+ \quad \Rightarrow \quad |f(x) - \ell| \leqslant \varepsilon \end{cases}$$

Posons alors $\alpha = \min\{\alpha^-, \alpha^+\}$ et montrons $\forall x \in I \quad |x - a| \leqslant \alpha \Rightarrow |f(x) - \ell| \leqslant \varepsilon$.
Soit $x \in I$ tel que $|x - a| \leqslant \alpha$, c'est-à-dire $a - \alpha \leqslant x \leqslant a + \alpha$. Alors

1. si $a - \alpha \leqslant x < a$, on a en fait $a - \alpha^- \leqslant x < a$ et donc $|f(x) - \ell| \leqslant \varepsilon$;
2. si $x = a$, $f(x) = f(a) = \ell$ et donc $|f(x) - \ell| \leqslant \varepsilon$;
3. si $a < x \leqslant a + \alpha$, on a en fait $a < x \leqslant a + \alpha^+$ et donc $|f(x) - \ell| \leqslant \varepsilon$.

Dans tous les cas on a bien $|f(x) - \ell| \leqslant \varepsilon$.
On a donc $f \underset{a}{\to} \ell$.

□

Exemple 2.2.5.
Le théorème précédent permet de montrer que,

l'application $f : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \begin{cases} \mathrm{e}^x & \text{si } x \geqslant 0 \\ 1-x & \text{si } x < 0 \end{cases} \end{array}$ tend vers 1 en 0.

Remarque 2.2.6.
On n'utilisera la caractérisation d'une limite par le théorème **??** que quand la fonction n'est pas définie de la même manière à gauche et à droite du point considéré. Sinon, cela n'a aucun intérêt et l'on travaillera directement avec la définition générale de limite, ou ses caractérisations.

Remarque 2.2.7.
On pourrait aussi définir, mais le besoin s'en fera rarement sentir, la notion de « limite épointée », que l'on noterait $f(x) \xrightarrow[\substack{x\to a\\ x\neq a}]{} \ell$, qui signifie $f_{|I\setminus\{a\}} \underset{a}{\to} \ell$.

De même, les notations $f(x) \xrightarrow[\substack{x\to a\\ x\leqslant a}]{} \ell$ et $f(x) \xrightarrow[\substack{x\to a\\ x\geqslant a}]{} \ell$ ne devraient pas vous faire peur.

3 Propriétés des limites de fonctions

3.1 Opérations sur les limites

Les résultats usuels valables pour les limites de suite restent valables :

1. Soit $f : I \to \mathbb{R}$, $a \in \overline{I}$ et $\ell \in \mathbb{R}$. Alors
$$f \underset{a}{\to} \ell \iff f - \ell \underset{a}{\to} 0$$
$$f \underset{a}{\to} 0 \iff |f(x)| \xrightarrow[x\to a]{} 0$$
$$f \underset{a}{\to} \ell \iff |f(x) - \ell| \xrightarrow[x\to a]{} 0$$

2. Soit $f, g : I \to \mathbb{R}$ et $a \in \overline{I}$. Si f est bornée au voisinage de a et $g \underset{a}{\to} 0$, alors $f \times g \underset{a}{\to} 0$.

Exemple 3.1.1.
Le deuxième point permet de montrer $\dfrac{\sin x}{x} \xrightarrow[x\to+\infty]{} 0$.

Pour les opérations usuelles (somme, produit et inverse), les résultats valables pour les limites de suites sont toujours valables pour les fonctions, et les démonstrations sont tout à fait similaires. Nous ne les redémontrerons donc pas, mais vous devez savoir les faire sans problème.

Voyons le théorème sur la composition de deux fonctions ayant une limite :

Théorème 3.1.2.
Soient $f : I \to \mathbb{R}$ et $g : J \to \mathbb{R}$ deux applications vérifiant $f(I) \subset J$ et soit $a \in \overline{I}$, $b \in \overline{J}$ et $\ell \in \overline{\mathbb{R}}$. Si $f \underset{a}{\to} b$ et $g \underset{b}{\to} \ell$, alors $g \circ f \underset{a}{\to} \ell$.

Remarque 3.1.3.
L'hypothèse $b \in \overline{J}$ est superflue : si $f : I \to J$ a une limite b en a, alors automatiquement, $b \in \overline{J}$.

Démonstration.
On a vingt-sept cas à distinguer, selon si a, b et ℓ sont chacun réel, $+\infty$ ou $-\infty$. Nous ne détaillerons pas tous ces cas, le lecteur intéressé saura les retrouver facilement.

Si $a \in \mathbb{R}$, $b \in \mathbb{R}$ et $\ell \in \mathbb{R}$. Soit $\varepsilon > 0$, posons $V_\ell = [\ell - \varepsilon, \ell + \varepsilon]$. Il existe $\alpha > 0$ tel que, pour tout $y \in J \cap V_b$, avec $V_b = [b-\alpha, b+\alpha]$, on a $g(y) \in V_\ell$. Il existe donc $\eta > 0$ tel que, pour tout $x \in I \cap V_a$, avec $V_a = [a-\eta, a+\eta]$, on a $f(x) \in V_b$. Soit $x \in I \cap V_a$. On a, d'une part, $f(x) \in V_b$ et, d'autre part, $f(x) \in J$. Donc $g(f(x)) \in V_\ell$. On a bien montré $g \circ f \underset{a}{\to} \ell$.

Si $a = +\infty$, $b = -\infty$ et $\ell = +\infty$. Soit $A \in \mathbb{R}$, posons $V_\ell = [A, +\infty[$. Il existe $B \in \mathbb{R}$ tel que, pour tout $y \in J \cap V_b$, avec $V_b =]-\infty, B]$, on a $g(y) \in V_\ell$. Il existe donc $C \in \mathbb{R}$ tel que, pour tout $x \in I \cap V_a$, avec $V_a = [A, +\infty[$, on a $f(x) \in V_b$. Soit $x \in I \cap V_a$. On a, d'une part, $f(x) \in V_b$ et, d'autre part, $f(x) \in J$. Donc $g(f(x)) \in V_\ell$. On a bien montré $g \circ f \underset{+\infty}{\to} +\infty$. □

Remarque 3.1.4.
La structure de la preuve précédente ne change pas en fonction des natures de a, b et ℓ, mais seulement les formes des intervalles V_a, V_b, V_ℓ.

À cause des vingt-sept cas à distinguer, cette démonstration est un exemple typique de démonstration où la notion de voisinage fait gagner du temps. Redémontrons donc ce résultat :

Démonstration.
Soit $V \in \mathscr{V}(\ell)$. Montrons qu'il existe un voisinage W de a vérifiant $(g \circ f)(W \cap I) \subset V$.

On a $g \underset{b}{\to} \ell$, donc il existe un voisinage W' de b vérifiant $g(W' \cap J) \subset V$.

Or $f \underset{a}{\to} b$, donc il existe un voisinage W de a vérifiant $f(W \cap I) \subset W'$.

Or $f(I) \subset J$, donc $f(W \cap I) \subset J$, donc $f(W \cap I) \subset W' \cap J$.

Donc $(g \circ f)(W \cap I) \subset g(W' \cap J) \subset V$.

On a donc bien $g \circ f \underset{a}{\to} \ell$. □

Remarque 3.1.5.
On a vu (remarque 2.1.3) que la définition de la limite d'une suite n'est qu'un cas particulier de celle de fonction. Ce théorème de composition sur les fonctions a donc pour corollaire celui qu'on a énoncé au chapitre concernant les limites de suites sur la composition d'une fonction et d'une suite.

Exemple 3.1.6.
Ce théorème permet de montrer par exemple que $\ln\left(\tan x^2\right) \xrightarrow[x\to\frac{\sqrt{\pi}}{2}]{} 0$.

Théorème 3.1.7 (Caractérisation séquentielle des limites)**.**
Soient $a \in \overline{I}$, $\ell \in \overline{\mathbb{R}}$. On a équivalence entre :

(i) $f(x) \xrightarrow[x\to a]{} \ell$

(ii) pour toute suite (u_n) telle que $u_n \in I$ et $u_n \xrightarrow[n\to+\infty]{} a$, on a $f(u_n) \xrightarrow[n\to+\infty]{} \ell$.

Démonstration.
Traitons les cas a et ℓ finis (les autres cas se traitent de manière similaire).

(i)⇒(ii) C'est une conséquence immédiate du résultat de composition d'une application et d'une suite.

¬(i)⇒ ¬(ii) Supposons $f \not\underset{a}{\to} \ell$. Alors il existe $\varepsilon > 0$ vérifiant

$$\forall \eta \in \mathbb{R}_+^* \exists x \in I \quad (x \in [a-\eta, a+\eta] \text{ et } |f(x)-\ell| > \varepsilon) \tag{XII.1}$$

Soit alors $n \in \mathbb{N}$. Comme $\frac{1}{n+1} \in \mathbb{R}_+^*$, d'après l'assertion (XII.1), il existe $u_n \in I$ vérifiant

(a) $u_n \in [a - \frac{1}{n+1}, a + \frac{1}{n+1}]$

(b) et $|f(u_n) - \ell| > \varepsilon$.

On a donc construit une suite u d'éléments de I. Le point (a) nous assure qu'elle converge vers a, le second que $f(u_n)$ ne tend pas vers ℓ (une suite minorée par un réel strictement positif ne saurait tendre vers 0).

□

Exemple 3.1.8.
$f : \begin{array}{ccc} \mathbb{R}_+^* & \to & \mathbb{R} \\ x & \mapsto & \sin(1/x) \end{array}$ n'a pas de limite en 0.
Il suffit en effet de considérer la suite de terme général $u_n = \dfrac{1}{\pi/2 + n\pi}$ pour $n \in \mathbb{N}$ pour s'en convaincre.

3.2 Passage à la limite et relations d'ordre

Les théorèmes suivants sont analogues à des résultats déjà vu sur les suites.

Théorème 3.2.1.
Soit $f : I \to \mathbb{R}$, $a \in \overline{I}$ et $(m, M, \ell) \in \mathbb{R}$.
Supposons $f \underset{a}{\to} \ell$ et $m < \ell < M$.
Alors, au voisinage de a, on a $m < f(x) < M$.

Démonstration.
On traite le cas $a \in \mathbb{R}$, les autres cas sont laissés au lecteur.

Soit $\varepsilon = \dfrac{\min(\ell - m, M - \ell)}{2} > 0$. On a bien $[\ell - \varepsilon; \ell + \varepsilon] \subset]m, M[$.

Ainsi, il existe $\alpha > 0$ tel que, pour tout $x \in [a - \alpha, a + \alpha] \cap I$, on a $f(x) \in [\ell - \varepsilon; \ell + \varepsilon]$, donc $f(x) \in]m, M[$. □

Avec les voisinages :

Démonstration.
$]m, M[$ est un intervalle ouvert contenant ℓ, c'est donc un voisinage de ℓ. Donc il existe un voisinage V de a tel que pour tout $x \in V \cap I$, on a $f(x) \in]m, M[$. □

Remarque 3.2.2.
Le plus souvent, ce résultat s'applique sous la forme suivante :

Soit $f : I \to \mathbb{R}$, $a \in \overline{I}$ vérifiant $f \underset{a}{\to} \ell$. Alors

(i) Soit $M \in \mathbb{R}$ vérifiant $\ell < M$. Alors au voisinage de a, $f(x) < M$.

(ii) Soit $m \in \mathbb{R}$ vérifiant $m < \ell$. Alors au voisinage de a, $f(x) > m$.

 Ce résultat est faux avec des inégalités larges : ainsi $x^2 \xrightarrow[x\to0]{} 0$ et donc sa limite est négative. Mais dire que pour x au voisinage de 0 on a $x^2 \leqslant 0$ est *faux*.

Corollaire 3.2.3 (Passage à la limite dans une inégalité)**.**
Soit $a \in \overline{I}$ et $f : I \to \mathbb{R}$ vérifiant $f \underset{a}{\to} \ell$. Soit $(m, M) \in \mathbb{R}^2$.

(i) Si M majore f au voisinage de a, alors $\ell \leqslant M$.

(ii) Si m minore f au voisinage de a, alors $m \leqslant \ell$.

Démonstration.
On traite le cas $a \in \mathbb{R}$, les autres cas sont laissés au lecteur.

(i) Supposons que M majore f sur l'intersection de I et d'un intervalle $V_1 = [a - \alpha, a + \alpha]$, avec $\alpha > 0$.
Par l'absurde, supposons $\ell > M$. D'après le théorème 3.2.1, il existe $\eta > 0$ tel que, avec $V_2 = [a - \eta, a + \eta]$, pour tout $x \in V_2 \cap I$, on a $f(x) > M$.
Pour tout $x \in V_1 \cap V_2 \cap I$, on a alors $f(x) > M$ et $f(x) \leqslant M$.
Or $V_1 \cap V_2 \cap I$ est non vide, c'est donc absurde.
On a donc $\ell \leqslant M$.

(ii) On constate qu'au voisinage de a, $-m$ majore $-f$ et l'on applique le résultat du (i) à $-f$, $-\ell$ et $-m$.

□

Corollaire 3.2.4 (Passage à la limite dans une inégalité, deuxième version)**.**
Soit $f, g : I \to \mathbb{R}$, $a \in \overline{I}$ et $(\ell, \ell') \in \mathbb{R}^2$.
Supposons $f \underset{a}{\to} \ell$, $g \underset{a}{\to} \ell'$ et $f(x) \leqslant g(x)$ au voisinage de a. Alors $\ell \leqslant \ell'$.

Démonstration.
On a $(g - f)(x) \geqslant 0$ pour x au voisinage de a et $g - f \underset{a}{\to} \ell' - \ell$. Donc d'après le corollaire 3.2.3, on a $\ell' - \ell \geqslant 0$, donc $\ell \leqslant \ell'$. □

 Les inégalités strictes ne sont pas conservées par passage à la limite. Par exemple, au voisinage de $+\infty$ on $\mathrm{e}^{-x} > 0$, mais on a $\mathrm{e}^{-x} \xrightarrow[x \to +\infty]{} 0$.

4 Théorèmes d'existence

4.1 Théorèmes des gendarmes et de minoration/majoration

On retrouve sur les limites de fonctions les mêmes théorèmes d'encadrement que pour les suites.

Théorème 4.1.1 (Théorème d'encadrement, ou théorème des gendarmes)**.**
Soit $f, m, M : I \to \mathbb{R}$ trois applications, $a \in \overline{I}$ et $\ell \in \mathbb{R}$.
Supposons qu'on a $m \underset{a}{\to} \ell$ et $M \underset{a}{\to} \ell$ et qu'au voisinage de a on a $m(x) \leqslant f(x) \leqslant M(x)$.
Alors, f tend vers ℓ en a.

Démonstration.
On traite le cas $a \in \mathbb{R}$. Les autres cas sont laissés au lecteur, la structure de la démonstration de changeant pas.
Soit $\varepsilon > 0$, posons $V_\ell = [\ell - \varepsilon, \ell + \varepsilon]$. Il existe $\alpha, \beta > 0$ tels que, pour tout $x \in I$,
— si $x \in V_a$, alors $m(x) \in V_\ell$;
— si $x \in V'_a$, alors $M(x) \in V_\ell$;
avec $V_a = [a - \alpha, a + \alpha]$ et $V'_a = [a - \beta, a + \beta]$. Soit enfin $\eta > 0$ tel que, pour tout $x \in I$, si $x \in I \cap V''_a$, avec $V''_a = [a - \eta, a + \eta]$, alors $m(x) \leqslant f(x) \leqslant M(x)$. Il suffit de remarquer que, si $x \in I \cap V_a \cap V'_a \cap V''_a$, alors $m(x) \leqslant f(x) \leqslant M(x)$ et $m(x), M(x) \in V_\ell$, donc $f(x) \in V_\ell$, car V_ℓ est un intervalle. On a donc bien $f \underset{a}{\to} \ell$. □

Théorème 4.1.2 (Théorème de minoration)**.**
Soit $f, m : I \to \mathbb{R}$ deux applications, $a \in \overline{I}$ et $\ell \in \mathbb{R}$.
Supposons qu'on a $m \underset{a}{\to} +\infty$ et qu' au voisinage de a, on a $m(x) \leqslant f(x)$.
Alors, f admet une limite en a et cette limite vaut $+\infty$.

Démonstration.
On traite le cas $a = -\infty$. Les autres cas sont laissés au lecteur, la structure de la démonstration de changeant pas.
Soit $A \in \mathbb{R}$, posons $V_{+\infty} = [A, +\infty[$. Il existe $B \in \mathbb{R}$ tel que, pour tout $x \in I$, avec $V_a =]-\infty, B]$, si $x \in V_a$, alors $m(x) \in V_{+\infty}$. Soit enfin $C \in \mathbb{R}$ tel que, avec $V'_a =]-\infty, C]$, pour tout $x \in I$, si $x \in V'_a$, alors $m(x) \leqslant f(x)$. Il suffit de remarquer que, si $x \in I \cap V_a \cap V'_a$, alors $m(x) \leqslant f(x)$ et $m(x) \in V_\ell$, donc $f(x) \in V_\ell$. On a donc bien $f \underset{a}{\to} +\infty$. □

Théorème 4.1.3 (Théorème de majoration)**.**
Soit $f, M : I \to \mathbb{R}$ deux applications, $a \in \overline{I}$ et $\ell \in \mathbb{R}$.
Supposons qu'on a $M \underset{a}{\to} -\infty$ et qu'au voisinage de a, on a $f(x) \leqslant M(x)$.

Alors, f admet une limite en a et cette limite vaut $-\infty$.

Démonstration.
Il suffit d'appliquer le théorème de minoration à $-f$. □

Corollaire 4.1.4.
Soient $f, g : I \to \mathbb{R}$ deux applications et $a \in \overline{I}$. Si au voisinage de a on a $|f| \leqslant g$ et si $g \underset{a}{\to} 0$, alors $f \underset{a}{\to} 0$.

Démonstration.
Il suffit de remarquer qu'au voisinage de a, on a $-g \leqslant f \leqslant g$. □

4.2 Théorème de la limite monotone

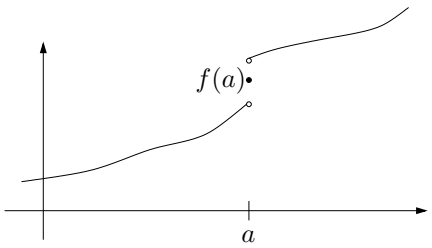


FIGURE XII.3 – Illustration de limite monotone : à retenir !

Théorème 4.2.1.
Soit $f : I \to \mathbb{R}$ une application croissante. On note α et β les bornes inférieures et supérieures de I dans $\overline{\mathbb{R}}$. Alors :

(i) f possède une limite à gauche (resp. à droite) en tout point a de $]\alpha, \beta]$ (resp. $[\alpha, \beta[$) et l'on a, pour chaque a où ces limites ont un sens,

$$f(x) \underset{\substack{x\to a\\ x<a}}{\longrightarrow} \sup_{I\cap]-\infty,a[} f$$

ainsi que

$$f(x) \underset{\substack{x\to a\\ x>a}}{\longrightarrow} \inf_{I\cap]a,+\infty[} f \ .$$

(ii) Soient $a, b \in \mathring{I}$ tels que $a < b$. Alors,

$$\lim_{a^-} f \leqslant f(a) \leqslant \lim_{a^+} f \leqslant \lim_{b^-} f \leqslant f(b) \leqslant \lim_{b^+} f.$$

(iii) Dans $\overline{\mathbb{R}}$, f admet une limite à droite en α. Si f est minorée, cette limite est finie, sinon elle vaut $-\infty$.

(iv) Dans $\overline{\mathbb{R}}$, f admet une limite à gauche en β. Si f est majorée, cette limite est finie, sinon elle vaut $+\infty$.

Si f est décroissante, on a bien sûr des résultats analogues.

Démonstration. **(i)** On ne montre le résultat que pour la limite à gauche.
Soit $a \in]\alpha, \beta]$. On pose $V = f(I\cap]-\infty, a[) = \{ f(x) \mid x < a \}$. L'ensemble V est non vide puisque $I\cap]-\infty, a[$ est non vide. Posons $\ell = \sup_{\substack{x\in I\\ x<a}} f(x)$.
On a $\ell = +\infty$ ou $\ell \in \mathbb{R}$. Distinguons ces deux cas :

(a) $\ell = +\infty$. Alors soit M un réel fixé, il existe $y \in I\cap]-\infty, a[$ tel que $f(y) \geqslant M$.
Alors, puisque f est croissante, pour tout $x \in]y, a[\cap I$, on a $f(x) \geqslant M$.
Donc f prend ses valeurs dans $[M, +\infty[$ sur au voisinage de a, à gauche.
On a donc bien $f \underset{a-}{\longrightarrow} +\infty$.

(b) $\ell \in \mathbb{R}$. Alors, soit $\varepsilon > 0$. Il existe $y \in I\cap]-\infty, a[$ tel que $f(y) \geqslant \ell - \varepsilon$.
Alors, pour tout $x \in]y, a[\cap I$, on a $f(x) \geqslant \ell - \varepsilon$, f étant croissante, et $f(x) \leqslant \ell$ par définition de ℓ.
On en déduit qu'au voisinage à gauche de a, f prend ses valeurs dans $[\ell - \varepsilon, \ell + \varepsilon]$.
f admet donc pour limite ℓ en a à gauche.

(ii) Remarquons tout d'abord que, f étant croissante $\{ f(x) \mid x \in I\cap]-\infty, a[\}$ est majoré par $f(a)$, donc d'après le point (i), on a $\lim_{a-} f \leqslant f(a)$.
De la même façon, on a $f(a) \leqslant \lim_{a^+} f$, $\lim_{b^-} f \leqslant f(b)$ et $f(b) \leqslant \lim_{b^+} f$.
Par ailleurs, $\lim_{b-} f$ majore $f(]a, b[)$ et $\lim_{a+}$ minore ce même ensemble, qui est non vide. Donc $\lim_{a^+} f \leqslant \lim_{b^-} f$.
On a donc le résultat.

(iii) (iii) (resp. (iv)) sont des conséquences immédiates de (i), l'existence d'un minorant (resp. majorant) étant équivalente au fait que la borne inférieure (resp. supérieure) soit finie.

Pour le cas d'une fonction décroissante, il suffit d'appliquer le résultat sur les fonctions croissantes à $-f$. □

5 Cas des fonctions à valeurs complexes

Dans cette partie, on considère une application complexe $f : I \to \mathbb{C}$.

Notons tout de suite que les notions de fonction complexe majorée, minorée ou monotone n'ont **aucun sens**, car il n'y a pas de relation d'ordre naturelle sur $\mathbb{C}$. Cependant, on peut définir la notion de fonction complexe bornée.

Définition 5.0.1.
On dit que f est *bornée* s'il existe $K \in \mathbb{R}^*$ tel que pour tout $x \in I$ on ait $|f(x)| \leqslant K$.

Remarque 5.0.2.
f est bornée si et seulement si $\operatorname{Re} f$ et $\operatorname{Im} f$ sont bornées.

Définition 5.0.3.
Soit $a \in \mathbb{C}$. Une propriété P est vraie au voisinage de a s'il existe $r > 0$ tel que, pour tout $z \in \mathbb{C}$, si $|z - a| \leqslant r$, alors $P(z)$ est vraie.

Remarque 5.0.4.
La notion bidimensionnelle de voisinage complexe donnée ici généralise assez bien la notion unidimensionnelle de voisinage réel, néanmoins d'autres définitions seraient possibles : on pourrait utiliser, à la place de disques fermés, des disques ouverts ou bien des rectangles (fermés ou ouverts).

Définition 5.0.5.
Soit $a \in \overline{I}$ et $\ell \in \mathbb{C}$. On dit que f *admet ℓ pour limite en a*, ou f *tend vers ℓ en a*, si $|f(x) - \ell| \xrightarrow[x \to a]{} 0$.

On note bien entendu ceci $f \underset{a}{\to} \ell$ ou encore $f(x) \xrightarrow[x \to a]{} \ell$.

Remarque 5.0.6.
Ceci nous ramène au cas d'une limite d'une fonction à valeurs réelles.

Remarque 5.0.7.
La définition quantifiée de « f tend vers ℓ en a » s'écrit comme pour une fonction réelle :

$$\forall \varepsilon > 0, \exists \alpha > 0, \forall x \in I, |x - a| \leqslant \alpha \Rightarrow |f(x) - \ell| \leqslant \varepsilon.$$

Théorème 5.0.8.
Soit $a \in \overline{I}$ et $\ell \in \mathbb{C}$. Les deux assertions suivantes sont équivalentes :

(i) $f \underset{a}{\to} \ell$;

(ii) $\operatorname{Re}(f) \underset{a}{\to} \operatorname{Re}(\ell)$ et $\operatorname{Im}(f) \underset{a}{\to} \operatorname{Im}(\ell)$.

Démonstration.
Cette démonstration s'effectue comme celle du théorème équivalent concernant les suites complexes. □

Exemple 5.0.9.

$$\frac{\mathrm{e}^{ix}}{1 + x^2} \xrightarrow[x \to +\infty]{} 0$$

Théorème 5.0.10.
Si f a une limite en un point de $\overline{I}$, cette limite est unique.

Démonstration.
Deux démonstrations sont possibles : ou bien on utilise le théorème 5.0.8, ou bien on reprend la démonstration donnée dans le cas réel (il suffit alors essentiellement de changer des $\mathbb{R}$ en $\mathbb{C}$). □

Certains autres résultats établis pour les fonctions réelles sont toujours valables pour les fonctions complexes :

1. toute fonction à valeurs complexes ayant une limite en un point est bornée au voisinage de ce point,
2. les limites à gauche et à droite en un point peuvent être également définies,
3. la caractérisation séquentielle de la limite est maintenue,
4. la corollaire 4.1.2 du théorème des gendarmes se généralise aux fonctions f à valeurs complexes, ce qui permet également de montrer que le produit d'une fonction bornée au voisinage d'un point a par une fonction de limite

nulle en a est une fonction de limite nulle en a.

5. les opérations sur les limites ne faisant pas intervenir de limite infinie demeurent.

Les grands théorèmes ne se généralisent pas, de nouveau à cause du manque de relation d'ordre naturelle sur $\mathbb{C}$.

Chapitre XIII

Continuité

Dans tout ce chapitre, I et J sont des intervalles de $\mathbb{R}$, $f : I \to \mathbb{R}$ et $a \in I$, sauf mention expresse du contraire.

1 Définitions et premières propriétés

1.1 Définitions

Définition 1.1.1.
On dit que f est *continue en a* si f admet une limite ***finie*** en a. Puisque $a \in I$, on sait que dans ce cas $f \underset{a}{\to} f(a)$, et donc f est continue en a s'écrit :

$$\forall \varepsilon > 0, \exists \alpha > 0, \forall x \in I, |x-a| \leqslant \alpha \Rightarrow |f(x)-f(a)| \leqslant \varepsilon$$

On dit que f est *continue sur I* si f est continue en tout point de I.

On note $\mathscr{C}(I, \mathbb{R})$ l'ensemble des fonctions continues de I dans $\mathbb{R}$.

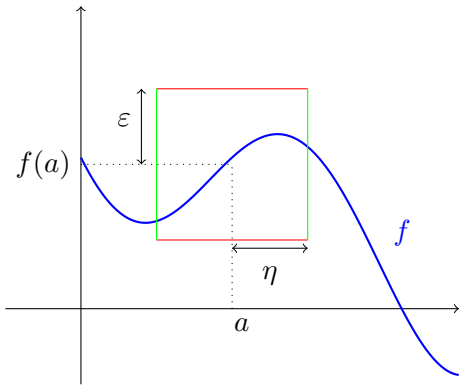


FIGURE XIII.1 – Illustration de la définition d'une fonction continue en a, ε et η étant fixés.

Remarque 1.1.2.
— On verra que cette définition est cohérente avec l'idée qu'une fonction est continue si et seulement si on peut en tracer le graphe sans lever le crayon.
— Attention à l'ordre des quantificateurs $\forall$ et $\exists$.

Exemple 1.1.3.
Quasiment toutes les fonctions usuelles sont continues.

— La fonction cos : pour tous réels x et x_0, on a en effet

$$|\cos x - \cos x_0| = \left|-2 \sin \frac{x+x_0}{2} \sin \frac{x-x_0}{2}\right| \leqslant 2 \left|\sin \frac{x-x_0}{2}\right| \leqslant |x-x_0|.$$

— La fonction $\sqrt{.}$: En effet, d'une part elle est continue en 0, car on a

$$\forall \varepsilon > 0 \quad \forall x \in \left[0, \varepsilon^2\right] \quad \sqrt{x} \leqslant \varepsilon.$$

D'autre part, soit $x_0 > 0$. Alors soit $x \in \mathbb{R}^+$, on a $|\sqrt{x} - \sqrt{x_0}| = \dfrac{|x-x_0|}{\sqrt{x}+\sqrt{x_0}} \leqslant \dfrac{|x-x_0|}{\sqrt{x_0}}$. Donc si $|x-x_0| \leqslant \dfrac{x_0}{2}$, alors $x \geqslant \dfrac{x_0}{2}$, d'où $\sqrt{x} + \sqrt{x_0} \geqslant \left(\dfrac{1}{\sqrt{2}} + 1\right)\sqrt{x_0}$. En notant C cette valeur (qui ne dépend pas de x), on a donc

$$\forall x \in \left[\frac{x_0}{2}, \frac{3x_0}{2}\right] \quad |\sqrt{x} - \sqrt{x_0}| \leqslant \frac{1}{C} |x-x_0|.$$

On a donc

$$\sqrt{x} \xrightarrow[x \to x_0]{} \sqrt{x_0}.$$

Définition 1.1.4 (Continuité à gauche et à droite)**.**
On dit que f est *continue à gauche* (resp à droite) si $f_{|I \cap]-\infty, a]}$ (resp. $f_{|I \cap [a, +\infty[}$) est continue en a, c'est-à-dire admet une limite en a, qui est alors nécessairement $f(a)$.

Remarque 1.1.5.
Cette fois, on ferme les intervalles en a dans les restrictions de f, à l'inverse de ce que l'on faisait pour les limites à gauche et à droite.

Théorème 1.1.6.
f est continue en a si et seulement si f est continue à gauche et à droite en a.

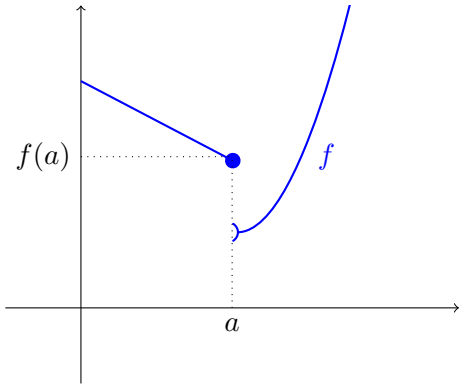


FIGURE XIII.2 – Illustration d'une fonction continue à gauche en a, mais pas à droite.

Démonstration.
D'une part f continue en a si et seulement si la limite de f en a existe, ce qui est vrai si et seulement si les limites de f en à, gauche et à droite, existent et valent $f(a)$.

D'autre part, f est continue à gauche (resp. à droite) si et seulement si la limite de f en a, à gauche (resp. à droite) existe et vaut $f(a)$. □

Exemple 1.1.7. — On reprend l'exemple du chapitre précédent :

$$f : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \begin{cases} \mathrm{e}^{\,x} & \text{si } x \geqslant 0 \\ 1-x & \text{sinon} \end{cases} \end{array}$$

Alors f est continue en 0.

— Posons

$$g : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \begin{cases} \frac{\ln(1+|x|)}{x} & \text{si } x \neq 0 \\ 0 & \text{sinon} \end{cases} \end{array}$$

Alors g a pour limite à droite 1 en 0, mais $g(0) \neq 1$, donc g n'est pas continue en 0.

Remarque 1.1.8.
On n'utilisera cette caractérisation de la continuité par les continuités à gauche et à droite que lorsque la fonction que l'on étudie est définie différemment à gauche et à droite du point considéré. Sinon, on reviendra à la définition générale.

1.2 Prolongement par continuité en un point

Définition 1.2.1.
Soit $a \in I$ et $f : I \setminus \{a\} \to \mathbb{R}$. On dit que f est *prolongeable par continuité en a* s'il existe une application $\tilde{f} : I \to \mathbb{R}$ qui coïncide avec f sur $I \setminus \{a\}$ (c'est-à-dire vérifiant $\tilde{f}_{|I\setminus\{a\}} = f$), et qui est continue en a.

Remarque 1.2.2.
Quand on prolonge en v une application f définie sur un intervalle $[u, v[$ ou $]u, v[$ (resp. $]v, u]$ et $]v, u[$) et qu'on prolonge f en v par continuité, on parle de prolongement par continuité à droite (resp à gauche).

Exercice 1.2.3.
Quels sont les prolongements par continuité en 0 de

1. $\begin{array}{ccc} \mathbb{R}^* & \to & \mathbb{R} \\ x & \mapsto & \dfrac{1}{x} \end{array}$?
2. $\begin{array}{ccc} \mathbb{R}^* & \to & \mathbb{R} \\ x & \mapsto & \dfrac{\sin(x)}{x} \end{array}$?
3. $\begin{array}{ccc} \mathbb{R}^* & \to & \mathbb{R} \\ x & \mapsto & \sin\dfrac{1}{x} \end{array}$?

Théorème 1.2.4.
Avec les mêmes hypothèses que dans la définition 1.2.1 : f est prolongeable par continuité en a si et seulement si la limite de f en a existe ***et est finie***. Dans ce cas le prolongement est unique, noté $\tilde{f}$ et défini par

$$\tilde{f} : \begin{array}{ccc} I & \to & \mathbb{R}, \\ x & \mapsto & \begin{cases} f(x) & \text{si } x \neq a, \\ \ell & \text{si } x = a, \end{cases} \end{array}$$

où ℓ est la limite de f en a.

Très souvent, par abus de notation, on notera f la fonction $\tilde{f}$.

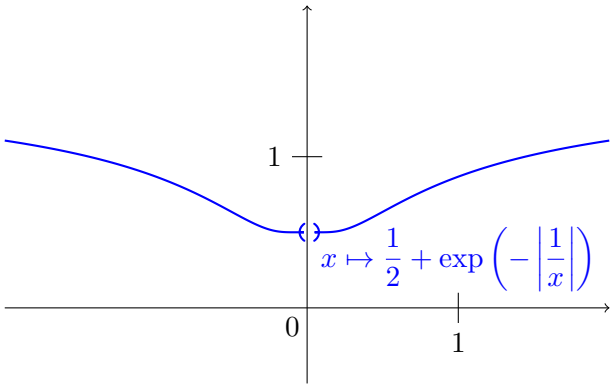


FIGURE XIII.3 – Illustration d'une fonction prolongeable par continuité en 0.

Démonstration.
Démontrons implication et réciproque :

— Soit $\tilde{f}$ un prolongement par continuité de f en a. $\tilde{f}$ est définie et continue en a, on a donc

$$\tilde{f}(x) \xrightarrow[\substack{x\to a\\ x\neq a}]{} \tilde{f}(a)$$

Or, pour tout $x \in I \setminus \{ a \}$, on a $\tilde{f}(x) = f(x)$, donc

$$f(x) \xrightarrow[x\to a]{} \tilde{f}(a)$$

Donc $\tilde{f}(a)$ est nécessairement la limite de f en a. Cette limite est donc finie. Donc $\tilde{f}$ est nécessairement l'application

$$\begin{array}{rcl} I & \to & \mathbb{R} \\ x & \mapsto & \begin{cases} f(x) & \text{si } x \neq a \\ \ell & \text{si } x = a \end{cases} \end{array}$$

Donc si f admet un prolongement par continuité alors la limite de f en a existe et est finie ; le prolongement par continuité est alors bien celui donné dans l'énoncé.

— Réciproquement, supposons que la limite de f en a existe et est finie, notons la ℓ. Alors, définissons $\tilde{f}$ comme donné dans l'énoncé. $\tilde{f}$ coïncide alors avec f sur $I \setminus \{ a \}$ et on a donc

$$\tilde{f}(x) \xrightarrow[\substack{x\to a\\ x\neq a}]{} \ell$$

Donc

$$\tilde{f}(x) \xrightarrow[\substack{x\to a\\ x\neq a}]{} \tilde{f}(a)$$

$\tilde{f}$ est donc continue en a.

□

Ce théorème est parfois utilisé sous la forme :

Corollaire 1.2.5.
Soient $a \in \mathring{I}$ et $g : I\setminus\{a\} \to \mathbb{R}$ une application. Si les limites de g en a, à gauche et à droite, existent, sont égales et ***sont finies***, alors, en notant ℓ cette limite, il existe un unique prolongement par continuité $\widetilde{g}$ de g obtenu en posant $\widetilde{g}(a) = \ell$.

Démonstration.
C'est immédiat, puisqu'on sait que la limite de g en a existe si et seulement si les limites de g en a, à gauche et à droite, existent et sont égales. □

Exemple 1.2.6.
Peut-on prolonger par continuité en 0 l'application

$$\begin{array}{rcl} f : \ ]-1,+\infty[\setminus\{0\} & \to & \mathbb{R} \\ x & \mapsto & \begin{cases} \frac{\sin x}{x} & \text{si } x > 0 \\ \frac{\ln(1+x)}{x} & \text{si } x < 0 \end{cases} \end{array}$$

Même question en -1.

1.3 Caractérisation séquentielle de la continuité

Théorème 1.3.1.
Les assertions suivantes sont équivalentes :

(i) f est continue en a ;

(ii) pour toute suite (u_n) à valeurs dans I vérifiant $u_n \xrightarrow[n\to+\infty]{} a$, on a $f(u_n) \xrightarrow[n\to+\infty]{} f(a)$.

Démonstration.
C'est une conséquence immédiate de la caractérisation séquentielle de la limite. □

1.4 Opérations sur la continuité

Lemme 1.4.1.
Soit $g : I \to \mathbb{R}$ continue en $a \in I$ et telle que $g(a) > 0$. Alors g est strictement positive dans un voisinage de a (idem avec < 0).

Démonstration.
Il suffit de remarquer que la limite de g en a est strictement positive et d'utiliser les résultats connus sur les limites. □

Théorème 1.4.2.
Soient $\lambda \in \mathbb{R}$ et $f, g : I \to \mathbb{R}$.

(i) Si f est continue en a alors $|f|$ et λf aussi.

(ii) Si f et g continues en a alors $f+g$, fg, $\sup(f,g)$ et $\inf(f,g)$ aussi et si $g(a) \neq 0$ alors $\dfrac{f}{g}$ aussi.

Démonstration.
Le théorème est une conséquence immédiate des résultats sur les limites et des remarques suivantes :

1. Pour tout $x \in I$,
$$\max(f(x), g(x)) = \frac{f(x) + g(x) + |f(x) - g(x)|}{2}$$
$$\min(f(x), g(x)) = \frac{f(x) + g(x) - |f(x) - g(x)|}{2}$$

2. Si $g(a) \neq 0$ et g continue en a, alors au voisinage de a, g ne s'annule pas, donc $\dfrac{f}{g}$ est bien définie.

□

Remarque 1.4.3.
Un corollaire immédiat de ce théorème est obtenu en remplaçant dans son énoncé «continue en a» par «continue sur I» et «$g(a) \neq 0$» par «g ne s'annule pas sur I».

Théorème 1.4.4.
Soient $g : I \to \mathbb{R}$ et $h : J \to \mathbb{R}$ deux applications, avec $g(I) \subset J$. Si g est continue en a et h est continue en $g(a)$, alors $h \circ g$ est continue en a.

Démonstration.
Immédiat avec les résultats avec les limites. □

Remarque 1.4.5.
On obtient un corollaire immédiat en remplaçant «continue en a» et «continue en $h(a)$» respectivement par «continue sur I» et «continue sur J».

2 Les grands théorèmes

2.1 Théorème des valeurs intermédiaires

Proposition 2.1.1 (Rappel)**.**
Les intervalles de $\mathbb{R}$ sont les parties convexes de $\mathbb{R}$, c'est-à-dire les parties I de $\mathbb{R}$ telles que tout réel compris entre deux élément de I appartient à I. Autrement dit, une partie I de $\mathbb{R}$ est un intervalle si et seulement si

$$\forall (x,y) \in I^2 \quad \forall t \in [0,1] \qquad x + t(y-x) \in I$$

Théorème 2.1.2 (TVI)**.**
L'image d'un intervalle par une fonction continue est un intervalle.

Remarque 2.1.3.
1. Soit $f : I \to \mathbb{R}$, une application telle que $f(I)$ soit un intervalle Alors pour tout $(a,b) \in I^2$, vérifiant $a < b$, $f(a)$ et $f(b)$ sont dans cet intervalle, donc tout élément compris entre $f(a)$ et $f(b)$ s'écrit sous la forme $f(c)$ avec $c \in [a,b]$.
2. Attention : le TVI assure l'existence de ce c mais absolument pas son unicité.
3. Réciproquement, le fait que pour tout a et tout b vérifiant $a < b$ et tout m compris entre $f(a)$ et $f(b)$ il existe $c \in [a,b]$ vérifiant $f(c) = m$ implique que $f(I)$ est un intervalle.

Démonstration.
Soit $f : I \to \mathbb{R}$ une application continue. D'après les remarques précédentes, il suffit de montrer que pour tout $(a,b) \in I^2$, vérifiant $a < b$, tout élément compris entre $f(a)$ et $f(b)$ s'écrit sous la forme $f(c)$ avec $c \in [a,b]$.

Soit donc $(a,b) \in I^2$ vérifiant $a < b$, et soit m compris entre $f(a)$ et $f(b)$.

Pour fixer les idées on suppose $f(a) \leqslant f(b)$ (le cas $f(b) \leqslant f(a)$ se traite de la même façon). Notons alors $\mathscr{E} = \{\, x \in [a,b] \mid f(x) \leqslant m \,\}$. On a évidemment $a \in \mathscr{E}$ et $\mathscr{E}$ est majoré par b. Donc $\mathscr{E}$ admet une borne supérieure c et on a $a \leqslant c \leqslant b$.

Montrons $f(c) = m$:

— Par l'absurde, supposons $f(c) < m$, alors comme f est continue en c, il existe $\varepsilon > 0$, tel que sur $[a,b] \cap [c-\varepsilon, c+\varepsilon]$, f ne prenne que des valeurs

strictement inférieures à m. En outre, c ne peut être l'extrêmité droite de $[a,b]$. Donc il existe $c' \in]c,b]$ vérifiant $f(c') < m$ ce qui est absurde.
Donc $f(c) \geqslant m$

— Par l'absurde, supposons $f(c) > m$, alors comme f est continue en c, il existe $\varepsilon > 0$ tel que sur $[a,b] \cap [c-\varepsilon, c+\varepsilon]$, f ne prenne que des valeurs strictement supérieures à m. Or c majore $\mathscr{E}$, donc $c-\varepsilon$ majore $\mathscr{E}$ également, donc c n'est pas la borne supérieure de $\mathscr{E}$, ce qui est absurde.
Donc $f(c) \leqslant m$.

On a donc $f(c) = m$. □

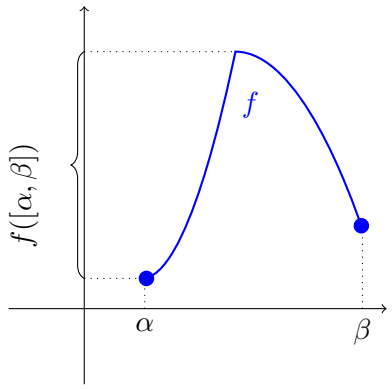


FIGURE XIII.4 – Illustration du TVI pour une fonction continue, sur un intervalle.

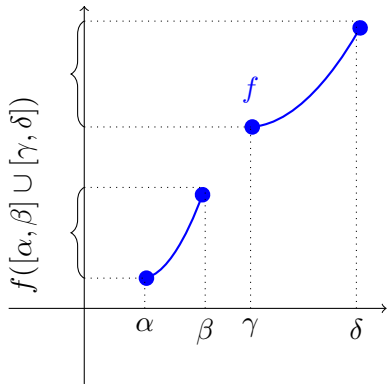


FIGURE XIII.5 – Contre-exemple au TVI pour une fonction continue, non sur un intervalle.

Corollaire 2.1.4.
Soit $f \in \mathscr{C}(I)$, et $a, b \in I$ tels que $f(a) > 0$ et $f(b) < 0$. Alors il existe c entre a et b tel que $f(c) = 0$.

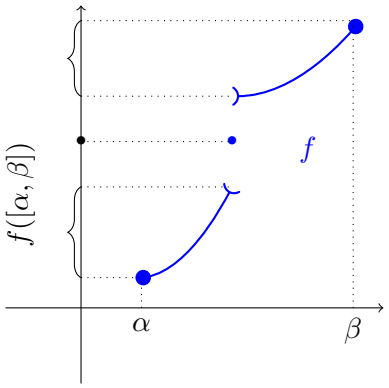


FIGURE XIII.6 – Contre-exemple au TVI pour une fonction non continue, sur un intervalle.

Remarque 2.1.5.
Une autre démonstration de ces résultats repose sur le principe de dichotomie, qui donne directement un algorithme. Voici un algorithme python. Pour tester si l'intervalle étudié est bien un intervalle où $f(a)$ et $f(b)$ sont de signes opposés, on étudie le signe du produit $f(a)f(b)$. On s'arrête lorsque la largeur de l'intervalle est inférieure à un pas donné.

```
def zeros (f,a,b,p) :
    """Recherche d'un zero de f dans
       l'intervalle [a,b]. Retourne le
       résultat avec une précision p.
       Précondition : f continue,
       a<b et f(a)*f(b)<=0"""
    g, d = a, b
    # [g,d] : Intervalle courant
    while g-d > p :
    # Invariant :
    # f s'annule entre g et d
    # soit (f(g)*f(d)<= 0)
    # Variant : g-d est divisé
    #       par deux à chaque étape
        m = (g+d)/2 # Milieu de [g,d]
        if (f(g)*f(m))<= 0 :
            d = m
```

```
        # On garde la moitié de gauche
    else :
        g = m
        # On garde celle de droite
return m
```

2.2 Image d'un segment par une fonction continue

Dans le cas d'un segment, le TVI peut-être complété.

Théorème 2.2.1.
L'image d'un segment par une fonction continue est un segment.

Démonstration.
Notons $I = [a, b]$, $f : I \to \mathbb{R}$ continue, et $J = f([a, b])$. D'après le TVI, J est un intervalle. Il suffit de montrer que ses extrémités gauche et droite sont réelles et lui appartiennent.

Notons M la borne supérieure de J dans $\overline{\mathbb{R}}$ et montrons $M \in J$.

1. Remarquons tout d'abord qu'on peut construire une suite u de points de I vérifiant $f(u_n) \xrightarrow[n\to+\infty]{} M$. En effet :
   - Supposons $M = +\infty$, alors J n'est pas majoré, donc pour tout $n \in \mathbb{N}$, il existe un élément de J appartenant à $[n, +\infty[$, on note alors u_n un antécédent par f d'un tel élément dans $[a, b]$. On a alors
   $$\forall x \in \mathbb{N} \quad f(u_n) \geqslant n$$
   Donc
   $$f(u_n) \xrightarrow[n\to+\infty]{} M$$
   - Supposons $M \in \mathbb{R}$. Alors pour tout n, il existe un élément de J dans l'intervalle $\left[M - \frac{1}{n+1}, M\right]$, on note alors u_n un antécédent par f d'un tel élément dans $[a, b]$. On a alors
   $$\forall n \in \mathbb{N} \quad f(u_n) \in \left[M - \frac{1}{n+1}, M\right]$$
   Donc
   $$f(u_n) \xrightarrow[n\to+\infty]{} M$$
2. u est à valeurs dans $[a, b]$ or d'après le théorème de Bolzano-Weierstrass, $[a, b]$ est compact, donc on peut extraire de u une suite v convergeant vers une valeur $c \in [a, b]$. Comme f est continue sur $[a, b]$, on en déduit que $(f(v_n))_{n\in\mathbb{N}}$ converge vers $f(c)$.
   Or $(f(v_n))_{n\in\mathbb{N}}$ est une suite extraite de $(f(u_n))_{n\in\mathbb{N}}$, donc elle tend vers M.
   On a donc $M = f(c)$, donc $M \in f([a, b]) = J$.

De la même manière, on montre $\inf(J) \in J$. □

Corollaire 2.2.2.
Toute fonction continue sur un segment est bornée et atteint ses bornes.

Démonstration.
Soit f continue sur un segment $[a, b]$. D'après le théorème, $f([a, b])$ est un segment $[c, d]$. f est donc majorée par d, minorée par c. Or $d \in f([a, b])$ donc d possède un antécédent dans $[a, b]$ par f. f atteint donc ce majorant (qui est donc un maximum). De la même façon, f atteint son minorant c, qui est donc un minimum de f sur $[a, b]$. □

Exemple 2.2.3.
C'est un résultat intuitif, voici des contre-exemples lorsque les hypothèses ne sont pas vérifiées.

- Sur un intervalle fermé, non borné : $\mathbb{R} \to \mathbb{R}, x \mapsto x$ est continue, mais n'a ni maximum ni minimum.
- Sur un intervalle ouvert non fermé : $]0, 1] \to \mathbb{R}, x \mapsto 1/x$ est continue mais n'a pas de maximum.
- Avec une fonction non continue : sur le segment $[0, 1]$, la fonction qui a un réel associe 0, sauf aux $1/n$ avec $n \in \mathbb{N}^*$ qui leur associe n. Cette fonction est discontinue et n'a pas de maximum.

Exemple 2.2.4.
Toute fonction périodique continue est bornée et atteint ses bornes.

Démonstration.
Soit $f : \mathbb{R} \to \mathbb{R}$ T-périodique, et $x \in \mathbb{R}$. Sur $[0, T]$, f est bornée et atteint son maximum M en x_M et son minimum m en x_m.

Or pour tout $x \in \mathbb{R}$, il existe $x' \in [0, T]$ tel que $x - x'$ soit un multiple entier de T (il est suffisant (et nécessaire) de prendre pour x' la valeur $T \times (x/T - \lfloor x/T \rfloor)$). On en déduit $f(x) \in [m, M]$. f est donc bornée sur $\mathbb{R}$ et atteint ses bornes en x_M et x_m. □

2.3 Rappels concernant les fonctions strictement monotones

Dissipons d'emblée une idée populaire, mais fausse : ce n'est pas parce qu'une fonction est dérivable en un point que l'on peut dire quoi que

ce soit quant au sens de variation de la fonction au voisinage de ce point.

Exemple 2.3.1.
Soit la fonction

$$f : \left\{ \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R}, \\ x & \longmapsto & \left\{ \begin{array}{lll} x^2 \sin\left(\frac{1}{x}\right) + \frac{x}{2} & \text{si} & x \neq 0, \\ 0 & \text{si} & x = 0. \end{array} \right. \end{array} \right.$$

Alors f est continue et dérivable sur $\mathbb{R}$, $f'(0) = 1/2$, mais f n'est monotone sur aucun voisinage de 0.

Dans la suite, nous ne parlerons pas du tout de dérivabilité.

Théorème 2.3.2.
Soit $(a, b) \in \overline{\mathbb{R}}$ vérifiant $a < b$. Supposons que f est continue sur I et ***strictement*** croissante sur I. Soit $\ell, \ell' \in \overline{\mathbb{R}}$ tels que $f \underset{a}{\to} \ell$ et $f \underset{b}{\to} \ell'$. Alors :

1. si $I = [a, b]$, alors $f(I) = [f(a), f(b)]$;
2. si $I =]a, b[$, alors $f(I) =]\ell, \ell'[$;
3. si $I = [a, b[$, alors $f(I) = [f(a), \ell'[$;
4. si $I =]a, b]$, alors $f(I) =]\ell, f(b)]$.

On a un résultat analogue lorsque f est ***strictement*** décroissante sur I.

Démonstration.
Remarquons que f étant strictement monotone, f admet une limite à droite en a et à gauche en b.

On se contente de donner le cas f strictement décroissante et $I =]a, b]$. On sait que $f(I)$ est un intervalle. On note $\alpha = \inf f(I)$ et $\beta = \sup f(I)$. f étant décroissante, $f(b)$ minore $f(I)$, or $f(b)$ est dans $f(I)$, donc $\alpha = f(b)$. Par ailleurs, comme f est strictement décroissante, on ne peut avoir $\beta \in f(I)$, car alors il existerait $c \in]a, b]$ vérifiant $f(c) = \beta$ et dans ce cas on aurait $f(\frac{a+c}{2}) > \beta$ et β ne majorerait plus $f(I)$, ce qui serait absurde.

Enfin, le théorème de limite monotone nous donne l'existence des limites manipulées. On en rappelle ici les arguments.

- Supposons $\beta = +\infty$, alors f n'est pas majorée, donc pour tout $M > 0$, il existe $c \in I$ tel que $f(c) > M$. Mais f est décroissante, donc pour tout $x \in]a, c]$, $f(x) > M$. On a donc $f \underset{a}{\to} +\infty = \beta$.
- Supposons $\beta \in \mathbb{R}$, alors pour tout $\varepsilon > 0$, $\beta - \varepsilon$ ne majore pas $f(I)$, donc il existe $d \in]\beta - \varepsilon, \beta]$ tel que $d \in f(I)$, donc il existe $c \in I$ tel que $f(c) \in]\beta - \varepsilon, \beta]$. Or f est décroissante, donc pour tout $x \in]a, c]$, on a $f(x) \in]\beta - \varepsilon, \beta]$. Ainsi $f(I) = [f(b), \ell'[$ ($\beta \notin f(I)$ car f est strictement décroissante). On a donc $f \underset{a}{\to} \beta$.

Dans les deux cas, on a bien $f(I) = [f(b), \ell'[$ □

Remarque 2.3.3.
Si la fonction f n'est supposée que monotone, $f(I)$ peut être fermé alors que I est ouvert (prendre f constante, par exemple).

2.4 Monotonie stricte, bijectivité et continuité

Explorons maintenant les liens entre ces trois notions.

Lemme 2.4.1 (Réciproque d'une application strictement monotone)**.**
Soit D et E deux parties de $\mathbb{R}$ et $f : D \to E$ une bijection strictement monotone. Alors l'application réciproque $f^{-1} : E \to D$ est strictement monotone, de même sens de variation que f.

Démonstration.
Montrons maintenant que f^{-1} est strictement monotone, de même sens de variation que f.

- Supposons que f soit strictement croissante. Alors, soit y_1 et y_2 deux éléments de $f(D)$ vérifiant $y_1 < y_2$ et soit $x_1 = f^{-1}(y_1)$ et $x_2 = f^{-1}(y_2)$. Si on avait $x_1 \geqslant x_2$ alors, comme f est croissante, on aurait $f(x_1) \geqslant f(x_2)$, c'est-à-dire $y_1 \geqslant y_2$, ce qui serait absurde. Donc $x_1 < x_2$, c'est-à-dire $f^{-1}(y_1) < f^{-1}(y_2)$.
  f^{-1} est donc strictement croissante.
- Supposons que f soit strictement décroissante. De la même façon, on montre que f^{-1} est alors strictement décroissante.

Dans les deux cas, f^{-1} est strictement monotone, de même sens de variation que f. □

Le résultat suivant est une réciproque partielle au théorème des valeurs intermédiaires.

Lemme 2.4.2.
Soit I un intervalle et $f : I \to \mathbb{R}$ une application monotone telle que $f(I)$ est un intervalle.

Alors f est continue sur I.

Démonstration.
Le cas où I est un intervalle vide ou réduit à un point est trivial. Nous supposons donc par la suite que I n'est ni vide, ni réduit à un point.

Nous étudions seulement ici le cas où f est croissante. Si f est décroissante, il suffit d'appliquer ce qui suit à $-f$.

Il suffit de montrer que d'une part que pour tout point $a \in I$ qui n'est pas l'extrémité gauche de I, on a $f \xrightarrow[a^-]{} f(a)$ et d'autre part que pour tout point $a \in I$ qui n'est pas l'extrémité droite de I, on a $f \xrightarrow[a^+]{} f(a)$.

Par l'absurde, supposons que ce n'est pas le cas. Pour fixer les idées, supposons qu'il existe $a \in I$ qui n'est pas l'extrémité gauche de I vérifiant $f \not\xrightarrow[a^-]{} f(a)$ (l'autre cas est similaire). Notons alors α un point de I vérifiant $\alpha < a$.

Alors, f étant croissante, on sait que la limite de f en a, à gauche, existe. Notons la ℓ. Alors, $f(\alpha) \leqslant \ell \leqslant f(a)$. Puisque $f \not\xrightarrow[a^-]{} f(a)$, on a $\ell < f(a)$. L'intervalle $]\ell, f(a)[$ n'est donc pas vide, on peut donc y choisir un point y. On a alors $f(\alpha) \leqslant \ell < y < f(a)$.

Or $f(I)$ est un intervalle, donc $y \in f(I)$. Donc il existe $c \in I$ vérifiant $f(c) = y$. On a $f(c) < f(a)$ et f croissante, donc $c < a$. Donc $f(c) \leqslant \ell$, donc $y \leqslant \ell$ ce qui est absurde. □

Lemme 2.4.3.
Soit I un intervalle et $f : I \to \mathbb{R}$, une application continue et injective. Alors f est strictement monotone.

Démonstration.
Supposons par l'absurde que f n'est pas strictement monotone, c'est-à-dire qu'elle n'est ni strictement croissante, ni strictement décroissante.

Comme f n'est pas strictement croissante, il existe $(x, y) \in I^2$ vérifiant $x < y$ et $f(x) \geqslant f(y)$.

De même, comme f n'est pas strictement décroissante, il existe $(x', y') \in I^2$ vérifiant $x' < y'$ et $f(x') \leqslant f(y')$.

Notons

$$\begin{array}{rccl} \alpha : & [0,1] & \to & \mathbb{R} \\ & t & \mapsto & (1-t)x + tx' \\ \beta : & [0,1] & \to & \mathbb{R} \\ & t & \mapsto & (1-t)y + ty' \\ \varphi : & [0,1] & \to & \mathbb{R} \\ & t & \mapsto & f(\alpha(t)) - f(\beta(t)) \end{array}$$

I est convexe donc pour tout $t \in [0,1]$, $\alpha(t)$ et $\beta(t)$ appartiennent à I, donc φ est bien définie.

Par ailleurs, on peut remarquer que, comme $x < y$ et $x' < y'$, pour tout $t \in [0,1]$, on a $\alpha(t) < \beta(t)$.

Enfin, on a :

(i) φ est continue sur $[0,1]$;

(ii) $\varphi(0) = f(x) - f(y) \geqslant 0$;

(iii) $\varphi(1) = f(x') - f(y') \leqslant 0$.

Donc φ s'annule en une valeur $t \in [0,1]$. On a alors $f(\alpha(t)) = f(\beta(t))$.

Or f est injective, donc $\alpha(t) = \beta(t)$. Or $\alpha(t) < \beta(t)$, donc c'est absurde. □

Théorème 2.4.4 (Théorème de la bijection strictement monotone)**.**
Soit I un intervalle de $\mathbb{R}$ et $f : I \to \mathbb{R}$ une application. Posons $J = f(I)$. Alors si deux quelconques des trois propriétés suivantes sont vraies, la troisième l'est également :

(i) J est un intervalle et f réalise une bijection de l'intervalle I sur l'intervalle $f(I)$.

(ii) f est strictement monotone sur I.

(iii) f est continue sur I.

De plus, lorsque ces conditions sont vérifiées, l'application réciproque $f^{-1} : J \to I$ est aussi une bijection continue strictement monotone.

Démonstration.
Pour ce qui est de la première partie du théorème :

- Dans le cas où (i) et (ii) sont vraies, $f(I)$ est un intervalle, f est donc continue d'après le lemme 2.3.3
- Dans le cas où (i) et (iii) sont vraies, f réalise une bijection de I sur $f(I)$ donc est injective, or elle est continue, donc strictement monotone d'après le lemme 2.3.4.
- Dans le cas où (ii) et (iii) sont vraies, f est strictement monotone donc injective, donc réalise une bijection de I sur $f(I)$. De plus, elle est continue donc $f(I)$ est un intervalle.

Pour ce qui est de la seconde partie, supposons donc ces conditions vérifiées.

Alors on sait que la bijection d'une application strictement monotone est monotone, donc $f^{-1} : J \to I$ est strictement monotone.

De plus f^{-1} réalise une bijection de l'intervalle J sur l'intervalle $f^{-1}(J) = I$.

La première partie assure donc que f^{-1} est continue. □

Exemple 2.4.5.
Cela permet de montrer que les fonctions Arccos, Arcsin et Arctan sont continues.

3 Extension au cas des fonctions à valeurs complexes

Les notions de continuité, continuité à gauche et à droite se généralisent sans problème aux fonctions à valeurs complexes, puisque c'est juste une histoire de limite. On a aussi le résultat suivant.

Théorème 3.0.1.
Soit $f : I \to \mathbb{C}$, $a \in I$. On a équivalence entre :

1. f est continue en a (resp. sur I)
2. $\mathrm{Im}(f)$ et $\mathrm{Re}(f)$ sont continues en a (resp. sur I).

La caractérisation séquentielle de la continuité est vraie comme pour les applications à valeurs dans $\mathbb{R}$, de même que toutes les résultats sur les opérations usuelles. En revanche, les grands théorèmes liés au TVI ne peuvent pas être étendus à $\mathbb{C}$: ils font appel à l'ordre $\leqslant$ sur $\mathbb{R}$.

Exemple 3.0.2.
Notons $f : \begin{array}{ccc} [0,\pi] & \to & \mathbb{C} \\ t & \mapsto & \mathrm{e}^{it} \end{array}$. Alors f est continue sur $[0,\pi]$, vaut 1 en 0, -1 en π mais ne s'annule pas.

Quant à l'image du segment $[0,\pi]$, il s'agit d'un demi-cercle et non d'un intervalle !

Chapitre XIV

Polynômes

Dans tout ce chapitre $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

1 $\mathbb{K}[X]$: définitions et résultats algébriques

1.1 Premières définitions

Définition 1.1.1.
On appelle support d'une suite u à valeurs dans $\mathbb{K}$ l'ensemble des entiers n tels que $u_n \neq 0$. Si cet ensemble est fini, u est dite à support fini.

Remarque 1.1.2.
1. Une suite u est à support fini si et seulement si elle est nulle à partir d'un certain rang.
2. Toute suite à support fini converge donc vers 0 mais la réciproque est évidemment fausse [1].

Définition 1.1.3 (Anneau des polynômes sur le corps $\mathbb{K}$)**.**
On admet qu'on peut construire un anneau commutatif $(\mathbb{K}[X], +, \times)$ appelé *anneau des polynômes à une indéterminée à coefficients dans* $\mathbb{K}$. Vérifiant les propriétés suivantes :

1. $\mathbb{K}[X]$ étend l'anneau $\mathbb{K}$, c'est-à-dire :
   (a) $\mathbb{K} \subset \mathbb{K}[X]$
   (b) l'addition et la multiplication de $\mathbb{K}[X]$ coïncident avec celles de $\mathbb{K}$ sur l'ensemble $\mathbb{K}$. Autrement dit : les opérations $+_{\mathbb{K}[X]}$ et $\times_{\mathbb{K}[X]}$ restreintes au sous-ensemble $\mathbb{K}$ sont exactement les opérations $+_{\mathbb{K}}$ et $\times_{\mathbb{K}}$.
   (c) le neutre pour l'addition sur $\mathbb{K}$ (0) est aussi le neutre pour l'addition sur $\mathbb{K}[X]$ et le neutre pour la multiplication sur $\mathbb{K}$ (1) est aussi le neutre pour la multiplication sur $\mathbb{K}[X]$. 0 est appelé *le polynôme nul*.
2. $\mathbb{C}[X]$ étend $\mathbb{R}[X]$.
3. Il existe un polynôme, noté X (appelé l'*indéterminée* de $\mathbb{K}[X]$).
4. Les polynômes de la forme αX^k pour $k \in \mathbb{N}$ et $\alpha \in \mathbb{K}$ sont appelés *monômes*.
5. Tout polynôme P peut s'écrire de façon *unique* sous *forme normale* [2](appelée aussi *forme développée réduite*) :

$$\sum_{k=0}^{+\infty} a_k X^k$$

où $(a_k)_{k\in\mathbb{N}}$ est une suite à support fini, appelée *suite des coefficients de* P (la suite des coefficients de P est donc unique).

Remarque 1.1.4.
1. Si on note φ l'application qui à tout polynôme P associe sa suite des coefficients et ψ l'application qui à toute suite à valeurs dans $\mathbb{K}$ à support fini u associe le polynôme $\sum_{k=0}^{+\infty} u_k X^k$, on constate que pour tout polynôme P, $(\psi \circ \varphi)(P) = P$ et que pour toute suite à support fini u, on a $(\varphi \circ \psi)(u) = u$. Ces deux applications sont donc des bijections réciproques : il y a donc une bijection (canonique) entre les suites à support fini et les polynômes.
2. Il est important de ne pas confondre X et x : $2X^3 + \sqrt{2}X + 7$ est un polynôme, $x \mapsto 2x^3 + \sqrt{2}x + 7$ désigne une fonction polynomiale (allant de $\mathbb{R}$ dans $\mathbb{R}$ ou de $\mathbb{R}$ dans $\mathbb{C}$ ou de $\mathbb{C}$ dans $\mathbb{C}$ selon le contexte). L'expression «$x^3 + \sqrt{2}x + 7$» est une erreur si x n'a pas été introduit ou si c'est une matrice carrée de taille 42. C'est un réel si x est un réel et un complexe si x est un complexe.

1. Par ailleurs, dans ce chapitre, le fait que les suites à support fini convergent n'est d'aucun intérêt.

2. La somme est une somme finie, prise pour les valeurs de k telle que $a_k \neq 0$. On a donc $P = \sum_{\substack{k\in\mathbb{N}\\ a_k\neq 0}} a_k X^k$ mais aussi $P = \sum_{k=0}^{n} a_k X^k$ si la suite (a_k) est nulle à partir du rang $n+1$.

Le polynôme 0 a pour suite de coefficients la suite nulle.

Pour tout $\lambda \in \mathbb{K}$, le polynôme λ a pour suite de coefficients la suite nulle partout sauf au rang 0, où elle a pour valeur λ. Les éléments de $\mathbb{K}$ sont appelés les polynômes constants.

Définition 1.1.5 (Degré)**.**
Soit P un polynôme de la forme $\sum_{k=0}^{+\infty} a_k X^k$. On appelle degré de P, et note $\deg P$ la valeur

$$\sup\{\, k \in \mathbb{N} \mid a_k \neq 0 \,\},$$

prise dans $\overline{\mathbb{R}}$.

(i) Si P est le polynôme nul, $\deg P = -\infty$.

(ii) Si P n'est pas le polynôme nul, le support de $(a_k)_{k\in\mathbb{N}}$ est un ensemble d'entiers non vide et majoré, donc $\deg P = \max\{\, k \in \mathbb{N} \mid a_k \neq 0 \,\}$.

(iii) Si P est non nul, le coefficient $a_{\deg P}$ est appelé *coefficient dominant* de P et on dit que $a_{\deg_P} X^{\deg P}$ est le *monôme dominant* de P.

(iv) Si le coefficient dominant de P vaut 1 on dit que P est *unitaire*.

Pour tout entier $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n.

Remarque 1.1.6. 1. $\mathbb{K}_n[X]$ **n'est pas** l'ensemble des polynômes de degré **égal** à n.

2. $\mathbb{K} = \mathbb{K}_0[X] \subset \mathbb{K}_1[X] \subset \mathbb{K}_2[X] \subset \cdots \subset \mathbb{K}[X]$.

3. $\mathbb{K}_n[X]$ est un sous-groupe de $(\mathbb{K}[X], +)$.

4. Soit P un polynôme de degré d et $n \in \mathbb{N}$ vérifiant $n \geqslant d$ (P est de degré *au plus* n), alors P peut s'écrire sous la forme $\sum_{k=0}^{n} a_k X^k$.

1.2 Somme et produit

Proposition 1.2.1.
Soit P et Q deux polynômes respectivement de la forme $\sum_{k=0}^{+\infty} a_k X^k$ et $\sum_{k=0}^{+\infty} b_k X^k$. Alors on a :

$$P + Q = \sum_{k=0}^{+\infty} (a_k + b_k) X^k.$$

Autrement dit, la suite des coefficients de $P+Q$ est la somme de leurs suites de coefficients respectives.

En ce qui concerne le produit, on a

$$P \times Q = \sum_{(i,j)\in\mathbb{N}^2} a_i b_j X^{i+j} = \sum_{k=0}^{+\infty} c_k X^k$$

où $(c_k)_{k\in\mathbb{N}}$ est la suite vérifiant, pour tout $k \in \mathbb{N}$,

$$c_k = \sum_{\substack{(i,j)\in\mathbb{N}^2 \\ i+j=k}} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=0}^{k} a_{k-i} b_i.$$

Démonstration.
Il s'agit essentiellement de constater que les sommes sont en fait finies. En notant S et S' les supports respectifs des suites de coefficients de P et Q, on a

$$P = \sum_{k\in S} a_k X^k = \sum_{k\in S\cup S'} a_k X^k,$$
$$Q = \sum_{k\in S'} b_k X^k = \sum_{k\in S\cup S'} b_k X^k,$$

d'où

$$P + Q = \sum_{k\in S\cup S'} (a_k X^k + b_k X^k)$$
$$= \sum_{k\in S\cup S'} (a_k + b_k) X^k.$$

Or a_k et b_k sont nuls pour tout $k \in \mathbb{N} \setminus (S \cup S')$, donc la somme

$$\sum_{k=0}^{+\infty} (a_k + b_k) X^k$$

est finie et vaut la même chose.

Pour le produit, notons, pour tout $k \in \mathbb{N}$, $c_k = \sum_{\substack{(i,j)\in\mathbb{N}^2 \\ i+j=k}} a_i b_j$. Il est clair que c_k est une somme finie (elle

comporte $k+1$ termes) et de plus, on a

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=0}^{k} a_{k-i} b_i.$$

Il reste à montrer qu'on a bien $P \times Q = \sum_{k=0}^{+\infty} c_k X^k$.

Posons $S'' = \{\, i+j \mid (i,j) \in S \times S' \,\}$, S'' est l'image directe de l'ensemble fini $S \times S'$ par l'application somme, donc S'' est un ensemble fini.

Remarquons tout de suite que pour $k \in \mathbb{N} \setminus S''$ et tout couple $(i,j) \in \mathbb{N}^2$ vérifiant $i+j=k$, on a $(i,j) \notin S \times S'$, donc $a_i = 0$ ou $b_j = 0$. Donc pour tout $k \in \mathbb{N} \setminus S''$, la somme $\sum_{\substack{(i,j)\in\mathbb{N}^2 \\ i+j=k}} a_i b_j$ ne comporte que des termes nuls.

En outre

$$\begin{aligned}
PQ &= \left(\sum_{i\in S} a_i X^i\right)\left(\sum_{j\in S'} b_j X^j\right) \\
&= \sum_{(i,j)\in S\times S'} a_i b_j X^{i+j} \\
&= \sum_{k\in S''} \left(\sum_{\substack{(i,j)\in S\times S' \\ i+j=k}} \left(a_i b_j X^{i+j}\right) \right) \\
&= \sum_{k\in S''} \left(\sum_{\substack{(i,j)\in S\times S' \\ i+j=k}} a_i b_j \right) X^k \\
&= \sum_{k\in S''} \left(\sum_{\substack{(i,j)\in \mathbb{N}^2 \\ i+j=k}} a_i b_j \right) X^k \\
&= \sum_{k=0}^{+\infty} \left(\sum_{\substack{(i,j)\in \mathbb{N}^2 \\ i+j=k}} a_i b_j \right) X^k.
\end{aligned}$$

d'où le résultat. □

1.3 Composition

Définition 1.3.1.
Soit P et Q deux polynômes de $\mathbb{K}[X]$. P s'écrit sous la forme

$$\sum_{k=0}^{+\infty} a_k X^k.$$

Alors, la somme

$$\sum_{k=0}^{+\infty} a_k Q^k$$

est une somme finie, appelée *composée de P et Q* (ou de Q par P) et est notée $P \circ Q$.

Proposition 1.3.2.
La composition est distributive **à droite** par rapport aux lois + et × et elle est également associative, c'est-à-dire que si P, Q et R désignent trois polynômes, on a :

(i) $(P+Q)\circ R = (P\circ R) + (Q\circ R)$;
(ii) $(PQ)\circ R = (P\circ R)\times(Q\circ R)$;
(iii) $(P\circ Q)\circ R = P\circ(Q\circ R)$.

Démonstration. (i) Direct.
(ii) Traiter d'abord le cas $P = X^n$ et $Q = X^m$, puis le cas P quelconque et $Q = X^m$, puis le cas général.
(iii) Montrer par récurrence que $Q^k \circ R = (Q\circ R)^k$.
□

 Attention à la composition à gauche, qui n'est pas distributive. Par exemple :

$$X^2 \circ (X+2) = (X+2)^2 \neq X^2 + 2^2$$
$$(1\circ X) + (1\circ 2) = 2 \neq 1 \circ (X+2)$$
$$(1+X)\circ(X.X) \neq ((1+X)\circ X).((1+X)\circ X).$$

Exemple 1.3.3.
Un polynôme P est dit pair si $P\circ(-X) = P$, impairs si $P\circ(-X) = -P$. Que peut-on dire des coefficients de tels polynômes ?

1.4 Opérations et degré

Théorème 1.4.1.
Soient $P, Q \in \mathbb{K}[X]$.

(i) $\deg(P+Q) \leqslant \max(\deg P, \deg Q)$;
(ii) $\deg(PQ) = \deg P + \deg Q$;
(iii) si Q n'est pas constant, alors $\deg(P\circ Q) = \deg P \times \deg Q$. Si Q est constant, $\deg P\circ Q = 0$ ou $-\infty$.

Remarque 1.4.2.
Méditez les exemples suivants :

(i) $P = X - 1$ et $Q = 2 - X$;

(iii) $P = X^2 - 1$ et $Q = 1$.

Démonstration.
Le théorème est évident si P ou Q est nul. On les supposera donc tous deux non nuls, et on pose $n = \deg P$ et $m = \deg Q$. Les polynômes P, Q et PQ s'écrivent respectivement sous la forme $\sum_{k=0}^{n} a_k X^k$ et $\sum_{k=0}^{m} b_k X^k$ et $\sum_{k=0}^{+\infty} c_k X^k$.

(i) Facile ;

(ii) On a $c_k = \sum_{i=0}^{k} a_i b_{k-i}$.
Soit $k \geqslant m+n$. Si $i > n$, alors $a_i = 0$, et si $i < n$, alors $b_{m+n-i} = 0$.
Ainsi, si $k = m+n$, la somme définissant c_k n'a qu'un terme non nul, et $c_{m+n} = a_n b_m \neq 0$.
Si $k > m+n$, tous les termes de la somme sont nuls, donc $c_k = 0$. Ceci prouve bien le résultat.

(iii) Q non constant équivaut à $\deg Q \geqslant 1$. Donc si k_1 et k_2 sont deux entiers tels que $k_2 > k_1$, on a $\deg Q^{k_2} > \deg Q^{k_1}$. Ainsi $\deg P \circ Q = \deg a_n Q^n = \deg(Q^n)$. Or d'après (ii), $\deg(Q^n) = n \deg Q$.

□

Corollaire 1.4.3.
$\mathbb{K}[X]$ est intègre.

Démonstration.
Il suffit de montrer que pour tout $(P, Q) \in \mathbb{K}[X]^2$, $PQ = 0 \Rightarrow (P = 0 \text{ ou } Q = 0)$. Soit donc $(P, Q) \in \mathbb{K}[X]^2$ vérifiant $PQ = 0$. Alors d'après le point (iii) du théorème **1.4.1**, $-\infty = \deg(PQ) = \deg P + \deg Q$, donc on a nécessairement $\deg P = -\infty$ ou $\deg Q = -\infty$. □

Corollaire 1.4.4.
Soient $P, A, B \in \mathbb{K}[X]$ tel que $P \neq 0$. Alors :

$$PA = PB \Leftrightarrow A = B.$$

Démonstration.
$PA = PB$ si et seulement si $P(A - B) = 0$ si et seulement si $(P = 0 \text{ ou } A - B = 0)$ si et seulement si $A - B = 0$ si et seulement si $A = B$. □

Corollaire 1.4.5.
$U(\mathbb{K}[X]) = \mathbb{K}^*$. Autrement dit, les seuls éléments inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls.

Démonstration.
Soient P un polynôme inversible. Il existe donc un polynôme Q tel $PQ = 1$. P et Q sont non nuls, et donc $\deg P \geqslant 0$ et $\deg Q \geqslant 0$. Mais $0 = \deg 1 = \deg PQ = \deg P + \deg Q$. Nécessairement, $\deg P = \deg Q = 0$. □

Il y a donc peu de polynômes inversibles. L'inversibilité est une propriété fort utile lorsqu'on veut simplifier une égalité de la forme $PA = PB$ (on multiplie alors des deux côtés par l'inverse de P) mais heureusement, elle n'est pas nécessaire pour cela : l'intégrite de $\mathbb{K}[X]$ suffit :

Définition 1.4.6.
Deux polynômes P et Q de $\mathbb{K}[X]$ sont dits associés s'il existe $\lambda \in \mathbb{K}^*$ vérifiant $P = \lambda Q$.

Remarque 1.4.7.
Ainsi, deux polynômes sont associés si et seulement si on passe de l'un à l'autre en multipliant par un polynôme inversible. On pourra effectuer un rapprochement avec les entiers ainsi qu'avec l'arithmétique sur les entiers : les éléments inversibles de $\mathbb{Z}$ sont 1 et -1, et les objets construits en arithmétique des entiers (PGCD, nombres premiers, etc.) le sont toujours « à un élément inversible près ». Ce sera encore le cas en arithmétique des polynômes.

1.5 Fonctions polynomiales

Dans cette section, on considère un entier naturel n fixé

Définition 1.5.1.
Soit $P = \sum_{k=0}^{+\infty} a_k X^k$ un polynôme et x un élément de $\mathbb{K}$.

On appelle *évaluation du polynôme P en x* et on note $\widetilde{P}(x)$ l'élément de $\mathbb{K}$ défini par

$$\widetilde{P}(x) = \sum_{k=0}^{+\infty} a_k \cdot x^k.$$

Remarque 1.5.2.
Comme précédemment, le symbole $\sum_{k=0}^{+\infty}$ a un sens car la suite (a_k) est à support fini. Cette somme est donc finie.

Exemple 1.5.3.
On pose $P = X^2 + 2X + 3$, que vaut l'évaluation de P en -2 ?

Proposition 1.5.4.
Soit $x \in A$ fixé. Alors, l'application d'évaluation en x, $\mathsf{eval}_x : \begin{array}{ccc} \mathbb{K}[X] & \to & A \\ P & \mapsto & \widetilde{P}(x) \end{array}$ est un morphisme d'anneau ; autrement dit pour tout $(P, Q) \in \mathbb{K}[X]^2$, on a

1. $\widetilde{P+Q}(x) = \widetilde{P}(x) + \widetilde{Q}(x)$;
2. $\widetilde{P \times Q}(x) = \widetilde{P}(x) \times \widetilde{Q}(x)$;
3. $\widetilde{1_{\mathbb{K}[X]}}(x) = 1_A$.

De plus, on a

$$\widetilde{P \circ Q}(x) = P(Q(x))$$

On note $\widetilde{P} : \begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & \widetilde{P}(x) \end{array}$.

Remarque 1.5.5.
D'après ce qui précède, on a donc, pour tous polynômes P et Q :

1. $\widetilde{P+Q} = \widetilde{P} + \widetilde{Q}$;
2. $\widetilde{P \times Q} = \widetilde{P} \times \widetilde{Q}$;
3. $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$

Exemple 1.5.6.
Posons $P = X^2 + 2X + 3$.

1. Que vaut $\widetilde{P}$.
2. A t-on $P = \widetilde{P}$?

En pratique, on note en général $P(x)$ la valeur de $\widetilde{P}(x)$. On va même parfois jusqu'à identifier P et $\widetilde{P}$, c'est-à-dire identifier les polynômes et les fonctions polynomiale. Cela se justifie par le résultat suivant :

Théorème 1.5.7.
Soient P et Q deux polynômes de $\mathbb{K}[X]$.

(i) $\widetilde{P}$ est la fonction identiquement nulle si et seulement si $P = 0$;

(ii) $\widetilde{P} = \widetilde{Q}$ si et seulement si $P = Q$.

Cependant, nous ne sommes pas en mesure de montrer tout de suite cette propriété. Nous nous contenterons donc pour l'instant de faire les remarques suivantes :

Remarque 1.5.8.
1. Les implications $P = 0 \Rightarrow \widetilde{P} = 0$ et $P = Q \Rightarrow \widetilde{P} = \widetilde{Q}$ sont évidentes. Il suffit donc de montrer les implications réciproques.
2. Si l'on admet pour tout P l'implication $\widetilde{P} = 0_{\mathbb{K}^{\mathbb{K}}} \Rightarrow P = 0$ alors, pour tout couple (P, Q), l'implication $\widetilde{P} = \widetilde{Q} \Rightarrow P = Q$ s'en déduit. En effet, il suffit de remarquer que $\widetilde{P - Q} = \widetilde{P} - \widetilde{Q}$, donc si $\widetilde{P} = \widetilde{Q}$, alors $\widetilde{P - Q}$ est nul donc $P - Q$ est nul donc $P = Q$.

Remarque 1.5.9 (à caractère culturel)**.**
On verra que la démonstration du résultat exploite le fait que $\mathbb{K}$ est un ensemble infini. Même si seuls les cas $\mathbb{K} = \mathbb{R}$ et $\mathbb{K} = \mathbb{C}$ sont au programme, il existe des corps $\mathbb{K}$ finis et on peut définir $\mathbb{K}[X]$ pour de tels corps. Dans le cas où $\mathbb{K}$ est un corps fini, le théorème 1.5.6 n'est plus vrai.

1.6 Division euclidienne

On peut définir une opération de division dans $\mathbb{K}[X]$ similaire à celle de la division euclidienne dans $\mathbb{Z}$.

Rappelons tout d'abord la définition de la division euclidienne dans $\mathbb{Z}$:

Définition 1.6.1 (Division euclidienne)**.**
Soit P et D deux entiers, avec $D \neq 0$. Alors il existe un unique couple (Q, R) d'entiers vérifiant les deux propriétés suivantes :

1. $P = D \times Q + R$

2. et $0 \leqslant R < |D|$.

Q et R sont respectivement appelé le quotient et le reste de la division euclidienne de P par D.

Définition 1.6.2 (Division euclidienne des polynômes)**.**
Soit P et D deux polynômes à coefficients dans $\mathbb{K}$, avec $D \neq 0$. Alors il existe un unique couple (Q, R) de polynômes à coefficients dans $\mathbb{K}$ vérifiant les deux propriétés suivantes :

1. $P = D \times Q + R$
2. et $\deg R < \deg D$.

Q et R sont respectivement appelé le quotient et le reste de la division euclidienne de P par D.

Exemple 1.6.3.
La division euclidienne de $3X^4 - 5X^3 + 7X^2 + 8X - 1$ par $X^2 - 3X + 2$ s'écrit :

$$\begin{aligned} &3X^4 - 5X^3 + 7X^2 + 8X - 1 \\ &= (X^2 - 3X + 2)(3X^2 + 4X + 13) + 39X - 27. \end{aligned}$$

On la pose comme suit.

$$\begin{array}{rrrrr|l} 3X^4 & -5X^3 & +7X^2 & +8X & -1 & X^2 -3X +2 \\ \cline{6-6} -(3X^4 & -9X^3 & +6X^2) & & & 3X^2 +4X +13 \\ \cline{1-3} & 4X^3 & +X^2 & +8X & -1 & \\ & -(4X^3 & -12X^2 & +8X) & & \\ \cline{2-4} & & 13X^2 & & -1 & \\ & & -(13X^2 & -39X & +26) & \\ \cline{3-5} & & & 39X & -27 & \end{array}$$

 On alignera toujours les monômes de mêmes degrés pour les additionner sans commettre d'erreur.

Remarque 1.6.4.
La preuve du théorème de division euclidienne repose sur l'idée mise en œuvre dans l'algorithme donnant cette division. On cherche en effet chaque fois à annuler le monôme de plus haut degré du dividende en multipliant le diviseur par un monôme convenable.

Démonstration.
• Commençons d'abord par montrer l'unicité :
Soient (Q_1, R_1) et (Q_2, R_2) deux couples convenables. Alors $DQ_2 + R_2 = DQ_1 + R_1$, et donc $D(Q_2 - Q_1) = R_1 - R2$, et donc $D|(R_1 - R_2)$. Si $R_1 - R_2 \neq 0$, alors nécessairement $\deg D \leqslant \deg(R_1 - R_2)$. Or $\deg R_1 < \deg D$ et $\deg R_2 < \deg D$, donc par somme $\deg(R_1 - R_2) < \deg D$. Par conséquent $R_1 - R_2 = 0$, donc $R_1 = R_2$. Il vient ensuite $D(Q_1 - Q_2) = 0$: puisque $D \neq 0$ et que $\mathbb{K}[X]$ est intègre, alors $Q_1 - Q_2 = 0$, soit finalement $(Q_1, R_1) = (Q_2, R_2)$.
• Montrons maintenant l'existence d'un tel couple. Cette démonstration peut se faire par récurrence sur le degré de P, ce qui a l'avantage de donner un algorithme de calcul du couple (Q, R). Nous verrons cette méthode sur des exemples. Donnons une démonstration plus théorique et un peu plus rapide : introduisons les ensembles $E = \{P - DS,\ S \in \mathbb{K}[X]\}$ et $\mathscr{E} = \{\deg A,\ A \in E\}$.
Si $0 \in E$, alors il existe $Q \in \mathbb{K}[X]$ tel que $P = DQ$, et le couple $(Q, 0)$ est donc celui que nous cherchons.
Sinon, si $0 \notin E$, $\mathscr{E}$ est un sous-ensemble de $\mathbb{N}$. Comme il est clairement non vide, il possède un minimum, noté m. Il existe donc $Q \in \mathbb{R}[X]$ tel que $P - DQ \in \mathbb{K}[X]$, et $\deg(P - DQ) = m \in \mathbb{N}$. La seule chose à montrer est que $m < \deg D$. Par l'absurde, supposons que $m \geqslant \deg D$. Notons aX^m et bX^d les monômes dominants de R et D respectivement. On sait alors que a et b sont non nuls car R et D sont non nuls, et nous avons supposé que $d \leqslant m$. Posons alors $A = R - \frac{a}{b}.D.X^{m-d}$. Alors $\deg A < \deg R$, par annulation du monôme dominant aX^m de R (ce résultat est aussi utilisé dans la démonstration par récurrence). De plus $A = P - DQ - \frac{a}{b}.D.X^{m-d} = P - D(Q + \frac{a}{b}X^{m-d})$, donc $\deg A \in \mathscr{E}$: ceci contredit la minimalité de m, donc par l'absurde, $m < d$, et le couple (Q, R) est le couple voulu. □

Remarque 1.6.5.
Si P et D sont à coefficients dans $\mathbb{R}$, on peut aussi les considérer comme polynômes à coefficients dans $\mathbb{C}$. Remarquer que dans les deux cas, le quotient et le reste de la division euclidienne de P par D sont les mêmes.

Définition 1.6.6.
Soit P et D deux polynômes à coefficients dans $\mathbb{K}$. On dit que D *divise* P ou que P *est un multiple de* D ou que P *est factorisable par* D et on note $D|P$ si et seulement s'il existe un polynôme Q à coefficients dans $\mathbb{K}$ vérifiant $P = D \times Q$.

Remarque 1.6.7. 1. Le polynôme nul est divisible par tout polynôme.

2. Le quotient Q, s'il existe, est unique.
3. Pour tout $n \in \mathbb{N}$ et tout $a \in \mathbb{K}$, on a
$$X - a | X^n - a^n$$
4. P est divisible par D si et seulement si le reste de la division euclidienne de P par D est nul.
5. En vertu de la remarque sur la division euclidienne, lorsque P et D sont deux polynômes à coefficients dans $\mathbb{R}$, P est divisible par D en tant qu'éléments de $\mathbb{R}[X]$ si et seulement si il l'est en tant qu'éléments de $\mathbb{C}[X]$.

Proposition 1.6.8.
Soit P et Q deux polynômes. $P|Q$ et $Q|P$ si et seulement s'il existe $\lambda \in \mathbb{K}^*$ vérifiant $P = \lambda Q$. On dit alors que P et Q sont *associés*.

Tout polynôme P non nul est associé à un unique polynôme unitaire : $\frac{1}{c}P$, où c est le coefficient dominant de P.

Démonstration.
Le résultat est évident si P ou Q est nul (et dans ce cas $P = Q = 0$).
Soient donc P et Q deux polynômes non nuls tels que $P|Q$ et $Q|P$. Alors on a à la fois $\deg P \leqslant \deg Q$ et $\deg P \geqslant \deg Q$. Ainsi $\deg P = \deg Q$. Puisque $P|Q$, il existe un polynôme R tel que $PR = Q$, et comme $\deg P = \deg Q$, R est un polynôme constant : P et Q sont bien associés.
Le sens réciproque est évident. □

1.7 L'algorithme de Horner

Soit $n \in \mathbb{N}$ et $P = \sum_{k=0}^{n} a_k X^k$ un polynôme de degré au plus n à coefficients dans $\mathbb{K}$ et $x_0 \in \mathbb{K}$.

On a $\widetilde{P}(x_0) = \sum_{k=0}^{\deg P} a_k x_0$. Connaissant x_0 et les a_k pour $k \in [\![0, n]\!]$, comment calculer $\widetilde{P}(x_0)$ de façon aussi efficace que possible ?

On peut évidemment calculer toutes les valeurs x_0^k pour $k \in [\![0, n]\!]$ (cela demande $n-1$ multiplications) puis les produits $a_k x_0^k$ (n multiplications supplémentaires), puis calculer la somme (n additions). Total : $2n-1$ multiplications et n additions.

On peut cependant faire mieux.

L'algorithme de Horner consiste à remarquer qu'on peut écrire $P(x_0)$ sous la forme

$$((\dots((a_n x_0 + a_{n-1})x_0 + a_{n-2})\dots)x_0 + a_1)x_0 + a_0$$

Autrement dit, en posant $r_n = a_n$, puis, pour k allant de $n-1$ à 0, $r_k = r_{k+1}x_0 + a_k$, la valeur de $P(x_0)$ est celle de r_0.

Ainsi on a calculé $P(x_0)$ en seulement n multiplications et n additions.

Exemple 1.7.1.
Posons $P = 2X^4 - 4X^3 - 7X^2 + 2X - 1$ par $X - x_0$ et $x_0 = 3$. On exécute parfois l'algorithme de Horner en traçant un tableau. Dans le cas présent, cela donne :

k	4	3	2	1	0
a_k	2	-4	-7	2	-1
r_k	2	2	-1	-1	-4

On a donc $P(x_0) = -4$.

Associé à la proposition suivante, l'algorithme de Horner permet également d'effectuer la division euclidienne d'un polynôme P par un polynôme de degré 1.

Proposition 1.7.2.
Soit $P \in \mathbb{K}[X]$ et $x_0 \in \mathbb{K}$. Alors il existe $Q \in \mathbb{K}[X]$ vérifiant $P = (X - x_0)Q + P(x_0)$.

Démonstration.
Nous donnerons deux démonstrations :

Première méthode Posons la division euclidienne de P par $X - x_0$: il existe $Q, R \in \mathbb{K}[X]$ tels que $P = (X - x_0)Q + R$, avec $\deg R = 0$ ou $-\infty$. R est donc un polynôme constant, notons-le λ.
Évaluons l'égalité $P = (X - x_0)Q + \lambda$ en x_0 : il reste exactement $P(x_0) = \lambda$, d'où le résultat.

Deuxième méthode Cette deuxième méthode ne fait pas appel à la division euclidienne. Elle consiste à constater, en posant $n = \deg P$ et en écrivant P sous la forme $\sum_{k=0}^{n} a_k X^k$, où $a_k \in \mathbb{K}$ pour $k \in [\![0, n]\!]$, que

pour tout $k \in \mathbb{N}$, $X^k - x_0^k$ s'écrit $(X - x_0)Q_k$, où $Q_k = \sum_{i=0}^{k-1} x_0^{k-1-i} X^i$, donc

$$\begin{aligned} P - P(x_0) &= \sum_{k=0}^{n} a_k \left(X^k - x_0^k\right) \\ &= \sum_{k=0}^{n} a_k (X - x_0) Q_k \\ &= (X - x_0) \sum_{k=0}^{n} a_k Q_k \end{aligned}$$

Donc en posant $Q = \sum_{k=0}^{n} a_k Q_k$, on a $P = (X - x_0)Q + P(x_0)$.

□

Calculer le reste de la division est facile par la méthode de Horner. Comment calculer le quotient Q ? Q est de la forme $\sum_{k=0}^{n-1} b_k X^k$. On a alors :

$$\sum_{k=0}^{n} a_k X^k = (X - x_0) \sum_{k=0}^{n-1} b_k X^k + P(x_0)$$

En identifiant les termes de même degré, il vient :

$$\begin{aligned} a_n &= b_{n-1} \\ a_{n-1} &= b_{n-2} - x_0 b_{n-1} \\ &\vdots \\ a_2 &= b_1 - x_0 b_2 \\ a_1 &= b_0 - x_0 b_1 \end{aligned}$$

On en déduit :

$$\begin{aligned} b_{n-1} &= a_n \\ b_{n-2} &= a_{n-1} + x_0 b_{n-1} \\ &\vdots \\ b_1 &= a_2 + x_0 b_2 \\ b_0 &= a_1 + x_0 b_1 \end{aligned}$$

On peut remarquer que les valeurs des coefficients de Q sont exactement celles calculées pour le calcul de $P(x_0)$: on constate en effet qu'on a

$$\begin{aligned} b_{n-1} &= r_n \\ b_{n-2} &= r_{n-1} \\ &\vdots \\ b_1 &= r_2 \\ b_0 &= r_1 \end{aligned}$$

Exemple 1.7.3.
En reprenant l'exemple 1.7.1, on trouve $P = (X - 3)(2X^3 + 2X^2 - X - 1) - 4$.

2 Décomposition

2.1 Racines, ordre de multiplicité

Définition 2.1.1.
Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. On dit que a est racine de P si et seulement si $P(a) = 0$.

Proposition 2.1.2.
Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. a est racine de P si et seulement si $X - a$ divise P. Autrement dit :

$$P(a) = 0 \iff X - a | P$$

Démonstration.
Le sens indirect est évident.
Le sens direct découle directement de la proposition 1.7.2 avec $x_0 = a$. □

Corollaire 2.1.3.
Soit $P \in \mathbb{K}[X]$, $n \in \mathbb{N}$ et $a_1, \ldots, a_n$ n éléments de $\mathbb{K}$ distincts. Alors $a_1, \ldots, a_n$ sont des racines de P si et seulement si $\prod_{k=1}^{n} (X - a_k)$ divise P.

Démonstration.
Là encore le sens indirect est évident.
Le sens direct se fait par récurrence sur le nombre de racines en utilisant la proposition précédente. □

Définition 2.1.4.
Soit $P \in \mathbb{K}[X]$ un polynôme non nul, $a \in \mathbb{K}$ et $r \in \mathbb{N}$. On dit que *a est racine d'ordre de multiplicité r de P* si r est le plus grand entier k tel que $(X-a)^k$ divise P. On dit que a est racine simple (resp. multiple) de P si $r = 1$ (resp. $r > 1$).

Remarque 2.1.5.
1. L'ensemble des k tel que $(X-a)^k \mid P$ contient 0 et est majoré par le degré de P, donc possède bien un plus grand élément.
2. Si a est racine d'ordre r, alors pour tout $k \in [\![0, r]\!]$, $(X-a)^k | P$.
3. a est racine d'ordre au moins 1 si et seulement si $X - a | P$, c'est-à-dire si et seulement si $P(a) = 0$.
4. a est racine multiple si et seulement si $(X-a)^2 | P$.

Proposition 2.1.6.
Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $r \in \mathbb{N}$. a est racine d'ordre r de P si et seulement si P s'écrit sous la forme $(X-a)^r Q$ où $Q(a) \neq 0$.

Démonstration.
Supposons que a est racine d'ordre r de P. Alors P est divisible par $(X-a)^r$, donc s'écrit sous la forme $(X-a)^r Q$. Par l'absurde, supposons $Q(a) = 0$, alors $X - a | Q$, donc $(X-a)^{r+1} | Q$, ce qui est absurde. Donc $Q(a) \neq 0$.

Supposons que P s'écrit sous la forme $(X-a)^r Q$ où $Q(a) \neq 0$. Alors l'ordre de multiplicité de a dans P est au moins r. Supposons par l'absurde que cet ordre soit strictement supérieur. Alors $(X-a)^{r+1}$ divise P, donc P s'écrit sous la forme $(X-a)^{r+1} R$, donc $(X-a)^{r+1} R = (X-a)^r Q$, donc $(X-a)R = Q$. Donc $Q(a) = 0$, ce qui est absurde. □

2.2 Nombres de racines

Proposition 2.2.1.
Soit $P \in \mathbb{K}[X]$ un polynôme non nul. Alors P a au plus $\deg(P)$ racines distinctes.

Démonstration.
Soit P un polynôme non nul de degré n, et $\lambda_1, \ldots, \lambda_{n+1}$ $n+1$ racines distinctes de P. Alors P est divisible par $\prod_{k=1}^{n+1}(X - \lambda_i)$, qui est un polynôme de degré strictement supérieur au degré de P : c'est absurde. □

Proposition 2.2.2.
Soit $n \in \mathbb{N}$ et $P \in \mathbb{K}_n[X]$. Si P admet au moins $n+1$ racines distinctes, alors P est le polynôme nul.

Démonstration.
C'est la contraposée du résultat précédent. □

Corollaire 2.2.3.
On déduit de cette proposition les résultats suivants :
1. Soit $n \in \mathbb{N}$ et $(P, Q) \in \mathbb{K}_n[X]^2$. Si P et Q coïncident sur au moins $n+1$ points, alors $P = Q$.
2. Soit $P \in \mathbb{K}[X]$. Si P admet une infinité de racines, alors P est le polynôme nul.
3. Soit $(P, Q) \in \mathbb{K}[X]^2$. Si P et Q coïncident sur une infinité de valeurs, alors $P = Q$.

Démonstration.
1. Appliquer la proposition précédente au polynôme $P - Q$.
2. Choisir un entier n vérifiant $n \geqslant \deg P$ et appliquer la proposition précédente.
3. Appliquer le premier point à un $n \in \mathbb{N}$ vérifiant $n \geqslant \max(\deg P, \deg Q)$ ou le second à $P - Q$.

□

En particulier, $\mathbb{K}$ étant infini, un polynôme P tel que $\widetilde{P}$ est l'application nulle sur $\mathbb{K}$ est nécessairement nul et deux polynômes P et Q tels que $\widetilde{P} = \widetilde{Q}$ sont nécessairement égaux, ce qui permet de conclure la démonstration du théorème 1.5.6.

Remarque 2.2.4.
(à caractère culturel) Il est essentiel pour ce résultat que $\mathbb{K}$ soit infini. Dans un corps fini $\mathbb{K}$ comportant n éléments $k_1, \ldots, k_n$, le polynôme $(X - k_1) \times (X - k_2) \times \cdots \times (X - k_n)$ est non nul (car de degré n) mais a pour racine tous les éléments du corps.

2.3 Polynômes scindés et relations coefficients/racines

Définition 2.3.1.
Soit $P \in \mathbb{K}[X]$.
On dit que P est *scindé* si et seulement si P est nul ou peut s'écrire comme produit de polynômes de degré 1, c'est-à-dire si et seulement s'il existe $n \in \mathbb{N}$, $\lambda \in \mathbb{K}$ et $(\alpha_1, \dots, \alpha_n) \in \mathbb{K}^n$ vérifiant

$$P = \lambda \prod_{i=1}^{n} (X - \alpha_i).$$

Remarque 2.3.2. 1. Dans cette écriture, si P est non-nul :
- n est le degré de P
- λ est son coefficent dominant.
- $(\alpha_1, \dots \alpha_n)$ sont les racines de P comptées avec ordre de multiplicité.

2. Un polynôme à coefficients réels peut être scindé dans $\mathbb{C}$ sans l'être dans $\mathbb{R}$: $P = X^2 + 1$.

Proposition 2.3.3 (Relations coefficients-racines.)**.**
Soit n un entier et $P = \sum_{i=0}^{n} a_i X^i$ un polynôme scindé de degré n sur $\mathbb{K}$. Alors P est de la forme

$$\lambda \prod_{k=1}^{n} (X - \alpha_k),$$

avec $\lambda = a_n$. Alors P s'écrit

$$\lambda \left(X^n + \sum_{k=1}^{n} (-1)^k \sigma_k X^{n-k} \right),$$

où

$$\begin{aligned}
\sigma_1 &= \alpha_1 + \alpha_2 + \cdots + \alpha_n = -\frac{a_{n-1}}{a_n} \\
\sigma_2 &= \alpha_1\alpha_2 + \cdots + \alpha_{n-1}\alpha_n = \frac{a_{n-2}}{a_n} \\
&\vdots \\
\sigma_k &= \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} \alpha_{i_1} \dots \alpha_{i_k} = (-1)^k \frac{a_{n-k}}{a_n} \\
&\vdots \\
\sigma_n &= \alpha_1 \dots \alpha_n = (-1)^n \frac{a_0}{a_n}.
\end{aligned}$$

Démonstration.
Il suffit d'identifier $\sum_{i=0}^{n} a_i X^i$ et $\lambda \prod_{k=1}^{n} (X - \alpha_k)$. □

Définition 2.3.4.
Les scalaires σ_i, pour $i \in 1, n$ sont appelés *fonctions symétriques élémentaires* des racines de P.

Toute expression polynomiale dépendant de variables α_1, …, α_n, symétrique en α_1, …, α_n (c'est-à-dire telle que l'échange de deux de ces variables ne change pas sa valeur) est appelée *fonction symétrique* de α_1, …, α_n.

Remarque 2.3.5 (à caractère culturel)**.**
Toute fonction symétrique de α_1, …, α_n peut s'écrire à partir des seules fonctions symétriques élémentaires de α_1, …, α_n.

Exemple 2.3.6.
Soit $(x_1, x_2) \in \mathbb{C}$. On pose $v = x_1^2 + 2x_1x_2 + 14x_1^2x_2 + x_2^2 + 14x_1x_2^2 + 49x_1^2x_2^2$.

v est fonction symétrique de x_1 et x_2. Comment l'exprimer à partir des fonctions symétriques élémentaires $\sigma_1 = x_1 + x_2$ et $\sigma_2 = x_1x_2$?

Une méthode systématique est la suivante [3] :

1. On repère tout d'abord le monôme «dominant». Parmi tous les monômes, le monôme

3. Source : article *Elementary symmetric polynomial* sur Wikipedia (`en.wikipedia.org`).

dominant fait partie de ceux dont la puissance de la dernière variable est maximale, et parmi ceux-ci, c'est celui dont la puissance de l'avant-dernière variable est maximale, etc. Ici, la puissance maximale pour x_2 est 2, et parmi les monômes x_2^2, $14x_1x_2^2$ et $49x_1^2x_2^2$, celui dont la puissance de x_1 est maximale est $49x_1^2x_2^2$.

2. Pour éliminer un monôme $\alpha x_1^{k_1}\dots x_n^{k_n}$, on soustrait $\alpha\sigma_1^{k_n-k_{n-1}}\dots\sigma_{n-1}^{k_2-k_1}\sigma_n^{k_1}$. Autrement dit, ici on soustrait $49\sigma_1^{2-2}\sigma_2^2$. On obtient donc $v-49\sigma_2^2 = x_1^2+2x_1x_2+14x_1^2x_2+x_2^2+14x_1x_2^2$.
3. On itére. Ici il convient donc d'éliminer le monôme $14x_1x_2^2$ et pour cela de soustraire $14\sigma_1^{2-1}\sigma_2$, ce qui donne $v-49\sigma_2^2-14\sigma_1\sigma_2 = x_1^2+2x_1x_2+x_2^2$.
   Le plus grand monôme est alors x_2^2 ; on soustrait donc σ_1^2, ce qui donne $v-49\sigma_2^2-14\sigma_1\sigma_2-\sigma_1^2=0$.
   On a donc $v = 49\sigma_2^2+14\sigma_1\sigma_2+\sigma_1^2$.

On remarque cependant qu'on pouvait aller beaucoup plus vite en remarquant dès le début $v=(x_1+7x_1x_2+x_2)^2=(\sigma_1+7\sigma_2)^2$.

NB : selon le programme officiel «Aucune connaissance spécifique sur le calcul des fonctions symétriques des racines n'est exigible».

Exercice 2.3.7.
Résoudre le système d'inconnues (x,y,z)

$$\begin{cases} x + y + z = 3 \\ x^2 + y^2 + z^2 = 11 \\ x^3 + y^3 + z^3 = 27 \end{cases}$$

2.4 Le théorème fondamental de l'algèbre

Définition 2.4.1 (Polynômes irréductibles)**.**
Soit $P\in\mathbb{K}[X]$, avec $\deg P\geqslant 1$. On dit que P est réductible dans $\mathbb{K}[X]$ s'il existe deux polynômes Q et R dans $\mathbb{K}[X]$ vérifiant

1. $\deg Q\geqslant 1$
2. et $\deg R\geqslant 1$
3. et $P=Q\times R$.

On dit que P est irréductible dans $\mathbb{K}[X]$ dans le cas contraire.

Remarque 2.4.2.
1. La notion de polynôme irréductible est comparable à celle de primalité dans $\mathbb{Z}$: un polynôme est irréductible si et seulement s'il est de degré au moins 1 et que ses seuls diviseurs sont les éléments de $\mathbb{K}$ et ses associés.
2. Attention : un polynôme peut être irréductible dans $\mathbb{R}[X]$ sans l'être dans $\mathbb{C}[X]$. Par exemple X^2+1 est irréductible dans $\mathbb{R}[X]$, mais se factorise en $(X-i)(X+i)$ dans $\mathbb{C}[X]$.
3. Tout polynôme à coefficients réels irréductible dans $\mathbb{C}[X]$ est irréductible dans $\mathbb{R}[X]$.
4. Tout polynôme de degré 1 est irréductible.
5. Tout polynôme de $\mathbb{K}[X]$ de degré supérieur ou égal à 2 admettant une racine dans $\mathbb{K}$ est réductible dans $\mathbb{K}[X]$.
6. Il existe des polynômes sans racines qui ne sont pas irréductibles. Par exemple X^4+2X^2+1 n'admet pas de racines réelles alors qu'il se décompose comme produit de deux polynômes de degré 2.

Proposition 2.4.3.
Tout polynôme non nul et non constant se décompose comme produit de polynômes irréductibles.

Démonstration.
Par récurrence forte sur le degré du polynôme. □

Reste au moins deux questions :

1. Cette décomposition est-elle unique ?
2. Quels sont les polynômes irréductibles de $\mathbb{R}[X]$ et de $\mathbb{C}[X]$?

On verra plus loin comment répondre au premier point. Pour le second, la réponse nous est fournie par le théorème de d'Alembert-Gauss, aussi appelé théorème fondamental de l'algèbre : comme ce dernier nom l'indique, ce résultat est effectivement d'une importance capitale en algèbre.

Théorème 2.4.4 (d'Alembert-Gauss)**.**
Tout polynôme non constant à coefficients dans $\mathbb{C}$ admet au moins une racine dans $\mathbb{C}$.

Démonstration.
Ce résultat est admis. Pour mémoire, une démonstration possible est de considérer un polynôme P et de montrer successivement :

1. Il existe $R > 0$ tel que pour tout z vérifiant $|z| > R$, $|P(z)| \geqslant |P(0)|$;
2. $z \mapsto |P(z)|$ admet un minimum sur le pavé des complexes de parties réelles et imaginaires appartenant à $[-R, R]$ en un point a (montrer que la borne inférieure de $|P(z)|$ est un minimimun en exploitant la compacité de ce pavé).
3. $z \mapsto |P(z)|$ admet donc un minimum sur $\mathbb{C}$ au point a.
4. Par l'absurde, on suppose $P(a) \neq 0$ et on pose $Q = \frac{1}{P(a)}(P \circ (X + a))$. Alors $Q(0)$ vaut 1 et $z \mapsto |Q(z)|$ admet un minimum (global) en 0.
5. En explicitant Q, on constate que son coefficient constant est égal à 1 et on montre qu'il existe z vérifiant $|Q(z)| < 1$, ce qui est absurde, donc $P(a) = 0$.

□

Corollaire 2.4.5.
Les polynômes irréductibles dans $\mathbb{C}[X]$ sont les polynômes de degré 1.

Démonstration.
On sait déjà que tous les polynômes de degré 1 sont irréductibles. De plus, pour tout $n \geqslant 2$, tout polynôme P de degré n admet une racine complexe a, donc est le produit de $X - a$ par un polynôme de degré $n - 1$. Or $n - 1 \geqslant 1$, donc P est réductible. □

Corollaire 2.4.6.
Tout polynôme non constant est scindé dans $\mathbb{C}[X]$.

Démonstration.
Il suffit d'utiliser les résultats 2.4.3 et 2.4.5. □

Pour les polynômes à coefficients réels, il est intéressant de noter le résultat suivant :

Proposition 2.4.7.
Soit P un polynôme à coefficients réels et $z \in \mathbb{C}$.

Alors z et $\overline{z}$ sont des racines de P de même multiplicité.

En particulier, z est racine de P si et seulement si $\overline{z}$ est racine de P.

Les racines de P non réelles sont donc deux à deux conjuguées.

Démonstration.
On note $\overline{P}$ le polynôme conjugué de P, c'est-à-dire le polynôme dont les coefficients sont les conjugués de ceux de P. On peut alors démontrer plusieurs résultats simples :

1. Si $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$, alors $\overline{P(\lambda)} = \overline{P}\left(\overline{\lambda}\right)$;
2. Si $P, Q \in \mathbb{K}[X]$, $\overline{PQ} = \overline{P}\,\overline{Q}$;
3. P est à coefficients réels si et seulement si $\overline{P} = P$.

Soit donc P un polynôme à coefficients réels, et z une racine complexe de P, de multiplicité exactement r. Alors il existe $Q \in \mathbb{C}[X]$ tel que $P = (X - z)^r Q$, avec $Q(z) \neq 0$. Mais alors $P = \overline{P} = \overline{(X - z)^r Q} = (X - \overline{z})^r \overline{Q}$. Donc $\overline{z}$ est racine de P multiplicité au moins r. Mais $\overline{Q}(\overline{z}) = \overline{Q(z)} \neq 0$, donc $\overline{z}$ est racine de P multiplicité exactement r.

On peut également démontrer ce résultat de la manière suivante, en utilisant le résultat 3.2.6 qui vient un peu plus loin : Soit $z \in \mathbb{C}$. On sait que z est racine d'ordre r de P si et seulement si $r = \min\left\{ k \in \mathbb{N} \;\middle|\; P^{(k)}(z) \neq 0 \right\}$ si et seulement si $r = \min\left\{ k \in \mathbb{N} \;\middle|\; \overline{P^{(k)}(z)} \neq 0 \right\}$.

Or pour tout k, $\overline{P^{(k)}(z)} = \overline{P^{(k)}}(\bar{z})$ et pour P à coefficients réels, $\overline{P^{(k)}} = P^{(k)}$, donc

$$\left\{ k \in \mathbb{N} \;\middle|\; \overline{P^{(k)}(z)} \neq 0 \right\} = \left\{ k \in \mathbb{N} \;\middle|\; P^{(k)}(\bar{z}) \neq 0 \right\}$$

Par conséquent z est racine d'ordre r de P si et seulement si $r = \min\left\{ k \in \mathbb{N} \;\middle|\; P^{(k)}(\bar{z}) \neq 0 \right\}$ si et seulement si z est racine d'ordre r de $\overline{P}$. □

On en déduit la proposition suivante

Proposition 2.4.8.
Soit P un polynôme à coefficients réels non constant n'admettant pas de racine réelle. Alors il est divisible par un polynôme à coefficients réels de degré 2.

Démonstration.
Notons a une racine complexe de P. D'après ce qui précède $\overline{a}$ est également une racine de P.

Dans $\mathbb{C}[X]$, P est divisible par $X-a$, donc s'écrit sous la forme $(X-a)Q$, où $Q \in \mathbb{C}[X]$. $a \notin \mathbb{R}$, donc $\overline{a}-a \neq 0$, or $P(\overline{a})=0$, donc $Q(\overline{a})=0$.

Donc Q s'écrit sous la forme $(X-\overline{a})R$ où $R \in \mathbb{C}[X]$.

Donc $P=(X-a)(X-\overline{a})R=\left(X^2-2\operatorname{Re}(a)+|a|^2\right)R$.

Or $X^2-2\operatorname{Re}(a)+|a|^2 \in \mathbb{R}[X]$ et $P \in \mathbb{R}[X]$, donc $R \in \mathbb{R}[X]$. □

D'où :

Proposition 2.4.9.
Les polynômes irréductibles dans $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle.

Démonstration.
Montrons déjà que les polynômes réels de degré deux sans racine réelle sont irréductibles. Soit P un tel polynôme, et Q, R deux polynômes réels tels que $P=QR$. Supposons que $\deg Q=1$. Alors Q est de la forme $aX+b$, où a et b sont des réels, avec $a \neq 0$. Il admet donc $-\dfrac{b}{a}$ comme récine réelle, et donc P a une récine réelle, ce qui est absurde. Ainsi $\deg Q=0$ ou 2, et P est irréductible.
Soit P un polynôme réel irréductible, de degré strictement supérieur à 1. S'il admet une racine réelle a, il est divisible par $X-a$ et n'est donc pas irréductible. S'il n'admet pas de racine réelle, il est divisible par un polynôme réel de degré 2. Donc si P est de degré strictement supérieur à 2, il est réductible. S'il est de degré 2, il est bien de la forme annoncée. □

2.5 Décomposition en produit de facteurs irréductibles

Le théorème de d'Alembert-Gauss a pour corollaire immédiat :

Corollaire 2.5.1.
Soit $n \in \mathbb{N}$, P un polynôme de degré n et de coefficient dominant c. Alors il existe $z_1, \ldots, z_n$ des complexes vérifiant :

$$P = c\prod_{k=1}^{n}(X-z_k)$$

où les z_k, pour $k \in [\![1,n]\!]$ sont les racines de P, éventuellement répétées.

Corollaire 2.5.2.
Soit $n \in \mathbb{N}$, $P \in \mathbb{C}[X]$ de degré n et de coefficient dominant c. Alors, en notant p le nombre de racines distinctes de P, $z_1, \ldots, z_p$ les racines distinctes de P, et $n_1, \ldots, n_p$ leurs multiplicités respectives, on a :

$$P = c\prod_{k=1}^{p}(X-z_k)^{n_k}$$
$$\text{et } n = \sum_{k=1}^{p} n_k$$

Démonstration.
La première égalité découle directement du corollaire précédent, et la seconde est l'égalité des degrés dans l'égalité polynomiale précédente. □

Et :

Théorème 2.5.3.
Soit P un polynôme à coefficients réels, alors on peut écrire P sous la forme

$$P = c\prod_{k=1}^{n}(X-a_k)\prod_{k=1}^{m}(X-z_k)(X-\overline{z}_k)$$

où $a_1, \ldots, a_n$ sont les racines réelles de P (répétées avec leur multiplicité), $z_1, \ldots, z_m, \overline{z}_1, \ldots, \overline{z}_m$ les racines complexes non réelles (répétées avec leur multiplicité), c le coefficient dominant de P, et $n+2m=\deg(P)$.

On a donc

$$P = c\prod_{k=1}^{n}(X-a_k)\prod_{k=1}^{m}\left(X^2-2\operatorname{Re}(z_k)X+|z_k|^2\right)$$

Corollaire 2.5.4.
Tout polynôme à coefficients réels de degré impair a au moins une racine réelle.

Démonstration.
Par contraposition : un polynôme à coefficients réels n'ayant pas de racine réelle s'écrit sous la forme

$c\prod_{k=1}^{m}\left(X^2-2\operatorname{Re}(z_k)X+|z_k|^2\right)$ et est donc de degré pair. □

Exercice 2.5.5.
Factoriser sur $\mathbb{R}$ les polynômes X^5+1 et X^4+1.

3 Dérivation des polynômes

On intoduit maintenant la notion de dérivation formelle de polynômes. Le mot « formel » est à prendre au sens suivant : on effectue des opérations *algébriques*, qui n'ont pas forcément de sens *analytique* (même si la dérivation formelle de polynômes coïncide avec la dérivation de fonctions polynomiales).

3.1 Définition

Définition 3.1.1.
Soit $P\in\mathbb{K}[X]$, que l'on écrit $P=\sum_{k=0}^{+\infty}a_kX^k$. Son polynôme dérivé est

$$P'=\sum_{k=1}^{+\infty}a_kkX^{k-1}.$$

Remarque 3.1.2.
• La somme ne commence qu'à l'indice 1 :

en effet, pour $k=0$, X^{k-1} n'existe pas.
• On a également, après changement d'indice :

$$P'=\sum_{k=0}^{+\infty}a_{k+1}(k+1)X^k.$$

Cette formule est intéressante lorsqu'il s'agit de manipuler plusieurs polynômes, tous exprimés comme sommes commençant à l'indice 0.
• Sur $\mathbb{R}[X]$, cette opération coïncide avec la dérivation des applications à valeurs réelles :

$$\forall P\in\mathbb{R}[X]\qquad \widetilde{(P')}=\left(\widetilde{P}\right)'.$$

• Si P est de degré 0 ou $-\infty$, alors $P'=0$. Sinon $\deg(P')=\deg(P)-1$.

• P est un polynôme vérifiant $P'=\sum_{k=0}^{+\infty}a_kX^k$ si et seulement s'il existe $C\in\mathbb{K}$ vérifiant

$$P=C+\sum_{k=0}^{+\infty}\frac{a_k}{k+1}X^{k+1}$$

(donner un nom aux coefficients de P, calculer P' et utiliser l'unicité de la forme développée réduite).
• Si $P'=0$, alors P est constant.

Définition 3.1.3.
Soit $P\in\mathbb{K}[X]$. On définit, pour $n\in\mathbb{N}$, le n-ième dérivé de P, noté $P^{(n)}$ par

$$P^{(0)}=P$$
$$\text{et }\forall n\in\mathbb{N}\qquad P^{(n+1)}=\left(P^{(n)}\right)'$$

3.2 Propriétés

Proposition 3.2.1.
Soit $(P,Q)\in\mathbb{K}[X]^2$ et $(\lambda,\mu)\in\mathbb{K}^2$. Alors

$$(\lambda P+\mu Q)'=\lambda P'+\mu Q' \tag{XIV.1}$$
$$(PQ)'=P'Q+PQ' \tag{XIV.2}$$
$$(P\circ Q)'=Q'\times(P'\circ Q) \tag{XIV.3}$$

Démonstration.
Écrivons P sous la forme $\sum_{k=0}^{+\infty}a_kX^k$ et Q sous la forme $\sum_{k=0}^{+\infty}b_kX^k$.
Alors on a

$$\begin{aligned}(\lambda P+\mu Q)' &= \left(\sum_{k=0}^{+\infty}(\lambda a_k+\mu b_k)X^k\right)'\\ &=\sum_{k=1}^{+\infty}(\lambda a_k+\mu b_k)X^{k-1}\\ &=\lambda\left(\sum_{k=1}^{+\infty}a_kX^{k-1}\right)+\mu\left(\sum_{k=1}^{+\infty}b_kX^{k-1}\right)\\ &=\lambda P'+\mu Q'\end{aligned}$$

Le premier point est donc assuré. Il se généralise évidemment par récurrence à toute combinaison linéaire finie de polynômes.

Montrons alors le second. Notons, pour tout $i \in \mathbb{N}$, A_i le monôme X_i et remarquons que pour tout $(i,j) \in \mathbb{N}^2$, on a $(A_iA_j)' = A_i'A_j + A_iA_j'$.

En effet, c'est évidemment vrai si $i = 0$ (auquel cas $A_i = 1$ et $A_i' = 0$) ou symétriquement si $j = 0$. Si ni i ni j n'est nul, on a $i \geqslant 1$ et $j \geqslant 1$, d'où

$$\begin{aligned}(A_iA_j)' &= (X^{i+j})' \\ &= (i+j)X^{i+j-1} \\ &= iX^{i-1}X^j + X^i \times jX^{j-1} \\ &= A_i'A_j + A_iA_j'\end{aligned}$$

On a alors successivement :

$$\begin{aligned}(PQ)' &= \left(\left(\sum_{i\in\mathbb{N}} a_iA_i\right)\left(\sum_{j\in\mathbb{N}} b_jA_j\right)\right)' \\ &= \left(\sum_{(i,j)\in\mathbb{N}^2} a_ib_jA_iA_j\right)' \\ &= \sum_{(i,j)\in\mathbb{N}^2} a_ib_j(A_iA_j)' \\ &= \sum_{(i,j)\in\mathbb{N}^2} a_ib_j\left(A_i'A_j + A_iA_j'\right) \\ &= \sum_{(i,j)\in\mathbb{N}^2} a_ib_jA_i'A_j + \sum_{(i,j)\in\mathbb{N}^2} a_ib_jA_iA_j'\end{aligned}$$

Or on a

$$\begin{aligned}\sum_{(i,j)\in\mathbb{N}^2} a_ib_jA_i'A_j &= \left(\sum_{i\in\mathbb{N}} a_iA_i'\right)\left(\sum_{j\in\mathbb{N}} b_jA_j\right) \\ &= P'Q \\ \text{et } \sum_{(i,j)\in\mathbb{N}^2} a_ib_jA_iA_j' &= \left(\sum_{i\in\mathbb{N}} a_iA_i\right)\left(\sum_{j\in\mathbb{N}} b_jA_j'\right) \\ &= PQ'\end{aligned}$$

Donc $(PQ)' = P'Q + PQ'$.

On en déduit par récurrence que pour tout entier $k \in \mathbb{N}^*$, on a $\left(Q^k\right)' = kQ' \times Q^{k-1}$. En outre, on a évidemment $\left(Q^0\right)' = \left(1_{\mathbb{K}[X]}\right)' = 0$.

On a alors successivement

$$\begin{aligned}(P \circ Q)' &= \left(\sum_{k=0}^{+\infty} a_kQ^k\right)' \\ &= \sum_{k=1}^{+\infty} a_kkQ' \times Q^{k-1} \\ &= Q' \times \sum_{k=1}^{+\infty} a_kkQ^{k-1} \\ &= Q' \times \left(\left(\sum_{k=1}^{+\infty} ka_kX^{k-1}\right) \circ Q\right) \\ &= Q' \times \left(P' \circ Q\right)\end{aligned}$$

□

Remarque 3.2.2.
Notamment, $P' = Q'$ si et seulement si il existe $C \in \mathbb{K}$ tel que $P = Q + C$.

Proposition 3.2.3 (Formule de Leibniz)**.**
Soit $(P,Q) \in \mathbb{K}[X]^2$ et $n \in \mathbb{N}$. Alors

$$(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)}Q^{(n-k)}$$

Démonstration.
Elle se démontre par récurrence et est laissée en exercice au lecteur, qui remarquera une très très forte ressemblance avec la démonstration d'une formule de début d'année. □

Lemme 3.2.4 (Formule de Taylor Mac-Laurin)**.**
Soit $n \in \mathbb{N}$ et $P \in \mathbb{K}_n[X]$. Alors

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!} X^k$$

Démonstration.
Démontrons-la par récurrence :
pour tout $n \in \mathbb{N}$, soit (H_n) : pour tout $P \in \mathbb{K}_n[X]$, $P = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!} X^k$.
• Pour $n = 0$, la propriété est évidente.
• Soit $n \in \mathbb{N}$ tel que la propriété soit vraie, et soit $P \in \mathbb{K}_{n+1}[X]$. Puisque $P' \in \mathbb{K}_n[X]$, on peut lui appliquer l'hypothèse de récurrence : $P' = \sum_{k=0}^{n} \frac{(P')^{(k)}(0)}{k!} X^k =$

$\sum_{k=0}^{n} \frac{P^{(k+1)}(0)}{k!} X^k$. Il existe donc une constante $C \in \mathbb{K}$ telle que $P = \sum_{k=0}^{n} \frac{P^{(k+1)}(0)}{(k+1)!} X^{k+1} + C = \sum_{k=1}^{n+1} \frac{P^{(k)}(0)}{k!} X^k + C$ après un changement d'indice. Pour calculer C, on peut étudier les fonctions polynomiales associés aux polynômes de l'égalité précédente, et les évaluer en 0 : on trouve alors $C = P(0) = \frac{P^{(k)}(0)}{k!} X^k$ avec $k = 0$, et donc H_{n+1} est bien vérifiée. □

Proposition 3.2.5 (Formule de Taylor)**.**
Soit $n \in \mathbb{N}$, $P \in \mathbb{K}_n[X]$ et $a \in \mathbb{K}$. Alors

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

Corollaire 3.2.6.
On en déduit immédiatement

$$P(a+X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} X^k$$

Démonstration.
Il suffit d'effectuer une "translation" à partir du théorème précédent : posons $Q = P \circ (X + a)$.
Alors $Q = \sum_{k=0}^{n} \frac{Q^{(k)}(0)}{k!} X^k$. Mais on vérifie facilement que pour tout k, $Q^{(k)} = P^{(k)} \circ (X + a)$ et donc $Q^{(k)}(0) = P^{(k)}(a)$.
Finalement, on a

$$\begin{aligned} P &= Q \circ (X - a) \\ &= \left(\sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} X^k \right) \circ (X - a) \\ &= \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} (X-a)^k \end{aligned}$$

□

Proposition 3.2.7.
Soit $P \in \mathbb{K}[X]$ non nul, $r \in \mathbb{N}$ et $a \in \mathbb{K}$.
a est racine d'ordre r de P si et seulement si $P^{(r)}(a) \neq 0$ et pour tout $k \in [\![0, r-1]\!]$, $P^{(k)}(a) = 0$

Démonstration.
a est racine d'ordre r de P si et seulement si $(X-a)^r | P$ et $(X-a)^{r+1} \nmid P$.
Or $P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} (X-a)^k$, donc $(X-a)^r | P$ ssi pour tout $k \in [\![0, r-1]\!]$, $P^{(k)}(a) = 0$. De même, $(X-a)^{r+1} \nmid P$ ssi il existe $k \in [\![0, r]\!]$ tel que $P^{(k)}(a) \neq 0$.
Le résultat voulu découle de la conjonction de ces deux dernières équivalences. □

Corollaire 3.2.8.
Soit $P \in \mathbb{K}[X]$, $r \in \mathbb{N}^*$ et $a \in \mathbb{K}$.
Si a est racine d'ordre r de P, alors a est racine d'ordre $r-1$ de P'.

 La réciproque est fausse ! Par exemple si $P = X^2 - 1$, alors 0 est racine de multiplicité 1 de P', mais n'est pas racine de multiplicité de P (ce n'est même pas une racine de P).
On peut par contre énoncer le résultat suivant : si a est racine d'ordre $r-1$ de P' et si a est racine, de P, alors a est racine d'ordre r de P.

4 Arithmétique de $\mathbb{K}[X]$

4.1 PGCD

Dans cette partie, pour tout $a \in \mathbb{K}[X]$, on note $\mathscr{D}(a)$ l'ensemble des diviseurs de a et pour tout couple $(a, b) \in \mathbb{K}[X]$, $\mathscr{D}(a, b)$ l'ensemble des diviseurs communs à a et b. On remarquera que $\mathscr{D}(a, b) = \mathscr{D}(a) \cap \mathscr{D}(b)$.

Remarque 4.1.1.
1. Soit d et d' deux polynômes. $\mathscr{D}(d) = \mathscr{D}(d')$ si et seulement si d et d' sont associés.
2. En particulier, si on a $\mathscr{D}(d) = \mathscr{D}(d')$ et que d et d' sont unitaires, alors $d = d'$ et pour tout polynôme d, il existe d' unitaire vérifiant $\mathscr{D}(d') = \mathscr{D}(d)$.

Lemme 4.1.2 (lemme d'Euclide)**.**
Soient $(a,b) \in \mathbb{K}[X]^2$, avec $b \neq 0$. Notons r le reste de la division euclidienne de a par b. Alors $\mathscr{D}(a,b) = \mathscr{D}(b,r)$.

Démonstration.
Soit $d \in \mathscr{D}(a,b)$. Alors a s'écrit sous la forme $bq+r$ donc $r = a - bq$, or $d|a$ et $d|b$, donc d divise bq, donc divise r. Donc $\mathscr{D}(a,b) \subset \mathscr{D}(b,r)$.

Réciproquement, soit $d \in \mathscr{D}(b,r)$, alors a s'écrit sous la forme $bq+r$ or $d|b$ et $d|r$ donc d divise a. Donc $\mathscr{D}(b,r) \subset \mathscr{D}(a,b)$. □

Théorème 4.1.3.
Soit $(a,b) \in \mathbb{K}[X]^2$ avec $(a,b) \neq (0,0)$. Alors, il existe $d \in \mathbb{K}[X]$ tel que $\mathscr{D}(a,b) = \mathscr{D}(d)$.

Démonstration.
Ce résultat repose sur un algorithme, appelé algorithme d'Euclide. En utilisant les objets «polynômes» fournis par la bibliothèque python `numpy`, cet algorithme s'écrit :

```
def euclide (a,b) :
    """Précondition (a,b) != (0,0)"""
    R0 = abs(a)
    R1 = abs(b)
    while R1 > 0 :
        # Invariant : D(R0,R1) = D(a,b)
        # et R0 >= 0 et R1 >= 0
        # et (R0, R1) != (0,0)
        # Variant : R1
        (q, R2) = diveuclide (R0,R1)
        R0 = R1
        R1 = R2
    # Sortie de boucle : R1 == 0
    return R0
```

Soit a et b deux polynômes non tous les deux nuls. Il est clair que l'appel `euclide(a,b)` termine. La valeur d retournée vérifie $\mathscr{D}(a,b) = \mathscr{D}(d,0)$ et $(d,0) \neq (0,0)$. Or $\mathscr{D}(d,0)$ est l'ensemble des diviseurs de d donc $\mathscr{D}(a,b)$ est bien l'ensemble des diviseurs d'un polynôme d.

Un autre point de vue sur cet algorithme est la suite r définie de la façon suivante :

$$\begin{cases} r_0 = a \\ r_1 = b \\ \forall n \in \mathbb{N},\ r_{n+2} = \begin{cases} \texttt{diveuclide}(r_n, r_{n+1}) & \text{si } r_{n+1} \neq 0 \\ 0 & \texttt{sinon} \end{cases} \end{cases}$$

À partir d'un certain rang, cette suite est nulle, sinon la suite $(\deg(r_n))_{n\in\mathbb{N}}$ serait strictement décroissante (du moins, à partir du rang 1), ce qui serait absurde. Par ailleurs, pour toutes les valeurs de n pour lesquelles $(r_n, r_{n+1}) \neq (0,0)$, on a $\mathscr{D}(r_n, r_{n+1}) = \mathscr{D}(a,b)$. En particulier, pour la dernière valeur non-nulle r_n, on a $\mathscr{D}(r_n, 0) = \mathscr{D}(a,b)$.

L'algorithme d'Euclide n'est rien d'autre que le calcul des termes successifs de la suite (r_n) : en numérotant les tours de boucle (à partir de 0) dans l'algorithme précédent, on peut d'ailleurs noter qu'au $n$ème tour de boucle, R_0 contient la valeur de r_n, et R_1 celle de r_{n+1}. □

Remarque 4.1.4.
D'après la remarque 4.1.1, il existe donc un unique d unitaire tel que $\mathscr{D}(a,b) = \mathscr{D}(d)$.

Définition 4.1.5.
Soit a et b deux polynômes avec $(a,b) \neq (0,0)$, alors on appelle plus grands diviseurs communs de a et b (pgcd de a et b) **les** polynômes d vérifiant $\mathscr{D}(d) = \mathscr{D}(a,b)$. L'unique polynôme unitaire parmi ceux-ci est appelé **le** pgcd de a et b et noté $\mathrm{PGCD}(a,b)$ ou $a \wedge b$.

On convient que $\mathrm{PGCD}(0,0) = 0$.

Remarque 4.1.6.
1. L'existence des pgcd assurée par le théorème 4.1.3. D'après la remarque 4.1.1, il y en a donc un nombre infini.
2. L'existence et l'unicité du pgcd unitaire est assurée par la remarque 4.1.4.
3. Les pgcd de a et b sont les polynômes de degré maximum de $\mathscr{D}(a,b)$.
4. Si a et b sont deux polynômes de $\mathbb{R}[X]$, nous avons déjà vu que leurs divisoions euclidiennes dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$ sont les mêmes. Le lemme d'Euclide assure donc que le PGCD de a et b dans $\mathbb{C}[X]$ est le même que leur PGCD dans $\mathbb{R}[X]$. L'unicité du PGCD permet également de s'en assurer.
5. La relation de divisibilité $|$ n'est pas une relation d'ordre sur $\mathbb{K}[X]$, mais induit une relation d'ordre sur l'ensemble des polynômes unitaires. Le pgcd de deux polynômes unitaire a et b est alors le maximum des polynômes unitaires de $\mathscr{D}(a,b)$ pour $|$ et est donc la borne inférieure de a et b pour $|$.

On peut donner la caractérisation suivante :

Proposition 4.1.7.
Soient $(a,b,d) \in \mathbb{K}[X]^3$. d est un pgcd de a et b si et seulement si $d|a$ et $d|b$ et pour tout $n \in \mathbb{K}[X]$ vérifiant $n|a$ et $n|b$, on a $n|d$.

Démonstration.
Remarquons successivement :

1. $d|a$ et $d|b \Leftrightarrow d \in \mathscr{D}(a,b) \Leftrightarrow \mathscr{D}(d) \subset \mathscr{D}(a,b)$. La dernière équivalence peut se démontrer comme suit : le sens direct provient de la transitivité de la relation de divisibilité (si d est un diviseur de a, tout diviseur de d est un diviseur de a ; idem avec b) ; le sens indirect vient du fait que $\mathscr{D}(d)$ contient d.
2. $\left[\forall n \in \mathbb{K}[X], (n|a \text{ et } n|b) \Rightarrow n|d\right] \Leftrightarrow \mathscr{D}(d) \supset \mathscr{D}(a,b)$ découle directement de la définition de $\mathscr{D}(d)$ et $\mathscr{D}(a,b)$.
3. Par conséquent, on a $\left[d|a \text{ et } d|b \text{ et } \forall n \in \mathbb{K}[X], (n|a \text{ et } n|b) \Rightarrow n|d\right]$ si et seulement si $\mathscr{D}(d) = \mathscr{D}(a,b)$, si et seulement si d est un pgcd de a et b.

□

On a également :

Proposition 4.1.8.
Soient $(a,b,c) \in \mathbb{K}[X]^3$. Alors $(ac) \wedge (bc) = \frac{1}{\lambda} c(a \wedge b)$, où λ est le coefficient dominant de c.

Démonstration.
Soit $\delta = a \wedge b$ et $\Delta = (ac) \wedge (bc)$. Il suffit de montrer que $c\delta$ et Δ sont associés, et pour cela nous allons montrer que $c\delta|\Delta$ et $\Delta|c\delta$.

1. $\delta|a$ et $\delta|b$, donc $c\delta|ac$ et $c\delta|bc$. Par suite $c\delta|\Delta$.
2. $c|ac$ et $c|bc$, donc $c|\Delta$. Ainsi il existe $p \in \mathbb{R}[X]$ tel que $\Delta = pc$. Donc $pc = \Delta|ac$ et $pc = \Delta|bc$. Le polynôme c étant non nul, on en déduit $p|a$ et $p|b$, et donc $p|\delta$. Finalement $\Delta = pc|\delta c$.

On a donc le résultat. □

Théorème 4.1.9 (Théorème de Bézout, première partie)**.**
Soient $(a,b) \in \mathbb{K}[X]^2$. Il existe deux polynômes u et v tels que $au + bv = a \wedge b$. Un tel couple est appelé un couple de Bézout de a et b.

Démonstration.
L'idée de la démonstration est de regarder ce qui se passe dans l'algorithme d'Euclide. On constate qu'à chaque étape, les variables R_0 et R_1 sont des combinaisons linéaires (à coefficients polynomiaux) de a et b. À la fin de l'algorithme, le pgcd R_0 est donc une combinaison linéaire de a et b.

Pour calculer les coefficients de Bézout, on aura recours à l'algorithme d'Euclide étendu. Celui-ci est un simple ajout à l'algorithme vu précédemment ; on introduit en effet des variables U_i et V_i pour $i = 0, 1$ qu'on va modifier au fur et à mesure de l'exécution de façon à garantir $R_0 = U_0 a + V_0 b$ et $R_1 = U_1 a + V_1 b$. En python, en supposant [4] que l'existence d'un type des polynômes, et à condition que les notation `+` et `*` soient autorisées pour la somme et le produit de polynômes (et pour le produit d'un polynôme par un scalaire), cet algorithme s'écrit :

```
def euclide_etendu (a, b) :
    """Précondition (a,b) != (0,0)"""
    R0 = abs(a)
    if a < 0 :
        U0 = -1
    else :
        U0 = 1
    V0 = 0
    # Invariant : R0 == U0*a + V0*b
    R1 = abs(b)
    U1 = 0
    if b < 0 :
        V1 = -1
    else :
        V1 = 1
    # Invariant : R1 == U1*a + V1*b
    # Invariant : D(R0,R1) == D(a,b)
    while R1 > 0 :
        # Invariants :
        # D(R0,R1) == D(a,b)
        # R1>=0 et R2>=0
        # (R1,R2) != (0,0)
        # R0 == U0*a + V0*b
        # R1 == U1*a + V1*b
        # Variant : R1
        (q,R2) = diveuclide(R0,R1)
        # donc R2 = R0 - q*R1
        U2 = U0-q*U1
        V2 = V0-q*V1
        # R2 = U2*a + V2*b
        R0, U0, V0 = R1, U1, V1
        R1, U1, V1 = R2, U2, V2
    # R1 == 0
    return (R0,U0,V0)
```

(attention cependant, l'algorithme ci-dessus ne retourne pas *le* pgcd mais *un* pgcd avec les coefficients de Bézout associés).

Là encore, une autre façon de considérer cet algorithme est de regarder les suites r, u et v, où r est la suite considérée précédemment, où u et v vérifient $r_i = u_i a + v_i b$ pour $i = 0, 1$ et pour n tel que r_{n+1} soit non nul, $u_{n+2} = u_n - a q_{n+1}$ et $v_{n+2} = v_n - q v_{n+1}$, où q est le

4. Il existe des bibliothèques pour cela (`numpy` par ex.) !

quotient de la division euclidienne de r_n par r_{n+1}. Là encore, il n'est pas difficile de montrer par récurrence double que tant que $(r_n, r_{n+1}) \neq (0,0)$, on a $r_n = u_n a + v_n b$. □

 Le couple des coefficients de Bézout n'est pas unique. Par exemple on a

$$\begin{array}{rrrr} 1\times & (2X^2+X) & -2X\times & X=X \\ (X+1)\times & (2X^2+X) & -(2X^2+3X)\times & X=X \end{array}$$

Exemple 4.1.10.
Calcul d'un couple de Bézout pour $P = 2X^5 - 3X^4 + 5X^3 - X^2 - X + 2$ et $Q = 2X^4 - 5X^3 + 9X^2 - 8X + 4$

4.2 Polynômes premiers entre eux

Définition 4.2.1.
Deux polynômes a et b sont dit premiers entre eux si et seulement si $(a,b) \neq (0,0)$ et $a \wedge b = 1$.

Remarque 4.2.2.
1. Le PGCD de deux polynômes réels étant le même dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$, alors deux polynômes réeles sont premiers dans $\mathbb{R}[X]$ si et seulement si ils le sont dans $\mathbb{C}[X]$.
2. a et b sont premiers entre eux si et seulement si leurs seuls diviseurs communs sont les éléments inversibles de $\mathbb{K}[X]$, en d'autres termes si et seulement si $\mathscr{D}(a,b) \subset \mathbb{K}^*$ (ce qui est équivalent à $\mathscr{D}(a,b) = \mathbb{K}^*$).
3. si a et b sont irréductibles, alors ils sont soit premiers entre eux, soit associés. En particulier, si a et b sont irréductibles et unitaires, alors ils sont soit premiers entre eux, soit égaux.

Théorème 4.2.3 (Théorème de Bézout, seconde partie)**.**
Soient $a, b \in \mathbb{K}[X]$. a et b sont premiers entre eux si et seulement s'il existe deux polynômes u et v tels que $au + bv = 1$.

Démonstration.
Le cas $(a,b) = (0,0)$ est trivial (dans ce cas, a et b ne sont pas premiers entre eux et il n'existe pas de couple de Bézout).

Considérons donc $(a,b) \in \mathbb{K}[X]^2 \setminus \{ (0,0) \}$.

Supposons a et b premiers entre eux. Alors, d'après le théorème de Bézout première partie, on a le résultat.

Réciproquement, supposons qu'il existe deux polynômes u et v vérifiant $au + bv = 1$. Soit alors $d \in \mathscr{D}(a,b)$. On a $d|a$ et $d|b$, donc $d|(au+bv)$, donc $d|1$, donc $d \in \mathbb{K}^*$. Donc $\mathscr{D}(a,b) \subset \mathbb{K}^*$. □

 $au+bv = 1$ implique $a \wedge b = 1$, mais $au+bv = d$ n'implique pas $a \wedge b = d$, mais simplement $(a \wedge b)|d$.

Corollaire 4.2.4.
Soit $a, b \in \mathbb{K}[X] \setminus \{ (0,0) \}$. Alors en posant $d = a \wedge b$, a et b s'écrivent respectivement sous la forme $a' \times d$ et $b' \times d$ où $(a', b') \in \mathbb{K}[X]^2$. On a alors $a' \wedge b' = 1$

Démonstration.
On utilise les deux versions du théorème de Bézout : On sait qu'il existe u et v vérifiant $d = au + bv$, d'où $1 = a'u + b'v$, d'où a' et b' sont premiers entre eux. □

Remarque 4.2.5.
Ce corollaire est très fréquemment utilisé.

Corollaire 4.2.6.
(i) Soient a premier avec k polynômes $b_1, b_2, \ldots, b_k$. Alors a est premier avec $b_1.b_2.\ldots.b_k$.

(ii) Si a et b sont premiers entre eux, alors pour tous $m, n \in \mathbb{N}^*$, a^m et b^n sont également premiers entre eux.

Démonstration. (i) On traite le cas $k = 2$, le cas général s'en déduit immédiatement par récurrence. Il existe a_i et b_i vérifiant $au_i + b_i v_i = 1$ pour $i = 1, 2$. En multipliant ces deux relations, il vient successivement

$$\begin{aligned} 1 &= (au_1 + b_1 v_1)(au_2 + b_2 v_2) \\ 1 &= a^2 u_1 u_2 + a u_1 b_2 v_2 + b_1 v_1 a u_2 + b_1 v_1 b_2 v_2 \\ 1 &= a(au_1 u_2 + u_1 b_2 v_2 + b_1 v_1 u_2) + b_1 b_2 (v_1 v_2) \end{aligned}$$

D'où le résultat.

(ii) On applique (i) à a et $b.b.b.\ldots.b$, puis (i) à b^n et $a.a.a.\ldots.a$. Plus proprement, la résultat se démontre par récurrence.

□

Théorème 4.2.7 (Théorème de Gauss)**.**
Soient $(a, b, c) \in \mathbb{K}[X]^3$. On suppose $a|bc$ et $a \wedge b = 1$. Alors $a|c$.

Démonstration.
On a $a \wedge b = 1$ donc 1 s'écrit sous la forme $au + bv$ avec $(u, v) \in \mathbb{K}[X]^2$. Donc $c = c \times 1 = a(cu) + (bc)v$. Donc c est combinaison linéaire à coefficients dans $\mathbb{K}[X]$ de a et bc. Or bc est un multiple de a donc c est un multiple de a. □

Théorème 4.2.8 (Unicité de la décomposition en facteurs irréductibles)**.**
Tout polynôme non nul se décompose de façon unique comme produit d'un scalaire par des irréductibles unitaires, à l'ordre près des facteurs.

Démonstration.
On a déjà vu l'existence. Il reste donc à montrer l'unicité. Par l'absurde, supposons qu'il existe un polynôme admettant deux décompositions. Alors il existe un polynôme P de degré minimal admettant deux décompositions distinctes $\lambda \prod_{k=1}^{a} A_k$ et $\mu \prod_{k=1}^{b} B_k$, où $(a, b) \in \mathbb{N}^2$, $(\lambda, \mu) \in \mathbb{K}^2$ et les A_k et les B_k sont irréductibles pour k appartenant respectivement à $[\![1, a]\!]$ et $[\![1, b]\!]$.

Alors λ et μ sont le coefficient dominant de P, donc sont égaux.

Donc $\prod_{k=1}^{a} A_k = \prod_{k=1}^{b} B_k$.

On a $a \neq 0$. En effet, sinon on aurait $b = 0$ et on aurait dans les deux cas à un produit vide, il aurait donc unicité.

De même $b \neq 0$.

Remarquons que pour tout $k \in [\![1, b]\!]$, A_a est premier avec B_k. En effet, sinon il existerait $k_0 \in [\![1, b]\!]$ tel que A_a et B_{k_0} ne soient pas premiers entre eux. Or ils sont irréductibles, donc ils sont égaux. Donc on a

$$\prod_{k=1}^{a-1} A_k = \prod_{\substack{k \in [\![1,b]\!] \\ k \neq k_0}} B_k$$

Il existe donc un polynôme de degré strictement plus petit que $\deg P$, admettant deux décompositions distinctes, ce qui est absurde.

Donc A_a est donc premier avec $\prod_{k=1}^{b} B_k$, donc avec P. Or A_a divise P et n'est pas un polynôme constant.

C'est donc absurde. □

Remarque 4.2.9.
Comme pour les entiers, nous pouvons donner les résultats suivants :

— Deux polynômes sont premiers entre eux si et seulement s'ils n'ont aucunn facteur irréductible en commun ;

— la notion de *valuation* d'un polynôme irréductible dans un polynôme peut se définir, et permet de calculer le PGCD de deux polynômes A et B, en considérant le minimum des valuations d'un même facteur irréductible dans A et B. En anticipant sur les paragraphes qui suivent, la valuation est également utilisée pour le PPCM de deux polynômes, mais aussi les PGCD et PPCM d'une famille de polynômes.

4.3 PGCD de n polynômes.

Comme dans le cas de l'arithmétique sur les entiers, on introduit la notion de PGCD de plusieurs polynômes et de polynômes premiers entre eux dans leur ensemble.

Définition 4.3.1.
Soit $(A_1, \ldots, A_n) \in \mathbb{K}[X]^n$, on note $\mathscr{D}(A_1, \ldots, A_n) = \bigcap_{i=1}^{n} \mathscr{D}(A_i)$ l'ensemble des diviseurs communs à tous ces polynômes.

Proposition 4.3.2.
Soit $(A_1, \ldots, A_n) \in \mathbb{K}[X]^n$, il existe un polynôme D unique à association près tel que $\mathscr{D}(A_1, \ldots, A_n) = \mathscr{D}(D)$.

Démonstration.
L'unicité à association près est évidente. On montre par récurrence que $\forall n \in \mathbb{N}^*, \mathscr{H}_n : \forall (A_1, \ldots, A_n) \in \mathbb{K}[X]^n, \exists D \in \mathbb{K}[X], \mathscr{D}(A_1, \ldots, A_n) = \mathscr{D}(D)$.

Initialisation : OK.

Hérédité : Soit $n \in \mathbb{N}^*$, supposons $\mathscr{H}_n$ et montrons $\mathscr{H}_{n+1}$. Soit $(A_1, \ldots, A_{n+1}) \in \mathbb{K}[X]^{n+1}$. D'après $\mathscr{H}_n$, il existe D_1 tel que $\mathscr{D}(A_1, \ldots, A_n) = \mathscr{D}(D_1)$. On a

alors

$$\begin{aligned}\mathscr{D}(A_1,\dots,A_{n+1}) &= \bigcap_{i=1}^{n+1}\mathscr{D}(A_i)\\ &= \mathscr{D}(A_1,\dots,A_n)\cap\mathscr{D}(A_{n+1})\\ &= \mathscr{D}(D_1)\cap\mathscr{D}(A_{n+1})\\ &= \mathscr{D}(D_1\wedge A_{n+1}),\end{aligned}$$

d'où $\mathscr{H}_{n+1}$.

□

Remarque 4.3.3.
On a toujours $\mathscr{D}(A_1,\dots,A_n,0)=\mathscr{D}(A_1,\dots,A_n)$.

Définition 4.3.4.
Soit $(A_1,\dots,A_n)\in\mathbb{K}[X]^n$, non tous nuls. On note alors $A_1\wedge\cdots\wedge A_n=\mathrm{PGCD}(A_1,\dots,A_n)$ l'unique polynôme unitaire D vérifiant $\mathscr{D}(A_1,\dots,A_n)=\mathscr{D}(D)$ (un polynôme non unitaire vérifiant ceci est *un* PGCD).

On convient que $\mathrm{PGCD}(0,\dots,0)=0$.

Corollaire 4.3.5.
Soit $A_1,\dots,A_n\in\mathbb{K}[X]$, tels que les $A_1,\dots,A_{n-1}$ soient non tous nuls. On a alors $A_1\wedge\cdots\wedge A_n=(A_1\wedge\cdots\wedge A_{n-1})\wedge A_n$.

Corollaire 4.3.6.
Soit $(A_1,\dots,A_n)\in\mathbb{K}[X]^n$, non tous nuls, soit $D\in\mathbb{K}[X]$ unitaire. Alors $D=A_1\wedge\cdots\wedge A_n$ si et seulement si

1. $\forall i\in\{1,\dots,n\},\ D|A_i$;
2. $\forall P\in\mathbb{K}[X],\ (\forall i\in\{1,\dots,n\},\ P|A_i)\Rightarrow P|D$.

Définition 4.3.7.
Des polynômes $A_1,\dots,A_n$ sont dits premiers entre eux *dans leur ensemble* si $A_1\wedge\cdots\wedge A_n=1$, c'est-à-dire si $\mathscr{D}(A_1,\dots,A_n)=\mathbb{K}^*$.

Théorème 4.3.8 (Théorème de Bézout.)**.**
Soit $(A_1,\dots,A_n)\in\mathbb{K}[X]^n$, non tous nuls.

1. Il existe $(U_1,\dots,U_n)\in\mathbb{K}[X]^n$ tel que
$$\sum_{i=1}^{n}A_iU_i=A_1\wedge\cdots\wedge A_n.$$
2. S'il existe $(U_1,\dots,U_n)\in\mathbb{K}[X]^n$ tel que $\sum_{i=1}^{n}A_iU_i=1$, alors les $(A_i)_{i=1}^n$ sont premiers entre eux dans leur ensemble.

Démonstration.
Exactement comme pour les entiers, en remarquant que s'il existe D et $U_1,\dots,U_n$ vérifiant $\sum_{i=1}^{n}A_iU_i=D$, alors $A_1\wedge\cdots\wedge A_n|D$. □

Remarque 4.3.9.
Si une famille finie de polynômes contient deux polynômes premiers entre eux, alors les polynômes de cette famille sont premiers entre eux dans leur ensemble.

Exemple 4.3.10.
Comme dans le cas des entiers, des polynômes qui ne sont pas premiers entre eux deux à deux peuvent être premiers entre eux dans leur ensemble. Exhiber une telle famille.

4.4 PPCM

Pour tout polynôme a, b, l'ensemble des multiples de a est noté $a\mathbb{K}[X]$. L'ensemble des multiples communes à a et b est donc $a\mathbb{K}[X]\cap b\mathbb{K}[X]$.

Remarque 4.4.1. 1. Soit d et d' deux polynômes. $d\mathbb{K}[X]=d'\mathbb{K}[X]$ si et seulement d et d' sont associés.

2. En particulier, si on a $d\mathbb{K}[X]=d'\mathbb{K}[X]$ et que d et d' sont unitaires, alors $d=d'$ et pour tout polynôme d, il existe d' unitaire vérifiant $d'\mathbb{K}[X]=d\mathbb{K}[X]$.

Théorème 4.4.2.
Soit $(a,b) \in \mathbb{K}[X]^2$. Alors il existe $m \in \mathbb{K}[X]$ tel que $a\mathbb{K}[X] \cap b\mathbb{K}[X] = m\mathbb{K}[X]$.

Démonstration.
Dans le cas où a ou b est nul, on a évidemment $a\mathbb{K}[X] \cap b\mathbb{K}[X] = 0\mathbb{K}[X]$. On suppose donc par la suite que a et b sont tous deux non nuls.

Posons $d = a \wedge b$. Alors a (resp. b) est de la forme $a'd$ (resp. $b'd$) et a' et b' sont premiers entre eux.

Posons $m = a'b'd$. m est un multiple de a et de b, donc $m\mathbb{K}[X] \subset a\mathbb{K}[X]$ et $m\mathbb{K}[X] \subset b\mathbb{K}[X]$. Donc $m\mathbb{K}[X] \subset a\mathbb{K}[X] \cap b\mathbb{K}[X]$.

Réciproquement, soit $c \in a\mathbb{K}[X] \cap b\mathbb{K}[X]$. Alors c est multiple de d donc c s'écrit $c'd$, où $c' \in \mathbb{K}[X]$. De plus c est multiple de a donc s'écrit sous la forme ua, où $u \in \mathbb{K}[X]$. Donc $c'd = ua'd$, donc $c' = ua'$. De même, c' est de la forme vb', où $v \in \mathbb{K}[X]$. Donc $b'|ua'$. Or a' et b' sont premiers entre eux, donc $b'|u$. Donc $b'a'd|ua'd$, or $m = b'a'd$ et $c = ua'd$. donc $c \in m\mathbb{K}[X]$. □

Définition 4.4.3.
Soit a et b deux polynômes. Alors on appelle plus petits communs multiples de a et b (ppcm de a et b) **les** polynômes d tels que l'ensemble $a\mathbb{K}[X] \cap b\mathbb{K}[X]$ des multiples communs à a et b soit l'ensemble $d\mathbb{K}[X]$ des multiples de d.

On appelle **le** ppcm de a et b le seul de ces ppcm qui soit unitaire ou nul. Il est noté $\mathrm{PPCM}(a,b)$ ou $a \vee b$.

Remarque 4.4.4.
1. Cette définition est justifiée par la remarque 4.4.1 et le théorème 4.4.2.
2. $a \vee b = 0$ si et seulement si a ou b est nul.

Remarque 4.4.5.
Sur l'ensemble des polynômes unitaires, le ppcm de deux polynômes a et b est donc la borne supérieure de a et b pour l'ordre $|$.

On peut donner la caractérisation suivante :

Proposition 4.4.6.
Soient $a,b,m \in \mathbb{Z}$. m est un ppcm de a et b si et seulement si on a
1. $a|m$;
2. et $b|m$;
3. et pour tout $n \in \mathbb{K}[X]$, $a|n$ et $b|n \Rightarrow m|n$.

On a également :

Proposition 4.4.7.
Soient $a,b,c \in \mathbb{K}[X]$, avec $c \neq 0$.
(i) $(ac) \vee (bc)$ et $c(a \vee b)$ sont associés.
(ii) ab et $(a \wedge b).(a \vee b)$ sont associés.

Exemple 4.4.8.
Calculer $X^2 - 4X + 3 \vee X^2 + X - 2$.

5 Formule d'interpolation de Lagrange

Dans cette partie, on considère un entier n et $(x_0, y_0), \ldots, (x_n, y_n)$ des couples d'éléments de $\mathbb{K}$.

On aimerait savoir s'il existe un polynôme P vérifiant

$$\forall i \in [\![0,n]\!] \quad P(x_i) = y_i, \tag{XIV.4}$$

dit autrement, on cherche s'il existe une fonction polynomiale dont le graphe passe par tous les points (x_i, y_i) pour $i \in [\![0,n]\!]$.

Il est bien évident que s'il existe i et j distincts tels que $x_i = x_j$ et $y_i = y_j$, on peut supprimer le couple (x_j, y_j) de la liste des couples considérés sans changer le problème.

Il est évident également que s'il existe i et j distincts tels que $x_i = x_j$ et $y_i \neq y_j$, il n'existe pas de solution.

C'est pourquoi, par la suite, **on suppose que $x_0, \ldots, x_n$ sont deux à deux distincts**.

Définition 5.0.1.
On appelle *base de Lagrange associée aux points* $x_0, \ldots, x_n$ le $(n+1)$-uplet $(L_0, \ldots, L_n)$ vérifiant pour tout $i \in [\![0,n]\!]$:

$$L_i = \frac{1}{\alpha_i} \prod_{\substack{j \in [\![0,n]\!] \\ j \neq i}} (X - x_j)$$

où

$$\alpha_i = \prod_{\substack{j\in[\![0,n]\!]\\ j\neq i}} (x_i - x_j).$$

Proposition 5.0.2.
Pour tout $(i,j) \in [\![0,n]\!]^2$, on a $L_i(x_i) = 1$ et $L_i(x_j) = 0$ si $j \neq i$.

Autrement dit, dans tous les cas, on a

$$L_i(x_j) = \delta_{i,j}.$$

Corollaire 5.0.3.
Soit $(\lambda_0, \dots, \lambda_n) \in \mathbb{K}^{n+1}$. Alors, en posant

$$P = \sum_{i=0}^{n} \lambda_i L_i,$$

on a pour tout $i \in [\![0,n]\!]$:

$$P(x_i) = \lambda_i.$$

Théorème 5.0.4.
Il existe un unique polynôme P de degré au plus n vérifiant l'équation (XIV.4). Il s'agit du polynôme

$$\sum_{i=0}^{n} y_i L_i.$$

Démonstration.Unicité sous réserve d'existence Soit P et Q deux polynômes de degré au plus n vérifiant la propriété demandée. Alors P et Q coïncident en $n+1$ points distincts et sont de degré au plus n donc P et Q sont égaux.

Existence Le polynôme donné dans l'énoncé vérifie évidemment l'équation (XIV.4). Par ailleurs, il s'agit d'une combinaison linéaire de polynômes qui sont tous de degré n. Il est donc de degré au plus n.

□

Exercice 5.0.5.
Montrer que pour tout $P \in \mathbb{K}_n[X]$, il existe un unique $(\lambda_0, \dots, \lambda_n) \in \mathbb{K}^{n+1}$ tel que $P = \sum_{i=0}^{n} \lambda_i L_i$.

Corollaire 5.0.6.
L'ensemble des polynômes vérifiant l'équation (XIV.4) est

$$\{\, P \times D + P_0 \mid P \in \mathbb{K}[X] \,\}$$

où

$$D = \prod_{i=0}^{n} (X - x_i),$$
$$P_0 = \sum_{i=0}^{n} y_i L_i.$$

Démonstration.
Remarquons tout d'abord que pour tout $i \in [\![0,n]\!]$, on a $D(x_i) = 0$.

Analyse Soit Q un polynôme vérifiant l'équation (XIV.4). En effectuant la division euclidienne de Q par D, on peut écrire Q sous la forme $P \times D + R$ où $P \in \mathbb{K}[X]$ et $R \in \mathbb{K}[X]$ avec $\deg R < n+1$. On a donc $\deg R \leqslant n$. De plus, pour tout $i \in [\![0,n]\!]$, on a $R(x_i) = Q(x_i) - P(x_i)D(x_i) = y_i - P(x_i) \times 0 = y_i$. Donc R est nécessairement le polynôme P_0 et P s'écrit sous la forme $P \times D + P_0$.

Synthèse Réciproquement, soit P un polynôme. Posons $Q = P \times D + P_0$. Alors pour tout $i \in [\![0,n]\!]$, on a $Q(x_i) = P(x_i) \times 0 + P_0(x_i) = y_i$. Donc Q vérifie l'équation (XIV.4).

Conclusion L'ensemble des polynômes vérifiant l'équation (XIV.4) est

$$\{\, P \times D + P_0 \mid P \in \mathbb{K}[X] \,\}.$$

□

Remarque 5.0.7.
En exprimant l'équation (XIV.4) sous la forme

$$(P(x_0), \dots, P(x_n)) = (y_0, \dots, y_n),$$

cet ensemble de solutions est encore un ensemble de la forme solution particulière plus l'ensemble des solutions de l'équation homogène associée.

6 Annexe : construction de $\mathbb{K}[X]$

La construction de $\mathbb{K}[X]$ n'est pas exigible, cette partie est une version alternative aux parties 1.1 et 1.2.

Définition 6.0.1.
On appelle support d'une suite u à valeurs dans $\mathbb{K}$ l'ensemble des entiers n tels que $u_n \neq 0$. Si cet ensemble est fini, u est dite à support fini.

Remarque 6.0.2.
1. Une suite u est à support fini si et seulement si elle est nulle à partir d'un certain rang.
2. Toute suite à support fini converge donc vers 0 mais la réciproque est évidemment fausse [5].

On peut alors construire l'anneau des polynômes à coefficients dans $\mathbb{K}$ comme suit.

Définition 6.0.3.
On note $\mathbb{K}[X]$ l'ensemble des suites à support fini à valeurs dans $\mathbb{K}$.

Définition 6.0.4.
Soit $P = (P_n)_{n\in\mathbb{N}}$ un polynôme. Si P n'est pas la suite nulle, le *degré* de P est le plus grand rang d pour lequel $P_d \neq 0$. Si P est la suite nulle, on considère que c'est $-\infty$.

Dans tous les cas, on peut écrire :

$$\deg P = \sup\{d \in \mathbb{N},\ P_d \neq 0\}.$$

Définition 6.0.5.
L'addition sur $\mathbb{K}[X]$ est celle de $\mathbb{K}^{\mathbb{N}}$, on la notera $+$. $(\mathbb{K}[X], +)$ est alors un groupe abélien.

5. Par ailleurs, dans ce chapitre, le fait que les suites à support fini convergent n'est d'aucun intérêt.

Remarque 6.0.6.
$\mathbb{K}[X]$ hérite aussi de la multiplication scalaire de $\mathbb{K}^{\mathbb{N}}$. On dira plus tard que c'en est un *sous-espace vectoriel*.

Remarque 6.0.7.
Par l'injection $\mathbb{K} \to \mathbb{K}[X], x \mapsto (x, 0, \dots)$, on voit $\mathbb{K}$ comme étant inclus dans $\mathbb{K}[X]$. C'en est aussi un sous-groupe (et un sous-espace vectoriel). On identifiera par exemple le réel 1 au polynôme $(1, 0, \dots)$.

Démonstration.
On montre que c'est un sous-groupe de $(\mathbb{K}^{\mathbb{N}}, +)$. La suite nulle est bien entendu à support fini. Il suffit donc de montrer que la différence de deux polynômes est un polynôme. Soit P et Q deux polynômes de degrés p et q respectivement. Si $n \geqslant \max(p, q)$, alors $P_n - Q_n = 0$ donc $P - Q$ est un polynôme. □

Définition 6.0.8.
Soit $P = (P_n)$ et $Q = (Q_n)$ deux polynômes, on définit le polynôme $P \times Q$ par :

$$PQ = \left(\sum_{k=0}^{n} P_k Q_{n-k}\right)_{n\in\mathbb{N}}.$$

Proposition 6.0.9.
Si P et Q sont deux polynômes, PQ est un polynôme de degré $\deg P + \deg Q$.

Démonstration.
Si P ou Q sont nuls, il est évident que $PQ = 0$. Sinon, notons p et q les degrés respectifs de P et de Q. Soit $n > p + q$, soit $k \in [\![0, n]\!]$. Si $k > p$, alors $P_k = 0$ et si $k \leqslant p$, $n - k \geqslant n - p > q$, donc $Q_{n-k} = 0$. Ainsi, si $n > p + q$, $\sum_{k=0}^{n} P_k Q_{n-k} = 0$ et PQ est donc bien un polynôme, de degré au plus $p + q$. Il suffit ensuite de voir que $(PQ)_{p+q} = P_p Q_q \neq 0$ pour obtenir le degré de PQ. □

Théorème 6.0.10.
$(\mathbb{K}[X], +, \times)$ est un anneau.

Remarque 6.0.11.
La structure multiplicative de $\mathbb{K}[X]$ est différente de celle de $\mathbb{K}^{\mathbb{N}}$, $\mathbb{K}[X]$ n'est pas un sous-anneau (notion HP) de $\mathbb{K}^{\mathbb{N}}$.

Démonstration.
Le caractère de groupe abélien a déjà été vu, le reste des propriétés se montre de manière élémentaire, mais fastidieuse. L'écriture canonique introduite plus bas permet un peu d'alléger les notations. □

Définition 6.0.12.
On note X la suite toujours nulle, sauf pour le terme de rang 1 qui vaut 1 : $X = (0, 1, 0, 0, \ldots)$.

Proposition 6.0.13.
Par convention, $X^0 = 1$. De plus, si $n \geqslant 1$,

$$X^n = (\underbrace{0, \ldots, 0}_{n \text{ fois}}, \underbrace{1}_{(n+1)^{\text{e}} \text{ position}}, 0, \ldots).$$

Plus formellement, si $k \in \mathbb{N}$,

$$(X^n)_k = \begin{cases} 1 & \text{si } k = n+1 \text{ ;} \\ 0 & \text{sinon.} \end{cases}$$

Démonstration.
On le montre aisément par récurrence sur n, en remarquant que pour tout polynôme P le k^{e} coefficient de PX est le $(k-1)^{\text{e}}$ coefficient de P. □

On obtient donc la représentation usuelle des polynômes.

Corollaire 6.0.14.
Soit $P = (P_n)_{n\in\mathbb{N}}$ un polynôme de degré d. On a alors

$$P = \sum_{n=0}^{d} P_n X^n.$$

De plus, pour tout entier $d' \geqslant d$,

$$P = \sum_{n=0}^{d'} P_n X^n.$$

On s'autorise donc à écrire

$$P = \sum_{n=0}^{+\infty} P_n X^n$$

et, pour tout polynôme $Q = \sum_{n=0}^{d} P_n X^n$, on a bien

$$P + Q = \sum_{n=0}^{+\infty} (P_n + Q_n) X^n$$

ainsi que

$$P \times Q = \sum_{n=0}^{+\infty} \left(\sum_{k=0}^{n} P_k Q_{n-k} \right) X^n.$$

Enfin, on retrouve les mêmes notations que classiquement.

Définition 6.0.15.
Soit P un polynôme de la forme $\sum_{k=0}^{+\infty} a_k X^k$, non nul.

Le coefficient $a_{\deg P}$ est appelé *coefficient dominant* de P et on dit que $a_{\deg_P} X^{\deg P}$ est le *monôme dominant* de P.

Si le coefficient dominant de P vaut 1 on dit que P est *unitaire*.

Pour tout entier $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n.

Remarque 6.0.16.
1. $\mathbb{K}_n[X]$ **n'est pas** l'ensemble des polynômes de degré **égal** à n.
2. $\mathbb{K} = \mathbb{K}_0[X] \subset \mathbb{K}_1[X] \subset \mathbb{K}_2[X] \subset \cdots \subset \mathbb{K}[X]$.
3. $\mathbb{K}_n[X]$ est un sous-groupe de $(\mathbb{K}[X], +)$.
4. Soit P un polynôme de degré d et $n \in \mathbb{N}$ vérifiant $n \geqslant d$ alors P peut s'écrire sous la forme $\sum_{k=0}^{n} a_k X^k$.

7 Annexe : fonctions polynomiales à valeurs dans un anneau

Dans cette section, on considère un entier naturel n fixé et on pose $A = \mathbb{K}$ ou $A = \mathscr{M}_n(\mathbb{K})$. Dans tous les cas, A, muni de l'addition et de la multiplication usuelle est un anneau. Notons 0_A et 1_A les neutres respectifs pour l'addition et la multiplication dans A. Il s'agit de 0 et 1 si $A = \mathbb{K}$ et de $0_{M_n(\mathbb{K})}$ et I_n si $A = \mathscr{M}_n(\mathbb{K})$.

Dans les deux cas, on dispose d'une loi de composition externe, que nous noterons $\cdot : \mathbb{K} \times A \to A$. C'est la multiplication usuelle dans $\mathbb{K}$ si $A = \mathbb{K}$ et la multiplication d'une matrice par un scalaire si $A = \mathscr{M}_n(\mathbb{K})$.

Dans les deux cas, on a d'une part les propriétés suivantes [6] :

1. La loi $\cdot$ est distributive à gauche par rapport à l'addition dans A et à droite par rapport à l'addition dans $\mathbb{K}$.
2. Elle vérifie la propriété d'associativité mixte par rapport à la multiplication dans $\mathbb{K}$.
3. l'élément neutre de $\mathbb{K}$ est neutre à gauche pour $\cdot$.

Autrement dit, pour tout $(\lambda, \mu) \in \mathbb{K}^2$ et tout $(x, y) \in A^2$:

1. $\lambda \cdot (x +_A y) = \lambda \cdot x +_A \lambda \cdot y$ et $(\lambda +_{\mathbb{K}} \mu) \cdot x = \lambda \cdot x +_A \mu \cdot x$.
2. $(\lambda \times_{\mathbb{K}} \mu) \cdot x = \lambda \cdot (\mu \cdot x)$.
3. $1 \cdot x = x$.

Dans les deux cas, on a de plus la propriété additionnelle [7] que pour tout (λ, μ) et tout (x, y), on a :

$$(\lambda \cdot x) \times_A (\mu \cdot y) = (\lambda \times_{\mathbb{K}} \mu) \cdot (x \times_A y)$$

Si on met l'accent sur ces seules propriétés, c'est parce qu'elles sont suffisantes pour montrer tout ce dont nous aurons besoin dans cette partie, sans plus avoir besoin de distinguer le cas $A = \mathbb{K}$ du cas $A = \mathscr{M}_n(\mathbb{K})$. Par exemple, le fait que pour élément x de A on a $0 \cdot x$ peut se montrer en remarquant qu'on a $0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x$.

Définition 7.0.1.
Soit $P = \sum_{k=0}^{+\infty} a_k X^k$ un polynôme et x un élément de $\mathbb{K}$.

On appelle *évaluation du polynôme P en x* et on note $\widetilde{P}(x)$ l'élément de A défini par

$$\widetilde{P}(x) = \sum_{k=0}^{+\infty} a_k \cdot x^k$$

Exemple 7.0.2.
On pose $P = X^2 + 2X + 3$

1. Que vaut l'évaluation de P en -2 ?
2. Que vaut l'évaluation de P en $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$?

Proposition 7.0.3.
Soit $x \in A$ fixé. Alors l'application d'évaluation en x, $\mathsf{eval}_x : \begin{array}{ccc} \mathbb{K}[X] & \to & A \\ P & \mapsto & \widetilde{P}(x) \end{array}$ est un morphisme d'anneau ; autrement dit pour tout $(P, Q) \in \mathbb{K}[X]^2$, on a

1. $\widetilde{P+Q}(x) = \widetilde{P}(x) + \widetilde{Q}(x)$;
2. $\widetilde{P \times Q}(x) = \widetilde{P}(x) \times \widetilde{Q}(x)$;
3. $\widetilde{1_{\mathbb{K}[X]}}(x) = 1_A$.

De plus, on a

$$\widetilde{P \circ Q}(x) = P(Q(x))$$

La suite du cours considère uniquement le cas $A = \mathbb{K}$, le cas $A = \mathscr{M}_n(\mathbb{K})$ fera l'objet d'une étude plus approfondie en spé.

6. On dit que $(A, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.
7. Un anneau $(A, +, \times)$ tel que $(A, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel et qui vérifie cette propriété est appelé une $\mathbb{K}$-algèbre.

Chapitre XV

Dérivabilité

Sauf mention du contraire, I et J sont deux intervalles de $\mathbb{R}$ et $f : I \to \mathbb{R}$, et $a \in I$.

1 Définitions et premières propriétés

1.1 Taux d'accroissement

Définition 1.1.1.
Soit $x, y \in I$ avec $x \neq y$, on note $\tau_f(x,y)$ le *taux d'accroissement* de f entre x et y, défini comme le réel $\dfrac{f(y)-f(x)}{y-x}$. Pour x fixé, on notera

$$\begin{array}{rccc} \tau_{f,x} : & I \setminus \{x\} & \to & \mathbb{R} \\ & t & \mapsto & \tau_f(x,t) \end{array} .$$

Remarque 1.1.2.
On a toujours $\tau_f(x,y) = \tau_f(y,x)$.

Remarque 1.1.3.
$\tau_f(x,y)$ est la pente de la corde de la courbe f reliant les points d'abscisses x et y.

1.2 Définitions

Définition 1.2.1.
Soit $a \in I$. On dit que f est dérivable en a si $\tau_{f,a}$ admet une limite finie en a. On appelle alors *dérivée de f en a* ou *nombre dérivé de f en a* cette limite, que l'on note $f'(a)$.

Remarque 1.2.2.
$\tau_{f,a}$ admet une limite finie en a si et seulement si $\dfrac{f(a+h)-f(a)}{h}$ admet une limite finie quand h tend vers 0 et ces deux limites sont alors égales.

Exemple 1.2.3.
1. Si f est constante, $f'(a) = 0$ pour tout $a \in I$.
2. Dérivée de $x \mapsto x^{n+1}$ en a, pour n entier naturel : pour tout $x \in \mathbb{R}$, $x^{n+1} - a^{n+1} = (x-a)\sum_{k=0}^{n} x^k a^{n-k}$, donc $\dfrac{x^{n+1}-a^{n+1}}{x-a} = \sum_{k=0}^{n} x^k a^{n-k}$. Il suffit alors de passer à la limite.

Proposition 1.2.4.
Soit ℓ un réel. Les propositions suivantes sont toutes équivalentes.

(i) f est dérivable en a et $f'(a) = \ell$;

(ii) $\tau_{f,a}$ admet pour limite ℓ en a ;

(iii) on peut prolonger $\tau_{f,a}$ par continuité en a et son prolongement est

$$\begin{array}{rccc} \hat{\tau}_{f,a} : & I & \to & \mathbb{R} \\ & x & \mapsto & \begin{cases} \tau_{f,a}(x) & \text{si } x \neq a \\ \ell & \text{si } x = a \end{cases} \end{array}$$

(iv) il existe une application $\varphi_{f,a} : I \to \mathbb{R}$ continue en a, vérifiant $\varphi_{f,a}(a) = \ell$ et

$$\forall x \in I \qquad f(x) = f(a) + (x-a)\varphi_{f,a}(x)$$

(v) il existe une fonction $\varepsilon : I \to \mathbb{R}$, de limite nulle en a, telle que pour tout $x \in I$,

$$f(x) = f(a) + (x-a)\cdot\ell + (x-a)\varepsilon(x).$$

Remarque 1.2.5.
On traduira plus tard le point (**? ?**) comme suit : « f admet, au voisinage de a, le développement limité $f(x) = f(a) + (x-a)\cdot\ell + o(x-a)$ ».

Démonstration.
On a évidemment (i) $\iff$ (ii) d'après la définition de la dérivée. Montrons les autres équivalences par implications successives.

(ii)⇒(iii) C'est immédiat à partir de la définition de prolongement par continuité.

(iii)⇒(iv) Supposons (iii). Posons $\varphi_{f,a} = \hat{\tau}_{f,a}$. Alors, $\varphi_{f,a}$ est continue en a et on a bien $\varphi_{f,a}(a) = \ell$.

Enfin, soit $x \in I$. Si $x = a$, on a clairement $f(x) = f(a) + (x-a)\varphi_{f,a}(x)$. Si $x \neq a$, on a $\varphi_{f,a}(x) = \frac{f(x)-f(a)}{x-a}$, d'où $f(x) - f(a) = (x-a)\varphi_{f,a}(x)$.

On a donc

$$\forall x \in I \qquad f(x) = f(a) + (x-a)\varphi_{f,a}(x)$$

(iv)⇒(v) Supposons (iv). $\varphi_{f,a}$ est continue en a donc tend vers $\varphi_{f,a}(a) = \ell$ en a. Il suffit alors de poser $\varepsilon = \varphi_{f,a} - \ell$.

(v)⇒(ii) Supposons (v). Alors, pour $x \in I \setminus \{a\}$, on a successivement :

$$f(x) = f(a) + (x-a)\cdot\ell + (x-a)\varepsilon(x),$$
$$\frac{f(x)-f(a)}{x-a} = \ell + \varepsilon(x),$$
$$\tau_{f,a}(x) = \ell + \varepsilon(x).$$

Donc $\tau_{f,a}(x) \xrightarrow[x\to a]{} \ell$.

□

Remarque 1.2.6.

1. La caractérisation (iv) est parfois appelée caractérisation de Carathéodory.
2. Lorsque f est dérivable en a, la fonction $\varphi_{f,a}$ de la caractérisation de Carathéodory coïncide nécessairement avec le taux d'accroissement $\tau_{f,a}$ sur $I \setminus \{a\}$ et est continue en a, c'est donc le prolongement par continuité $\hat{\tau}_{f,a}$ du taux d'acroissement en a.
3. La caractérisation (v) est parfois appelée caractérisation de Hilbert.
4. Sous la forme donnée plus haut, la caractérisation de Carathéodory et celles de Hilbert sont utiles lorsqu'on veut *utiliser* une hypothèse disant que f est dérivable en a. Lorsqu'on veut les utiliser pour *montrer* que f est dérivable en a, on les utilisera plutôt sous les formes

$$\forall x \in I \qquad f(x) - f(a) = (x-a)\varphi_{f,a}(x)$$
$$f(x) - f(a) = (x-a)\cdot\ell + o(x-a)$$

Théorème 1.2.7.
Si f est dérivable en a, alors f est continue en a.

Démonstration.
C'est une conséquence directe de la caractérisation de Carathéodory (et de celle de Hilbert). □


La réciproque est fausse :

1. L'application valeur absolue n'est pas dérivable en 0, son taux d'accroissement en 0 ayant des limites à gauche et à droite distinctes en 0.
2. L'application racine carrée n'est pas dérivable en 0, son taux d'accroissement tendant vers $+\infty$ en 0.

Cela nous amène à la notion de dérivabilité à gauche et à droite :

Définition 1.2.8.
On dit que f est *dérivable à gauche en a* (resp. à droite en a) si la fonction $f|_{]-\infty,a]\cap I}$ (resp $f|_{[a,+\infty[\cap I}$) est dérivable en a, c'est-à-dire si le taux d'accroissement $\tau_{f,a}$ de f en a admet une limite finie à gauche (resp. une limite finie à droite).

Dans ce cas, cette limite est appelée dérivée à gauche (resp. à droite) de f en a et est notée $f'_g(a)$ (resp. $f'_d(a)$).

Exemple 1.2.9.
L'application valeur absolue est dérivable à gauche en 0 (de dérivée à gauche -1), ainsi qu'à droite (de dérivée à droite -1).

Remarque 1.2.10.
Si f est dérivable à droite (resp. à gauche) alors elle est continue à droite (resp. à gauche).

Définition 1.2.11 (Interprétation géométrique)**.**
Si f est dérivable (resp. dérivable à gauche, resp. dérivable à droite) en a, on appelle *tangente à f en a* (resp. *demi-tangente à f à gauche en a*, resp. *demi-tangente à f à droite en a*) la droite d'équation

$$y = f(a) + f'(a)(x-a)$$

(resp. la demi-droite d'équation $y = f(a) + f'_g(a)(x-a)$ et $x \leqslant a$, resp. la demi-droite d'équation $y = f(a) + f'_d(a)(x-a)$ et $x \geqslant a$).

Remarque 1.2.12.
Le membre droit de cette équation n'est autre que la partie linéaire du développement limité donné par la caractérisation de Hilbert.

Théorème 1.2.13.
f est dérivable en a si et seulement si f est dérivable à gauche et à droite en a ***et*** $f'_g(a) = f'_d(a)$.

Démonstration.
C'est une conséquence directe des résultat sur les limites de fonction : le taux d'accroissement $\tau_{f,a}$ de f en a, qui n'est pas défini en a admet une limite en a si et seulement s'il admet des limites à gauche et à droite en a et que ces limites sont égales. □

Exemple 1.2.14. 1. Valeur absolue en 0.

2. La fonction

$$f : \left\{ \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \left\{ \begin{array}{lll} \ln(1+2x) & \text{si} & x \geqslant 0 \\ 2\mathrm{e}^{\,x} - 2 & \text{si} & x < 0 \end{array} \right. \end{array} \right.$$

est-elle dérivable en 0 ?

On calcule les dérivées à gauche et à droite en revenant à la définition : à gauche, on constate $\dfrac{2(\mathrm{e}^{\,x}-1)}{x} \xrightarrow[x\to 0^-]{} 2$, à droite, $\dfrac{\ln(1+2x)}{x} \xrightarrow[x\to 0^+]{} 2$, donc f est dérivable en 0 et $f'(0) = 2$.

3. Les fonctions

$$f_n : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \begin{cases} x^n \sin\dfrac{1}{x} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases} \end{array}$$

pour $n \in \mathbb{N}$, sont-elles dérivables en 0 ?

Définition 1.2.15.
Si f est dérivable en tout point de I, on dit qu'elle est *dérivable sur I*. On appelle alors *fonction dérivée de f* et on note f', voire $\mathrm{D}f$ ou $\dfrac{\mathrm{d}f}{\mathrm{d}x}$, l'application $x \mapsto f'(x)$.

1.3 Opérations sur la dérivabilité

Théorème 1.3.1.
si $f, g : I \to \mathbb{R}$ sont dérivables en a, alors :

1. $f+g$ aussi, et $(f+g)'(a) = f'(a) + g'(a)$;
2. $f \times g$ aussi, et $(f\times g)'(a) = f'(a)\times g(a) + f(a)\times g'(a)$;
3. λf aussi et $(\lambda f)'(a) = \lambda f'(a)$;
4. si g ne s'annule pas au voisinage de a, alors $1/g$ est dérivable au voisinage de a et $\left(\frac{1}{g}\right)'(a) = -\frac{g'(a)}{g(a)^2}$
5. si g ne s'annule pas au voisinage de a, alors f/g est aussi dérivable en a et

$$(f/g)'(a) = \frac{f'(a)g(a) - g'(a)f(a)}{(g(a))^2}$$

Démonstration.
On donne une première démonstration en utilisant directement la définition de la dérivée. Supposons f et g dérivable en a.

1. Soit $x \in I \setminus \{a\}$, Alors $\dfrac{(f+g)(x)-(f+g)(a)}{x-a} = \dfrac{f(x)-f(a)}{x-a} + \dfrac{g(x)-g(a)}{x-a}$, d'où le résultat par passage à la limite en a.
2. Soit $x \in I \setminus \{a\}$, Alors

$$\frac{(f\times g)(x)-(f\times g)(a)}{x-a}$$
$$= f(x)\left(\frac{g(x)-g(a)}{x-a}\right) + g(a)\left(\frac{f(x)-f(a)}{x-a}\right)$$

d'où le résultat par passage à la limite en a.

3. Ce cas est une conséquence directe du précédent (en considérant le réel λ comme la fonction constante de valeur λ).
4. Supposons que g ne s'annule pas au voisinage de a, alors pour x au voisinage épointé de a, on a

$$\frac{1/g(x) - 1/g(a)}{x-a} = -\frac{1}{g(x)g(a)} \times \frac{g(x)-g(a)}{x-a}$$

Lorsque x tend vers a, le membre droit de cette égalité tend vers $-g'(a)/g(a)^2$, d'où le résultat.

5. Ce résultat se déduit cas du produit appliqué à f et $1/g$: En effet, supposons que g ne s'annule pas au voisinage de a. Alors $1/g$ est dérivable en a d'après le point précédent, donc $f \times 1/g$ est dérivable en a. De plus

$$(f\times 1/g)'(a) = f'(a)\times 1/g(a) + f(a)\times\left(-\frac{g'(a)}{g(a)^2}\right)$$
$$= \frac{f'(a)g(a) - g'(a)f(a)}{g(a)^2}$$

□

La démonstration ci-dessus a l'avantage de n'utiliser que la définition de la dérivée. Elle a deux inconvénients : d'une part, le cas du produit n'est pas évident à retrouver ; d'autre part cette méthode ne marchera pas dans le cas de la composition.

Voici une autre méthode qui n'a pas l'inconvénient précédent :

Démonstration.
Supposons f et g dérivables en a et notons $\varphi_{f,a}$ et $\varphi_{g,a}$ leurs taux d'accroissements en a respectifs, prolongés en a par continuité. Soit alors $x \in I$, on a

$$\begin{aligned} f(x) =& f(a) + (x-a)\varphi_{f,a}(x) \\ g(x) =& g(a) + (x-a)\varphi_{g,a}(x) \end{aligned}$$

1. On a donc

$$(f+g)(x) - (f+g)(a) = (x-a)(\varphi_{f,a} + \varphi_{g,a})(x)$$

Or $\varphi_{f,a} + \varphi_{g,a}$ a pour limite $f'(a) + g'(a)$ en a, donc c'est une application continue, donc d'après la caractérisation de Carathéodory, $f+g$ est dérivable en a, de dérivée $f'(a) + g'(a)$.

2. On a

$$\begin{aligned} &(f\times g)(x) - (f\times g)(a) \\ =&(f(a) + (x-a)\varphi_{f,a}(x)) \times (g(a) + (x-a)\varphi_{g,a}(x)) \\ &- f(a)g(a) \\ =&(x-a)\varphi_{f,a}(x)g(a) + f(a)(x-a)\varphi_{g,a}(x) \\ &+ (x-a)^2\varphi_{f,a}(x)\varphi_{g,a}(x) \\ =&(x-a)\Big(\varphi_{f,a}(x)g(a) + f(a)\varphi_{g,a}(x) \\ &+ (x-a)\varphi_{f,a}(x)\varphi_{g,a}(x)\Big) \end{aligned}$$

Or, lorsque x tend vers a, $\varphi_{f,a}(x)g(a) + f(a)\varphi_{g,a}(x) + (x-a)\varphi_{f,a}(x)\varphi_{g,a}(x)$ tend vers $f'(a)g(a) + f(a)g'(a)$. Donc $f\times g$ est dérivable en a, de dérivée $f'(a)g(a) + f(a)g'(a)$.

3. On a

$$(\lambda f)(x) - (\lambda f)(a) = (x-a)(\lambda\varphi_{f,a})(x)$$

4. On a $\dfrac{1}{g(x)} - \dfrac{1}{g(a)} = \dfrac{g(a)-g(x)}{g(a)g(x)} = -\dfrac{(x-a)\psi_{g,a}(x)}{g(a)g(x)}$ et $-\dfrac{\psi_{f,a}(x)}{g(a)g(x)} \xrightarrow[x\to a]{} -\dfrac{g'(a)}{g(a)^2}$

□

Remarque 1.3.2.
On peut également effectuer cette démonstration en utilisant la caractérisation de Hilbert plutôt que celle de Carathéodory.

Théorème 1.3.3.
Soit $g : J \to \mathbb{R}$, $f : I \to \mathbb{R}$ vérifiant $f(I) \subset J$ et $a \in I$.

1. Si f est dérivable en a et g dérivable en $f(a)$, alors $g\circ f$ est dérivable en a et
$$(g\circ f)'(a) = f'(a) \times g'(f(a))$$
2. Si g est dérivable sur J et f sur I, alors $g\circ f$ est dérivable sur J et
$$(g\circ f)' = f' \times (g'\circ f)$$

Le second point est évidemment une conséquence immédiate du premier.

Démonstration (Erronée)**.**
f est dérivable en a donc continue en a, donc $f(x) \xrightarrow[x\to a]{} f(a)$.
Par composition, on a donc
$$\frac{g(f(x)) - g(f(a))}{f(x) - f(a)} \xrightarrow[x\to a]{} g'(f(a))$$
De plus
$$\frac{f(x)-f(a)}{x-a} \xrightarrow[x\to a]{} f'(a)$$
Par produit, on obtient bien le résultat voulu. □

Remarque 1.3.4.
La démonstration précédente est erronée, car elle utilise une hypothèse implicite sur f qui n'est pas nécessairement vérifiée. Laquelle ?

Démonstration.
Supposons f (resp. g) étant dérivable en a (resp. en $f(a)$) ; on note alors φ (resp. ψ) son taux d'accroissement en a (resp. en $f(a)$) prolongé par continuité en a (resp. en $f(a)$). On a alors, pour tout $x \in I$
$$\begin{aligned}(g\circ f)(x) - (g\circ f)(a) &= (f(x)-f(a))\psi(f(x)) \\ &= (x-a)\varphi(x)\psi(f(x))\end{aligned}$$
f étant dérivable en a, elle est nécessairement continue en a ; on en déduit
$$\varphi(x)\psi(f(x)) \xrightarrow[x\to a]{} f'(a)\times g'(f(a))$$
D'où le résultat. □

Théorème 1.3.5.
Soit $f : I \to J$ bijective continue (de réciproque $f^{-1} : J \to I$). Soit $a \in I$, on note $f(a) = b$. Si f est dérivable en a (resp. sur I) et si f' ne s'annule pas en a (resp. sur I), alors f^{-1} est dérivable en b (resp. sur J) et $(f^{-1})'(b) = \dfrac{1}{f'(a)}$ (resp. $(f^{-1})' = \dfrac{1}{f' \circ f^{-1}}$).

Remarque 1.3.6.
1. Moyen mnémotechnique : $f \circ f^{-1} = \mathrm{Id}$, donc est dérivable de dérivée 1. Or on sait d'après le th. de composition, $(f \circ f^{-1})' = (f^{-1})' \times f' \circ f^{-1}$.
2. Ce résultat est faux sans l'hypothèse de continuité. Considérer par exemple

$$\begin{array}{rccl} f : & [0,2[& \to & [-1,1[\\ & x & \mapsto & x - 2\lfloor x \rfloor \end{array}$$

f est bijective et dérivable en 0 de dérivée 1 mais sa réciproque n'est même pas continue en $f(0)$. En effet il s'agit de

$$\begin{array}{rccl} f^{-1} : & [-1,1[& \to & [0,2[\\ & x & \mapsto & x - 2\lfloor x \rfloor \end{array}$$

On peut même construire des contre-exemples où a n'est pas une extrémité de l'intervalle.
3. Le graphe de f^{-1} étant le symétrique de celui de f par rapport à la droite d'équation $y = x$, la tangente à f^{-1} en un point $f(a)$, si elle existe, est la symétrique de la tangente à f en a par rapport à la droite d'équation $y = x$. Par conséquent, si $f'(a) = 0$, f^{-1} a une tangente verticale en $f(a)$, et sa dérivée en ce point n'existe pas.

Démonstration.
Supposons f dérivable en a de dérivée $f'(a)$ non nulle. Notons alors φ le prolongement par continuité en a de son taux d'accroissement en a.

On a, pour tout $x \in I$, $f(x) - f(a) = (x - a)\varphi(x)$.

Soit alors $y \in J$. Alors on a $f(f^{-1}(y)) - f(a) = (f^{-1}(y) - a)\varphi(f^{-1}(y))$, donc

$$y - b = \big(f^{-1}(y) - f^{-1}(b)\big)\varphi(f^{-1}(y))$$

Si $y \neq b$, on a $y - b \neq 0$, donc $\varphi(f^{-1}(y)) \neq 0$, et si $y = b$, on sait déjà que $\varphi(f^{-1}(y)) \neq 0$. Donc dans les deux cas, on a :

$$(f^{-1}(y) - f^{-1}(b)) = (y - b)\frac{1}{\varphi(f^{-1}(y))}$$

On sait $\frac{1}{\varphi(f^{-1}(b))} = \frac{1}{f'(a)}$, donc pour conclure, il suffit de montrer que $y \mapsto \frac{1}{\varphi(f^{-1}(y))}$ est continue en b.

Or f est une bijection continue de I sur J donc f^{-1} est également continue sur J donc en particulier en b et vaut a en b. Par ailleurs on sait déjà que φ est continue en a. On en déduit donc le résultat. □

Exemple 1.3.7.
On admet que exp et sin sont dérivables. Grâce aux résultats précédents, on peut montrer les résultats connus de dérivabilité de toutes les fonctions usuelles (ln, cos, tan, Arctan, Arcsin, Arccos, ch, sh, th, Argth, Argch, Argsh)

Exercice 1.3.8.
Se faire un formulaire reprenant tout ça sur un intervalle, ainsi notamment que les cas de $(f + g)'$, $(fg)'$, $(f^n)'$, $(f \circ g)'$, $(1/f)'$, $(f^{-1})'$, $(\ln \circ f)'$, $(\exp \circ f)'$.

1.4 Dérivées successives

Définition 1.4.1.
On définit les dérivées successives par récurrence. Rappel de notations : $\mathscr{D}(I, \mathbb{R})$, $\mathscr{D}^k(I, \mathbb{R})$, $\mathscr{C}^k(I, \mathbb{R})$, $\mathscr{C}^\infty(I, \mathbb{R}) = \bigcap_{k \in \mathbb{N}} \mathscr{C}^k(I, \mathbb{R})$, avec la remarque usuelle : $\mathscr{D}^{k+1} \subsetneq \mathscr{C}^k \subsetneq \mathscr{D}^k$.

Exemple 1.4.2.
$x \mapsto x^2 \sin 1/x$ est dérivable en 0 et sur $\mathbb{R}$, mais sa dérivée n'est pas continue en 0.

Exemple 1.4.3.
Soit $n \in \mathbb{Z}, k \in \mathbb{N}$. $\begin{array}{rccl} f_n : & \mathbb{R}_+^* & \to & \mathbb{R}_+^* \\ & x & \mapsto & x^n \end{array}$. Alors, si $n = 0$, $f_0 = 1 \in \mathscr{C}^\infty$, si $n > 0$, si $k \leqslant n$, $f_n^{(k)} = \dfrac{n!}{(n-k)!}x^{n-k}$ (par récurrence), si $k > n$, $f_n^{(k)} = 0$, si $n < 0$, $f_n^{(k)} = (-1)^k \dfrac{(k-1-n)!}{(-n-1)!}x^{n-k}$.

Théorème 1.4.4.
Soit $n \in \mathbb{N}$. Soient $f, g \in \mathscr{C}^n(I, \mathbb{R})$. Alors :

1. $(f+g) \in \mathscr{C}^n(I, \mathbb{R})$ et $(f+g)^{(n)} = f^{(n)} + g^{(n)}$.
2. $(fg) \in \mathscr{C}^n(I, \mathbb{R})$ et $(fg)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(k)}.g^{(n-k)}$ (formule de Leibniz).
3. Cas particulier : pour $\lambda \in \mathbb{R}$, $(\lambda f)^{(n)} = \lambda f^{(n)}$.
4. Si g ne s'annule pas, $(f/g) \in \mathscr{C}^n(I, \mathbb{R})$.

Démonstration. 1. Facile par récurrence, en notant pour f et g fixées et pour tout $n \in \mathbb{N}$, (H_n) l'assertion «si f et g appartiennent à $\mathscr{C}^n(I, \mathbb{R})$ alors $(f+g) \in \mathscr{C}^n(I, \mathbb{R})$ et $(f+g)^{(n)} = f^{(n)} + g^{(n)}$».

2. On fait encore une démonstration par récurrence, en notant (H_n) l'assertion «si f et g appartiennent à $\mathscr{C}^n(I, \mathbb{R})$ alors $(fg) \in \mathscr{C}^n(I, \mathbb{R})$ et $(fg)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(k)}.g^{(n-k)}$» :
   — (H_0) est évidemment vraie.
   — L'hérédité se démontre à l'aide de la formule 2 du théorème 1.2.1, et se conduit de la même manière que la démonstration de la formule du binôme de Newton.

4. Encore une récurrence, mais plus subtile car cette fois on ne fixe pas f et g. Pour $n \in \mathbb{N}$, on note (H_n) l'assertion «***pour toutes*** $f, g \in \mathscr{C}^n(I, \mathbb{R})$ telles que g ne s'annule pas, on a $f/g \in \mathscr{C}^n$».
   — De nouveau (H_0) se démontre aisément.
   — Soit $n \in \mathbb{N}$. Supposons (H_n) et montrons (H_{n+1}). Soit $f, g \in \mathscr{C}^{n+1}(I, \mathbb{R})$, g ne s'annulant pas. Alors on sait que f/g est dérivable et $(f/g)' = \dfrac{f'g - fg'}{g^2}$. Mais $f'g - fg'$ est de classe $\mathscr{C}^n$, ainsi que g^2, et g^2 ne s'annule pas. On peut donc appliquer l'hypothèse de récurrence (H_n) à $f'g - fg'$ et g^2 et en déduire que $(f/g)'$ est de classe $\mathscr{C}^n$, donc que f/g est de classe $\mathscr{C}^{n+1}$.

□

Théorème 1.4.5.
Soit $n \in \mathbb{N}^*$. Soient $f \in \mathscr{C}^n(I, \mathbb{R})$ et $g \in \mathscr{C}^n(J, I)$. Alors $(f \circ g) \in \mathscr{C}^n(J, \mathbb{R})$.

Démonstration.
(non exigible). La démonstration se fait là encore par récurrence, avec la même subtilité que dans la démonstration précédente. Pour $n \in \mathbb{N}$, on note (H_n) l'assertion «***pour toutes*** $f \in \mathscr{C}^n(I, \mathbb{R})$ et $g \in \mathscr{C}^n(J, I)$, on a $(f \circ g) \in \mathscr{C}^n(J, \mathbb{R})$».
— De nouveau (H_0) est triviale.
— Soit $n \in \mathbb{N}$. Supposons (H_n) et montrons (H_{n+1}). Soit $f \in \mathscr{C}^{n+1}(I, \mathbb{R})$ et $g \in \mathscr{C}^{n+1}(J, I)$. Alors on sait que $f \circ g$ est dérivable et que $(f \circ g)' = g'.f' \circ g$. Or f' est de classe $\mathscr{C}^n$, ainsi que g. En appliquant l'hypothèse de récurrence (H_n) à f' et g, on obtient que $f' \circ g$ est de classe $\mathscr{C}^n$. Or g' est aussi de classe $\mathscr{C}^n$, donc le produit $g'.f' \circ g$ est de classe $\mathscr{C}^n$. Ainsi $(f \circ g)'$ est de classe $\mathscr{C}^n$, donc $f \circ g$ est de classe $\mathscr{C}^{n+1}$.

□

Théorème 1.4.6.
Soit $n \in \mathbb{N}^*$. Soit $f \in \mathscr{C}^n(I, J)$. Si f est bijective et f' ne s'annule pas alors $f^{-1} \in \mathscr{C}^n(J, I)$.

Démonstration.
(non exigible). La démonstration se fait par récurrence de la même manière que les deux démonstrations précédentes.

□

2 Les grands théorèmes

2.1 Extremums locaux

Définition 2.1.1.
On dit que f a un *minimum (resp. maximum) local* en a s'il existe un voisinage V de a tel que pour tout $x \in V \cap I$, $f(x) \geqslant f(a)$ (resp. $f(x) \leqslant f(a)$). On dit que f a un *extremum local en a* si f a un minimum ou un maximum local en a.

Remarque 2.1.2. 1. La condition $\forall x \in V \cap I \quad f(a) \geqslant f(x)$ est équivalente à chacune des assertions suivantes :

(i) $f_{|V \cap I}$ admet un maximum global en a ;
(ii) f est majorée par $f(a)$ sur $V \cap I$;
(iii) $f(V \cap I)$ est majoré par $f(a)$;
(iv) $f(a) = \sup_{x \in V \cap I} f(x)$;
(v) $f(a) = \max_{x \in V \cap I} f(x)$.

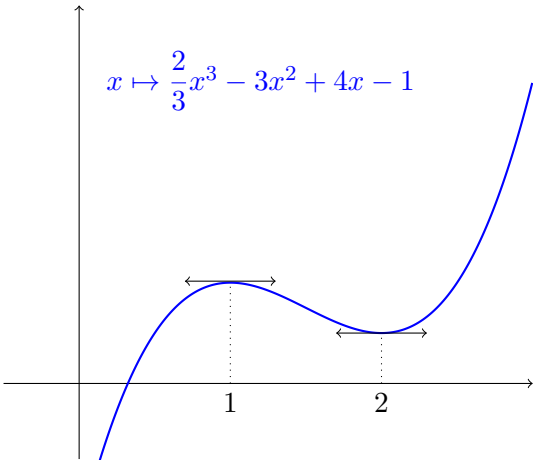


FIGURE XV.1 – Exemple de fonction possédant des extremums locaux, mais non globaux.

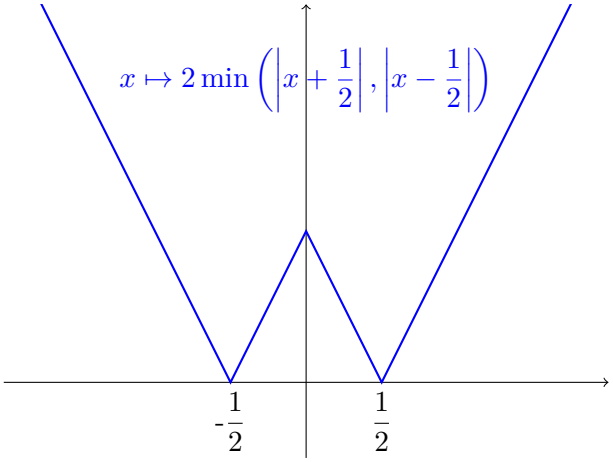


FIGURE XV.2 – Exemple de fonction possédant des minimums globaux non uniques.

2. Une fonction peut avoir un minimum en un point a sans qu'elle ne soit croissante sur un voisinage à droite ni décroissante sur un voisinage à gauche. Considérer par exemple l'application

$$\begin{array}{rccl} f: & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & \begin{cases} 0 & \text{si } x = 0 \\ x^2(\sin 1/x) + 1 & \text{sinon} \end{cases} \end{array}$$

Théorème 2.1.3.
Soit $a \in \overset{\circ}{I}$. Si f possède un extremum local en a et si f est dérivable en a, alors $f'(a) = 0$.

Remarque 2.1.4. 1. Il est essentiel que a appartiennent à l'intérieur de I. Si a est une extrémité de I, on peut considérer le contre-exemple $\mathrm{Id}_{[0,1]}$, qui possède un minimum global en 0 et un maximum global en 1 et est dérivable sur $[0,1]$ mais dont la dérivée ne s'annule ni en 0 ni en 1.

2. La réciproque est fausse. Ainsi $x \mapsto x^3$ a une dérivée nulle en 0 sans avoir d'extremum.

Démonstration.
Sans perte de généralité, on suppose que f admet un maximum local en a. Il existe donc un voisinage V_1 de a tel que f soit majorée par $f(a)$ sur $V_1 \cap I$.

a étant intérieur à I, il existe un voisinage V_2 de a inclus dans I.

On a alors $V_1 \cap V_2 \subset V_1 \cap I$, f est donc majorée par $f(a)$ sur $V_1 \cap V_2$.

De plus, $V_1 \cap V_2$ est un voisinage donc contient un segment $[a-\varepsilon, a+\varepsilon]$ où $\varepsilon > 0$.

On a alors, pour tout $x \in [a-\varepsilon, a+\varepsilon]$, $f(x) - f(a) \leqslant 0$.

Donc d'une part

$$\forall x \in [a-\varepsilon, a[\quad \frac{f(x)-f(a)}{x-a} \geqslant 0$$

donc par passage à la limite $f'(a) \geqslant 0$.

Et d'autre part,

$$\forall x \in]a, a+\varepsilon] \quad \frac{f(x)-f(a)}{x-a} \leqslant 0$$

donc par passage à la limite $f'(a) \leqslant 0$.

Donc $f'(a) = 0$. □

Définition 2.1.5.
Supposons f dérivable, un point $a \in I$ est un *point critique* de f si $f'(a) = 0$.

Remarque 2.1.6.
Le théorème 2.1.3 s'énonce donc ainsi : tous les extremums locaux d'une fonction dérivable à l'intérieur de son ensemble de définition sont des points critiques de cette fonction. Ou bien : une condition nécessaire pour qu'un point a, à l'intérieur de l'ensemble de définition d'une fonction f

dérivable, soit un extremum local de f est que a soit un point critique de f.

Remarque 2.1.7.
Cette condition nécessaire n'est pas suffisante, comme le montre le contre-exemple $x \mapsto x^3$ en 0.

L'étude des extremums (locaux ou globaux) d'une fonction dérivable commencera donc la plupart du temps par une étude systématique de ses points critiques.

2.2 Le théorème de Rolle

Théorème 2.2.1 (Théorème de Rolle)**.**
Soient $a, b \in I$ avec $a < b$ et $f \in \mathscr{C}^0([a,b],\mathbb{R}) \cap \mathscr{D}(]a,b[,\mathbb{R})$ vérifiant $f(a) = f(b)$, alors il existe $c \in]a,b[$ tel que $f'(c) = 0$.

Remarque 2.2.2.
Toutes les hypothèses sont importantes. On pourra considérer les applications suivantes qui sont toutes des contre-exemples correspondant à l'oubli d'une hypothèse :

$$\begin{array}{rccc} f_1 : & [0,1] & \to & \mathbb{R} \\ & x & \mapsto & x \\ f_2 : & [0,1] & \to & \mathbb{R} \\ & x & \mapsto & x - \lfloor x \rfloor \\ f_3 : & [-1,1] & \to & \mathbb{R} \\ & x & \mapsto & |x| \end{array}$$

Démonstration.
f est continue sur $[a,b]$, donc elle est bornée et atteint ses bornes. On note m son mininmum et M son maximum.

- Si $f(a) = f(b) \neq m$, alors $m < f(a)$ et $m < f(b)$, et donc m est atteint sur $]a,b[$, donc f' s'annule en ce point.
- Même raisonnement si $f(a) = f(b) \neq M$.
- Sinon, cela signifie que $f(a) = f(b) = m = M$, et donc f est nécessairement constante sur $]a,b[$. f' y est donc identiquement nulle.

□

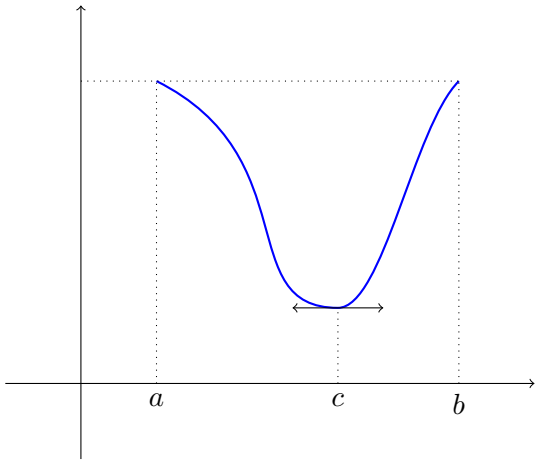


FIGURE XV.3 – Illustration du théorème de Rolle (existence d'une tangente horizontale, d'un point critique).

2.3 Égalité et inégalité des accroissements finis

Théorème 2.3.1 (Égalité des accroissements finis, ou TAF)**.**
Soient $(a,b) \in I^2$ avec $a < b$ et $f \in \mathscr{C}^0([a,b],\mathbb{R}) \cap \mathscr{D}(]a,b[,\mathbb{R})$. Alors il existe $c \in]a,b[$ tel que

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

Remarque 2.3.2.
1. Ce théorème est une généralisation du théorème de Rolle : les hypothèses sont les mêmes, à l'exception de l'hypothèse $f(a) = f(b)$, qui n'est ici pas nécessaire, et la conclusion est la même que celle du théorème de Rolle dans le cas où $f(a) = f(b)$.
2. Cependant, on va utiliser le théorème de Rolle pour démontrer le théorème des accroissements finis. Dans ces conditions affirmer que le théorème de Rolle n'est qu'un corollaire du TAF laisserait croire que l'on n'a pas bien saisi l'enchaînement des démonstrations.
3. Un autre énoncé de ce théorème est le suivant : Soient $(a,b) \in I^2$ avec $a \neq b$ et

f continue sur l'intervalle $[a,b]$ (ou $[b,a]$ si $b<a$) et dérivable sur l'intérieur de ce même intervalle. Alors il existe $\theta \in]0,1[$ tel que $f'(a+\theta(b-a)) = \dfrac{f(b)-f(a)}{b-a}$.

Démonstration.
Posons $p = \dfrac{f(b)-f(a)}{b-a}$ et

$$\begin{array}{rccc} \varphi : & [a,b] & \to & \mathbb{R} \\ & x & \mapsto & f(x)-px \end{array}$$

Alors $\varphi(b)-\varphi(a) = f(b)-f(a)-p(b-a) = 0$, donc $\varphi(a)=\varphi(b)$.

De plus, φ est continue sur $[a,b]$ et dérivable sur $]a,b[$. Donc d'après le théorème de Rolle, il existe $c \in]a,b[$ vérifiant $\varphi'(c)=0$. Or $\varphi'(c) = f'(c)-p$, donc $f'(c) = p = \dfrac{f(b)-f(a)}{b-a}$. □

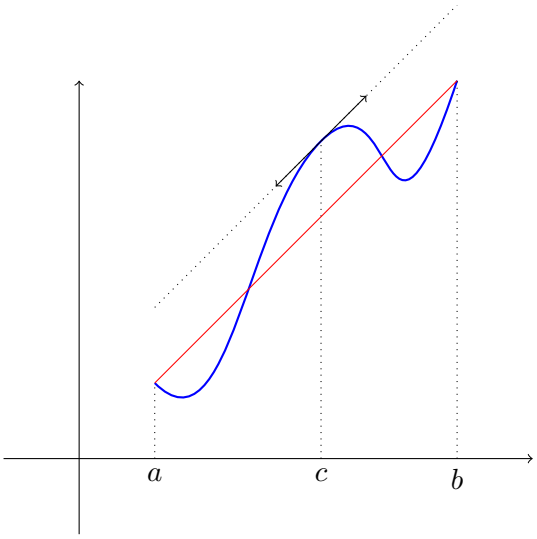


FIGURE XV.4 – Illustration du théorème des accroissements finis (existence d'une tangente de même pente que la corde).

Pour montrer le TAF, on se ramène à Rolle par une transformation géométrique $(x,y) \mapsto (x, y-px)$. Où p est la pente de la droite D. passant par les points $(a,f(a))$ et $(b,f(b))$. En effet, on peut remarquer que D est parallèle au graphe de $p\mathrm{Id}$, donc $f(a)-pa = f(b)-pb$. On peut alors appliquer le théorème de Rolle à l'application $f-p\mathrm{Id}$.

Théorème 2.3.3 (Inégalité des accroissements finis, ou IAF)**.**
Soient $(a,b) \in I^2$ avec $a<b$ et $f \in \mathscr{C}^0([a,b],\mathbb{R}) \cap \mathscr{D}(]a,b[,\mathbb{R})$.

1. Si f' est minorée par un réel m sur $]a,b[$, alors $m(b-a) \leqslant f(b)-f(a)$.
2. Si f' est majorée par un réel M sur $]a,b[$, alors $f(b)-f(a) \leqslant M(b-a)$.
3. Si $|f'|$ est majorée par $K>0$, alors $|f(b)-f(a)| \leqslant K|b-a|$.

Démonstration.
Par application du TAF à f, on sait qu'il existe $c \in]a,b[$ vérifiant $f'(c) = \dfrac{f(b)-f(a)}{b-a}$

1. Sous les hypothèses données, on a $m \leqslant f'(c) = \dfrac{f(b)-f(a)}{b-a}$, d'où le résultat.
2. De même, on a $\dfrac{f(b)-f(a)}{b-a} = f'(c) \leqslant M$, d'où le résultat.
3. De même, $\dfrac{|f(b)-f(a)|}{|b-a|} = |f'(c)| \leqslant K$, d'où le résultat.

   Notez que l'hypothèse $a<b$ n'est ici pas nécessaire : dans le cas où $a=b$ le résultat est évident ; dans le cas où $a>b$, il suffit d'échanger les rôles de a et b.

□

Définition 2.3.4.
Soit $K \in \mathbb{R}_+^*$. On dit que f est *K-lipschitzienne* si $\forall (x,y) \in I^2$, $|f(x)-f(y)| \leqslant K|x-y|$.

Remarque 2.3.5.
Si $x \neq y$, on a donc $\left|\dfrac{f(x)-f(y)}{x-y}\right| \leqslant K$, donc les pentes des cordes du graphe de f sont bornées par K.

Proposition 2.3.6.
Toute fonction lipschitzienne est continue.

Démonstration.
Direct en revenant aux définitions. □

Exemple 2.3.7.
La fonction $f : \begin{array}{ccc} [1,+\infty[& \to & \mathbb{R} \\ x & \mapsto & \dfrac{1}{x} \end{array}$ est 1-lipschitzienne. En effet, $|1/x - 1/y| = \left|\dfrac{x-y}{xy}\right| \leqslant 1 \times |x-y|$

Corollaire 2.3.8. 1. Soit $f \in \mathscr{D}(I,\mathbb{R})$. Si $|f'|$ est bornée par K sur I, alors f est K-lipschitzienne sur I

2. Si $f \in \mathscr{C}^1([a,b],\mathbb{R})$, alors f est lipschitzienne sur $[a,b]$.

Démonstration. 1. Immédiat avec le second point de l'IAF.

2. f' est continue sur un segment, donc bornée sur ce segment, et on peut donc appliquer le premier point. □

Exemple 2.3.9.
Utiliser l'IAF permet de montrer aisément que pour tout $x \in \mathbb{R}$, $|\sin x| \leqslant |x|$.

Exemple 2.3.10.
Soit $x > 0$. Montrer

$$\left(1+\frac{1}{x}\right)^x \leqslant \mathrm{e} \leqslant \left(1+\frac{1}{x}\right)^{x+1} \qquad \text{(XV.1)}$$

On a successivement les équivalences :

$$(XV.1) \iff x\ln\left(1+\frac{1}{x}\right) \leqslant 1 \leqslant (x+1)\ln\left(1+\frac{1}{x}\right)$$
$$(XV.1) \iff \frac{1}{x+1} \leqslant \ln\left(1+\frac{1}{x}\right) \leqslant \frac{1}{x}$$
$$(XV.1) \iff \frac{1}{x+1} \leqslant \ln(x+1) - \ln x \leqslant \frac{1}{x}$$

Or ce dernier encadrement s'obtient par application de l'IAF à la fonction ln sur $[x, x+1]$.

2.4 Dérivabilité et sens de variation

Résultats déjà connus, que l'on précise et démontre. On rappelle l'hypothèse primordiale : I est un intervalle de $\mathbb{R}$.

Théorème 2.4.1.
Soit $f \in \mathscr{D}(I,\mathbb{R})$.

1. f est croissante (resp décroissante) sur I ssi $f' \geqslant 0$ (resp $f' \leqslant 0$) sur I.
2. f est constante sur I ssi $f' = 0$ sur I.
3. f est strictement croissante (resp. strictement décroissante) sur I si et seulement si $f' \geqslant 0$ (resp. $f' \leqslant 0$) et l'ensemble $\{x \in I, f'(x) = 0\}$ ne contient aucun intervalle non trivial (non vide et non réduit à un point).

Démonstration.
On ne traite que les cas où f est croissante.

1. ($\Rightarrow$) On suppose f croissante sur I, alors son taux d'accroissement en tout point fixé $a \in I$ est positif. Par passage à la limite, on obtient $f'(a) \geqslant 0$.
   ($\Leftarrow$) On suppose $f' \geqslant 0$. Soit alors $(x,y) \in I^2$ avec $x < y$. Par application du TAF à f entre x et y, on sait qu'il existe $c \in]x,y[$ vérifiant $f'(c)(y-x) = f(y) - f(x)$. Or $f'(c) \geqslant 0$ et $y - x \geqslant 0$, donc $f(y) - f(x) \geqslant 0$.
   Donc f est croissante.
2. f est constante si et seulement si f est croissante et décroissante. On conclut par utilisation du point précédent.
3. ($\Rightarrow$) On suppose f strictement croissante. On sait déjà que $f' \geqslant 0$. On pose $\mathscr{E} = \{ x \in I \mid f'(x) = 0 \}$. Soit $(a,b) \in I^2$, $a \leqslant b$, tel que $[a,b] \subset \mathscr{E}$. Il suffit de montrer que $a = b$. On a $f'|_{[a,b]} = 0$ donc $f|_{[a,b]}$ est constante. En particulier $f(a) = f(b)$. Or f est strictement croissante, donc on ne peut pas avoir $a < b$, donc $a = b$.
   ($\Leftarrow$) Supposons que l'ensemble des points où f' s'annule ne contient aucun intervalle non trivial. Alors f est croissante. Par l'absurde, supposons que f ne soit pas strictement croissante. Alors il existe $(x,y) \in I^2$ avec $x < y$ et $f(x) = f(y)$. Alors puisque f est croissante, f est constante sur $[x,y]$, et donc $f'|_{[x,y]} = 0$. Mais alors par hypothèse, $x = y$, ce qui est absurde. Donc f est strictement croissante.

□

Remarque 2.4.2. 1. On a $f' > 0 \Rightarrow f$ strictement croissante, mais pas la réciproque : une fonction strictement croissante peut avoir une dérivée qui s'annule (mais pas n'importe comment), ex : $x \mapsto x^3$ (il s'agit souvent d'un point d'inflexion).

2. I doit être un intervalle. Le théorème est faux dans le cas où I est une réunion d'intervalles disjoints (considérer par exemple l'application $x \mapsto 1/x$, de $]-\infty, 0[\cup]0, +\infty[$ dans $\mathbb{R}$).
3. Si on suppose seulement $f'(a) > 0$, alors f n'est pas nécessairement strictement croissante au voisinage de a. Exemple :

$$f : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \begin{cases} 0 & \text{si } x = 0 \\ x^2 \sin 1/x + (x/2) & \text{sinon} \end{cases} \end{array}$$

En calculant la limite du taux d'accroissement de f en zéro, on obtient $f'(0) = 1/2$, mais pour $x \neq 0$, $f'(x) = 1/2 + 2x \sin 1/x - \cos 1/x$, et cette expression prend des valeurs négatives dans tout voisinage de 0.

4. En général, pour étudier les variations de f sur I avec ce théorème, il suffit que f soit dérivable sur l'intérieur de I et continue sur I tout entier. En effet, si une application f continue sur I est croissante (resp. strictement croissante, resp. décroissante, resp. strictement décroissante) sur $\mathring{I}$ alors elle l'est aussi sur I.

2.5 Limite de la dérivée

Théorème 2.5.1 (de la limite de la dérivée)**.**
Soit $a < b$, $f : I \to \mathbb{R}$ et $\ell \in \overline{\mathbb{R}}$. On suppose

1. f continue sur $[a, b]$
2. et f dérivable sur $]a, b]$
3. et $f'(x) \xrightarrow[x \to a^+]{} \ell$.

Alors $\dfrac{f(x) - f(a)}{x - a} \xrightarrow[x \to a^+]{} \ell$. En particulier

— dans le cas où $\ell = +\infty$ (resp. $\ell = -\infty$), f n'admet pas de dérivée à droite en a et son graphe admet une demi-tangente verticale en $(a, f(a)$ dirigée vers le haut (resp. vers le bas) ;

— dans le cas où ℓ est réel, on a

1. f est dérivable (à droite) en a
2. et $f'(a) = \ell = \lim_{x \to a^+} f'(x)$
3. et f' est continue (à droite) en a.

On a le même résultat à gauche en un point (inverser haut et bas dans le cas des limite infinies) et des deux côtés (limite globale) en un même point.

Remarque 2.5.2.
Ce théorème permet de conclure sur la dérivabilité ou non-dérivabilité de f en a dans le cas où la dérivée au voisinage épointé de a admet une limite (finie ou infinie) en a. En revanche il ne permet pas de dire quoi que ce soit dans le cas où la dérivée n'admet pas de limite.

Exemple 2.5.3. 1. On considère les fonctions f_n pour $n \in \mathbb{N}$ définies au point 3 de l'exemple 1.1.13. Pour $n \geqslant 1$, f_n est continue sur $\mathbb{R}$ et dérivable sur $\mathbb{R}^*$. De plus

$$\forall x \in \mathbb{R}^*,\ f_n'(x) = nx^{n-1} \sin\left(\frac{1}{x}\right) - x^{n-2} \cos\left(\frac{1}{x}\right)$$

Pour $n \geqslant 3$, $f_n'(x) \xrightarrow[\substack{x \to 0 \\ x \neq 0}]{} 0$. Donc, d'après le théorème ci-dessus, pour tout $n \geqslant 3$, f_n est dérivable en 0, de dérivée égale à 0 et on a même $f_n \in \mathscr{C}^1(\mathbb{R}, \mathbb{R})$.

Pour $n \in \{1, 2\}$, f_n' n'a pas de limite en 0. Le théorème précédent ne permet alors de conclure ni à la dérivabilité, ni à la non-dérivabilité de f_n en 0. Et pour cause : f_2 est bien dérivable en 0, de dérivée nulle tandis que f_1 ne l'est pas. En effet, le taux d'accroissement de f_n en 0 est l'application $x \mapsto x^{n-1} \sin\left(\frac{1}{x}\right)$, qui tend vers 0 en 0 si $n = 2$ et n'a pas de limite en 0 si $n = 1$.

2. Notons f l'application racine carrée de $\mathbb{R}_+$ dans $\mathbb{R}$. f est dérivable sur $\mathbb{R}_+^*$ et pour tout $x \in \mathbb{R}_+^*$, $f'(x) = \frac{1}{2\sqrt{x}}$.

Donc $f'(x) \xrightarrow[x \to 0^+]{} +\infty$, donc $\frac{f(x) - f(0)}{x - 0} \xrightarrow[x \to 0^+]{} +\infty$, donc f n'est pas dérivable en 0.

Remarquez cependant qu'il était ici tout aussi aisé de calculer directement le taux d'accrois-

sement de f en 0 et de vérifier qu'il ne convergeait pas.

Remarque 2.5.4.
On voit sur ces exemples qu'il est erroné de croire que la non-dérivabilité de f en a implique que f' n'a pas de limite en a (cas de la racine carrée).

Il est tout aussi erroné de croire que l'absence de limite pour f' en a implique que f n'est pas dérivable en a (cas de f_2).

Exercice 2.5.5.
Soient $a, b \in \mathbb{R}$, et $f : \begin{cases} \mathbb{R} \to \mathbb{R} \\ x \mapsto \begin{cases} \mathrm{e}^{\,x} & \text{si } x \leqslant 1 \\ x^2 + ax + b & \text{si } x > 1 \end{cases} \end{cases}$. Trouver les valeurs de a et b pour lesquelles f est de classe $\mathscr{C}^1$.

Solution : Remarquons que f est dérivable sur $\mathbb{R}\setminus\{1\}$ et que sa dérivée est continue sur $\mathbb{R}\setminus\{1\}$.

De plus f est continue à gauche et dérivable à gauche en 1, de dérivée à gauche $f'_g(1) = e$.

Analyse Supposons $f \in \mathscr{C}^1(\mathbb{R}, \mathbb{R})$. Alors f est continue, donc $f(x) \xrightarrow[x\to 1^+]{} f(1)$, donc $1 + a + b = \mathrm{e}$.

De plus f est dérivable. Sa dérivée à gauche en 1 est e. Pour $x > 1$, on a $f'(x) = 2x + a$, donc $f'(x) \xrightarrow[x\to 1^+]{} 2 + a$, donc f' est dérivable à droite en 1, de dérivée $2 + a$.

f étant dérivable en 1, on a $\mathrm{e} = f'_g(1) = f'_d(1) = 2 + a$.

Donc $a = \mathrm{e} - 2$ et $b = 1$.

Synthèse Supposons $a = \mathrm{e} - 2$ et $b = 1$. Alors, on montre aisément que f est continue à droite en 1, donc f est continue en 1.

f est dérivable en tout $x \in]1, +\infty[$, et $f'(x) = 2x + a$, donc $f'(x) \xrightarrow[x\to 1^+]{} 2 + a$, donc f est dérivable à droite en 0 et $f'_d(1) = 2 + a = \mathrm{e}$.

Donc f est dérivable en 1, de dérivée e. f est donc dérivable sur $\mathbb{R}$.

De plus f' est continue à droite et à gauche en 1, donc f' est continue en 1, donc sur $\mathbb{R}$.

Donc $f \in \mathscr{C}^1(\mathbb{R}, \mathbb{R})$.

Conclusion $f \in \mathscr{C}^1(\mathbb{R}, \mathbb{R})$ si et seulement si $a = \mathrm{e} - 2$ et $b = 1$.

Démonstration.
La difficulté est de montrer $\dfrac{f(x) - f(a)}{x - a} \xrightarrow[x\to a^+]{} \ell$, le reste s'en déduisant immédiatement.

Pour tout $x \in]a, b]$, f est dérivable sur $]a, x[$ et continue sur $[a, x]$ donc il existe $c \in]a, x[$ vérifiant $f'(c) = \dfrac{f(x) - f(a)}{x - a}$.

On peut ainsi définir une application $g :]a, b] \to]a, b]$, vérifiant pour tout $x \in]a, b]$, $g(x) \in]a, x[$ et $f'(g(x)) = \dfrac{f(x) - f(a)}{x - a}$.

Donc $g(x) \xrightarrow[x\to a^+]{} a$. Or $f' \xrightarrow[a^+]{} \ell$ donc $f'(g(x)) \xrightarrow[x\to a^+]{} \ell$.

Donc $\dfrac{f(x) - f(a)}{x - a} \xrightarrow[x\to a^+]{} \ell$. □

Le théorème de la limite de la dérivée peut se généraliser par récurrence. Nous donnons ici un énoncé de prolongement en un point intérieur à un intervalle, mais comme en 2.4.1 on pourrait l'énoncé pour un point qui serait la borne d'un intervalle :

Corollaire 2.5.6 (Théorème de classe $\mathscr{C}^k$ par prolongement)**.**
Soit f de classe $\mathscr{C}^k$ sur $I\setminus\{a\}$. Si pour tout $i \in [\![0, k]\!]$ $f^{(i)}$ possède une limite finie en a, alors f admet un unique prolongement $\tilde{f}$ de classe $\mathscr{C}^k$ sur I, et l'on a pour tout $i \in [\![0, k]\!]$, $f^{(i)} \underset{a}{\to} \tilde{f}^{(i)}(a)$.

Démonstration.
On voit déjà facilement que $(\tilde{f})' = \tilde{f}'$.

Elle se fait par réccurence sur k.

Pour tout $k \in \mathbb{N}$, posons : (H_k) : « pour toute fonction f de classe $\mathscr{C}^k$ sur $I\setminus\{a\}$ telle que pour tout $i \in [\![0, k]\!]$ $f^{(i)}$ possède une limite finie en a, f admet un unique prolongement $\tilde{f}$ de classe $\mathscr{C}^k$ sur I, et l'on a pour tout $i \in [\![0, k]\!]$ $f^{(i)}$, $f^{(i)} \underset{a}{\to} \tilde{f}^{(i)}(a)$ ».

On sait déjà que le résultat est vrai pour $k = 0$ et pour $k = 1$.

Soit $k \in \mathbb{N}$ tel que (H_k) soit vrai au rang k. Soit f de classe $\mathscr{C}^{k+1}$ sur $I\setminus\{a\}$ telle que pour tout $i \in [\![0, k+1]\!]$ $f^{(i)}$ possède une limite finie en a.

Puisque $k + 1 > 0$, f admet un unique prolongement $\tilde{f}$ tel que $\tilde{f}$ soit dérivable en a, $f \underset{a}{\to} \tilde{f}(a)$ et $f' \underset{a}{\to} \tilde{f}'(a)$.

On peut ensuite appliquer l'hypothèse de récurrence à f'. Le prolongement de f' ainsi obtenu ne peut être que $\tilde{f}'$ puisque $f' \underset{a}{\to} \tilde{f}'(a)$, ce qui assure que (H_{k+1}) est vraie. □

2.6 Théorème des accroissements finis et suites récurrentes

Le TAF fournit un outil supplémentaire pour étudier les suites récurrentes. Si une telle suite converge, elle converge vers un point fixe de f, et se prête à une approximation des points fixes de f.
Le TAF, dans certaines conditions, assure qu'une telle suite converge (1er résultat) sans avoir à étudier la monotonie de f ni celle de (u_n), et assure que la convergence est rapide (2eme résultat).

Exemple 2.6.1.
$f : I \to \mathbb{R}$, I stable par f, et $\ell \in I$ un point fixe de f. Soit $u_0 \in I$. On considère la suite $u_{n+1} = f(u_n)$.

Si $|f'|$ est majorée par M tel que $0 \leqslant M < 1$, alors pour tout n, $|u_n - \ell| \leqslant M^n |u_0 - \ell|$ (le montrer par récurrence). Et donc $|u_n - \ell| \to 0$. De plus, la convergence est géométrique ce qui est rapide. Par exemple, si $M = \dfrac{1}{10}$, alors on gagne une décimale de précision à chaque étape.

Exemple 2.6.2.
Trouver une approximation du point fixe de $f : \mathbb{R}_+ \to \mathbb{R}$, $x \mapsto \dfrac{1}{1+x}$ à 10^{-2}. $\mathbb{R}_+$ est stable par f, f est dérivable sur $\mathbb{R}_+$, de dérivée $x \mapsto -\dfrac{1}{(1+x)^2}$ bornée par 1.

Malheureusement cette borne est insuffisante pour appliquer les idées vues ci-dessus : on aimerait avoir une borne K strictement inférieure à 1.

Pour cela, on va chercher un intervalle stable par f sur lequel f' est bornée par un $K < 1$. f' étant strictement croissante et à valeurs négatives, il suffit de trouver un invervalle de la forme $[a, b]$ avec $a < b$ et $a > -1$.

Le point fixe de f est par calcul $\alpha = \dfrac{-1+\sqrt{5}}{2}$. On peut constater que $f(1) = 1/2$, et comme $\alpha \leqslant 1$, en déduire que $1/2 \leqslant f(\alpha) = \alpha$.

On peut alors constater aisément que $[1/2, 1]$ est stable par f. On peut choisir une valeur arbitraire dans $[1/2, 1]$. En itérant f sur cette valeur on obtient des approximations successives de α convergeant vers α.

Supposons maintenant que $f : I \to I$ soit dérivable et que sa dérivée soit bornée par $K < 1$.

Par récurrence, on montre facilement que pour tout $n \in \mathbb{N}$, $|u_{n+1} - u_n| \leqslant K^n |u_1 - u_0|$. Alors, si $n \in \mathbb{N}$,

$$\begin{aligned} |u_n - u_0| &= \left| \sum_{k=0}^{n-1} u_{k+1} - u_k \right| \\ &\leqslant \sum_{k=0}^{n-1} |u_{k+1} - u_k| \\ &\leqslant |u_1 - u_0| \sum_{k=0}^{n-1} K^k \\ &\leqslant \frac{1}{1-K} |u_1 - u_0|. \end{aligned}$$

Ainsi, (u_n) est bornée.

3 Extension au cas des fonctions complexes

Soit $f : I \to \mathbb{C}$, où I est un intervalle de $\mathbb{R}$.

• La définition de dérivée en a est exactement la même que pour les fonctions réelles, mais la dérivée est à valeurs dans $\mathbb{C}$. On a aussi le résultat (simple) suivant.

Proposition 3.0.1.
La fonction f est dérivable (en un point ou sur I) si et seulemet si $\mathrm{Re}(f)$ et $\mathrm{Im}(f)$ le sont aussi. Dans ce cas, on a $f' = \mathrm{Re}(f)' + i\,\mathrm{Im}(f)'$.

• Les résultats concernant les opérations sur la dérivabilité se généralisent : $+, \times, /$.

• Par contre, attention à la composition : dériver $f \circ g$ n'a de sens (dans notre cadre) que si g est à valeurs réelles, et f peut être à valeurs complexes ! Dans ce cas, on a le même résultat que dans le cas réel.

• Pour démontrer tout cela, on utilise la proposition 3.0.3.

• Les grands théorèmes :

- le théorème de Rolle ne se généralise pas. Ex : $\mathbb{R} \to \mathbb{C}$, $x \mapsto \mathrm{e}^{ix}$.

- TAF : faux aussi (normal, çela impliquerait le théorème de Rolle).

- IAF : On peut le formuler comme suit.

Théorème 3.0.2 (IAF version complexe)**.**
Soit $(a,b) \in \mathbb{R}^2$ avec $a < b$ et $f \in \mathscr{C}([a,b],\mathbb{C}) \cap \mathscr{D}(]a,b[,\mathbb{C})$ tel qu'il existe $K > 0$ vérifiant $\forall x \in]a,b[\quad |f'(x)| \leqslant K$. Alors $|f(b)-f(a)| \leqslant K(b-a)$.

Démonstration. 1. On va d'abord s'intéresser au cas particulier où $f(b) - f(a)$ est un réel. Dans ce cas, on considérons l'application $\mathrm{Re}(f) : [a,b] \to \mathbb{R}$. Elle est continue sur $[a,b]$ et dérivable sur $]a,b[$. De plus, pour tout $x \in]a,b[$, on a $|\mathrm{Re}(f)'(x)| = |\mathrm{Re}(f'(x))| \leqslant |f'(x)| \leqslant K$. Donc on peut appliquer l'IAF à $\mathrm{Re}(f)$ et en déduire : $|\mathrm{Re}(f)(b) - \mathrm{Re}(f)(a)| \leqslant K(b-a)$. Or $\mathrm{Re}(f)(b) - \mathrm{Re}(f)(a) = \mathrm{Re}(f(b) - f(a)) = f(b) - f(a)$. On a donc le résultat.

2. Montrons maintenant le cas général. $f(b) - f(a)$ est de la forme $\mathrm{e}^{i\theta}|f(b) - f(a)|$. Notons alors

$$\begin{array}{rccc} \varphi : & [a,b] & \to & \mathbb{R} \\ & x & \mapsto & \mathrm{e}^{-i\theta} f(x) \end{array}$$

φ est clairement dérivable sur $]a,b[$ et continue sur $[a,b]$. De plus pour tout $x \in]a,b[$, $\varphi'(x) = \mathrm{e}^{-i\theta} f'(x)$, donc $|\varphi'(x)| = |f'(x)| \leqslant K$.

De plus $\varphi(b) - \varphi(a) = \mathrm{e}^{-i\theta}(f(b) - f(a)) = |f(b) - f(a)|$.

$\varphi(b) - \varphi(a)$ est donc réel, donc on peut appliquer le point ci-dessus à φ : $|\varphi(b) - \varphi(a)| \leqslant K|b - a|$.

Or $|\varphi(b) - \varphi(a)| = |f(b) - f(a)|$, d'où le résultat.

□

Les notions de monotonie d'une fonction f ou de signe de f' n'ont évidemment pas de sens dans le cas des fonctions à valeurs complexes, mais on a cependant le résultat suivant.

Théorème 3.0.3.
Soit $f \in \mathscr{D}(I,\mathbb{C})$. Alors f est constante si et seulement si $f' = 0$.

Démonstration.
f est constante si et seulement si $\mathrm{Re}(f)$ et $\mathrm{Im}(f)$ sont constantes ce qui équivaut à $(\mathrm{Re}(f))' = (\mathrm{Im}(f))' = 0$, ce qui équivaut à $(\mathrm{Re}(f))' + i(\mathrm{Im}(f))' = 0$ c'est-à-dire à $f' = 0$. □

Chapitre XVI

Fractions rationnelles

Dans ce chapitre, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.
Nous allons étudier un nouveau corps : $\mathbb{K}(X)$, qui est le corps des *fractions rationnelles*. Sa construction est hors-programme, mais on peut mentionner que l'on obtient $\mathbb{K}(X)$ à partir de $\mathbb{K}[X]$ de la même manière que l'on obtient $\mathbb{Q}$ à partir de $\mathbb{Z}$: on rajoute de nouveaux éléments qui seront les inverses pour la loi $\times$ de tous les éléments non nuls, c'est-à-dire que l'on introduit les éléments $\frac{1}{P}$, où $P \in \mathbb{K}[X]\backslash\{0\}$. Ainsi, $\mathbb{K}(X)$ est le corps contenant les fractions de polynômes.

1 Corps des fractions rationnelles $\mathbb{K}(X)$

1.1 Définitions

La construction de l'ensemble des fractions rationnelles étant hors-programme, on introduit celui-ci de façon axiomatique.

Définition 1.1.1.
Il existe un ensemble $\mathbb{K}(X)$ vérifiant :

(i) À tout couple $(A, B) \in \mathbb{K}[X]^2$ tel que $B \neq 0$, on peut associer un élément de $\mathbb{K}(X)$ noté $\frac{A}{B}$;

(ii) Réciproquement, tout élément de $\mathbb{K}(X)$ s'écrit $\frac{A}{B}$, avec $A, B \in \mathbb{K}[X]$, $B \neq 0$;

(iii) Si $A, B, C, D \in \mathbb{K}[X]$ tels que B et D soient non nuls, on a : $\frac{A}{B} = \frac{C}{D} \Leftrightarrow AD = BC$.

Cette définition permet de donner sans ambiguïté tous les éléments de $\mathbb{K}(X)$: ce n'est qu'une définition ensembliste.
Cet ensemble est appelé *l'ensemble des fractions rationnelles à coefficients dans* $\mathbb{K}$.

 L'écriture (**?** **?**) n'est pas unique !

Remarque 1.1.2.
Remarquons que cette définition dit notamment que pour toute fraction rationnelle $\frac{A}{B}$ et tout polynôme non-nul C, les fractions rationnelles $\frac{AC}{BC}$ sont égales (en effet $AC \times B = A \times BC$).

Définition 1.1.3.
Soit $R \in \mathbb{K}(X)$, un couple $(A, B) \in \mathbb{K}[X]^2$ tel que $R = \frac{A}{B}$ est appelé *représentant* de la fraction rationnelle R.

Passons maintenant à des définitions algébriques.

Définition 1.1.4 (Lois sur $\mathbb{K}(X)$)**.**
On définit trois lois sur $\mathbb{K}(X)$, les deux premières sont des lois internes, la troisième est une loi externe.

$$\textbf{Addition } + : \begin{cases} \mathbb{K}(X) \times \mathbb{K}(X) & \longrightarrow & \mathbb{K}(X) \\ \left(\frac{A}{B}, \frac{C}{D}\right) & \longmapsto & \frac{AD+BC}{BD} \end{cases}$$

$$\textbf{Produit } \times : \begin{cases} \mathbb{K}(X) \times \mathbb{K}(X) & \longrightarrow & \mathbb{K}(X) \\ \left(\frac{A}{B}, \frac{C}{D}\right) & \longmapsto & \frac{AC}{BD} \end{cases}$$

$$\textbf{Multiplication par un scalaire } \cdot : \begin{cases} \mathbb{K} \times \mathbb{K}(X) & \longrightarrow & \mathbb{K}(X) \\ \left(\lambda, \frac{A}{B}\right) & \longmapsto & \frac{\lambda A}{B} \end{cases}$$

Alors $(\mathbb{K}(X), +, \times)$ est un corps.
De plus, tout polynôme de $\mathbb{K}[X]$ s'identifie à l'élément $\frac{P}{1}$ de $\mathbb{K}(X)$. Cette identification permet de considérer $(\mathbb{K}[X], +, \times)$ comme un sous-anneau de $(\mathbb{K}(X), +, \times)$.

Le neutre de la loi + et 0, celui de la loi $\times$ est 1. L'opposé de $\frac{A}{B}$ et $\frac{-A}{B}$, son inverse est $\frac{B}{A}$.

Remarque 1.1.5.
On verra bientôt que $(\mathbb{K}(X), +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.

Démonstration.

 Les définitions ci-dessus sont a priori ambiguës : par exemple lorsqu'on veut additionner deux fractions rationnelles R_1 et R_2, on dispose de plusieurs représentants pour R_1 et de plusieurs représentants pour R_2 (il y en a

même une infinité). Lesquels choisir pour appliquer la définition ? On peut en fait montrer que le résultat ne dépend pas du choix des représentants. En effet, considérons deux représentants $\frac{A_1}{B_1}$ et $\frac{C_1}{D_1}$ pour R_1 et deux représentants $\frac{A_2}{B_2}$ et $\frac{C_2}{D_2}$ pour R_2.

On a $A_iD_i = B_iC_i$ pour $i = 1, 2$. Montrons alors qu'on a $\frac{A_1B_2 + A_2B_1}{B_1B_2} = \frac{C_1D_2 + C_2D_1}{D_1D_2}$.

Il suffit de remarquer qu'on a successivement :

$$\begin{aligned}(A_1B_2 + A_2B_1)D_1D_2 &= (A_1D_1)B_2D_2 + (A_2D_2)B_1D_1\\ &= (B_1C_1)B_2D_2 + (B_2C_2)B_1D_1\\ &= (C_1D_2 + C_2D_1)B_1B_2\end{aligned}$$

On a aisément de même $\frac{A_1A_2}{B_1B_2} = \frac{C_1C_2}{D_1D_2}$ et $\frac{\lambda A_1}{B_1} = \frac{\lambda C_1}{D_1}$.

On procède de même (mais plus simplement) pour le produit et la multiplication scalaire. □

1.2 Fonctions rationnelles

Définition 1.2.1.
Soit $R \in \mathbb{K}(X)$. On appelle *forme irréductible* de R toute écriture de R de la forme $R = \frac{P}{Q}$ avec $P, Q \in \mathbb{K}[X]$ tels que $P \wedge Q = 1$.

Exemple 1.2.2.
$\frac{X^2-1}{X(X-1)}$ n'est pas irréductible, mais $\frac{X+1}{X}$ l'est.

Remarque 1.2.3.

Il existe une infinité de formes irréductibles : ainsi $\frac{1}{X}$, $\frac{2}{2X}$ et $\frac{3}{3X}$ sont trois formes irréductibles d'une même fraction rationnelle.

Cependant, si $\frac{A}{B}$ et $\frac{C}{D}$ sont deux formes irréductibles d'une même fraction rationelle, alors il existe $\lambda \in \mathbb{K}^*$ vérifiant $C = \lambda A$ et $D = \lambda B$. (en effet, on a alors $AD = BC$ donc $D|BC$ or D et C sont premiers entre eux, donc D divise B ; de même $B|AD$ donc $B|D$, B et D sont donc associés, il existe donc λ non nul vérifiant $D = \lambda B$, donc $\lambda AB = BC$, or $B \neq 0$ donc $C = \lambda A$).

Définition 1.2.4.
Soient $R \in \mathbb{K}(X)$ et $\frac{A}{B}$ ***une*** forme irréductible de R. Alors si $\tilde{A}$ et $\tilde{B}$ sont les fonctions polynômiales associées à A et B, on appelle *fonction rationnelle associée à* R la fonction $\tilde{R} : \begin{array}{ccc}\mathbb{K}\backslash\mathscr{A} & \to & \mathbb{K}\\ x & \mapsto & \frac{\tilde{A}(x)}{\tilde{B}(x)}\end{array}$,
où $\mathscr{A}$ est l'ensemble des racines de B.

Remarque 1.2.5.
1. Ce problème du domaine de définition explique pourquoi l'on travaille avec des formes irréductibles : avec une forme réductible, le domaine de définition serait encore plus restreint (et en tout cas différent, donc pas très pratique), car le dénominateur aurait encore plus de racines. Par exemple, pour $R = 1$ si l'on écrit $R = \frac{X}{X}$, la fonction rationnelle associée ne serait pas définie en 0, ce qui est idiot pour une fonction constante.
2. La remarque 1.2.3 permet de conclure que $\tilde{R}$ ne dépend pas de la forme irréductible choisie.

Proposition 1.2.6.
Soient R_1, R_2 deux fractions rationnelles. Alors $R_1 = R_2 \Leftrightarrow \tilde{R}_1 = \tilde{R}_2$.

Démonstration.
Le sens direct découle des propriétés de l'égalité en mathématiques.

Étudions le sens indirect : on note $R_1 = \frac{P}{Q}$ et $R_2 = \frac{A}{B}$, deux formes irréductibles. Alors les fonctions $\frac{\tilde{P}}{\tilde{Q}}$ et $\frac{\tilde{A}}{\tilde{B}}$ coïncident sur leur ensemble de définition D, d'où $\tilde{P}\tilde{B}$ et $\tilde{A}\tilde{Q}$, qui sont deux fonctions polynomiales, coïncident sur D, qui est infini. Donc les polynômes sous-jacents sont égaux, i.e. $PB = AQ$. Donc on a $R_1 = R_2$. □

1.3 Dérivées, degrés et pôles

Définition 1.3.1.
Soit $R = \dfrac{A}{B}$. On appelle *dérivéee* de R la fraction rationnelle $\dfrac{A'B - B'A}{B^2}$. Cette fraction rationnelle ne dépend pas du choix de A et de B, et est donc bien définie.
On a alors les propriétés suivantes, pour $R_1, R_2 \in \mathbb{K}(X)$ et $\lambda \in \mathbb{K}$:

(i) $(R_1 + \lambda R_2)' = R_1' + \lambda R_2'$

(ii) $(R_1 \times R_2)' = R_1' R_2 + R_1 R_2'$

(iii) si $R_2 \neq 0$, $\left(\dfrac{R_1}{R_2}\right)' = \dfrac{R_1' R_2 - R_1 R_2'}{R_2^2}$.

Démonstration. — Montrons que R' ne dépend pas du choix de A et B : si $R = \dfrac{P}{Q} = \dfrac{A}{B}$, avec $\dfrac{A}{B}$ irréductible. Alors $PB = AQ$, donc $A|PB$ et, avec le lemme de Gauss, $A|P$, d'où il existe $C \in \mathbb{K}[X]$ tel que $P = AC$, et par suite $Q = BC$. Dans ce cas, $\left(\dfrac{P}{Q}\right)' = \dfrac{P'Q - Q'P}{Q^2} = \dfrac{(A'C + AC')BC - (B'C + BC')AC}{B^2C^2} = \dfrac{C^2(A'B - AB')}{C^2B^2} = \dfrac{A'B - AB'}{B^2} = \left(\dfrac{A}{B}\right)'$.
— Il suffit de remplacer les expressions par leurs définitions et d'un simple calcul pour vérifier les propriétés énoncées.

□

Remarque 1.3.2.
La dérivation sur $\mathbb{K}(X)$ prolonge celle sur $\mathbb{K}[X]$.

Définition 1.3.3 (Degré)**.**
Soit $R = \dfrac{A}{B}$, avec $A, B \in \mathbb{K}[X]$, $B \neq 0$. On appelle *degré* de R, noté $\deg R$, la quantité $\deg R = \deg A - \deg B$. Si $A \neq 0$, il s'agit d'un entier relatif. Sinon, $\deg R = -\infty$. Cette définition ne dépend là encore pas du représentant choisi.

Démonstration.
Si $F = \dfrac{A}{B} = \dfrac{C}{D}$, alors $AD = BC$, donc $\deg(AD) = \deg(BC)$, soit $\deg(A) + \deg(D) = \deg(B) + \deg(C)$. On obtient donc $\deg(A) - \deg(B) = \deg(C) - \deg(D)$. □

Remarque 1.3.4.
Le degré sur $\mathbb{K}(X)$ prolonge celui sur $\mathbb{K}[X]$.

Remarque 1.3.5.
La fraction rationnelle nulle est la seule à ne pas avoir pour degré un entier.

Exemple 1.3.6.
$\deg \dfrac{X^4}{X(X-1)} = 4 - 2 = 2$;
$\deg \dfrac{X(X^2+5)}{X^3(X^2+X-2)} = 3 - 5 = -2$;
$\deg \dfrac{X^2(X+1)}{X^3 - 2X + 3} = 3 - 3 = 0$, et on voit là qu'une fraction rationnelle de degré nul n'est pas forcément constante.

Proposition 1.3.7.
Soient $R_1, R_2 \in \mathbb{K}(X)$.

(i) $\deg(R_1 + R_2) \leqslant \max(\deg R_1, \deg R_2)$

(ii) $\deg(R_1 R_2) = \deg R_1 + \deg R_2$

(iii) si $\deg R_1 \neq 0$, alors $\deg R_1' = \deg R_1 - 1$.

Démonstration.
On note $R_1 = \dfrac{P}{Q}$ et $R_2 = \dfrac{A}{B}$.

(i) On a : $R_1 + R_2 = \dfrac{PB + AQ}{QB}$. Donc $\deg(R_1 + R_2) = \deg(PB + AQ) - \deg(QB) \leqslant \max(\deg(PB), \deg(AQ)) - \deg Q - \deg B = \max(\deg P + \deg B, \deg A + \deg Q) - \deg Q - \deg B = \max(\deg P + \deg B - \deg Q - \deg B, \deg A + \deg Q - \deg Q - \deg B) = \max(\deg P - \deg Q, \deg A - \deg B) = \max(\deg(P/Q), \deg A/B) = \max(\deg(R_1), \deg(R_2))$.

(ii) Simple calcul.

(iii) On note $d = \deg P$, $e = \deg Q$, p le coefficient dominant de P et q celui de Q.
• Si $e = 0$, alors R_1 est un polynôme et le résultat est alors connu.
• Si $d = 0$ et $e \neq 0$, alors $\deg R_1 = -e$ et $R_1' = -\dfrac{Q'}{Q^2}$, dont le degré est $e - 1 - 2e = -e - 1 = \deg R_1 - 1$.
• Si $d \neq 0$ et $e \neq 0$, alors on a $R_1' = \dfrac{P'Q - Q'P}{Q^2}$, donc $\deg P'Q = \deg PQ' = \deg P + \deg Q - 1 = d + e - 1$. Le coefficient de degré $d + e - 1$ de $P'Q - Q'P$ est $dpq - epq = (d - e)pq \neq 0$ car $d - e = \deg R_1 \neq 0$, donc $\deg R_1' = d + e - 1 - \deg(Q^2) = d + e - 1 - 2e = d - e - 1 = \deg R_1 - 1$.

□

 si $\deg R = 0$, on peut juste dire $\deg R' < \deg R - 1$, car avec les notations de la démonstration on a $e = d$.

Exemple 1.3.8.
• si $R = 1$, $\deg R' = -\infty$.
• si $R = \dfrac{1}{X}$, $R' = -\dfrac{1}{X^2}$ donc $\deg R' = \deg R - 1$.
• si $R = \dfrac{X}{X+1} = 1 - \dfrac{1}{X+1}$, $R' = \dfrac{1}{(X+1)^2}$, donc $\deg R' = \deg R - 2$.

1.4 Zéros et pôles

Définition 1.4.1.
Soit $R = \dfrac{A}{B}$, irréductible.

1. Toute racine de A est appelée *racine* ou *zéro* de R. Si elle est de multiplicité m dans A, on dira aussi qu'elle est de multiplicité m dans R.
2. Toute racine de B est appelée *pôle* de R. Si elle est de multiplicité m dans B, on dira aussi qu'elle est de multiplicité m dans R.

On utilise les expressions *pôle ou racine simple ou double* quand la multiplicité vaut 1 ou 2.

 À nouveau, la multiplicité n'est bien définie que si la fraction est irréductible : 1 n'a pas la même multiplicité dans les dénominateurs de $\dfrac{X(X-1)}{(X-1)^2}$ et $\dfrac{X}{X-1}$. De plus 1 n'est pas racine de ces fractions rationnelles, car 1 n'est pas racine de la forme irréductible.
En allant encore plus loin, soit $R = \dfrac{A}{B}$ une fraction rationnelle. Alors $R = \dfrac{A(X-\lambda)^n}{B(X-\lambda)^n}$, et ce pour tous $\lambda \in \mathbb{K}$ et $n \in \mathbb{N}$. Donc, si on oubliait l'hypothèse « forme irréductible », on pourrait montrer que tout scalaire est racine et pôle de toute fraction rationnelle, avec n'importe quelle multiplicité.

Remarque 1.4.2.
On pourra, si besoin, considérer la convention suivante : un scalaire est racine (resp. pôle) de multiplicité zéro de $R = A/B$ s'il n'est pas racine de A (resp. B).

2 Étude locale d'une fraction rationnelle

2.1 Partie entière

Théorème 2.1.1.
Soit $R \in \mathbb{K}(X)$ Alors il existe un unique couple $(E, Q) \in \mathbb{K}[X] \times \mathbb{K}(X)$ tel que $\deg Q < 0$ et $R = E + Q$. Le polynôme E est appelé la *partie entière* de R.

Démonstration.
On note $R = \dfrac{A}{B}$.

Existence On effectue la division euclidienne de A par B, qui donne $A = EB + T$, avec $\deg T < \deg B$. Ainsi $R = \dfrac{EB+T}{B} = E + Q$, avec $Q = \dfrac{T}{B}$: on a bien $\deg Q < 0$.

Unicité Soient (E, Q) et (D, U) deux couples convenables. Alors $E + Q = D + U$, soit $E - D = U - Q$. Si $E - D \neq 0$, on a $\deg(E - D) \geqslant 0$. Or $\deg(U - Q) \leqslant \max(\deg Q, \deg U) < 0$. Ceci est contradictoire, donc $E - D = 0$, i.e. $E = D$. Il s'ensuit que $Q = U$.

□

Exemple 2.1.2.
Après division euclidienne, on obtient $\dfrac{X^6 + X^3 + X^2 - 1}{X^2 + 3} = X^4 - 3X^2 + X + 10 + \dfrac{-3X - 31}{X^2 + 3}$, et ainsi la partie entière de $\dfrac{X^6 + X^3 + X^2 - 1}{X^2 + 3}$ est $X^4 - 3X^2 + X + 10$.

2.2 Partie polaire associée à un pôle

Définition 2.2.1.
Soit $m \in \mathbb{N}$, $R \in \mathbb{K}(X)$, et λ un pôle de R de multiplicité m. Alors il existe une unique famille

$a_1, \dots, a_m \in \mathbb{K}$ et une unique fraction rationnelle S n'ayant pas λ pour pôle vérifiant

$$R = \sum_{k=1}^{m} \frac{a_k}{(X-\lambda)^k} + S.$$

La somme $\sum_{k=1}^{m} \frac{a_k}{(X-\lambda)^k}$ est appelée *partie polaire de R associée au pôle λ.*

De plus :

1. le coefficient a_m est non-nul ;
2. les autres pôles de R sont exactement les pôles de S, avec la même multiplicité.

Démonstration.
Hors-programme. □

Exemple 2.2.2.
Par exemple, il existe $a, b, c \in \mathbb{R}$ et $P \in \mathbb{K}[X]$ uniques tels que $\frac{X+1}{(X-1)^3(X-2)^2} = \frac{a}{X-1} + \frac{b}{(X-1)^2} + \frac{c}{(X-1)^3} + \frac{P}{(X-2)^2}$.

2.3 Décomposition en éléments simples dans $\mathbb{C}(X)$

Théorème 2.3.1 (Décomposition dans $\mathbb{C}(X)$)**.**
Soit $R \in \mathbb{C}(X)$. Alors R est la somme de sa partie entière et de ses parties polaires. Cette décomposition s'appelle la *décomposition en éléments simples de R.*

Plus précisément : si $\lambda_1, \dots, \lambda_n$ sont les pôles de R, de multiplicités respectives $m_1, \dots, m_n$, alors il existe une unique famille d'éléments de $\mathbb{C}$ $a_{1,1}, \dots, a_{1,m_1}, \dots, a_{n,1}, \dots, a_{n,m_n}$ (le premier indice représentant le pôle et le second indice allant de 1 à la multiplicité de ce pôle), vérifiant

$$R = E + \sum_{k=1}^{n} \left(\sum_{j=1}^{m_k} \frac{a_{k,j}}{(X-\lambda_k)^j} \right)$$

où E est la partie entière de R.

Démonstration.
Hors programme. □

Exemple 2.3.2.
$\frac{X^5+X^2-3}{(X-1)^3(X-2)^2}$ s'écrit de manière unique sous la forme

$$1 + \frac{a_1}{X-1} + \frac{a_2}{(X-1)^2} + \frac{a_3}{(X-1)^3} + \frac{b_1}{X-2} + \frac{b_2}{(X-2)^2} \quad \text{(XVI.1)}$$

2.4 Décomposition en éléments simples dans $\mathbb{R}(X)$

Dans $\mathbb{R}(X)$, le dénominateur d'une fraction rationnelle n'est pas nécessairement scindé ce qui complique la décomposition en éléments simples des fractions rationnelles. Nous commençons par donner un énoncé valable à la fois dans $\mathbb{C}(X)$ et $\mathbb{R}(X)$ et nous verrons ensuite ce qu'il donne dans le cas particulier de $\mathbb{C}(X)$.

Théorème 2.4.1 (Décomposition dans $\mathbb{K}(X)$)**.**
Soit $R \in \mathbb{K}(X)$. R s'écrit sous forme irréductible $\frac{P}{Q}$ avec Q unitaire. Le polynôme Q s'écrit alors sous la forme $H_1^{n_1} \dots H_p^{n_p}$ où $H_1, \dots, H_p$ sont des polynômes irréductibles unitaires distincts et $n_1, \dots, n_p$ des naturels non nuls.

Alors R se décompose de façon unique sous la forme

$$R = E + F_1 + \dots F_p$$

où E est un polynôme et pour tout $k \in [\![1, p]\!]$, F_k s'écrit sous la forme $\sum_{j=1}^{n_k} \frac{J_{k,j}}{H_k^j}$, où pour tout $j \in [\![1, n_k]\!]$, on a $\deg J_{k,j} < \deg H_k$. Cette décomposition s'appelle la *décomposition en éléments simples de R dans $\mathbb{K}(X)$.*

De plus E est nécessairement la partie entière de R.

Démonstration.
Hors programme. □

Remarque 2.4.2. 1. Dans $\mathbb{C}(X)$, les irréductibles sont de degré 1 et les $J_{k,j}$ sont donc

tous des polynômes constants : on retrouve l'énoncé donné spécifiquement pour $\mathbb{C}(X)$.

2. Dans $\mathbb{R}(X)$, les irréductibles sont de degré 1 ou 2, d'où l'énoncé qui suit.

Théorème 2.4.3 (Décomposition dans $\mathbb{R}(X)$)**.** Soit $R \in \mathbb{R}(X)$. R s'écrit sous forme irréductible $\frac{P}{Q}$ avec Q unitaire. Le polynôme Q s'écrit alors sous la forme $\prod_{i=1}^{q}(X-\lambda_i)^{m_i} \times \prod_{i=1}^{p} H_i^{n_i}$, où λ_1, …, λ_q sont les racines (deux à deux distinctes) de Q et H_1, …, H_p sont des polynômes de degré deux sans racines réelles.

Alors R se décompose de façon unique sous la forme

$$R = E + \sum_{k=1}^{q}\sum_{j=1}^{m_k} \frac{a_{k,j}}{(X-\lambda_k)^j} + \sum_{k=1}^{p}\sum_{j=1}^{n_j} \frac{b_{k,j}X + c_{k,j}}{H_j^k}$$

où E est un polynôme et tous les $a_{k,j}$, les $b_{k,j}$ et les $c_{k,j}$ sont des réels.

Cette décomposition s'appelle la *décomposition en éléments simples de R dans $\mathbb{R}(X)$*.

De plus E est nécessairement la partie entière de R.

2.5 Quelques méthodes de calcul

L'objectif est d'obtenir le plus rapidement possible la décomposition en éléments simples d'une fraction rationnelle, bien entendu sans faire d'erreurs de calculs. Il est donc *fortement conseillé* de suivre les méthodes suivantes, en essayant d'utiliser les méthodes les plus appropriées dans le contexte.

Enfin, si vous en avez le temps, pensez bien à vérifier vos calculs, par exemple en recomposant la fraction rationnelle.

a Avant même de commencer

Pour décomposer une fraction rationnelle F, on commence par l'écrire sous forme $E + R$ où $\deg R < 0$ et E est sa partie entière.

Toutes les méthodes ci-dessous s'appliquent à la fraction rationnelle R *qui est de degré strictement négatif.*

b Simplification par symétrie, parité et imparité

Il convient à chaque fois de simplifier au maximum le problème posé en réduisant le nombre de coefficients à chercher. Pour cela, on exploite les symétries repérées dans la fraction rationnelle.

Traitons un exemple : la fraction rationnelle $R = \dfrac{1}{(X-1)^2(X+1)^2}$ est paire, car $R(-X) = R(X)$. Mais on sait qu'il existe $a, b, c, d \in \mathbb{R}$ tels que $R = \dfrac{a}{X-1} + \dfrac{b}{(X-1)^2} + \dfrac{c}{X+1} + \dfrac{d}{(X+1)^2}$. Et donc $R(-X) = -\dfrac{a}{X+1} + \dfrac{b}{(X+1)^2} + -\dfrac{c}{X-1} + \dfrac{d}{(X-1)^2}$. Par unicité des coefficients de la décomposition en éléments simples, on en déduit que $a = -c$ et $b = d$: le calcul de a et b suffit donc (deux coefficients au lieu de quatre !).

On a la même chose avec les fractions rationnelles impaires.

On pourra aussi exploiter d'autres types de symétries. En voici un exemple : $F = \dfrac{1}{X(X-1)}$. Les pôles (0 et 1) sont « symétriques » par rapport à $\dfrac{1}{2}$, ce qui se voit par $F(X) = F(1-X)$. Si l'on écrit $F = \dfrac{\alpha}{X} + \dfrac{\beta}{X-1}$, on obtient alors $F(1-X) = \dfrac{-\beta}{X} + \dfrac{-\alpha}{X-1}$, ce qui donne $\alpha = -\beta$.

c Simplification par conjugaison de fractions rationnelles réelles

Soit $R \in \mathbb{R}(X)$, et soit $\lambda \in \mathbb{C} \setminus \mathbb{R}$ un pôle complexe non réel de R, de multiplicité m. Alors $\overline{\lambda}$ est aussi un pôle de R de multiplicité m. On a donc : $R = \dfrac{a_1}{X-\lambda} + \dfrac{a_2}{(X-\lambda)^2} + \ldots + \dfrac{a_m}{(X-\lambda)^m} + \dfrac{b_1}{X-\overline{\lambda}} + \dfrac{b_2}{(X-\overline{\lambda})^2} + \ldots + \dfrac{b_m}{(X-\overline{\lambda})^m} + G$, où G n'admet ni λ ni $\overline{\lambda}$ pour pôle. Mais on a $\overline{R} = R$,

et donc $R = \overline{R} = \frac{\overline{a_1}}{X-\overline{\lambda}} + \frac{\overline{a_2}}{(X-\overline{\lambda})^2} + \ldots + \frac{\overline{a_m}}{(X-\overline{\lambda})^m} + \frac{\overline{b_1}}{X-\lambda} + \frac{\overline{b_2}}{(X-\lambda)^2} + \ldots + \frac{\overline{b_m}}{(X-\lambda)^m} + \overline{G}$. Par identification on obtient donc : $a_1 = \overline{b}_1, \ldots, a_m = \overline{b}_m$ et $G = \overline{G}$ (i.e. $G \in \mathbb{R}(X)$). Là encore, cela permet de réduire le nombre de coefficients à calculer.

d Méthode de base

Soit $R = \frac{A}{B}$ avec $\deg R < 0$ à décomposer, avec A et B deux polynômes non nuls, B étant de la forme $C \times (X-\lambda)^n$ où λ n'est pas racine de C.

R s'écrit $\sum_{k=1}^{m} \frac{a_k}{(X-\lambda)^k} + S$. On peut trouver le coefficient a_m (et seulement celui-là !) en multipliant R par $(X-\lambda)^m$ et en évaluant le résultat en λ.

En effet, on a

$$\begin{aligned}\frac{A}{C} &= (X-\lambda)^m R \\ &= \sum_{k=1}^{m} a_k (X-\lambda)^{m-k} + (X-\lambda)^m S \\ &= \sum_{h=0}^{m-1} a_{m-h} (X-\lambda)^h + (X-\lambda)^m S \\ &= a_m + \sum_{h=1}^{m-1} a_{m-h} (X-\lambda)^h + (X-\lambda)^m S\end{aligned}$$

D'où :

$$\frac{A(\lambda)}{C(\lambda)} = a_m + 0$$

On a donc trouvé a_m :

$$a_m = \frac{A(\lambda)}{C(\lambda)}$$

On calcule alors $T = R - \frac{a_m}{(X-\lambda)^m}$, et on continue en cherchant à décomposer T.

Remarque 2.5.1.
On a la garantie que, soit λ n'est pas pôle de T (c'est le cas si $m = 1$ ou si les coefficients $a_1, \ldots, a_{m-1}$ sont tous nuls), soit λ est pôle pour T de multiplicité strictement plus petite que m. En itérant l'algorithme on va donc terminer la décomposition pour la partie polaire associée à λ. On peut s'intéresser ensuite à un autre pôle, soit en partant de la dernière fraction obtenue, soit en repartant de la fraction initiale.

Remarque 2.5.2 (Cas d'un pôle simple)**.**
Dans le cas où $m = 1$, on a

$$a_1 = \frac{A(\lambda)}{C(\lambda)}$$

Si on ne connaît pas C mais juste B, plutôt que factoriser B par $X-\lambda$, on peut remarquer $B' = C'(X-\lambda) + C$, donc $B'(\lambda) = C(\lambda)$, donc

$$a_1 = \frac{A(\lambda)}{B'(\lambda)}$$

Il est souvent plus simple de calculer B' que de décomposer B en $C \times (X-\lambda)$, d'où l'intérêt de cette remarque.

Exemple 2.5.3.
Si $R = \frac{X^2 - X - 2}{4X^{10} - X^8 + 6X^3 - 9X^2 + 3X - 3} = \frac{A}{B}$. On remarque que $B(1) = 0$, mais $B'(1) = (40X^9 - 8X^7 + 18X^2 - 18X + 3)(1) = 35 \neq 0$, donc 1 est pôle simple de R. Or $\frac{A(1)}{B'(1)} = \frac{-2}{35}$, donc $R = -\frac{2/35}{X-1} + S$, et S n'a pas 1 pour pôle.

Remarque 2.5.4.
C'est méthode est **celle à privilégier** car elle fonctionne dans tous les cas et est souvent la plus rapide. Mais on peut la conjuguer ponctuellement à d'autres méthodes pour accélérer les calculs.

e Identification

C'est la méthode la plus naïve, mais elle doit vraiment être réservée au cas où la fraction rationnelle a au plus deux ou trois pôles avec multiplicité, sinon elle est trop lourde.

Par exemple on sait qu'il existe $a, b \in \mathbb{R}$ tels que $\frac{1}{X(X+1)} = \frac{a}{X} + \frac{b}{X+1}$. Or $\frac{a}{X} + \frac{b}{X+1} =$

$\frac{(a+b)X+a}{X(X+1)}$, donc on doit avoir $a+b=0$ et $a=1$, soit $a=1$ et $b=-1$.

f Résidus

Soit λ un pôle de R : on appelle *résidu* de R en λ le coefficient du terme $\frac{1}{X-\lambda}$. C'est en pratique le terme de la partie polaire associée à λ le plus compliqué à calculer, car c'est le dernier terme que l'on peut calculer avec la méthode de base. On note ce résidu $\mathrm{Res}(R,\lambda)$, et on note R_λ la partie polaire de R associée au pôle λ.

Alors, quelle que soit la multiplicité de λ, on a : $xR_\lambda(x) \xrightarrow[x\to+\infty]{} \mathrm{Res}(R,\lambda)$. En sommant cette relation sur tous les pôles de R, on obtient, dans le cas où $\lim\limits_{x\to+\infty} xR(x)$ est finie (i.e. $\deg R \leqslant -1$) : $R(x) \xrightarrow[x\to+\infty]{} \sum\limits_{\lambda \text{ pôle de } R} \mathrm{Res}(R,\lambda)$. Et donc si $\deg R \leqslant -2$, on a $\sum\limits_{\lambda \text{ pôle de } R} \mathrm{Res}(R,\lambda) = 0$.

Par exemple, si $R = \frac{1}{(X-1)^2(X+1)} = \frac{a}{X-1} + \frac{b}{(X-1)^2} + \frac{c}{X+1}$: on a $c = \frac{1}{(-1-1)^2} = \frac{1}{4}$, et $b = \frac{1}{(1+1)} = \frac{1}{2}$. Mais $\lim\limits_{x\to+\infty} xR(x) = 0$, donc $a+c=0$, et ainsi $a = -\frac{1}{4}$.

g Évaluation en un point différent d'un pôle

Si nous avons n coefficients à calculer, on peut écrire l'égalité entre la fraction rationnelle et sa décomposition (aux coefficients inconnus) et évaluer les deux membres de cette égalité en n points deux à deux distincts qui ne sont pas des pôles. On obtient alors n équations à n inconnues qui permettent de calculer les n coefficients voulus. Cette méthode est surtout efficace quand il ne reste qu'un ou deux coefficients à calculer, qui ne sont pas des coefficients associés à des pôles simples, sinon la méthode de base est plus rapide.

Par exemple, décomposons $\frac{X-2}{(X+1)(X+2)^3}$ sous la forme $\frac{a}{X+1} + \frac{b}{(X+2)^3} + \frac{c}{(X+2)^2} + \frac{d}{X+2}$.

La méthode de base nous donne immédiatement $a=-3$ et $b=4$. Par ailleurs, la méthode des résidus nous donne $a+d=0$, donc $d=3$.

En évaluant alors, par exemple en 2, on obtient :

$$\begin{aligned} 0 &= \frac{-3}{2+1} + \frac{4}{(2+2)^3} + \frac{c}{(2+2)^2} + \frac{3}{2+2} \\ &= \frac{-3}{16} + \frac{c}{16} \end{aligned}$$

d'où $c=3$.

On aurait bien sûr pu évaluer en un autre point, par exemple, en évaluant en -3, on obtient :

$$\frac{-5}{2} = \frac{-3}{-2} + \frac{4}{-1} + \frac{c}{1} + \frac{3}{-1}$$

d'où $c=3$.

h Développements limités

Prenons l'exemple d'une fraction rationnelle R admettant un pôle double.

Alors $R = \frac{a}{X-\lambda} + \frac{b}{(X-\lambda)^2} + G$, où G est une fraction rationnelle n'admettant pas λ pour pôle.

Pour h au voisinage épointé de 0, on a donc :

$$h^2R(\lambda+h) = b + ah + h^2G(\lambda+h)$$

Or G n'a pas pour pôle λ, donc G est bornée au voisinage de λ.

Donc $h^2R(\lambda+h)$ admet le développement limité $b+ah+o(h)$ pour h au de 0. Les développements limités étant uniques (sous réserve d'existence), il suffit de calculer le développement limité de $h^2R(\lambda+h)$ pour obtenir a et b.

Cette méthode s'applique aussi très bien à des pôles de multiplicité supérieure à 2, quitte à développer assez loin.

Par exemple posons $R = \frac{3X-1}{(X-1)^2(X^2+1)}$ et cherchons la partie polaire de R associée à 1. Pour h

au voisinage de 0, on a

$$\begin{aligned} h^2R(1+h) &= \frac{3(h+1)-1}{(h+1)^2+1} \\ &= \frac{3h+2}{2+2h+h^2} \\ &= \frac{1}{2}.\frac{3h+2}{1+h+h^2/2} \\ &= \frac{1}{2}(3h+2)(1-h+o(h)) \\ &= \frac{1}{2}(3h+2-2h+o(h)) \\ &= 1+h/2+o(h) \end{aligned}$$

donc la partie polaire associée à 1 est $\frac{1}{2(X-1)} + \frac{1}{(X-1)^2}$.

2.6 Décomposition de P'/P

Proposition 2.6.1.
Soit $P \in \mathbb{C}[X]$ un polynôme non nul. Alors, en notant $a_1, \ldots, a_n$ les n racines distinctes de P et $r_1, \ldots, r_n$ leurs ordres respectifs, on a

$$\frac{P'}{P} = \sum_{k=1}^{n} \frac{r_k}{X-a_k}$$

Démonstration.
Remarquons tout d'abord que $\frac{P'}{P}$ est de degré strictement négatif, donc sa partie entière est nulle.

Les seuls pôles possibles pour $\frac{P'}{P}$ sont les racines de P. Soit a une racine de P ; notons r sa multiplicité. Alors P s'écrit $(X-a)^r A$ où A est un polynôme dont a n'est pas racine. Alors on a

$$\begin{aligned} \frac{P'}{P} &= \frac{r(X-a)^{r-1}A + (X-a)^r A'}{(X-a)^r A} \\ &= \frac{r}{X-a} + \frac{A'}{A} \end{aligned}$$

et a n'est pas un pôle de $\frac{A'}{A}$. Donc $\frac{r}{X-a}$ est la partie polaire de $\frac{P'}{P}$ associée au pôle a (a est donc un pôle simple).

$\frac{P'}{P}$ étant la somme de sa partie entière et de ses parties polaires, on en déduit le résultat. □

Proposition 2.6.2.
Soit $P \in \mathbb{R}[X]$ un polynôme non nul. Alors P s'écrit

$$\lambda \prod_{k=1}^{n} H_k^{p_k}$$

où $\lambda \in \mathbb{R}$ et où les H_k, pour $k = 1, \ldots, n$ sont des polynômes irréductibles deux à deux distincts et $p_1, \ldots, p_k$ sont des entiers naturels non nuls.

Alors

$$\frac{P'}{P} = \sum_{k=1}^{n} \frac{p_k H_k'}{H_k}$$

Cet énoncé est une simple généralisation de l'énoncé précédent. Il est en fait vrai dans $\mathbb{R}(X)$ comme dans $\mathbb{C}(X)$.

Démonstration.
Remarquons tout d'abord que $\frac{P'}{P}$ est de degré strictement négatif, donc sa partie entière est nulle.

Les seuls facteurs irréductibles du dénominateur de P sont les H_k, pour $k = 1, \ldots, n$, donc ce sont les seuls à considérer pour décomposer P.

Soit $k \in [\![1, n]\!]$. Alors P s'écrit $H_k^{p_k} A_k$, où A_k est un polynôme dont H_k n'est pas un facteur. Alors on a

$$\begin{aligned} \frac{P'}{P} &= \frac{p_k H_k' H_k^{p_k-1} A_k + H_k^{p_k} A_k'}{H_k^{p_k} A_k} \\ &= \frac{p_k H_k'}{H_k} + \frac{A_k'}{A_k} \end{aligned}$$

et H_k n'est pas un facteur de A_k. Donc $\frac{p_k H_k'}{H_k}$ est la partie de la décomposition de $\frac{P'}{P}$ associée au facteur H_k.

$\frac{P'}{P}$ étant la somme de sa partie entière et des parties associées aux facteurs irréductibles du dénominateur, on en déduit le résultat. □

3 Application au calcul intégral

On va voir ici comment la décomposition en éléments simples permet de calculer $\int^x R(t)\,\mathrm{d}t$, où $R \in \mathbb{K}(X)$.

3.1 Si $\mathbb{K} = \mathbb{C}$

C'est le cas le plus simple. On commence par décomposer R en éléments simples. Il suffit alors de savoir intégrer les polynômes ainsi que toute

fonction de la forme $t \mapsto \dfrac{1}{(t-\lambda)^k}$, avec $k \in \mathbb{N}^*$. Traitons différents cas :

Si $k = 1$ on sépare alors la partie réelle et la partie imaginaire de $\dfrac{1}{(t-\lambda)^k}$, puis on intègre. Si on note $\lambda = \alpha + i\beta$, cela donne :

$$\begin{aligned}\frac{1}{t-\lambda} &= \frac{t-\alpha+i\beta}{(t-\alpha)^2+\beta^2}\\ &= \frac{t-\alpha}{(t-\alpha)^2+\beta^2} + \frac{i\beta}{(t-\alpha)^2+\beta^2}\end{aligned}$$

Or

$$\int^x \frac{t-\alpha}{(t-\alpha)^2+\beta^2}\,\mathrm{d}t = \frac{1}{2}\ln\left((x-\alpha)^2+\beta^2\right)$$

et $\displaystyle\int^x \frac{\beta}{(t-\alpha)^2+\beta^2}\,\mathrm{d}t = \operatorname{Arctan}\left(\frac{x-\alpha}{\beta}\right)$

Si $k > 1$ alors

$$\int^x \frac{1}{(t-\lambda)^k}\,\mathrm{d}t = -\frac{1}{k-1}\times\frac{1}{(x-\lambda)^{k-1}}$$

3.2 Si $\mathbb{K} = \mathbb{R}$

Il s'agit de savoir intégrer d'une part les $\dfrac{1}{(t-\lambda)^k}$, ce qu'on sait déjà faire et d'autre part les termes de la forme $t \mapsto \dfrac{at+b}{(t^2+\beta t+\gamma)^n}$ où a, b, β et γ sont des constantes réelles, où n est un naturel non nul et où le polynôme $X^2+\beta X+\gamma$ n'admet pas de racine réelle.

On se limitera au cas où $n = 1$. Pour gérer les autres cas, on peut décomposer R en éléments simple dans $\mathbb{C}(X)$ et calculer l'intégrale par les méthodes données ci-dessus.

En posant $\Delta = \beta^2 - 4\gamma$, on a donc $\Delta < 0$.

On écrit alors

$$\frac{at+b}{t^2+\beta t+\gamma} = \frac{a}{2}\frac{2t+\beta}{t^2+\beta t+\gamma} + \frac{\gamma-\frac{a\beta}{2}}{t^2+\beta t+\gamma}$$

Le premier terme est un rapport de la forme u'/u :

$$\int^x \frac{a}{2}\frac{2t+\beta}{t^2+\beta t+\gamma}\,\mathrm{d}t = \frac{a}{2}\ln|x^2+\beta x+\gamma|$$

et la valeur absolue s'enlève sans problème car $X^2+\beta X+\gamma$ étant irréductible, il n'a pas de racine et est donc de signe constant.

Le second terme se réécrit quant à lui

$$\frac{b-\frac{a\beta}{2}}{t^2+\beta t+\gamma} = \frac{b-\frac{a\beta}{2}}{(t+\beta/2)^2+(\gamma-\beta^2/4)}$$

Or $\gamma - \beta^2/4 = -\Delta/4 = \left(\dfrac{1}{2}\sqrt{-\Delta}\right)^2$ car $\Delta < 0$.

En posant alors $\theta = \dfrac{1}{2}\sqrt{-\Delta}$, on a $\theta > 0$ et

$$\int^x \frac{b-\frac{a\beta}{2}}{(t+\beta/2)^2+\theta^2}\,\mathrm{d}t = \frac{b-\frac{a\beta}{2}}{\theta}\operatorname{Arctan}\left(\frac{x+\beta/2}{\theta}\right)$$

Chapitre XVII

Analyse asymptotique

1 Comparaison asymptotique de suites

Une première manière de comparer deux suites est de regarder si elles ont ou pas une limite, et si ces limites sont égales. Si deux suites n'ont pas la même limite, on peut dire que ces deux suites n'ont pas le même comportement. Mais si elles ont la même limite, on ne peut rien dire : exemple : $u_n = n$ et $v_n = \mathrm{e}^n$, 0, $1/n$ et $(-1)^n/n$. Même limite, mais pas du tout le même comportement. Pour une analyse plus fine, on utilise des outils de comparaison.

Dans tout cette section, (u_n), (v_n), (u'_n), (v'_n) et (w_n) sont des suites réelles.

1.1 Définitions : notations de Landau

Définition 1.1.1.
Soient (u_n) et (v_n) deux suites. Les définitions suivantes vont être données dans le cas particulier où (v_n) **ne s'annule pas**. Il existe des définitions plus générales des relations de comparaison, dans le cas où (v_n) s'annule, mais elles ne sont pas au programme.

(i) On dit que (u_n) est *dominée* par (v_n), ce qui se note $u_n = O(v_n)$, et se lit « (u_n) est un grand O de (v_n) », si la suite (u_n/v_n) est bornée.

(ii) On dit que (u_n) est *négligeable* devant (v_n), ce qui se note $u_n = o(v_n)$, et se lit « (u_n) est un petit o de (v_n) », si $u_n/v_n \to 0$.

Remarque 1.1.2.
• Petit o implique évidemment grand O.
• Une suite est un $O(1)$ si et seulement si elle est bornée, et est un $o(1)$ si et seulement si elle tend vers 0.
• À l'écrit, prenez soin de bien différentier les tailles de o et O.

Remarque 1.1.3.
On traduira souvent la relation $u_n = o(v_n)$ par : il existe une suite (ε_n) telle que

— $\varepsilon_n \xrightarrow[n\to+\infty]{} 0$;
— $\forall n \in \mathbb{N},\ u_n = \varepsilon_n v_n$.

Exemple 1.1.4. 1. $n = o(\mathrm{e}^n)$.
2. $0 = o(1/n)$.
3. $1/n = O((-1)^n/n)$.
4. $\sin n = O(1)$ et $1/n = o(1)$.
5. $v_n = \dfrac{n^4+n^2}{n+1}$ et $u_n = \dfrac{n^2+n}{n+2}$. On calcule u_n/v_n, ça tend vers 0.

Exemple 1.1.5.
Les croissances comparées vues lors du chapitre sur les suites peuvent se réécrire grâce au symbole o :
1. pour tous $\alpha, \beta \in \mathbb{R}$, si $\alpha < \beta$ alors $n^\alpha = o(n^\beta)$.
2. pour tous $\alpha, \beta, \gamma \in \mathbb{R}_+^*$, $\ln^\beta(n) = o(n^\alpha)$ et $n^\alpha = o(\mathrm{e}^{\gamma n})$.

 En accord avec l'hypothèse essentielle de la définition 1.1.1, écrire $u_n = o(0)$ ou $u_n = O(0)$ n'a aucun sens.

Remarque 1.1.6.
Une utilisation fondamentale des relations de comparaison repose sur l'écriture suivante : $u_n = v_n + o(w_n)$, qui signifie $u_n - v_n = o(w_n)$. L'égalité $u_n = v_n + o(w_n)$ exprime que v_n est une approximation de u_n, et que l'erreur de cette approximation est une quantité négligeable devant w_n. Cette égalité est intéressante si u_n est une suite « compliquée », que v_n est une suite « plus simple », et que w_n est elle-même « petite devant u_n et v_n ». Approcher une suite par une autre qui a un comportement plus difficile à étudier n'a en effet aucun intérêt, même si cela peut être tout à fait correct. De même que dire qu'un objet mesure environ 10 cm, au mètre près.

Exemple 1.1.7.
$\mathrm{e}^{1/n} = 1 + \dfrac{1}{n} + \dfrac{1}{2n^2} + o(1/n^2)$. Si on veut être plus précis, on écrit $\mathrm{e}^{1/n} = 1 + \dfrac{1}{n} + \dfrac{1}{2n^2} + \dfrac{1}{6n^3} + o(1/n^3)$, et on a bien $\dfrac{1}{6n^3} + o(1/n^3) = o(1/n^2)$. Attention,

écrire $\mathrm{e}^{1/n} = 1 + \frac{1}{n} + \frac{1}{2n^2} + \frac{1}{6n^3} + o(1/n^2)$ est juste mais n'apporte rien de plus que $\mathrm{e}^{1/n} = 1 + \frac{1}{n} + \frac{1}{2n^2} + o(1/n^2)$. Pire : $\mathrm{e}^{1/n} = 1 + \frac{1}{n} + \frac{1}{2n^2} + \frac{40000}{n^3} + o(1/n^2)$ est juste aussi !

Définition 1.1.8.
Soient (u_n) et (v_n) deux suites. Là encore la définition donnée n'est valable que dans le cas particulier où (v_n) **ne s'annule pas**.
On dit que (u_n) est *équivalente* à (v_n), ce qui se note $u_n \sim v_n$, si $u_n/v_n \to 1$.

 Là encore, $u_n \sim 0$ n'a aucun sens.

Remarque 1.1.9.
On traduira souvent la relation $u_n \sim v_n$ par : il existe une suite (ε_n) telle que
— $\varepsilon_n \xrightarrow[n\to+\infty]{} 1$;
— $\forall n \in \mathbb{N},\ u_n = \varepsilon_n v_n$.

Proposition 1.1.10.
Les propositions suivantes sont équivalentes :

(i) $u_n \sim v_n$
(ii) $u_n - v_n = o(v_n)$
(iii) $u_n = v_n + o(v_n)$
(iv) $v_n = u_n + o(u_n)$

Démonstration.
(i) implique (ii) : $u_n/v_n \to 1$ et $v_n/v_n \to 1$, donc $(u_n - v_n)/v_n \to 0$.
(ii) implique (i) : même raisonnement.
(iii) et (iv) ne sont que des reformulations des points précédents. □

Exemple 1.1.11.
• $1/n \sim 1/n + 1/n^2$.
• $n \not\sim \mathrm{e}^{n}$.
• On traduit la limite usuelle

$$\frac{\mathrm{e}^{1/n} - 1}{1/n} \xrightarrow[n\to+\infty]{} 1$$

par

$$\left[\mathrm{e}^{1/n} - 1\right] \sim \frac{1}{n}$$

ou, mieux, par

$$\mathrm{e}^{1/n} = 1 + \frac{1}{n} + o\left(\frac{1}{n}\right).$$

1.2 Opérations

a *o* et *O*

Théorème 1.2.1.
Soit $\lambda \in \mathbb{R}^*$, φ une extractrice.

(i) Multiplication par un réel non nul : si $u_n = o(v_n)$ alors $u_n = o(\lambda v_n)$ et $\lambda u_n = o(v_n)$.
(ii) Somme : si $u_n = o(v_n)$ et $w_n = o(v_n)$ alors $u_n + w_n = o(v_n)$.
 Ce sont des petits *o* de la même suite.
(iii) Transitivité : si $u_n = o(v_n)$ et $v_n = o(w_n)$, alors $u_n = o(w_n)$.
(iv) Produit 1 : si $u_n = o(v_n)$, alors $w_n u_n = o(w_n v_n)$.
(v) Produit 2 : si $u_n = o(v_n)$ et $u'_n = o(v'_n)$ alors $u_n u'_n = o(v_n v'_n)$.
(vi) Suites extraites : si $u_n = o(v_n)$ alors $u_{\varphi(n)} = o(v_{\varphi(n)})$.
(vii) Tout reste vrai en remplaçant les *o* par des grands *O*.

Démonstration.
Simple : revenir à la définition. □

 Deux opérations sur les *o* sont formellement INTERDITES :
• Sommer deux égalités en *o* si les suites dans les *o* ne sont pas les mêmes. Ex : $1/n = o(1)$ et $1/n = o(-1)$, mais $2/n \neq o(0)$.
• Composer une égalité en *o* par une fonction : $u_n = o(v_n) \not\Rightarrow f(u_n) = o(f(v_n))$. Ex : $f(x) = 1/x$, $1/n = o(1)$ mais $n \neq o(1)$. De même, $1/n^2 = o(1/n)$ mais $\mathrm{e}^{1/n^2} \neq o(\mathrm{e}^{1/n})$.

b Équivalents

Théorème 1.2.2.
Soit φ une extractrice.

(i) La relation $\sim$ est une relation d'équivalence (a : réflexive, b : symétrique, c : transitive).

(ii) Dans un petit o, on peut remplacer la suite par toute suite équivalente : si $u_n = o(v_n)$ et $v_n \underset{n\to+\infty}{\sim} w_n$, alors $u_n = o(w_n)$.

(iii) Deux suites équivalentes ont le même signe à partir d'un certain rang.

(iv) Produit : si $u_n \underset{n\to+\infty}{\sim} v_n$ et $u'_n \underset{n\to+\infty}{\sim} v'_n$ alors $u_n u'_n \underset{n\to+\infty}{\sim} v_n v'_n$.

(v) Passage à l'inverse : si $u_n \underset{n\to+\infty}{\sim} v_n$ alors $1/u_n \sim 1/v_n$.

(vi) Puissances : si $u_n \underset{n\to+\infty}{\sim} v_n$ et si $u_n > 0$ à partir d'un certain rang, alors pour tout $a \in \mathbb{R}$, $u_n^a \underset{n\to+\infty}{\sim} v_n^a$.

(vii) Suites extraites : si $u_n \underset{n\to+\infty}{\sim} v_n$ alors $u_{\varphi(n)} \underset{n\to+\infty}{\sim} v_{\varphi(n)}$.

Démonstration.
Simple : revenir aux définitions. □

 Trois opérations sur les équivalents sont INTERDITES :

• Sommer des équivalents. Ex : $n \underset{n\to+\infty}{\sim} n$, $-n+1 \underset{n\to+\infty}{\sim} -n$ mais $-1 \not\sim 0$.

• Composer par une fonction. Ex : $n^2 \underset{n\to+\infty}{\sim} n^2+n$ mais $\mathrm{e}^{n^2} \not\sim \mathrm{e}^{n+n^2}$.

• Élever un équivalent à une puissance dépendant de n : $1+\dfrac{1}{n} \sim 1$ mais $\left(1+\dfrac{1}{n}\right)^n \sim \mathrm{e}$. Remarquons que c'est un cas particulier de composition.

Théorème 1.2.3.
Soit $\ell \in \mathbb{R}$.

(i) $u_n \to \ell \in \mathbb{R}^*$ si et seulement si $u_n \underset{n\to+\infty}{\sim} \ell$.

(ii) Si $u_n \underset{n\to+\infty}{\sim} v_n$, alors (u_n) a une limite dans $\overline{\mathbb{R}}$ ssi (v_n) en a une aussi. Dans le cas d'existence de la limite, ces deux limites sont égales. La réciproque est fausse, sauf si $u_n \xrightarrow[n\to+\infty]{} \ell \in \mathbb{R}^*$.

Démonstration.
Simple : revenir aux définitions. □

 La réciproque de (**? ?**) est fausse. Ex : $n \to +\infty$, $n^2 \to +\infty$, $1/n \to 0$, $1/n^2 \to 0$. Pire : $u_n \not\sim u_{n+1}$ si $u_n = (1/2)^n$.

 Il est tentant d'utiliser les symboles $\sim$ et o à tort et à travers, ce qui mène souvent à de graves erreurs.

• Il est interdit de les utiliser simultanément.

• On s'interdira le plus souvent d'écrire une équivalence à une somme, on préfèrera dans ce cas l'écriture en o.

1.3 Exemples classiques (formulaire)

• Les exemples donnés dans le formulaire sont à connaître par cœur.

• Ne pas oublier l'hypothèse $u_n \xrightarrow[n\to+\infty]{} 0$.

• Les formules en $\underset{n\to+\infty}{\sim}$ ne sont pas des doublons de celles en o. Il est faux d'écrire $(1+u_n)^a \underset{n\to+\infty}{\sim} 1+au_n+o(u_n)$ et idiot d'écrire $(1+u_n)^a \underset{n\to+\infty}{\sim} 1+au_n$ (pourquoi ?).

Démonstration.
Démontrons les formules du formulaire.
La technique générale est la suivante : on part d'une fonction f définie et dérivable au voisinage de 0, et on utilise $f'(0) = \lim\limits_{t\to 0} \dfrac{f(t)-f(0)}{t}$, ce qui, en composant avec u_n donne $\dfrac{f(u_n)-f(0)}{u_n} = f'(0)+o(1)$, et finalement, $f(u_n) = f(0)+f'(0)u_n+o(u_n)$.
Pour cos et ch, une autre méthode est nécessaire : pour cos on utilise $\cos(2x) = 1-2\sin^2(x)$, et on l'applique à $x = \dfrac{u_n}{2}$.
Idem avec ch avec $\mathrm{ch}(2x) = 1+2\,\mathrm{sh}^2(x)$. □

Exemple 1.3.1.
Voici des exemples d'utilisation des relations d'équivalence :

• Donner un équivalent de $\left(\frac{\ln(n+1)}{\ln n}\right)^n - 1$.

• Calculer la limite de la suite $u_n = \left(2 - \cos\frac{1}{n}\right)^n$.

• Calculer la limite de $u_n = \mathrm{e}^{-n}\,\mathrm{ch}\,\sqrt[4]{n^4+1}$.

2 Comparaison de fonctions

Nous allons maintenant adapter les outils de la section précédente aux fonctions.

Dans toute cette section, I et J sont des intervalles de $\mathbb{R}$, $f, g, h, k : I \to \mathbb{R}$ sont quatre applications, et $a \in \bar{I}$.

2.1 Définitions

a o et O

Définition 2.1.1.
Encore une fois, nous supposons que la fonction g ne s'annule pas au voisinage de a, sauf éventuellement en a.

(i) On dit que f est *dominée par g au voisinage de a* , ce qui se note $f =_a O(g)$ ou $f(x) \underset{x\to a}{=} O(g(x))$, et se lit « f est un grand O de g au voisinage de a », si f/g est bornée au voisinage de a.
Cette définition se généralise au cas où f et g ne sont pas définies en a : il suffit de remplacer tous les I par des $I\backslash\{a\}$.

(ii) On dit que f est *négligeable devant g au voisinage de a* , ce qui se note $f =_a o(g)$ ou $f(x) \underset{x\to a}{=} o(g(x))$, et se lit « f est un petit o de g au voisinage de a », si $\lim\limits_a f/g = 0$.
Cette définition se généralise au cas où f et g ne sont pas définies en a : il suffit de remplacer tous les I par des $I\backslash\{a\}$.

Remarque 2.1.2.
Ces définitions sont les mêmes que pour les suites, à ceci près que pour des fonctions il faut spécifier un point au voisinage duquel ces relations sont valables. Pour les suites, il s'agissait toujours de $+\infty$.

Remarque 2.1.3.
Comme pour les suites, on traduira souvent $f \underset{x\to a}{=} o(g)$ par : il existe $\varepsilon : I \to \mathbb{R}$ vérifiant
— $\varepsilon(x) \xrightarrow[x\to a]{} 0$;
— $\forall x \in I,\ f(x) = \varepsilon(x)g(x)$.

Remarque 2.1.4.
• Comme pour les suites, $f =_a o(0)$ ou $f =_a O(0)$ n'ont pas de sens.
• Comme pour les suites, petit o implique O.
• $f =_a O(1)$ signifie que f est bornée au voisinage de a, et $f =_a o(1)$ signifie que $f \underset{a}{\to} 0$.

Exemple 2.1.5.
Fondamental : les croissances comparées s'expriment ainsi.
En $+\infty$:

1. Soient $\alpha, \beta \in \mathbb{R}$ tels que $\alpha < \beta$.
   Alors $x^\alpha \underset{x\to+\infty}{=} o(x^\beta)$.
2. Soient $a, b \in \mathbb{R}$ tels que $0 < a < b$.
   Alors $a^x \underset{x\to+\infty}{=} o(b^x)$.
3. Soient $\alpha, \beta \in \mathbb{R}$ avec $\alpha > 0$.
   Alors $(\ln x)^\beta \underset{x\to+\infty}{=} o(x^\alpha)$.
4. Soient $a, \alpha \in \mathbb{R}$ avec $a > 1$.
   Alors $x^\alpha \underset{x\to+\infty}{=} o(a^x)$.

En 0 :

1. Soient $\alpha, \beta \in \mathbb{R}$ tels que $\alpha < \beta$.
   Alors $x^\beta \underset{x\to0}{=} o(x^\alpha)$.
2. Soient $\alpha, \beta \in \mathbb{R}$ avec $\alpha > 0$.
   Alors $|\ln x|^\beta \underset{x\to0}{=} o(x^{-\alpha})$.
3. Soient $\alpha, \beta \in \mathbb{R}$ avec $\alpha > 0$.
   Alors $x^\alpha \underset{x\to0}{=} o\Big(|\ln x|^\beta\Big)$.

Exemple 2.1.6. 1. $x^2 \underset{x\to+\infty}{=} o(x^4)$, et $x^4 \underset{x\to0}{=} o(x^2)$.

2. $1/x^4 \underset{x\to+\infty}{=} o(1/x^2)$, et $1/x^2 \underset{x\to0}{=} o(1/x^4)$.

b Équivalents

Définition 2.1.7.
Nous supposons que la fonction g ne s'annule pas au voisinage de a, sauf éventuellement en a.
On dit que f est *équivalente à g au voisinage de a* , ce qui se note $f \sim_a g$ ou $f(x) \underset{x\to a}{\sim} g(x)$, et se lit « f est équivalente à g au voisinage de a », si $f/g \underset{a}{\to} 1$.
Cette définition se généralise au cas où f et g ne sont pas définies en a : il suffit de remplacer tous les I par des $I\backslash\{a\}$.

 $f \sim_a 0$ n'a pas de sens.

Remarque 2.1.8.
Comme pour les suites, on traduira souvent $f \underset{x\to a}{\sim} (g)$ par : il existe $\varepsilon : I \to \mathbb{R}$ vérifiant
— $\varepsilon(x) \xrightarrow[x\to a]{} 1$;
— $\forall x \in I,\ f(x) = \varepsilon(x)g(x)$.

Remarque 2.1.9.
Comme pour les suites, $\sim$ implique O.

Théorème 2.1.10.
$f \sim_a g$ si et seulement si $f - g =_a o(g)$ si et seulement si $f - g =_a o(f)$.

 Les propositions « $\lim\limits_{x\to a} \dfrac{f(x)}{g(x)} = 1$ » et « $(f(x) - g(x)) \xrightarrow[x\to a]{} 0$ » ne sont en aucun cas équivalentes : aucune n'implique l'autre ! Avec le théorème précédent, on voit en effet que $\dfrac{f(x)}{g(x)} \xrightarrow[x\to a]{} 1$ signifie $f - g \underset{x\to a}{=} o(g)$ tandis que $(f(x) - g(x)) \xrightarrow[x\to a]{} 0$ signifie $f - g \underset{x\to a}{=} o(1)$.
Par exemple, $x + 1 \underset{x\to+\infty}{\sim} x$, mais $(x+1) - x \underset{x\to+\infty}{\not\to} 0$.

Exemple 2.1.11. 1. $\dfrac{1}{x} \underset{x\to+\infty}{\sim} \dfrac{1}{x} + \dfrac{1}{x^2}$.

2. $x \underset{x\to+\infty}{\not\sim} \mathrm{e}^x$.

Théorème 2.1.12. (i) Si $f \sim_a g$, alors soit f et g ont toutes les deux une même limite dans $\overline{\mathbb{R}}$ en a, soit aucune des deux n'a de limite en a.
(ii) Si $f(x) \xrightarrow[x\to a]{} \ell \in \mathbb{R}^*$, alors $f(x) \underset{x\to a}{\sim} \ell$.

2.2 Opérations

a o et O

Théorème 2.2.1.
Soit $\lambda \in \mathbb{R}^*$.
(i) Multiplication par un réel non nul : si $f =_a o(g)$, alors $f =_a o(\lambda g)$ et $\lambda f =_a o(g)$.
(ii) Somme : si $f =_a o(g)$ et $h =_a o(g)$, alors $f + h =_a o(g)$.
 Ce sont des o de la même fonction.
(iii) Transitivité : si $f =_a o(g)$ et $g =_a o(h)$, alors $f =_a o(h)$.
(iv) Produit 1 : si $f =_a o(g)$, alors $fh =_a o(gh)$.
(v) Produit 2 : si $f =_a o(g)$ et $h =_a o(k)$, alors $fh =_a o(gk)$.
(vi) Composition **à droite** : si $b \in \bar{\mathbb{R}}$, et si φ est une fonction définie au voisinage de b à valeurs dans I et telle que $\varphi \underset{b}{\to} a$, alors si $f =_a o(g)$, on a aussi $f \circ \varphi =_b o(g \circ \varphi)$.
(vii) Tout ceci reste vrai en remplaçant les o par des grands O.

Démonstration.
Simple : revenir aux définitions. □

 Deux opérations sont formellement INTERDITES :

1. Les sommes des deux côtés : $f =_a o(g)$ et $h =_a o(k) \not\Rightarrow f + h =_a o(g + k)$.

2. La composition à gauche : si ψ est une application de $\mathbb{R}$ dans $\mathbb{R}$ $f =_a o(g) \not\Rightarrow \psi \circ f =_{\psi(a)} o(\psi \circ g)$. Par exemple $x^2 \underset{x\to 0}{=} o(x)$, mais $\mathrm{e}^{x^2} \underset{x\to 0}{\neq} o(\mathrm{e}^x)$.

Remarque 2.2.2.
Le point (vi) permet de faire des translations : par exemple, $x^4 \underset{x\to 0}{=} o(x^2)$ donc $(x-1)^4 \underset{x\to 1}{=} o((x-1)^2)$.
Il permet aussi de passer d'une relation au voisinage de 0 à une relation au voisinage de $\pm\infty$, et vice-versa. Par exemple, $x^5 \underset{x\to 0}{=} o(x)$ implique $\frac{1}{x^5} \underset{x\to+\infty}{=} o\left(\frac{1}{x}\right)$.

Remarque 2.2.3.
Comme avec les suites, écrire $f = g + o(h)$ signifie que $f - g = o(h)$. Cela permet de faire des développements, comme avec les suites.

b Équivalents

Théorème 2.2.4.
Soit $\lambda \in \mathbb{R}$.

(i) La relation $\sim$ est une relation d'équivalence (a : réflexive, b : symétrique, c : transitive).

(ii) Dans un petit o, on peut remplacer la fonction par toute fonction équivalente : si $f =_a o(g)$ et $g \sim_a h$, alors $f =_a o(h)$.

(iii) Deux fonctions équivalentes au voisinage de a ont le même signe sur un voisinage de a.

(iv) Produit : si $f \sim_a g$ et $h \sim_a k$, alors $fh \sim_a gk$.

(v) Inverse : si $f \sim_a g$, alors $\frac{1}{f} \sim_a \frac{1}{g}$.

(vi) Puissances : pour tout $\alpha \in \mathbb{R}$, si $f \sim_a g$ et si $f > 0$ au voisinage de a, alors $f^\alpha \sim_a g^\alpha$.

(vii) Composition **à droite** : si $b \in \bar{\mathbb{R}}$, et si φ est une fonction définie au voisinage de b à valeurs dans I et telle que $\varphi \underset{b}{\to} a$, alors si $f \sim_a g$, on a aussi $f \circ \varphi \sim_b g \circ \varphi$.

Démonstration.
Simple : revenir aux définitions. □


Trois opérations sont formellement INTERDITES :

1. Les sommes d'équivalents : $f \sim_a g$ et $h \sim_a k \not\Rightarrow f + h \sim_a g + k$.
2. La composition à gauche : si ψ est une application de $\mathbb{R}$ dans $\mathbb{R}$ $f =\sim_a g \not\Rightarrow \psi \circ f \sim \psi(a)\psi \circ g$. Par exemple $x \underset{x\to+\infty}{\sim} x+1$, mais $\mathrm{e}^x \underset{x\to+\infty}{\not\sim} \mathrm{e}^{x+1}$.
3. Élever un équivalent à une puissance dépendant de x (cas particulier de la composition à gauche) : $1 + x \underset{x\to 0}{\sim} 1$ mais $(1+x)^{1/x} \underset{x\to 0}{\sim} \mathrm{e}$

Exemple 2.2.5.
Donner la limite en 0 de $x \mapsto \dfrac{\ln(1+\tan(2x))}{\sin(4x)}$.

3 Développements limités

Nous allons maintenant utiliser les relations de comparaison dans un cas particulier : celui du développement limité, qui est une approximation d'une fonction en un point par un polynôme.

Dans tout ce chapitre, n est un entier naturel, I et J sont deux intervalles de $\mathbb{R}$, f est une fonction de I dans $\mathbb{R}$ et x_0 un point de I.

3.1 Définition et premières propriétés

Définition 3.1.1.
On dit que f admet un ***développement limité d'ordre n au voisinage d'un point*** $x_0 \in I$ s'il existe des réels $a_0 \dots a_n$ tels que

$$f(x) \underset{x\to x_0}{=} a_0 + a_1(x-x_0) + a_2(x-x_0)^2 + \dots + a_n(x-x_0)^n + o((x-x_0)^n).$$

On dit que le polynôme

$$a_0 + a_1(x-x_0) + a_2(x-x_0)^2 + \dots + a_n(x-x_0)^n$$

est la ***partie principale*** ou ***régulière*** du DL, et que le terme $o((x-x_0)^n)$ est son ***reste***.
L'écriture

$$f(x) \underset{x\to x_0}{=} (x-x_0)^p\Big(a_0 + a_1(x-x_0) + a_2(x-x_0)^2 + \ldots + a_n(x-x_0)^n + o((x-x_0)^n)\Big)$$

avec $a_0 \neq 0$ est appelée *forme normalisée* du DL, c'est aussi

$$f(x) \underset{x\to x_0}{=} a_0(x-x_0)^p + a_1(x-x_0)^{p+1} + a_2(x-x_0)^{p+2} + \ldots + a_n(x-x_0)^{p+n} + o((x-x_0)^{p+n}).$$

L'entier p est alors la *valuation* du DL : c'est le degré du premier terme non nul du DL.

Remarque 3.1.2.
Dans la suite on utilisera la notation « f admet un $\mathrm{DL}(x_0, n)$ » (ou $\mathrm{DL}_n(x_0)$) pour dire que f admet un DL d'ordre n en x_0.

 Cette notation n'a **rien** d'officiel et ne devra **en aucun cas** être utilisée ailleurs qu'en cours et en TD.

Exemple 3.1.3.
La fonction $x \mapsto \dfrac{1}{1-x}$ admet un $\mathrm{DL}(0,n)$ pour tout n, et l'on en connaît explicitement le reste, à savoir : $\dfrac{1}{1-x} \underset{x\to 0}{=} 1+x+x^2+x^3+\ldots+x^n+\dfrac{x^{n+1}}{1-x}$, et en 0 on a bien $\dfrac{x^{n+1}}{1-x} \underset{x\to 0}{=} o(x^n)$.

Remarque 3.1.4.
f admet un $\mathrm{DL}(x_0,n)$ si et seulement si $h \mapsto f(x_0+h)$ admet un $\mathrm{DL}(0,n)$. Autrement dit, en posant $h = x - x_0$, on peut toujours se ramener à un DL en zéro.

Remarque 3.1.5.
Si f admet un DL d'ordre n en x_0, et si $m \in \mathbb{N}$ est inférieur à n, alors f admet un DL d'ordre m en x_0. En effet, il suffit de ne garder que les termes de degré inférieur à m : on réalise ainsi une *troncature* du DL. En particulier, le premier terme non nul d'un DL fournit un équivalent de f.
Par exemple, si
$f(x) \underset{x\to x_0}{=} 2(x-x_0)^2 - (x-x_0)^3 + o((x-x_0)^3)$,
alors $f(x) \underset{x\to x_0}{\sim} 2(x-x_0)^2$.

Théorème 3.1.6 (unicité du DL)**.**
La partie principale d'un $\mathrm{DL}(x_0,n)$ de f est unique, c'est-à-dire : si $a_0 \ldots a_n$ et $b_0 \ldots b_n$ sont tels que

$$f(x) \underset{x\to x_0}{=} a_0 + a_1(x-x_0) + a_2(x-x_0)^2 + \ldots + a_n(x-x_0)^n + o((x-x_0)^n)$$
$$\text{et } f(x) \underset{x\to x_0}{=} b_0 + b_1(x-x_0) + b_2(x-x_0)^2 + \ldots + b_n(x-x_0)^n + o((x-x_0)^n)$$

alors $\forall i \in \{0,\ldots,n\},\ a_i = b_i$.

Démonstration.
En effet, en faisant la différence des deux développements, on a

$$(a_0-b_0) + (a_1-b_1)(x-x_0) + \ldots + (a_n-b_n)(x-x_0)^n = o((x-x_0)^n).$$

Si on considère le plus petit entier $k \in \{0,\ldots,n\}$ tel que $a_k \neq b_k$ alors, en divisant par $(x-x_0)^k$, on a

$$(a_k-b_k) + \sum_{i=k+1}^{n} (a_i-b_i)(x-x_0)^{i-k} = o(x-x_0)^{n-k}.$$

Par passage à la limite en x_0, $a_k = b_k$. □

Corollaire 3.1.7.
Si f est paire (resp. impaire) et admet un $\mathrm{DL}(0,n)$, alors la partie principale de ce DL est un polynôme pair (resp. impair).

Démonstration.
Traitons le cas où f est paire, le cas où f est impaire se traitant de la même manière. On a $f(x) \underset{x\to 0}{=} a_0 + a_1x + a_2x^2 + \ldots + a_nx^n + o(x^n)$.
En écrivant que $f(x) = f(-x)$, on obtient que $a_0 - a_1x + a_2x^2 - a_3x^3 + \ldots + (-1)^n a_n x^n + o(x^n)$ est aussi un $\mathrm{DL}(0,n)$ de f. Par unicité de ce DL, on peut identifier tous les coefficients, ce qui assure que les coefficients des termes de degré impair sont nuls. □

Théorème 3.1.8. (i) f est continue en x_0 ssi f admet un $\mathrm{DL}(x_0, 0)$. En effet, on a alors $f(x) \underset{x\to x_0}{=} f(x_0) + o(1)$. Le coefficient constant d'un $\mathrm{DL}(x_0, n)$ de f donne toujours la valeur de f en x_0.

(ii) f est dérivable en x_0 ssi f admet un $\mathrm{DL}(x_0, 1)$. En effet, si

$$f(x) \underset{x\to x_0}{=} f(x_0) + f'(x_0)(x - x_0) + o(x - x_0)$$

alors le coefficient du terme de degré 1 d'un $\mathrm{DL}(x_0, n)$ de f donne toujours la valeur de f' en x_0.

 **Attention** ! Les termes de degrés supérieurs ne donnent pas les dérivées suivantes de f. Et même pire : une fonction peut admettre un $\mathrm{DL}(x_0, 2)$ et ne pas être deux fois dérivable en x_0.

Exemple 3.1.9.

$$x \mapsto x^3 \mathbf{1}_{\mathbb{Q}}(x)$$

Exemple 3.1.10.

$$x \mapsto \begin{cases} x^3 \sin \frac{1}{x^3} & \text{si } x \neq 0 \\ 0 & \text{sinon} \end{cases}$$

Exemple 3.1.11.
Notons $f : \mathbb{R} \to \mathbb{R}$,
$$x \mapsto \begin{cases} \mathrm{e}^{-\frac{1}{x^2}} \sin\left(\mathrm{e}^{\frac{1}{x^2}}\right) & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases}$$
• Montrons que f admet un $\mathrm{DL}(0, n)$ pour tout n : on a $\left|\frac{f(x)}{x^n}\right| \leqslant \frac{\mathrm{e}^{-\frac{1}{x^2}}}{x^n} = \left(\frac{2}{nx^2}\mathrm{e}^{-\frac{2}{nx^2}}\right)^{\frac{n}{2}} \left(\frac{n}{2}\right)^{\frac{n}{2}}$. Or $u\mathrm{e}^{-u} \xrightarrow[u\to+\infty]{} 0$ donc $\frac{f(x)}{x^n} \xrightarrow[x\to 0]{} 0$, ce qui montre bien que $f(x) \underset{x\to 0}{=} o(x^n)$. f admet donc bien un DL en 0 à tout ordre, de partie principale nulle.
• Ceci implique donc que $f(0) = 0$ et $f'(0) = 0$. f est donc dérivable en 0, mais montrons que f' n'est pas continue en 0. Ainsi f n'est pas deux fois dérivable en 0. On calcule pour $x \neq 0$:

$$f'(x) = \frac{2f(x)}{x^3} - \frac{2}{x^3}\cos\left(\mathrm{e}^{\frac{1}{x^2}}\right)$$

D'après ce qui précède, $\frac{2f(x)}{x^3} \xrightarrow[x\to 0]{} 0$. Montrons que

$$\frac{2}{x^3}\cos\left(\mathrm{e}^{\frac{1}{x^2}}\right)$$

n'a pas 0 pour limite en 0 : ainsi on aura bien $f'(x) \underset{x\to 0}{\not\to} f'(0)$. Si l'on pose $u_n = \frac{1}{\sqrt{\ln(2n\pi)}}$, on a : $\frac{2}{u_n^3}\cos\left(\mathrm{e}^{\frac{1}{u_n^2}}\right) = \frac{2}{u_n^3} = \left(\ln(2n\pi)\right)^{\frac{3}{2}}$, qui a pour limite $+\infty$ quand n tend vers $+\infty$. On conclut avec l'argument de composition de limites.

3.2 Opérations sur les DL

Nous allons maintenant voir comment effectuer des opérations sur les DL. Le point délicat n'est pas tant d'effectuer les calculs, mais d'anticiper le degré du DL obtenu, connaissant les degrés des DL initiaux intervenant dans les calculs.
Au cours des calculs, plusieurs restes vont apparaître, mais à chaque étape, les restes les plus petits, ou les plus précis, s'effacent devant le reste dominant. C'est le degré de ce reste dominant qu'il faut savoir déterminer a fortiori.

a Somme

Proposition 3.2.1.
Si f et g admettent un DL en x_0, respectivement d'ordre n et m, alors $f + g$ admet un DL en x_0, d'ordre $\min(n, m)$, obtenu en faisant la somme des DL de f et g.

Démonstration.
Les parties principales des deux DL donnent un polynôme. À ce polynôme s'ajoutent deux restes : l'un d'ordre n et l'autre d'ordre m. C'est le plus petit exposant, *i.e.* $\min(n, m)$ qui désigne le reste dominant. □

 L'ordre du DL d'une somme est le min des ordres des deux DL. En additionnant un DL

d'ordre 3 à un DL d'ordre 2, on n'a aucune chance de récupérer un DL d'ordre 3 !

Exemple 3.2.2.
On a les DL suivants,

$$\begin{aligned}\cos(x) &\underset{x\to 0}{=} 1 \quad - \frac{1}{2}x^2 + o(x^2)\\ \exp(x) &\underset{x\to 0}{=} 1 + x + \frac{1}{2}x^2 + \frac{1}{6}x^3 + o(x^3)\\ &\underset{x\to 0}{=} 1 + x + \frac{1}{2}x^2 + o(x^2)\end{aligned}$$

donc on obtient de DL à l'ordre 2 :

$$\cos(x) + \exp(x) = 2 + x + o(x^2).$$

Remarque 3.2.3.
On prendra soin, en additionnant deux DL, d'aligner verticalement les termes de mêmes degrés.

b Produit

Étudions d'abord un cas particulier :

Proposition 3.2.4.
Soient f et g admettant chacune un DL en x_0, respectivement d'ordre n et m. Supposons que les termes constants de ces deux DL sont non nuls. Alors fg admet un DL en x_0, d'ordre exactement $\min(n,m)$, obtenu en faisant le produit des DL de f et g, dont on ne garde que les termes de degré inférieur à $\min(n,m)$.

Démonstration.
Lorsque l'on développe le produit de ces deux DL, il apparaît plusieurs restes. Parmi ces restes il y a le terme constant du DL de f fois le reste du DL de g, et le terme constant du DL de g fois le reste du DL de f. L'un de ces deux restes est forcément le terme dominant du DL du produit. □

Exemple 3.2.5.
Avec

$$\begin{aligned}f(x) &\underset{x\to 0}{=} 2 - x + 3x^2 + o(x^2)\\ g(x) &\underset{x\to 0}{=} 1 + 2x - 3x^2 + x^3 + o(x^3)\\ &\underset{x\to 0}{=} 1 + 2x - 3x^2 + o(x^2)\end{aligned}$$

on a

$$\begin{aligned}f(x)g(x) &\underset{x\to 0}{=} 2 + 4x - 6x^2 + o(x^2)\\ &\quad - x - 2x^2 + o(x^2)\\ &\quad + 3x^2 + o(x^2)\\ &\underset{x\to 0}{=} 2 + 3x - 5x^2 + o(x^2).\end{aligned}$$

Traitons maintenant le cas général :

Proposition 3.2.6.
Soient f et g admettant chacune un DL en x_0, respectivement d'ordre n et m, et de valuation p et q. Alors fg admet un DL en x_0, d'ordre exactement $\min(n-p, m-q)+p+q$ ($> \min(n,m)$ si p et q sont non nuls).

Démonstration.
Écrivons les formes normalisées des deux DL :

$$\begin{aligned}f(x) &\underset{x\to x_0}{=} (x-x_0)^p\Big(a_0 + a_1(x-x_0)\\ &\quad + a_2(x-x_0)^2 + \dots\\ &\quad + a_{n-p}(x-x_0)^{n-p} + o((x-x_0)^{n-p})\Big)\end{aligned}$$

et

$$\begin{aligned}g(x) &\underset{x\to x_0}{=} (x-x_0)^q\Big(b_0 + b_1(x-x_0)\\ &\quad + b_2(x-x_0)^2 + \dots\\ &\quad + b_{m-q}(x-x_0)^{m-q} + o((x-x_0)^{-q}m)\Big)\end{aligned}$$

Le produit de ces deux DL est donc

$$\begin{aligned}(x-x_0)^{p+q}\Big((a_0 + \dots + o((x-x_0)^{n-p})\\ (b_0 + \dots + o((x-x_0)^{m-q})\Big)\end{aligned}$$

Le DL entre les grandes parenthèses est le produit de deux DL dont les termes constants sont non nuls. Son degré est donc $\min(n-p, m-q)$ d'après 3.2.2. □

Exemple 3.2.7.
Avec $f(x) \underset{x\to 0}{=} x - 2x^2 + o(x^2)$ et $g(x) \underset{x\to 0}{=} x + x^2 + o(x^2)$, on a

$$\begin{aligned}f(x)g(x) &\underset{x\to 0}{=} x^2(1 - 2x + o(x))(1 + x + o(x))\\ &\underset{x\to 0}{=} x^2(1 - x + o(x))\\ &\underset{x\to 0}{=} x^2 - x^3 + o(x),\end{aligned}$$

qui est bien un DL d'ordre 3.

c Composition

Proposition 3.2.8.
Soit f admettant un $\mathrm{DL}(0,n)$, de partie principale F, dont le terme constant est nul, c'est-à-dire vérifiant $f(0)=0$, et soit g admettant un $\mathrm{DL}(0,n)$, de partie principale G. Alors $g\circ f$ admet un $\mathrm{DL}(0,n)$ dont la partie principale est $G\circ F$ dont on a retiré les termes de degré supérieur à n.

Démonstration.
On a $f(h) \underset{x\to 0}{=} F(h)+o(h^n)$ et : $g(k) \underset{x\to 0}{=} G(k)+o(k^n)$.
Un calcul simple (par exemple avec le binôme de Newton) assure que :

$$\forall k\in\mathbb{N},\ (F(h)+o(h^n))^k \underset{x\to 0}{=} (F(h))^k+o(h^n).$$

Sachant cela, on a :

$$\begin{aligned}(g\circ f)(h) &\underset{x\to 0}{=} g\Big(\underbrace{F(h)+o(h^n)}_{k}\Big)+o(k^n)\\ &\underset{x\to 0}{=} G\big(F(h)+o(h^n)\big)+o(k^n)\\ &\underset{x\to 0}{=} G(F(h))+o(h^n)+o(k^n).\end{aligned}$$

Or k se factorise par h, donc $k^n=o(h^n)$, d'où le résultat. □

Remarque 3.2.9.
Ce résultat s'étend tout à fait au cas où f admet un $\mathrm{DL}(x_0,n)$ avec $f(x_0)=a_0$, et où g admet un $\mathrm{DL}(a_0,n)$: il suffit alors de composer les DL en ne gardant que les termes de degré inférieur à n.

Exemple 3.2.10.
Trouver un $\mathrm{DL}(0,4)$ de $\mathrm{e}^{\cos x}$: on a

$$\cos x \underset{x\to 0}{=} 1-x^2/2+x^4/24+o(x^4)=1+X.$$

D'où

$$\mathrm{e}^{\cos x} \underset{x\to 0}{=} \mathrm{e}^{X} \underset{x\to 0}{=} \mathrm{e}\,(1+X+X^2/2+o(X^2)).$$

Il suffit en effet de s'arrêter au terme de degré 2 dans le DL de l'exponentielle, car $X\sim \dfrac{-1}{2}x^2$, donc les termes négligeables devant X^2 (le $o(X^2)$) seront négligeables devant x^4. On calcule alors, avec

$$X \underset{x\to 0}{=} \frac{-x^2}{2}+\frac{x^4}{24}+o(x^4),$$

et on obtient

$$\mathrm{e}^{\cos x} \underset{x\to 0}{=} \mathrm{e}\,(1-x^2/2+x^4/6)+o(x^4).$$

d Quotient

Traitons un premier cas :

Proposition 3.2.11.
Si g admet un $\mathrm{DL}(x_0,n)$ de valuation $p=0$ (ainsi le terme constant de g n'est pas nul), alors $1/g$ admet aussi un $\mathrm{DL}(x_0,n)$.

Démonstration.
On écrit
$g(x) \underset{x\to x_0}{=} b_0+b_1(x-x_0)+b_2(x-x_0)^2+\ldots+b_n(x-x_0)^n+o((x-x_0)^n) \underset{x\to x_0}{=} b_0(1-u)$ avec $u=-\dfrac{b_1(x-x_0)+b_2(x-x_0)^2+\ldots+b_n(x-x_0)^n+o((x-x_0)^n)}{b_0}$.
Il suffit de composer ce DL avec celui de $\dfrac{1}{1-u}$. □

Proposition 3.2.12.
Si f et g admettent un $\mathrm{DL}(x_0,n)$ et si le terme constant de g n'est pas nul, alors f/g admet aussi un $\mathrm{DL}(x_0,n)$.

Démonstration.
Il suffit de multiplier le $\mathrm{DL}(x_0,n)$ de f avec celui de $1/g$. □

Exemple 3.2.13.

$$\begin{aligned}\tan x =&\frac{\sin x}{\cos x}\\ =&\frac{x-x^3/6+x^5/120+o(x^5)}{1-x^2/2+x^4/24+o(x^5)}\\ =&\Big(x-x^3/6+x^5/120+o(x^5)\Big)\\ &\times\Big(1+u(x)+u(x)^2+o\Big(u(x)^3\Big)\Big)\\ &\text{où } u(x)=x^2/2-x^4/24+o(x^5)\end{aligned}$$

Il est inutile de calculer u^3 qui donnera des termes en x^6. En effet, $u(x) \underset{x\to 0}{\sim} \dfrac{x^2}{2}$, donc $o(u(x)^3)\subset$

$o(x^5)$. Donc

$$\begin{aligned}\tan x &\underset{x\to 0}{=} \left(x - \frac{x^3}{6} + \frac{x^5}{120} + o(x^5)\right) \\ &\quad \times \left(1 + \frac{x^2}{2} - \frac{x^4}{24} + \frac{x^4}{4} + o(x^5)\right) \\ &\underset{x\to 0}{=} x\left(1 - \frac{x^2}{6} + \frac{x^4}{120} + o(x^4)\right) \\ &\quad \times \left(1 + \frac{x^2}{2} - \frac{x^4}{24} + \frac{x^4}{4} + o(x^4)\right) \\ &\underset{x\to 0}{=} x + \frac{x^3}{3} + \frac{2x^5}{15} + o(x^5)\end{aligned}$$

Et le cas général :

Proposition 3.2.14.
Soit f admettant un DL en x_0 d'ordre n et de valuation p. Alors $1/f$ admet en x_0 un développement de la forme $\dfrac{P(x-x_0)+o((x-x_0)^{n-p})}{(x-x_0)^p}$, où P est un polynôme de terme constant non nul. Si $p>0$, ce développement est dit *asymptotique*.

Démonstration.
Il suffit d'écrire le DL de f sous forme normalisée : $f(x) = (x-x_0)^p.(F(x-x_0)+o((x-x_0)^{n-p})$, où F est un polynôme de terme constant non nul. Alors $1/f = \dfrac{1}{(x-x_0)^p}\cdot\dfrac{1}{F(x-x_0)+o((x-x_0)^{n-p})}$, et d'après **??**, $\dfrac{1}{F(x-x_0)+o((x-x_0)^{n-p})}$ admet un DL à l'ordre $n-p$, d'où l'existence du polynôme P de l'énoncé. Mais comme le terme constant de P n'est pas nul, si $p>0$, $\dfrac{P(x-x_0)}{(x-x_0)^p}$ n'est pas un polynôme mais une fraction rationnelle qui tend vers l'infini (en valeur absolue) en x_0, et le développement est dit asymptotique. □

Exemple 3.2.15.
Donner un développement de $\dfrac{1}{x^2+2x^3-x^4+o(x^5)}$ en 0.

3.3 Intégration et dérivation

Proposition 3.3.1.
Si f est continue et dérivable au voisinage de x_0 et si f' admet un DL(x_0,n), alors f admet un DL$(x_0,n+1)$ dont la partie principale est la primitive de la partie principale du DL de f' qui vaut $f(x_0)$ en x_0.

Démonstration.
Donnons la démonstration dans le cas $x_0=0$. On a

$$f'(x) \underset{x\to 0}{=} a_0 + a_1x + a_2x^2 + \ldots + a_nx^n + o(x^n)$$

Posons

$$\begin{array}{rccl} F: & I & \to & \mathbb{R} \\ & x & \mapsto & f(x) - f(0) - a_0x - \dfrac{a_1}{2}x^2 - \ldots - \dfrac{a_n}{n+1}x^{n+1} \end{array}$$

Alors $F(0)=0$ et

$$\forall x\in I \quad F'(x) = f'(x) - a_0 - a_1x - a_2x^2 - \ldots - a_nx^n$$

On a donc $F'(x) \underset{x\to 0}{=} o(x^n)$. En appliquant le TAF entre 0 et x on obtient : il existe $\theta_x \in]0,1[$ tel que

$$\begin{aligned} F(x) - F(0) &= xF'(\theta_x x) \\ \text{d'où } F(x) &\underset{x\to 0}{=} xo(\theta_x^n x^n) \\ \text{donc } F(x) &\underset{x\to 0}{=} o(x^{n+1}) \end{aligned}$$

On a donc

$$f(x) \underset{x\to 0}{=} f(0) + a_0x + \frac{a_1}{2}x^2 + \ldots + \frac{a_n}{n+1}x^{n+1} + o(x^{n+1})$$

□

Exemple 3.3.2.
Cette proposition permet de déterminer les DL de $\ln(1-x)$, $\ln(1+x)$ et $\operatorname{Arctan} x$, en primitivant les DL de $-1/(1-x)$, $1/(1+x)$ et $1/(1+x^2)$.

Proposition 3.3.3.
Si f admet un DL(x_0,n) **et si l'on sait que f' admet un DL**$(x_0,n-1)$ (par exemple parce que f est de classe $\mathscr{C}^n$), alors le DL de f' s'obtient en dérivant celui de f.

Exemple 3.3.4.
Dériver le DL de $\sqrt{1+x}$ redonne celui de $\dfrac{1}{\sqrt{1+x}}$.
Dériver celui de $\dfrac{1}{1+x}$ donne celui de $\dfrac{1}{(1+x)^2}$.

3.4 Formule de Taylor-Young

Théorème 3.4.1 (Formule de Taylor-Young)**.**
Si f est de classe $\mathscr{C}^n$ sur I, alors f possède un DL(x_0, n) donné par la formule de Taylor-Young :

$$f(x) \underset{x\to x_0}{=} \sum_{k=0}^{n} \frac{f^{(k)}(x_0)}{k!}(x-x_0)^k + o((x-x_0)^n),$$

soit

$$f(x) \underset{x\to x_0}{=} f(x_0) + f'(x_0)(x-x_0)\frac{f''(x_0)}{2}(x-x_0)^2 + \ldots + \frac{f^{(n)}(x_0)}{n!}(x-x_0)^n + o((x-x_0)^n).$$

Démonstration.
Démontrons le résultat par récurrence. Pour $n \in \mathbb{N}$, on note $P(n)$ l'assertion «$\forall f \in \mathscr{C}^n(I,\mathbb{R})\ f(x) \underset{x\to x_0}{=} \sum_{k=0}^{n} \frac{f^{(k)}(x_0)}{k!}(x-x_0)^k + o((x-x_0)^n)$».

$P(0)$ est vrai d'après les résultats sur les fonctions continues.

Montrons $\forall n \in \mathbb{N},\ P(n) \Rightarrow P(n+1)$.

Soit $n \in \mathbb{N}$, supposons $P(n)$. Montrons $P(n+1)$. Soit f de classe $\mathscr{C}^{n+1}$. Alors f' est de classe $\mathscr{C}^n$, et on puisqu'on a $P(n)$, on a

$$\begin{aligned} f'(x) &\underset{x\to x_0}{=} \sum_{k=0}^{n} \frac{(f')^{(k)}(x_0)}{k!}(x-x_0)^k + o((x-x_0)^n) \\ &\underset{x\to x_0}{=} \sum_{k=0}^{n} \frac{f^{(k+1)}(x_0)}{k!}(x-x_0)^k + o((x-x_0)^n) \end{aligned}$$

D'après la proposition 3.3.3, on a donc :

$$\begin{aligned} f(x) &\underset{x\to x_0}{=} f(x_0) + \sum_{k=0}^{n} \frac{f^{(k+1)}(x_0)}{(k+1)k!}(x-x_0)^{k+1} + o((x-x_0)^{n+1}) \\ &\underset{x\to x_0}{=} f(x_0) + \sum_{k=0}^{n} \frac{f^{(k+1)}(x_0)}{(k+1)!}(x-x_0)^{k+1} + o((x-x_0)^{n+1}) \\ &\underset{x\to x_0}{=} f(x_0) + \sum_{k=1}^{n+1} \frac{f^{(k)}(x_0)}{k!}(x-x_0)^{k} + o((x-x_0)^{n+1}) \\ &\underset{x\to x_0}{=} \sum_{k=0}^{n+1} \frac{f^{(k)}(x_0)}{k!}(x-x_0)^{k} + o((x-x_0)^{n+1}). \end{aligned}$$

□

Exemple 3.4.2.
La formule de Taylor-Young permet d'obtenir les DL des fonctions exp, sin, cos, $x \mapsto (1+x)^\alpha$, sh et ch.

Ils sont à savoir par cœur : vous les trouverez dans le formulaire déjà distribué.

3.5 Applications

a Calculs de limites et d'équivalents

Revenir sur la feuille de calcul de limites de suites : les équivalents permettent de déterminer efficacement ces limites. On remarquera que les factorisations effectuées alors reviennent à former ces équivalents !

Voici un équivalent célèbre.

Proposition 3.5.1 (Formule de Stirling)**.**
$n! \sim \sqrt{2n\pi}\left(\frac{n}{\mathrm{e}}\right)^n$.

b Allure d'une courbe au voisinage d'un point

Proposition 3.5.2.
Si f admet en x_0 un DL de la forme $f(x) = a_0 + a_1(x-x_0) + a_k(x-x_0)^k + o\Big((x-x_0)^k\Big)$, où $k \geqslant 2$ et a_k est *non nul*, alors f est dérivable en x_0, de dérivée a_1.

La tangente à sa courbe en $(x_0, f(x_0))$ a pour équation $y = a_1(x-x_0) + a_0$ et la position de sa courbe par rapport à cette tangente est donnée par le signe du terme $a_k(x-x_0)^k$.

Les quatres positions possibles au voisinage de x_0 sont illustrées dans les figures **??**, **??**, **??** et **??**.

En particulier, la courbe traverse la tangente (on dit qu'on a un point d'inflexion) si et seulement si k est impair.

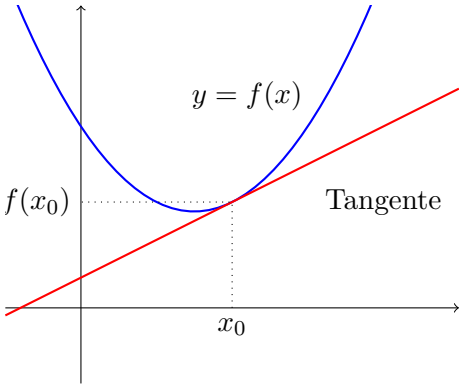


FIGURE XVII.1 – Cas k pair, $a_k > 0$

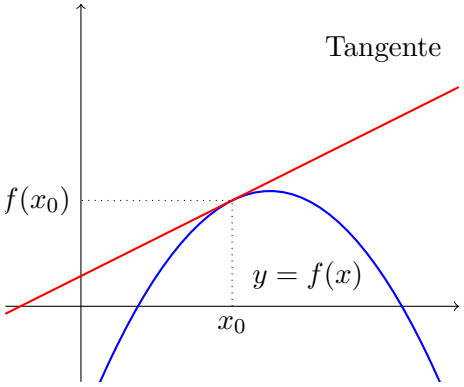


FIGURE XVII.2 – Cas k pair, $a_k < 0$

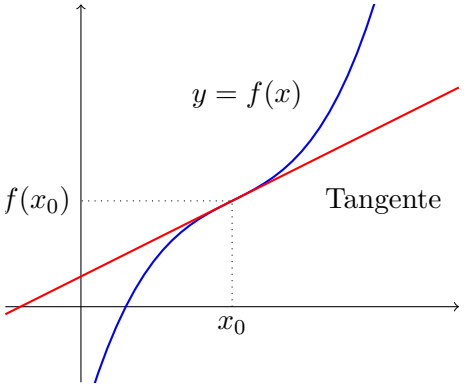


FIGURE XVII.3 – Cas k impair, $a_k > 0$

Exemple 3.5.3.
Considérer les applications $x \mapsto x^3$, $x \mapsto x^2$, $x \mapsto x^4$, sin, $x \mapsto x\cos x$ et $x \mapsto x(1+\sin^3 x)$ en 0

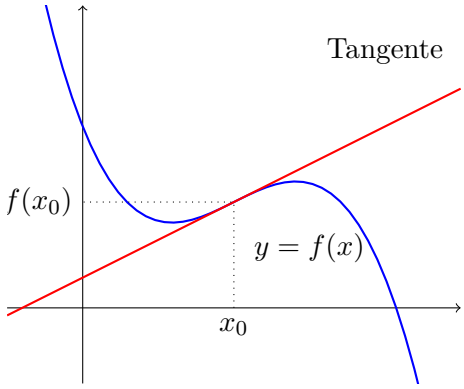


FIGURE XVII.4 – Cas k impair, $a_k < 0$

Corollaire 3.5.4.
Si f, de classe $\mathscr{C}^2$ admet un point d'inflexion en x_0, on a nécessairement $f''(x_0) = 0$.

Remarque 3.5.5.
On pourra regarder ce que donne cette condition sur les exemples précédents. En particulier, on verra clairement que la réciproque est fausse.

Nous savons déjà que si f a un extremum local en a, alors $f'(a) = 0$, mais la réciproque est fausse. Allons plus loin, en utilisant la proposition 3.5.2 :

Corollaire 3.5.6.
Soit f telle que $f'(a) = 0$. Si $f''(a) \neq 0$, f a un extremum local en a.

Démonstration.
$f'(a) = 0$, donc la tangente de f en a est horizontale. De plus la première dérivée non nulle en a est d'ordre 2, donc le graphe de f, dans un certain voisinage de a, est en-dessous ou au -dessus de la tangente en a. Ceci s'écrit : (pour tout t dans ce voisinage, $f(t) \geqslant f(a)$) ou (pour tout t dans ce voisinage, $f(t) \leqslant f(a)$). Donc f a un extremum local en a. □

c Prolongement de fonction

On considère une fonction f non définie en a mais définie au voisinage épointée de a.

Proposition 3.5.7.
Soit $n \in \mathbb{N}$. Si f admet un développement limité d'ordre n en a, alors elle est prolongeable par continuité en a en une fonction $\hat{f}$ et la valeur de $\hat{f}$ en a est le terme constant du développement limité de f. De plus, $\hat{f}$ admet en a le même développement limité que f.

Corollaire 3.5.8.
En particulier si f admet un DL d'ordre au moins 1 en a, alors $\hat{f}$ est dérivable en a.

Exercice 3.5.9.
Étudier la fonction f en 0 (continuité, dérivabilité, position) :

$$f(t) = \frac{1}{t} - \frac{1}{\sin t}$$

d Développements asymptotiques

Nous avons déjà vu dans la Proposition 3.2.12 de la Partie 3.2.9 un exemple de développement asymptotique.
Plus généralement, un développement asymptotique a ceci en commun avec un DL d'être une approximation d'une fonction, que l'on présente également comme une somme de fonctions, allant de la plus « grosse » à la plus « petite », et d'un reste, négligeable devant tous les autres termes de la somme. C'est ce que l'on appelle une *échelle de comparaison*. Ces fonctions sont de nature quelconque, alors qu'un DL ne contient que des termes polynomiaux (on travaille avec des échelles de comparaisons polynomiales).

Exemple 3.5.10.
Dans l'échelle de comparaison $\left\{x \mapsto x^k, k \in \mathbb{Z}\right\}$, ordonnée par l'ordre usuel au voisinage de $+\infty$, on peut écrire :

$$\begin{aligned}\frac{3x^2+2}{x-1} &\underset{x\to+\infty}{=} 3x + \frac{3x+2}{x-1} = 3x + o(x)\\ &\underset{x\to+\infty}{=} 3x + 3 + \frac{5}{x-1} = 3x + 3 + o(1)\\ &\underset{x\to+\infty}{=} 3x + 3 + \frac{5}{x} + o\left(\frac{1}{x}\right).\end{aligned}$$

Notamment,

$$\frac{5}{x-1} = \frac{5}{x} \times \frac{1}{1-\frac{1}{x}} \underset{x\to+\infty}{=} \frac{5}{x}(1+o(1)) \underset{x\to+\infty}{=} \frac{5}{x} + o\left(\frac{1}{x}\right).$$

Exemple 3.5.11.
Dans l'échelle de comparaison $\left\{x \mapsto x^\alpha \ln^\beta x,\ (\alpha,\beta) \in \mathbb{R}^2\right\}$ au voisinage de $+\infty$, ordonnée par l'ordre lexicographique sur (α, β), on peut écrire en développant le carré :

$$\begin{aligned}&\left(x + \ln x + \frac{1}{\ln x}\right)^2\\ &\underset{x\to+\infty}{=} x^2 + o(x)\\ &\underset{x\to+\infty}{=} x^2 + 2x\ln x + o(x\ln(x))\\ &\underset{x\to+\infty}{=} x^2 + 2x\ln x + 2\frac{x}{\ln x} + o\left(\frac{x}{\ln x}\right).\end{aligned}$$

e Branche infinie d'une courbe $y = f(x)$

Principe : écrire un développement asymptotique de f au voisinage de l'infini, en général en exprimant $f(x)$ en fonction de $1/x$:

Exercice 3.5.12.
Étudier les branches infinies de

$$\begin{array}{rccc} f: & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & \dfrac{x^2-x+2}{x+1}\mathrm{e}^{-\frac{1}{x}} \end{array}.$$

4 Théorèmes de comparaison pour les séries

Proposition 4.0.1.
Soit (u_n) une suite à valeurs positives et $S_n = \sum_{k=0}^{n} u_k$. Alors la suite (S_n) est croissante et converge donc si et seulement si elle est majorée.

Démonstration.
Tout simplement, $S_{n+1} - S_n = u_{n+1} \geqslant 0$. □

Proposition 4.0.2.
Soient (u_n) et (v_n) deux suites réelles telles que pour tout $n \in \mathbb{N}$, $0 \leqslant u_n \leqslant v_n$.

(i) Si $\left(\sum_{n=0}^{N} v_n\right)_{N\in\mathbb{N}}$ converge, alors $\left(\sum_{n=0}^{N} u_n\right)_{N\in\mathbb{N}}$ également et

$$0 \leqslant \lim_{N\to+\infty} \sum_{n=0}^{N} u_n \leqslant \lim_{N\to+\infty} \sum_{n=0}^{N} v_n.$$

(ii) Si $\left(\sum_{n=0}^{N} u_n\right)_{N\in\mathbb{N}}$ diverge, alors $\left(\sum_{n=0}^{N} v_n\right)_{N\in\mathbb{N}}$ également.

Démonstration.
Il suffit de remarquer que si $(S_n) = \left(\sum_{n=0}^{N} u_n\right)_{N\in\mathbb{N}}$ et $(S'_n) = \left(\sum_{n=0}^{N} v_n\right)_{N\in\mathbb{N}}$, alors pour tout $n \in \mathbb{N}$, $0 \leqslant S_n \leqslant S'_n$.

(i) (S'_n) converge, donc est majorée, donc (S_n) est également majorée, et comme elle est croissante, elle converge également. Il reste alors à passer à la limite dans la relation $0 \leqslant S_n \leqslant S'_n$.

(ii) c'est le théorème de minoration.

□

Remarque 4.0.3.
La condition de positivité des suites est **PRIMORDIALE**. Considérer par exemple les suites constantes $u_n = -1$ et $v_n = 0$.

Remarque 4.0.4.
Si la comparaison n'est valide qu'à partir d'un certain rang, le résultat de convergence est toujours vrai, mais pas la comparaison des limites.

Exercice 4.0.5.
En considérant $u_n = \dfrac{1}{n(n+1)}$ et $v_n = \dfrac{1}{(n+1)^2}$, montrer que $\left(\sum_{n=0}^{N} \dfrac{1}{(n+1)^2}\right)_{N\in\mathbb{N}}$ converge et majorer sa limite.

Corollaire 4.0.6.
Soient (u_n) et (v_n) deux suites réelles **positives**, (v_n) ne s'annulant pas à partir d'un certain rang.

(i) Si $u_n = O(v_n)$, alors la convergence de $\left(\sum_{n=0}^{N} v_n\right)_{N\in\mathbb{N}}$ entraîne celle de $\left(\sum_{n=0}^{N} u_n\right)_{N\in\mathbb{N}}$.

(ii) Si $u_n = o(v_n)$, alors la convergence de $\left(\sum_{n=0}^{N} v_n\right)_{N\in\mathbb{N}}$ entraîne celle de $\left(\sum_{n=0}^{N} u_n\right)_{N\in\mathbb{N}}$.

(iii) Si $u_n \sim v_n$ (donc (u_n) ne s'annule pas à partir d'un certain rang), alors $\left(\sum_{n=0}^{N} v_n\right)_{N\in\mathbb{N}}$ et $\left(\sum_{n=0}^{N} u_n\right)_{N\in\mathbb{N}}$ sont de même nature.

Démonstration. (i) $\dfrac{u_n}{v_n}$ est bornée par un certain réel $M > 0$, donc à partir d'un certain rang, $0 \leqslant u_n \leqslant Mv_n$ car (u_n) et (v_n) sont positives. On conclut donc avec 4.0.14.

(ii) si $u_n = o(v_n)$, alors en particulier $u_n = O(v_n)$.

(iii) si $u_n \sim v_n$, alors $u_n = O(v_n)$ et $v_n = O(u_n)$.

□

Exemple 4.0.7.
Puisque $\sin\left(\dfrac{1}{2^n}\right) \sim \dfrac{1}{2^n}$, d'après le résultat sur les séries géométriques, $\left(\sum_{n=0}^{N} \sin\left(\dfrac{1}{2^n}\right)\right)_{N\in\mathbb{N}}$ converge.

Pour pouvoir utiliser le dernier corollaire, nous avons besoin de « séries étalon » dont la nature est bien connue, et auxquelles on compare les séries à étudier. Les quelques exemples déjà étudiés font partie de ces séries de référence standard, mais la famille de séries la plus utilisée est celle des *séries*

de Riemann, dont font partie la *série harmonique* et la série $\left(\sum_{n=0}^{N} \frac{1}{(n+1)^2}\right)_{N\in\mathbb{N}}$.

Théorème 4.0.8.
Soit $\alpha \in \mathbb{R}$. La suite $\left(\sum_{n=1}^{N} \frac{1}{n^\alpha}\right)_{N\in\mathbb{N}}$ converge si et seulement si $\alpha > 1$.

Démonstration.
Si $\alpha = 1$, remarquons que $\frac{1}{n} \sim \ln(n+1) - \ln n$. Donc $\left(\sum_{n=1}^{N} \frac{1}{n^\alpha}\right)_{N\in\mathbb{N}}$ est de même nature que $\left(\sum_{n=1}^{N} (\ln(n+1) - \ln n)\right)_{N\in\mathbb{N}}$, qui elle-même est de même nature que la suite $(\ln n)$ par sommation télescopique, d'où la divergence.

Si $\alpha \neq 1$, $\frac{1}{n^\alpha} \sim \frac{1}{\alpha-1}\left(\frac{1}{n^{\alpha-1}} - \frac{1}{(n+1)^{\alpha-1}}\right)$ (effectuer un développement asymptotique de $\frac{1}{n^{\alpha-1}} - \frac{1}{(n+1)^{\alpha-1}}$ ou appliquer l'inégalité des accroissements finis à $x \mapsto x^{1-\alpha}$). La série de terme général $\frac{1}{n^{\alpha-1}} - \frac{1}{(n+1)^{\alpha-1}}$ est de même nature que la suite $\left(\frac{1}{n^{\alpha-1}}\right)$, d'où le résultat. □

Chapitre XVIII

Espaces vectoriels

Dans tout ce chapitre, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. L'important est que $\mathbb{K}$ soit un corps, mais le programme se limite à $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

1 Espaces vectoriels et combinaisons linéaires

1.1 Définitions

Définition 1.1.1.
On appelle $\mathbb{K}$-*espace vectoriel* ou *espace vectoriel sur* $\mathbb{K}$ (noté $\mathbb{K}$-ev) tout triplet $(E, +, \cdot)$ où E est un ensemble muni d'une loi interne $+$ appelée addition et d'une loi externe $\cdot$, i.e. une application $\cdot : \mathbb{K} \times E \to E$, vérifiant :

(i) $(E, +)$ est un groupe commutatif dont le neutre est noté 0 ;

(ii) En notant 1 (ou $1_{\mathbb{K}}$) le neutre de $\mathbb{K}$ pour la multiplication, on a : $\forall x \in E \quad 1 \cdot x = x$;

(iii) $\forall (\lambda, \mu) \in \mathbb{K}^2 \quad \forall x \in E \quad (\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$ (distributivité à droite) ;

(iv) $\forall \lambda \in \mathbb{K} \quad \forall x, y \in E \quad \lambda \cdot (x+y) = \lambda \cdot x + \lambda \cdot y$ (distributivité à gauche) ;

(v) $\forall \lambda, \mu \in \mathbb{K} \quad \forall x \in E \quad (\lambda \times \mu) \cdot x = \lambda \cdot (\mu . x)$ (associativité mixte).

Les éléments de E sont appelés *vecteurs*, et ceux de $\mathbb{K}$ sont appelés *scalaires*.

Remarque 1.1.2.
Les vecteurs mathématiques étant des objets mathématiques comme les autres, on ne les marquera plus d'une flèche comme c'est traditionnellement l'usage dans les petites classes (cet usage est d'ailleurs réservé à la géométrie euclidienne, alors qu'on verra de nombreux exemples d'espaces vectoriels où les vecteurs ne sont ni ceux du plan, ni ceux de l'espace euclidien).

Remarque 1.1.3.
On ommet souvent, pour alléger les notations, de noter le $\cdot$ de la multiplication scalaire. Ainsi, on pourra écrire λx au lieu de $\lambda \cdot x$, pour un scalaire λ et un vecteur x.

Exemple 1.1.4.
1. L'ensemble des vecteurs du plan euclidien, celui des vecteurs de l'espace euclidien, ou de façon équivalente [1] $(\mathbb{R}^2, +, \cdot)$ et $(\mathbb{R}^3, +, \cdot)$, d'où les mots «vecteur» et «scalaire». De manière générale, tous les $\mathbb{R}^n$.
2. $(\mathbb{R}, +, \times)$ est un $\mathbb{R}$-espace vectoriel. Remarquez que la loi $\times$ est à la fois loi interne et externe sur $\mathbb{R}$ (c'est aussi un $\mathbb{Q}$-espace vectoriel).
3. $(\mathbb{C}, +, \times)$ est à la fois un $\mathbb{C}$-espace vectoriel et un $\mathbb{R}$-espace vectoriel (et également un $\mathbb{Q}$-espace vectoriel).
4. $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$ ne sont pas des espaces vectoriels ni sur $\mathbb{R}$ ni sur $\mathbb{C}$ avec les opérations usuelles [2].
5. $\mathbb{R}[X]$, $\mathbb{C}[X]$, $\mathbb{R}(X)$ et $\mathbb{C}(X)$ sont des espaces-vectoriels (sur quels corps ?)
6. $\mathscr{M}_{n,p}(\mathbb{K})$ est un $\mathbb{K}$-ev.

Remarque 1.1.5.
Tout $\mathbb{C}$-espace vectoriel est aussi un $\mathbb{R}$-espace vectoriel. La réciproque fausse : $\mathbb{R}$ n'est pas un $\mathbb{C}$-espace vectoriel, du moins pas avec les lois usuelles [3]

Dans toute la suite, $(E, +, \cdot)$ désigne un $\mathbb{K}$-ev.

1.2 Règles de calcul

Théorème 1.2.1 (Règles de calcul)**.**
Soit $\lambda \in \mathbb{K}$ et $x \in E$.

(i) $\lambda \cdot x = 0_E \Leftrightarrow \lambda = 0_{\mathbb{K}}$ ou $x = 0_E$ et, en particulier, $0_{\mathbb{K}} \cdot x = 0_E$ et $\lambda \cdot 0_E = 0_E$.

(ii) $-x = (-1) \cdot x$ (l'opposé de x dans $(E, +)$ est égal à l'opposé de 1 dans $(\mathbb{K}, +, \times)$ multiplié par x).

1. Il conviendrait, en anticipant un peu, de dire plutôt : «de façon isomorphe».
2. En fait, c'est même vrai quelle que soit la loi qu'on essaie d'y définir. Pourquoi ?
3. Il y aurait moyen d'en définir une, qui serait complètement «tordue» en utilisant le fait que $\mathbb{R}$ et $\mathbb{C}$ peuvent être mis en bijection mais ça n'aurait vraisemblablement aucun intérêt.

Démonstration. (i) (a) Remarquons tout d'abord qu'on a $0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x$ et donc par simplification dans $(E,+)$, donc $0 \cdot x = 0$.

(b) Remarquons ensuite qu'on a $\lambda \cdot 0 = \lambda(0+0) = \lambda \cdot 0 + \lambda \cdot 0$, d'où $\lambda \cdot 0 = 0$.

(c) On en déduit $\lambda = 0_{\mathbb{K}}$ ou $x = 0_E \Rightarrow \lambda \cdot x = 0_E$.

(d) Réciproquement, supposons $\lambda \cdot x = 0$. Alors, si $\lambda \neq 0$, on a $x = 1 \cdot x = \left(\lambda \times \frac{1}{\lambda}\right) \cdot x = \frac{1}{\lambda} \cdot (\lambda.x) = \frac{1}{\lambda} \cdot 0 = 0$

(ii) On a $x + (-1) \cdot x = 1 \cdot x + (-1) \cdot x = (1-1) \cdot x = 0 \cdot x = 0$. Donc $(-1) \cdot x$ est bien l'opposé de x dans $(E,+)$. □

1.3 Exemples

Théorème 1.3.1 (Espace vectoriel produit)**.** Soient $n \in \mathbb{N}^*$ et $(E_1, +_1, \cdot_1) \dots (E_n, +_n, \cdot_n)$ des $\mathbb{K}$-ev. On considère l'ensemble produit $E = E_1 \times \dots \times E_n$ que l'on munit des deux lois $+ : E \times E \to E$ et $\cdot : \mathbb{K} \times E \to E$ définies, par les relations suivantes pour toutes familles $(x_k)_{k \in [\![1,n]\!]}$ et $(y_k)_{k \in [\![1,n]\!]}$ et tout $\lambda \in \mathbb{K}$:

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 +_1 y_1, \dots, x_n +_n y_n)$$
$$\lambda \cdot (x_1, \dots, x_n) = (\lambda \cdot_1 x_1, \dots, \lambda \cdot_n x_n)$$

Alors, $(E, +, \cdot)$ est un $\mathbb{K}$-ev appelé *espace vectoriel produit.*

Démonstration.
Il suffit de vérifier les 5 points de la définition d'espace vectoriel :

(i) $(E,+)$ est un groupe (cf. exercices sur les groupes produits vu en TD), et commutatif car tous les E_i le sont.

(ii) Soit $(x_1, \dots, x_n) \in E$, on a $1 \cdot (x_1, \dots, x_n) = (1 \cdot_1 x_1, \dots, 1 \cdot_n x_n) = (x_1, \dots, x_n)$.

(iii) Soit $(\lambda, \mu) \in \mathbb{K}^2$, $(x_1, \dots, x_n) \in E$. En posant

$$z = (\lambda + \mu) \cdot (x_1, \dots, x_n)$$

on a successivement :

$$\begin{aligned} z &= ((\lambda+\mu) \cdot_1 x_1, \dots, (\lambda+\mu) \cdot_n x_n) \\ &= (\lambda \cdot_1 x_1 + \mu \cdot_1 x_1, \dots, \lambda \cdot_n x_n + \mu \cdot_n x_n) \\ &= (\lambda \cdot_1 x_1, \dots, \lambda \cdot_n x_n) + (\mu \cdot_1 x_1, \dots, \mu \cdot_n x_n) \\ &= \lambda \cdot (x_1, \dots, x_n) + \mu \cdot (x_1, \dots, x_n). \end{aligned}$$

(iv) Soit $\lambda \in \mathbb{K}$, $(x_1, \dots, x_n) \in E$ et $(y_1, \dots, y_n) \in E$. En posant

$$z = \lambda \cdot (x_1 +_1 y_1, \dots, x_n +_n y_n)$$

on a successivement :

$$\begin{aligned} z &= (\lambda \cdot (x_1 +_1 y_1), \dots, \lambda.(x_n +_n y_n)) \\ &= (\lambda \cdot_1 x_1 +_1 \lambda \cdot_1 y_1, \dots, \lambda \cdot_n x_n +_n \lambda \cdot_n y_n) \\ &= (\lambda \cdot_1 x_1, \dots, \lambda \cdot_n x_n) + (\lambda \cdot_1 y_1, \dots, \lambda \cdot_n y_n) \\ &= \lambda \cdot (x_1, \dots, x_n) + \lambda \cdot (y_1, \dots, y_n). \end{aligned}$$

(v) Soit $(\lambda, \mu) \in \mathbb{K}^2$ et $(x_1, \dots, x_n) \in E$. On a successivement :

$$\begin{aligned} (\lambda \times \mu) \cdot (x_1, \dots, x_n) &= ((\lambda \times \mu) \cdot_1 x_1, \dots, (\lambda \times \mu) \cdot_n x_n) \\ &= (\lambda \cdot_1 (\mu \cdot_1 x_1), \dots, \lambda \cdot_n (\mu \cdot_n x_n)) \\ &= \lambda \cdot (\mu \cdot_1 x_1, \dots, \mu \cdot_n x_n) \\ &= \lambda \cdot [\mu \cdot (x_1, \dots, x_n)]. \end{aligned}$$

□

Remarque 1.3.2.
Cas particuliers :

1. Déjà vu : $\mathbb{R}^2$.
2. Se généralise à tous les $\mathbb{R}^n$, $n \in \mathbb{N}^*$. Exemple de calcul dans $\mathbb{R}^6$.

Théorème 1.3.3 (Espaces d'applications)**.** Soit X un ensemble non vide et E un $\mathbb{K}$-ev. On considère $\mathscr{F} = E^X$, que l'on munit de deux lois :

$$+ : \left\{ \begin{array}{ccc} \mathscr{F} \times \mathscr{F} & \longrightarrow & \mathscr{F} \\ (f,g) & \longmapsto & \left\{ \begin{array}{ccc} X & \to & E \\ x & \mapsto & f(x) + g(x) \end{array} \right. \end{array} \right.$$

et

$$\cdot : \left\{ \begin{array}{ccc} K \times \mathscr{F} & \longrightarrow & \mathscr{F} \\ (\lambda, f) & \longmapsto & \left\{ \begin{array}{ccc} X & \to & E \\ x & \mapsto & \lambda \cdot (f(x)) \end{array} \right. \end{array} \right. .$$

Alors $(\mathscr{F}, +, \cdot)$ est un $\mathbb{K}$-ev.

Démonstration.
Il suffit de vérifier les 5 points de la définition d'ev. On a déjà vu que $(E^X, +)$ était un groupe commutatif. Le lecteur saura vérifier les points (ii) à (v). □

Exemple 1.3.4. 1. Soit I un intervalle, alors $(\mathbb{R}^I, +, \times)$ est un $\mathbb{R}$-espace vectoriel, $(\mathbb{C}^I, +, \times)$ est à la fois un $\mathbb{R}$-espace vectoriel et un $\mathbb{C}$-espace vectoriel.

2. L'ensemble des suites à valeurs réelles $\mathbb{R}^{\mathbb{N}}$ est un $\mathbb{R}$-espace vectoriel, celui des suites à valeurs complexes est à la fois un $\mathbb{R}$-espace vectoriel et un $\mathbb{C}$-espace vectoriel.

1.4 Combinaisons linéaires

Définition 1.4.1.
Soient $u_1, \dots, u_n$ des vecteurs de E, avec $n \in \mathbb{N}$. On appelle *combinaison linéaire* de $u_1, \dots, u_n$ tout vecteur de la forme $u = \sum_{k=1}^{n} \lambda_k \cdot u_k = \lambda_1 \cdot u_1 + \dots + \lambda_n \cdot u_n$, avec $\lambda_1, \dots, \lambda_n \in \mathbb{K}$.

Par convention la combinaison linéaire de 0 vecteur vaut 0_E.

Exemple 1.4.2. 1. 0 est toujours combinaison linéaire de deux vecteurs quelconques u et v car $0_E = 0_{\mathbb{K}} u + 0_{\mathbb{K}} v$.

2. Décomposition dans une base dans le plan ou l'espace.

Remarque 1.4.3.
Attention : il n'y a pas nécessairement unicité des λ_i. Exemple :

$$(1,1) = 1 \cdot (1,0) + 1 \cdot (1,3) + 1 \cdot (-1,-2)$$
$$(1,1) = \frac{1}{2} \cdot (1,0) + 0 \cdot (1,3) - \frac{1}{2} \cdot (-1,-2)$$

Exemple 1.4.4.
Exemples menant, comme souvent, à la résolution d'un système :

1. $(3,-3,0)$ est-il combinaison linéaire de $(1,0,0)$, $(0,-1,2)$ et $(1,0,-3)$?
2. $(-1,2,3)$ est-il combinaison linéaire de $(1,1,0)$ et $(-1,1,3)$?

Remarque 1.4.5.
Pour la deuxième question, on sait y répondre avec le déterminant. Pour l'instant ce n'est possible que pour les vecteurs du plan mais bientôt... (à suivre).

On peut généraliser la définition précédente au cas des familles quelconques.

Définition 1.4.6.
Soit I un ensemble $(x_i)_{i\in I}$ une famille de vecteurs indexées par I. On appelle *combinaison linéaire* de la famille $(x_i)_{i\in I}$ tout vecteur de la forme

$$\sum_{i\in I} \lambda_i \cdot x_i$$

où $(\lambda_i)_{i\in I}$ est une famille de scalaire à **support fini** c'est-à-dire telle que l'ensemble des $i \in I$ tels que $\lambda_i \neq 0$ **soit fini**.

Exemple 1.4.7.
Quelles sont les combinaisons linéaires de la famille $\left(X^k\right)_{k\in\mathbb{N}}$ dans $\mathbb{R}[X]$? et de la famille $\left(X^{2k}\right)_{k\in\mathbb{N}}$ dans $\mathbb{R}[X]$?

Remarque 1.4.8. 1. La somme de deux combinaisons linéaires d'une même famille est encore une combinaison linéaire de cette famille.

2. Le produit par un scalaire d'une combinaison linéaire d'une famille est encore une combinaison linéaire de cette famille.

2 Sous-espaces vectoriels

Dorénavant, nous ommetrons d'écrire le $\cdot$ de la multiplication scalaire.

2.1 Définitions

Définition 2.1.1.
Soit $F \subset E$. On dit que F est un *sous-espace vectoriel* (sev) de E si :

(i) $0 \in F$;

(ii) F est stable par combinaisons linéaires quelconques de deux vecteurs, *i.e.* pour tout $\lambda, \mu \in \mathbb{K}$, et pour tous $x, y \in F$, $\lambda x + \mu y \in F$.

Remarque 2.1.2.
Il est clair que tout sous-espace vectoriel est stable par multiplication externe ainsi que par l'addition.

Par récurrence, on en déduit que, pour tout $n \in \mathbb{N}$, toute combinaison linéaire de n vecteurs d'un sous-espace vectoriel appartient encore à ce sous-espace vectoriel. Donc tout sous-espace vectoriel est stable par toute combinaison linéaire de ses vecteurs.

Proposition 2.1.3.
Soit $F \subset E$. Toutes les propositions suivantes sont équivalentes :

(i) F est un sous-espace vectoriel de E ;

(ii) F est non vide, stable par addition et par multiplication externe ;

(iii) F est un sous-groupe de E stable par multiplication externe ;

(iv) F est non vide et $\forall \lambda, \mu \in \mathbb{K} \quad \forall (x,y) \in F^2 \quad \lambda x + \mu y \in F$;

(v) $O_E \in F$ et $\forall \lambda, \mu \in \mathbb{K} \quad \forall (x,y) \in F^2 \quad \lambda x + \mu y \in F$;

Remarque 2.1.4.
On remplace aussi parfois les propositions (**? ?**) et (**? ?**) par, respectivement,

$$F \neq \varnothing \text{ et } \forall \lambda \in \mathbb{K} \quad \forall (x,y) \in F^2 \quad \lambda x + y \in F$$

ainsi que

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

Démonstration.
On remarque successivement :

(i) ⇒ (ii) Il suffit de prendre $\lambda = 1$ pour la stabilité par addition et $y = 0$ pour la stabilité par multiplication externe.

(ii) ⇒ (iii) Supposons (ii). Alors F est stable par multiplication externe, donc en particulier $\forall x \in E \quad (-1).x \in E$. Donc F est stable par opposé. Par ailleurs, F est non vide et stable par addition, c'est donc un sous-groupe de E.

(iii) ⇒ (iv) Supposons (iii). Alors F est un sous-groupe donc n'est pas vide. Soit $\lambda, \mu \in \mathbb{K}$ et $(x,y) \in F^2$. F est stable par multiplication externe, donc $\lambda x \in F$ et $\mu \in F$. F est un sous-groupe de E, donc $\lambda x + \mu y \in F$.

(iv) ⇒ (v) Supposons (iv). Alors F est non vide et contient donc un élément x_0, donc contient 0_E car $0_E = (-1) \cdot x_0 + x_0$. On en déduit (v).

(v) ⇒ (i) Supposons (v). Alors, pour tout $(x,y) \in F^2$, $x + y = 1x + 1y$ donc F est stable par addition. Et pour tout $x \in E$ et tout $\lambda \in \mathbb{K}$, $\lambda x = \lambda x + 0 \cdots 0_E$, donc F est stable par multiplication externe. On en déduit (i).

□

Remarque 2.1.5.
En pratique pour montrer qu'un sous-ensemble de E est un sous-espace vectoriel, on utilisera (iv) ou (v), qui est généralement le plus rapide à démontrer.

Exemple 2.1.6.
E et $\{0\}$ sont des sev de E, dits *triviaux*.

Exemple 2.1.7.
L'ensemble des solutions d'une équation différentielle linéaire homogène dont la variable est une fonction de I dans $\mathbb{R}$ est un sev de $\mathbb{R}^I$.

Théorème 2.1.8.
Soit F un sous-ensemble de E. Alors F muni des lois induites de E est un $\mathbb{K}$-espace vectoriel si et seulement si F est un sous-espace vectoriel de E.

Démonstration.
— Supposons que F muni des lois de E soit un $\mathbb{K}$-espace vectoriel. Alors $(F,+)$ est un groupe abélien donc c'est un sous-groupe de $(F,+)$. De plus, F est stable par multiplication externe, donc c'est bien un sous-espace vectoriel de F.

— Réciproquement, si F est un sous-espace vectoriel de E, on sait qu'il s'agit d'un sous-groupe de $(E,+)$, donc $(F,+)$ est un groupe abélien. De plus, F est stable par multiplication externe, donc la multiplication externe de E induit bien une multiplication externe sur F. On peut aisément vérifier que les propriétés (ii) à (v) des espaces vectoriels sont alors vérifiées par les lois induites sur F.

□

Remarque 2.1.9.
En pratique, pour montrer qu'un ensemble est un espace vectoriel, il est plus rapide de montrer que c'est un sous-espace vectoriel d'un espace vectoriel plus gros : on le fera donc quasiment **TOUJOURS**, et l'on ne reviendra presque **JAMAIS** à la définition complète.

2.2 Exemples

Exemples géométriques :

Droites dans $\mathbb{R}^2$ Soient $(a, b, c) \in \mathbb{R}^3$, avec $(a, b) \neq (0, 0)$. À quelle condition la droite d'équation $ax+by = c$ est-elle un sous-espace vectoriel de $\mathbb{R}^2$?

Plans dans $\mathbb{R}^3$ Même question pour un plan d'équation $ax + by + cz + d = 0$.

Cercles dans $\mathbb{R}^2$ Même question pour un cercle dans le plan.

Exemples avec polynômes et fractions rationnelles : quels sont les liens entre $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}[X]$, $\mathbb{C}[X]$, $\mathbb{R}(X)$ et $\mathbb{C}(X)$?

2.3 Opérations sur les sous-espaces vectoriels

Dans toute la suite du chapitre, F et G sont deux sous-espaces vectoriels de E.

a Intersection

Théorème 2.3.1. 1. $F \cap G$ est un sous-espace vectoriel de E.

2. $F \cup G$ est un sous-espace vectoriel de E si et seulement si $F \subset G$ ou $G \subset F$.

Démonstration. 1. On a évidemment $0 \in F \cap G$. On vérifie aisément que pour tout $(x, y) \in (F \cap G)^2$ et tout $\lambda \in \mathbb{K}$, on a $\lambda x + y \in F \cap G$.

2. Si un des deux espaces vectoriels est inclus dans l'autre, alors $F \cup G$ est trivialement un sous-espace vectoriel de E.

   Supposons à l'inverse qu'aucun des deux sous-espaces vectoriels ne soit inclus dans l'autre et montrons qu'alors $F \cup G$ n'est pas un sous-espace vectoriel. $F \setminus G$ contient au moins un élément x, et $G \setminus F$ au moins un élément y. Posons alors $z = x + y$. Si z appartenait à F, on aurait $y = z - x \in F$ ce qui n'est pas le cas. De même, on ne peut avoir $z \in G$. Donc $z \notin F \cup G$, donc $F \cup G$ n'est pas stable par addition.

□

Exemple 2.3.2.
Dans l'espace, toute droite passant par 0 est l'intersection de deux plans passant par 0, donc est un sous-espace vectoriel.

Cette propriété se généralise en fait à une intersection d'une famille quelconque de sous-espaces vectoriels :

Théorème 2.3.3.
Soit $(F_i)_{i\in I}$ (resp. $\mathscr{F}$) une famille (resp. un ensemble) de sous-espaces vectoriels de E. Alors

$$\bigcap_{i\in I} F_i \quad \text{resp.} \quad \bigcap_{F\in\mathscr{F}} F$$

est un sous-espace vectoriel de E.

Démonstration.
Remarquons que le cas de l'intersection d'un ensemble se traite comme le cas particulier d'une famille : il s'agit de l'intersection de la famille des $(F_i)_{F\in I}$ où $I = \mathscr{F}$ et pour tout $G \in I$, $F_G = G$.

La démonstration s'effectue alors comme la précédente. Notons F l'intersection des F_i pour $i \in I$.

1. On a évidemment $0 \in F_i$ pour tout $i \in I$, donc $0 \in F$.
2. Pour tout $(x, y) \in \mathbb{F}^2$ et tout $\lambda \in \mathbb{K}$, on a successivement :

$$\begin{aligned} \forall i \in I \quad & (x, y) \in F_i^2 \\ \forall i \in I \quad & \lambda x + y \in F_i^2 \\ & \lambda x + y \in \bigcap_{i\in I} F_i \end{aligned}$$

□

Un exemple important d'intersection a priori infinie est donnée dans la partie suivante.

b Sous-espace vectoriel engendré par une partie

Définition 2.3.4 (Sous-espace vectoriel engendré par une partie)**.**
Soit X une partie (quelconque) du $\mathbb{K}$-espace vectoriel E. On appelle $\mathbb{K}$-*sous-espace vectoriel engendré par* X et on note $\mathrm{Vect}_{\mathbb{K}}(X)$ (ou $\mathrm{Vect}(X)$ lorsqu'il n'y a pas d'ambiguïté) le plus petit sous-espace vectoriel de E contenant X (« plus petit » est à entendre au sens de l'inclusion).

Démonstration.
Cette définition présuppose qu'un tel sous-espace existe et

qu'il est unique. L'unicité sous réserve d'existence du plus petit élément d'un ensemble muni d'une relation d'ordre est connue. Montrons l'existence.

Notons $\mathscr{F}$ l'ensemble des F tels que :

1. F est un sous-espace vectoriel de E ;
2. et $X \subset F$.

On veut montrer que cet ensemble $\mathscr{F}$ possède un plus petit élément pour l'inclusion.

Posons alors

$$V = \bigcap_{F \in \mathscr{F}} F$$

et montrons que V est ce plus petit élément.

Pour cela montrons tout d'abord $V \in \mathscr{F}$.

Pour tout $F \in \mathscr{F}$, on a $X \subset F$, donc

$$X \subset \bigcap_{F \in \mathscr{F}} F = V$$

De plus, V est une intersection de sous-espaces vectoriels de E donc c'est un sous-espace vectoriel de E.

Donc on a $V \in \mathscr{F}$.

Il suffit donc maintenant de montrer que V est un minorant de $\mathscr{F}$, c'est-à-dire que pour tout $F \in \mathscr{F}$, on a $V \subset F$.

Soit $F \in \mathscr{F}$. On a

$$V = \bigcap_{G \in \mathscr{F}} G$$

donc tout élément de V appartient à tout élément de $\mathscr{F}$, donc en particulier à F. On a donc $V \subset F$.

V minore donc $\mathscr{F}$ pour l'inclusion.

V est donc un élément de $\mathscr{F}$ qui minore $\mathscr{F}$: c'est donc son plus petit élément. □

Remarque 2.3.5. 1. Tout sous-espace vectoriel de E contenant X contient donc $\mathrm{Vect}(X)$.

2. Si F est un sous-espace vectoriel de E, alors F est le plus petit sous-espace vectoriel contenant F, donc $\mathrm{Vect}(F) = F$.

Remarque 2.3.6.
Soit I un ensemble et $(x_i)_{i \in I}$ une famille de vecteurs de E. On notera $\mathrm{Vect}\left((x_i)_{i \in I}\right)$ le sous-espace $\mathrm{Vect}\left(\{\, x_i \mid i \in I \,\}\right)$. En particulier si I est de la forme $[\![1, n]\!]$, on notera $\mathrm{Vect}\left(x_1, \ldots, x_n\right)$ le sous-espace $\mathrm{Vect}\left(\{\, x_1, \ldots, x_n \,\}\right)$.

Le procédé de construction de $\mathrm{Vect}(X)$ présenté plus haut est très élégant et peut s'utiliser dans de nombreuses situations. En revanche, il est assez peu concret. Heureusement, le théorème suivant nous dit très précisément ce que contient $\mathrm{Vect}(X)$.

Théorème 2.3.7.
Soit X une partie de E. Alors $\mathrm{Vect}(X)$ est exactement l'ensemble de toutes les combinaisons linéaires d'éléments de X. Autrement dit :

1. Pour tout $n \in \mathbb{N}$, toute combinaison linéaire d'éléments de X appartient à $\mathrm{Vect}(X)$.
2. Pour tout élément x de $\mathrm{Vect}(X)$, il existe une famille de coefficients $(\lambda_\alpha)_{\alpha \in X}$ à support fini telle qu'on a

$$x = \sum_{\alpha \in X} \lambda_\alpha \alpha.$$

Dit autrement : il existe un entier $n \in \mathbb{N}$, des vecteurs $u_1, \ldots, u_n$ de X ($\forall k \in [\![1, n]\!], u_k \in X$) et des scalaires $\lambda_1, \ldots, \lambda_n$ tels qu'on a

$$x = \sum_{k=1}^{n} \lambda_k u_k.$$

Démonstration.
Notons V l'ensemble des combinaisons linéaires d'éléments de X.

Pour montrer $V = \mathrm{Vect}(X)$, nous allons montrer que V est le plus petit sous-espace vectoriel de E contenant X.

1. V est un sous-espace vectoriel de E. En effet :
   (a) il contient 0_E (combinaison linéaire de 0 vecteur de X) ;
   (b) il est stable par addition car la somme d'une combinaison linéaire de p vecteurs de X et d'une combinaison linéaire de q vecteurs de X est une combinaison linéaire (d'au plus) $p + q$ vecteurs de X ;
   (c) il est stable par multiplication par un scalaire car le produit par un scalaire λ d'une combinaison linéaire de n vecteurs de X est la combinaison linéaire de ces mêmes vecteurs où les coefficients ont tous été multiplié par λ.
2. V contient X. En effet pour tout $x \in X$, x est la combinaison linéaire $1 \cdot x$, donc appartient à V. Donc $X \subset V$.
3. V minore l'ensemble des sous-espaces vectoriels de E contenant X. En effet, soit F un sous-espace vectoriel de E contenant X. Montrons $V \subset F$.
   Soit $x \in V$ alors x est combinaison linéaire d'éléments de X. Or F contient X et est un sous-espace-vectoriel donc est stable par combinaison linéaire. Il contient donc x en particulier. On a donc $\forall x \in V \quad x \in F$.

Donc $V \subset F$.

Donc V est le plus petit sous-espace vectoriel de E contenant X. □

Remarque 2.3.8.
En particulier, pour toute famille de vecteurs finie de $x_1, \ldots, x_n$, $\mathrm{Vect}(x_1, \ldots, x_n)$ est l'ensemble

$$\left\{ \sum_{k=1}^{n} \lambda_k x_k \;\middle|\; (\lambda_1, \ldots, \lambda_k) \in \mathbb{K}^n \right\}.$$

Exemple 2.3.9. 1. Pour $\alpha \in \mathbb{R}$, on note

$$f_\alpha : \left\{ \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \mathrm{e}^{\alpha x} \end{array} \right. .$$

Alors $\mathrm{Vect}\left((f_\alpha)_{\alpha\in\mathbb{R}}\right)$ est un sous-espace vectoriel de $\mathbb{R}^{\mathbb{R}}$ qui contient les fonctions sh, ch mais pas sin ni þ (indication : il suffit de remarquer que les seules fonctions bornées de ce sous-espace vectoriel sont les fonctions constantes).

2. En géométrie dans $\mathbb{R}^2$, si $(\overrightarrow{\imath}, \overrightarrow{\jmath})$ est une base, tout vecteur de $\mathbb{R}^2$ est combinaison linéaire de $\overrightarrow{\imath}$ et $\overrightarrow{\jmath}$, donc $\mathbb{R}^2 = \mathrm{Vect}(\overrightarrow{\imath}, \overrightarrow{\jmath})$.
3. Dans $\mathbb{R}^3$, si $\mathscr{D}$ est une droite vectorielle de vecteur directeur u, alors $\mathscr{D} = \{ \lambda u \mid u \in \mathbb{K} \} = \mathrm{Vect}(u)$. Si $\mathscr{P}$ est un plan vectoriel de vecteurs directeurs $u = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}$ et $v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}$, alors en écrivant une équation paramétrique de $\mathscr{P}$, on voit que tout point P de l'espace est dans $\mathscr{P}$ si et seulement s'il existe $t_1, t_2 \in \mathbb{R}$ tel que $P = t_1 u + t_2 v$, donc $\mathscr{P} = \mathrm{Vect}(u, v)$. Exemple avec $2x - y + z = 0$.
4. $\mathbb{R} = \mathrm{Vect}_{\mathbb{R}}(1)$ et $\mathbb{C} = \mathrm{Vect}_{\mathbb{C}}(1) = \mathrm{Vect}_{\mathbb{R}}(1, i)$.
5. $E = (\mathscr{F}(\mathbb{R}, \mathbb{R}), +, .)$ est un ev. On note les fonctions suivantes, définies sur $\mathbb{R}$ par exp : $x \mapsto \mathrm{e}^{\,x}$; $\widetilde{\exp} : x \mapsto e^{-x}$; $f : x \mapsto x\sin(2x)$ et $g : x \mapsto x\sin(3x)$. Avec $F = \mathrm{Vect}(\exp, \widetilde{\exp})$ et $G = \mathrm{Vect}(f, g)$, on a $\mathrm{ch} \in F$ mais $\sin \notin G$.
6. L'ensemble des solutions de l'équation différentielle $y'' + y' - 2y = 0$ est $\mathrm{Vect}(f, g)$ avec $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto \mathrm{e}^{-2x}$ et $g = \exp$.

Proposition 2.3.10.
Soit X et Y deux parties de E. Alors :

1. $X \subset Y \Rightarrow \mathrm{Vect}(X) \subset \mathrm{Vect}(Y)$;
2. $\mathrm{Vect}(\mathrm{Vect}(X)) = \mathrm{Vect}(X)$.

Démonstration. 1. Supposons $X \subset Y$. Alors $X \subset Y \subset \mathrm{Vect}(Y)$. Donc $\mathrm{Vect}(Y)$ est un sous-espace vectoriel de E contenant X donc contient $\mathrm{Vect}(X)$.

2. Posons $F = \mathrm{Vect}(X)$. F est un sous-espace vectoriel de E. Donc d'après la remarque faite plus haut, $\mathrm{Vect}(F) = F$.

□

c Somme

Définition 2.3.11.
On appelle *somme de F et G* l'ensemble de E noté $F+G$ défini par $F+G = \{ x + y \mid x \in F, y \in G \}$.

Théorème 2.3.12. (i) $F + G$ est un sev de E ;

(ii) $F + G$ est le plus petit sev qui contient F et G : $F + G = \mathrm{Vect}(F \cup G)$.

Démonstration. (i) Immédiat.

(ii) Montrons d'abord que $F \subset F + G$: soit $f \in F$. alors $f = f + 0$, et $0 \in G$, donc $f \in F + G$. On montre bien sûr de même que $G \subset F + G$. On a donc $(F \cup G) \subset (F + G)$.

Il suffit ensuite de montrer que pour tout sous-espace vectoriel H de E contenant $F \cup G$, on a $(F+G) \subset H$.

Soit H un sous-espace vectoriel de E. Supposons $F \subset H$ et $G \subset H$. Montrons $(F + G) \subset H$.

Soit $z \in F + G$. Alors il existe $x \in F$ et $y \in G$ vérifiant $z = x + y$. On a alors $x \in H$ et $y \in H$ donc $x + y \in H$, donc $z \in H$.

Donc $F + G \subset H$.

□

Remarque 2.3.13.
Si $A = F + G$ et $a \in A$, il n'y a pas forcément unicité de la décomposition $a = f + g$, avec $f \in F$ et $g \in G$, loin de là ! Considérer par exemple le cas $F + F$.

Exemple 2.3.14.
Si $F \subset G$, alors $F + G = G$.

 $F + G \neq F \cup G$ (sauf si $F \subset G$ ou $G \subset F$).

Exemple 2.3.15.
Soit $\mathscr{D}$ et $\mathscr{D}'$ deux droites du plan passant par 0 et non confondues. Alors $\mathbb{R}^2 = \mathscr{D} + \mathscr{D}'$.

Proposition 2.3.16.
1. Soit X et Y des parties de E. Alors $\text{Vect}(X) + \text{Vect}(Y) = \text{Vect}(X \cup Y)$.
2. Étant donnés deux sous-espaces vectoriels F_1 et F_2 de E, on a $F_1 + F_2 = F_2 + F_1 = \text{Vect}(F_1 \cup F_2)$.
3. Étant donnés trois sous-espaces vectoriels F_1, F_2 et F_3 de E, on a $F_1 + (F_2 + F_3) = (F_1 + F_2) + F_3 = \text{Vect}(F_1 \cup F_2 \cup F_3)$
4. Étant donnés $n \in \mathbb{N}^*$ et $F_1, \ldots, F_n$ des sous-espaces vectoriels de E, la façon de parenthéser l'expression de $F_1 + \ldots + F_n$ n'a pas d'importance et

$$F_1 + \ldots + F_n = \text{Vect}(F_1 \cup \ldots \cup F_n).$$

Démonstration.
1. $\text{Vect}(X \cup Y)$ est un espace vectoriel contenant $X \cup Y$, donc contient X. Or tout espace vectoriel contenant X contient $\text{Vect}(X)$, donc $\text{Vect}(X \cup Y)$ contient $\text{Vect}(X)$. De même, il contient $\text{Vect}(Y)$. $\text{Vect}(X \cup Y)$ est donc un espace vectoriel contenant les deux sous-espaces vectoriels $\text{Vect}(X)$ et $\text{Vect}(Y)$, donc il contient leur somme. On a donc $\text{Vect}(X) + \text{Vect}(Y) \subset \text{Vect}(X \cup Y)$.
   Par ailleurs, $\text{Vect}(X) + \text{Vect}(Y)$ contient $\text{Vect}(X)$, donc contient X. De même, il contient Y. Il contient donc $X \cup Y$. Or $\text{Vect}(X) + \text{Vect}(Y)$ est un sous-espace vectoriel, donc il contient $\text{Vect}(X \cup Y)$. On a donc $\text{Vect}(X \cup Y) \subset \text{Vect}(X) + \text{Vect}(Y)$.
   On a donc $\text{Vect}(X \cup Y) = \text{Vect}(X) + \text{Vect}(Y)$.
2. En remarquant que $\text{Vect}(F_i) = F_i$ pour $i = 1, 2$, on a :

$$\begin{aligned} F_1 + F_2 &= \text{Vect}(F_1) + \text{Vect}(F_2) \\ &= \text{Vect}(F_1 \cup F_2) \\ &= \text{Vect}(F_2 \cup F_1) \\ &= F_2 + F_1. \end{aligned}$$

3. De même :

$$\begin{aligned} F_1 + (F_2 + F_3) &= \text{Vect}(F_1) + \text{Vect}(F_2 \cup F_3) \\ &= \text{Vect}(F_1 \cup F_2 \cup F_3) \\ &= \text{Vect}(F_1 \cup F_2) + \text{Vect}(F_3) \\ &= (F_1 + F_2) + F_3. \end{aligned}$$

4. Ce point se démontre par récurrence sur le nombre de sous-espaces vectoriels considérés. On sait déjà $\text{Vect}(F_1) = F_1$, ce qui montre la propriété dans le cas où $n = 1$ (on aurait même pu commencer à zéro, en considérant que la somme de 0 sev est $\{ 0_E \}$ qui est aussi $\text{Vect}(\varnothing)$).
   La propriété d'hérédité se montre en posant $S = F_1 + \ldots + F_n + F_{n+1}$ et en écrivant

$$\begin{aligned} S &= \text{Vect}(F_1 \cup \ldots \cup F_n) + \text{Vect}(F_{n+1}) \\ &= \text{Vect}(F_1 \cup \ldots \cup F_n \cup F_{n+1}). \end{aligned}$$

□

d Somme directe

Étant donné des sous-espaces vectoriels $F_1, \ldots, F_n$ de E, $F_1 + \ldots + F_n$ est l'ensemble des vecteurs x de E pouvant s'écrire au moins d'une façon sous la forme $x_1 + \ldots + x_n$ avec, pour tout $i \in [\![1, n]\!]$, $x_i \in F_i$. On va s'intéresser ici au cas où, pour tout x, la décomposition est unique.

Définition 2.3.17 (Somme directe)**.**
Étants donnés $n \in \mathbb{N}^*$ et $F_1, \ldots, F_n$ des sous-espaces vectoriels de E, on dit que $F_1, \ldots, F_n$ sont *en somme directe* ou que la somme $F_1 + \ldots + F_n$ est *directe* si tout élément x de $F_1 + \ldots + F_n$ se décompose de manière unique sous la forme $x_1 + \ldots + x_n$ avec, pour tout $i \in [\![1, n]\!]$, $x_i \in F_i$.

Dans ce cas, le sous-espace vectoriel $F_1 + \ldots + F_n$ est noté

$$F_1 \oplus \ldots \oplus F_n$$

ou

$$\bigoplus_{i=1}^{n} F_i.$$

Dans la suite de cette partie, n désigne un entier naturel et $F_1, \ldots, F_n$ des sous-espaces vectoriels de E.

Proposition 2.3.18.
Les propositions suivantes sont équivalentes.

(i) $F_1, \ldots, F_n$ sont en somme directe.

(ii) La seule décomposition possible du vecteur nul sous la forme $x_1 + \ldots + x_n$ avec $x_i \in F_i$ pour $i \in [\![1, n]\!]$ est la décomposition triviale $0 + \ldots + 0$.

(iii) Tout élément de E s'écrit au plus d'une façon sous la forme $x_1 + \ldots + x_n$ avec $x_i \in F_i$ pour $i \in [\![1, n]\!]$.

Démonstration. **(i)⇒ (ii)** Supposons que $F_1, \ldots, F_n$ sont en somme directe. Le vecteur nul appartient à $F_1 \oplus \ldots \oplus F_n$, donc se décompose d'une et une seule façon comme somme d'éléments de $F_1, \ldots, F_n$. Or il s'écrit sous la forme $0 + \ldots + 0$, qui est donc la seule décomposition possible de x.

(ii)⇒ (iii) Supposons que la seule décomposition du vecteur nul sous la forme d'une somme d'éléments de $F_1, \ldots, F_n$ soit sous la forme $0 + \ldots + 0$.

Soit alors x un élément de E. Supposons que x s'écrive à la fois $x_1 + \ldots + x_n$ et sous la forme $y_1 + \ldots + y_n$ où, pour tout $i \in [\![1, n]\!]$ $x_i \in F_i$ et $y_i \in F_i$. Alors on a

$$0 = x - x = (x_1 - y_1) + \ldots + (x_n - y_n).$$

Or pour tout $i \in [\![1, n]\!]$, $x_i - y_i \in F_i$, donc on a trouvé une décomposition du vecteur nul. Or on sait que cette décomposition est nécessairement la décomposition triviale, donc pour tout $i \in [\![1, n]\!]$, on a $x_i - y_i = 0$.

On a donc $x_i = y_i$ pour tout $i \in [\![1, n]\!]$, c'est-à-dire $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$.

Donc x se décompose d'au plus une façon.

Donc tout élément de E s'écrit au plus d'une façon sous la forme $x_1 + \ldots + x_n$ avec $x_i \in F_i$ pour $i \in [\![1, n]\!]$.

(iii)⇒(i) Supposons (iii) et montrons (i). Soit $x \in F_1 + \ldots + F_n$. Alors x se décompose d'au moins une façon comme sous la forme $x_1 + \ldots + x_n$ avec, pour tout $i \in [\![1, n]\!]$, $x_i \in F_i$.

De plus, d'après (iii), x se décompose au plus d'une façon sous cette forme.

Il se décompose donc de façon unique sous cette forme.

Donc la somme $F_1 + \ldots + F_n$ est directe.

□

Remarque 2.3.19.
La somme $F_1 + \cdots + F_n$ est donc directe si et seulement si l'application $F_1 \times \ldots F_n \to E$, $(x_1, \ldots, x_n) \mapsto x_1 + \cdots + x_n$ est injective. C'est évidemment un morphisme (de groupes, mais aussi d'ev. comme nous le verrons plus tard). La proposition précédente revient à étudier le noyau de ce morphisme.

Proposition 2.3.20 (Somme directe de **deux** sous-espaces vectoriels)**.**
Soit F et G deux sous-espaces vectoriels.

Alors la somme $F+G$ est directe si et seulement si $F \cap G = \{ 0_E \}$.

Démonstration.
Montrons la double implication.

Sens direct Supposons $F+G$ en somme directe. Comme $F \cap G$ est un espace vectoriel, on a évidemment $\{ 0_E \} \subset F \cap G$. Il suffit donc de montrer $F \cap G \subset \{ 0_E \}$ pour conclure qu'on a $F \cap G = \{ 0_E \}$.

Soit $x \in F \cap G$. On a alors $0_E = x + (-x)$ et $x \in F$ et $-x \in G$. Or F et G sont en somme directe donc cette décomposition est nécessairement la décomposition nulle : on a donc $(x, -x) = (0, 0)$ donc $x = 0$.

Sens indirect Supposons $F \cap G = \{ 0_E \}$. Alors montrons que 0 a la décomposition triviale pour seule décomposition comme somme d'un élément de F et de G.

Supposons que 0 s'écrive sous la forme $x + y$ avec $x \in F$ et $y \in G$. Alors $x = -y \in G$, donc $x \in F \cap G = \{ 0 \}$, donc $x = 0$ et $y = -x = 0$.

0 admet donc pour seule décomposition la décomposition triviale.

□

Remarque 2.3.21.


Ce résultat n'est valable que pour la somme de **deux** sous-espaces vectoriels, pas plus.

Exercice 2.3.22.
Trouver trois sous-espaces vectoriels F, G, H de $\mathbb{R}^2$ tels qu'on a $F \cap G \cap H = \{ 0 \}$ (ou même tels que $F \cap G = G \cap H = H \cap F = \{ 0 \}$) bien que F, G et H ne soient pas en somme directe.

En revanche, on a le résultat suivant :

Proposition 2.3.23.
Soit $p \in \mathbb{N}^*$ et $q \in \mathbb{N}^*$ et $F_1, \ldots, F_p$ et $G_1, \ldots G_q$ respectivement p et q sous-espaces vectoriels de E. On pose $F = F_1 + \ldots + F_p$ et $G = G_1 + \ldots + G_q$.

Alors la somme $F_1 + \ldots + F_p + G_1 + \ldots + G_q$ est directe si et seulement si les trois conditions suivantes sont vérifiées :

1. la somme $F_1 + \ldots + F_p$ est directe ;
2. la somme $G_1 + \ldots + G_q$ est directe ;
3. la somme $F + G$ est directe.

Démonstration.
Montrons la double implication.

Sens direct Supposons que la somme $F_1 + \ldots + F_p + G_1 + \ldots + G_q$ est directe. Alors

1. Montrons que la somme $F_1 + \ldots + F_p$ est directe. Considérons une décomposition du vecteur nul sous la forme $x_1 + \ldots + x_p$ où $x_i \in F_i$ pour $i \in [\![1, p]\!]$. En posant, pour $i \in [\![1, q]\!]$, $y_i = 0$, on a
$$0 = x_1 + \ldots + x_p + y_1 + \ldots + y_q.$$
Or la somme $F_1 + \ldots + F_p + G_1 + \ldots + G_q$ est directe, donc pour tout $i \in [\![1, p]\!]$, $x_i = 0$ et pour tout $i \in [\![1, q]\!]$, $y_i = 0$.
2. De même, la somme $G_1 + \ldots + G_p$ est directe.
3. Montrons que la somme $F + G$ est directe. Supposons que 0 s'écrive sous la forme $x + y$ avec $x \in F$ et $y \in G$. On a $x \in F$, donc x s'écrit sous la forme $x_1 + \ldots + x_p$ où $x_i \in F_i$ pour $i \in [\![1, p]\!]$. De même y s'écrit sous la forme $y_1 + \ldots + y_q$ où $y_i \in G_i$ pour $i \in [\![1, q]\!]$.
On a donc
$$0 = x_1 + \ldots + x_p + y_1 + \ldots + y_q.$$
Or la somme $F_1 + \ldots + F_p + G_1 + \ldots + G_q$ est directe, donc pour tout $i \in [\![1, p]\!]$, $x_i = 0$ et pour tout $i \in [\![1, q]\!]$, $y_i = 0$. Donc $x = 0$ et $y = 0$.
La seule décomposition de 0 comme somme d'un élément de F et d'un élément de G est donc la décomposition triviale. Donc la somme $F + G$ est directe.

Sens indirect Supposons que les trois conditions sont vérifiées et montrons que la somme $F_1 + \ldots + F_p + G_1 + \ldots + G_q$ est directe.
Considérons une décomposition de 0 sous la forme
$$0 = x_1 + \ldots + x_p + y_1 + \ldots + y_q,$$
où $x_i \in F_i$ pour tout $i \in [\![1, p]\!]$ et $y_i \in G_i$ pour tout $i \in [\![1, q]\!]$.
Alors, en posant $x = x_1 + \ldots + x_p$ et $y = y_1 + \ldots y_q$, on a $0 = x + y$ et $x \in F$ et $y \in G$. Or F et G sont en somme directe donc $x = 0$ et $y = 0$. On a donc
$$0 = x_1 + \ldots + x_p.$$
Or $F_1, \ldots, F_p$ sont en somme directe donc pour tout $i \in [\![1, p]\!]$, $x_i = 0$. De même pour tout $i \in [\![1, q]\!]$, $y_i = 0$.
Donc 0 admet la décomposition triviale pour seule décomposition comme somme d'éléments de $F_1, \ldots, F_p, G_1, \ldots, G_q$. Donc la somme $F_1 + \ldots + F_p + G_1 + \ldots + G_q$ est directe.

□

Corollaire 2.3.24.
Soit $n \in \mathbb{N}^*$ et $F_1, \ldots, F_{n+1}$ $n + 1$ sous-espaces vectoriels de E. Alors les trois conditions suivantes sont équivalentes :

1. la somme $F_1 + \ldots + F_{n+1}$ est directe ;
2. la somme $F_1 + \ldots + F_n$ est directe et la somme de $F_1 \oplus \ldots \oplus F_n$ et de F_{n+1} est directe ;
3. la somme $F_1 + \ldots + F_n$ est directe et $(F_1 \oplus \ldots \oplus F_n) \cap F_{n+1} = \{ 0 \}$.

Démonstration.
L'équivalence des deux premiers points découle de la propriété précédente (avec $p = n$ et $q = 1$). Celle des deux derniers, de la caractérisation de la somme directe de deux sous-espaces vectoriels. □

Définition 2.3.25.
On dit que F est ***un*** *supplémentaire* de G (ou que F et G sont *supplémentaires*) si
$$E = F \oplus G,$$
i.e. si les deux conditions suivantes sont remplies :

1. la somme $F + G$ est directe ;
2. $E = F + G$.

Proposition 2.3.26.
F et G sont supplémentaires si et seulement si tout élément de E s'écrit *de manière unique* comme somme d'un élément de F et d'un élément de G.

Démonstration.
Direct d'après les définitions. □

Exemple 2.3.27.
Montrons que dans $\mathbb{R}^2$, deux droites passant par 0 et non confondues sont toujours supplémentaires.

Exercice 2.3.28.
Dans $\mathbb{R}^2$, on note $\mathscr{D} : x+y=0$, $\mathscr{D}' : x-y=0$ et $\mathscr{D}'' : x-2y=0$.

1. Montrer $\mathbb{R}^2 = \mathscr{D} \oplus \mathscr{D}'$
2. Montrer $\mathbb{R}^2 = \mathscr{D} \oplus \mathscr{D}''$

Remarquez qu'il n'y a donc pas unicité du supplémentaire (croire le contraire est une faute classique et très grave !).

Remarque 2.3.29.
On peut montrer de même que dans $\mathbb{R}^3$, un plan et une droite passant par 0 et tel que le plan ne contienne pas la droite sont toujours supplémentaires.

Exemple 2.3.30.
$\mathscr{P} : x-y+z=0$ et $\mathscr{D} : x=t+1, y=0, z=2t+2$. On montre que $(\overrightarrow{I}, \overrightarrow{J}, \overrightarrow{K})$ est une base de $\mathbb{R}^3$, avec $\overrightarrow{I}$ vecteur directeur de $\mathscr{D}$ et $(\overrightarrow{J}, \overrightarrow{K})$ base de $\mathscr{P}$.

Exemple 2.3.31.
$\mathbb{R}$ et $i\mathbb{R}$ dans $\mathbb{C}$.

Exercice 2.3.32.
On note E l'ensemble des applications de $\mathbb{R}$ dans $\mathbb{R}$, I celui des applications impaires, et P celui des applications paires.

Montrer $E = I \oplus P$.

3 Translations, sous-espaces affines

Les sous-espaces affines (sea) généralisent la notion de sev, en s'affranchissant de la contrainte « passer par 0 ». Ainsi, dans la théorie des ev, un sev passe toujours par 0.
Là encore on pourra identifier points et vecteurs, mais on essaiera de noter les points avec des majuscules et les vecteurs avec des minuscules, comme en géométrie, mais nous passerons souvent d'un point de vue à l'autre.

Définition 3.0.1.
Soit $A, B \in E$, on note $\overrightarrow{AB} = B - A$.

Remarque 3.0.2.
La loi + des ev permet de donner un sens à $B-A$, vus comme points, qui vaut alors $\overrightarrow{AB} = \overrightarrow{OB} - \overrightarrow{OA}$.

3.1 Translations

Définition 3.1.1.
Soit un vecteur $u \in E$. On appelle *translation* de vecteur u l'application $\begin{array}{ccc} E & \to & E \\ x & \mapsto & x+u \end{array}$.

3.2 Sous-espaces affines

Définition 3.2.1.
On appelle *sous-espace affine* de E toute partie de E qui est le translaté d'un sev de E, *i.e.* toute partie $\mathscr{F}$ de la forme $\mathscr{F} = u+F = \{ u+x \mid x \in F \}$, où F est un sev de E et u est un vecteur de E, ensemble que l'on note aussi $u+F$.

L'ensemble $\{ b-a \mid (a,b) \in \mathscr{F}^2 \}$ est appelé *la direction* de $\mathscr{F}$ et ses éléments sont appelés les *vecteurs directeurs* de $\mathscr{F}$.

Proposition 3.2.2.
Soit $u \in E$, F un sous-espace vectoriel de E. Alors la direction du sous-espace affine $u+F$ est F. En particulier cette direction est un espace vectoriel.

Démonstration.
Notons D la direction de $u+F$.
On a

$$\begin{aligned} D &= \{ b-a \mid (a,b) \in \mathscr{F}^2 \} \\ &= \{ (u+x)-(u+y) \mid (x,y) \in F^2 \} \\ &= \{ x-y \mid (x,y) \in F^2 \}. \end{aligned}$$

Or on a évidemment

$$F \subset \{ x-0 \mid x \in F^2 \} \subset \{ x-y \mid (x,y) \in F^2 \} \subset F,$$

donc $D = F$. □

Remarque 3.2.3.
Notation fréquente : $\mathscr{F}$ étant un sea de E, on note F ou $\overrightarrow{F}$ sa direction.

Exemple 3.2.4.
Tout sev est un sea.

Exemple 3.2.5.
Dessin dans l'espace.

Exemple 3.2.6.
$E = \mathbb{R}^{\mathbb{R}}$. On considère l'équation différentielle $y' + 3y = x^2$ (E). Montrer que l'ensemble $\mathscr{S}_0$ des solutions de l'équation homogène forme un sev de E, et l'ensemble $\mathscr{S}$ des solutions de (E) forme un sea de direction $\mathscr{S}_0$.

Lemme 3.2.7.
Soit F un sous-espace vectoriel de E, a et b deux éléments de E. Alors on a équivalence entre les assertions suivantes :

(i) $b - a \in F$;
(ii) $b \in a + F$;
(iii) $b + F \subset a + F$;
(iv) $a - b \in F$;
(v) $a \in b + F$;
(vi) $a + F \subset b + F$;
(vii) $a + F = b + F$.

Démonstration. **(i)⇒ (ii)** Supposons $b - a \in F$, alors $a + (b - a) \in a + F$, donc $b \in a + F$.

(ii)⇒(iii) Supposons $b \in a + F$, alors b s'écrit sous la forme $a + u$ où $u \in F$. Donc pour tout $v \in F$, on a $b + v = a + (u + v) \in a + F$. Donc on a (iii).

(iii)⇒(i) Supposons $b+F \subset a+F$. Alors comme $b \in b+F$, on a $b \in a + F$, donc b s'écrit sous la forme $a + u$ où $u \in F$. Donc $b - a = u \in F$.

(iv), (v) et (vi) sont équivalents C'est exactement la même chose que ce qui précède, en échangeant le rôle de a et b.

(i)<=>(iv) F étant un sous-espace vectoriel de E, on a $b - a \in F$ si et seulement si $-(b - a) \in F$. Or $-(b - a) = a - b$, c'est donc évident.

(i) ⇒ (vii) Si on a (i), d'après ce qui précède toutes les assertions (i) à (vi) sont vraies, en particulier on a (iii) et (vi). On a donc immédiatement (vii).

(vii)⇒(vi) C'est évident.

□

Théorème 3.2.8.
Soit $\mathscr{F}$ un sea de direction F.

(i) $\mathscr{F}$ est le translaté de sa direction par n'importe lequel de ses points : $\forall a \in \mathscr{F} \quad \mathscr{F} = a + F$.

(ii) Soit $a \in \mathscr{F}$ et $b \in E$. Alors on a

$$b \in \mathscr{F} \iff a - b \in F.$$

Démonstration.
$\mathscr{F}$ est de la forme $c + F$, où $c \in E$.

(i) Soit $a \in \mathscr{F}$. On a alors $a \in c + F$, donc d'après le lemme, on a $a + F = c + F = \mathscr{F}$.

(ii) On a donc $\mathscr{F} = a + F$. Or d'après le lemme, on a $b \in a + F \iff a - b \in F$.

□

Remarque 3.2.9.
Tout sea contenant 0 est donc un sev.

Corollaire 3.2.10.
Deux sea sont égaux si et seulement s'ils ont même direction et un point en commun.

Démonstration.
⇒ : évident.
⇐ : soient $\mathscr{F}_1$ et $\mathscr{F}_2$ de même direction F et $a \in \mathscr{F}_1 \cap \mathscr{F}_2$. Alors d'après le th., $\mathscr{F}_1 = a + F = \mathscr{F}_2$. □

Définition 3.2.11.
Soient $\mathscr{F}$ et $\mathscr{G}$ deux sea de directions F et G.

(i) On dit que $\mathscr{F}$ est parallèle à $\mathscr{G}$ si $F \subset G$.

(ii) On dit que $\mathscr{F}$ et $\mathscr{G}$ sont parallèles si $F = G$.

 Vocabulaire : « être parallèle à » n'est pas une relation symétrique.

Exemple 3.2.12.
Une droite est parallèle à un plan, mais certainement pas l'inverse.

Théorème 3.2.13 (Intersections de sea)**.**
Soient $\mathscr{F}$ et $\mathscr{G}$ deux sea de directions F et G. Si $\mathscr{F} \cap \mathscr{G} \neq \varnothing$, alors on dit que $\mathscr{F}$ et $\mathscr{G}$ sont *concourants* ou *sécants*, et dans ce cas $\mathscr{F} \cap \mathscr{G}$ est un sea de direction $F \cap G$.

Démonstration.
Supposons $\mathscr{F} \cap \mathscr{G} \neq \varnothing$, alors il existe $a \in \mathscr{F} \cap \mathscr{G}$. Donc $\mathscr{F} = a + F$ et $\mathscr{G} = a + G$.
Montrons alors que $\mathscr{F} \cap \mathscr{G} = a + F \cap G$:
Soit $b \in E$. On a successivement :

$$\begin{aligned} b \in \mathscr{F} \cap \mathscr{G} &\iff b \in \mathscr{F} \text{ et } b \in \mathscr{G} \\ &\iff b - a \in F \text{ et } b - a \in G \\ &\iff b - a \in F \cap G \\ &\iff b \in a + F \cap G \end{aligned}$$

D'où le résultat. □

Théorème 3.2.14 (Parallélisme et intersection)**.**
Si $\mathscr{F}$ est parallèle à $\mathscr{G}$, alors soit $\mathscr{F} \cap \mathscr{G} = \varnothing$, soit $\mathscr{F} \subset \mathscr{G}$.

En particulier si $\mathscr{F}$ et $\mathscr{G}$ sont parallèles, alors soit $\mathscr{F} \cap \mathscr{G} = \varnothing$, soit $\mathscr{F} = \mathscr{G}$.

Démonstration.
Supposons $F \subset G$. Si $\mathscr{F} \cap \mathscr{G} \neq \varnothing$, alors il existe $a \in \mathscr{F} \cap \mathscr{G}$, donc $\mathscr{F} = a + F$, or $F \subset G$, donc$a + F \subset a + G = \mathscr{G}$.
Dans le cas particulier où $\mathscr{F}$ et $\mathscr{G}$ sont parallèles, on a $\mathscr{F} \subset \mathscr{G}$ et $\mathscr{G} \subset \mathscr{F}$, d'où $\mathscr{F} = \mathscr{G}$. □

3.3 Barycentres (hors programme)

Le barycentre est maintenant hors-programme. Cette partie ne sera pas nécessairement traitée en cours mais est laissée :
— à titre culturel ;
— parce qu'elle peut être utile en sciences physiques.

Définition 3.3.1.
• On appelle *système pondéré* toute famille de la forme $((A_1, \lambda_1), \ldots, (A_n, \lambda_n))$, où chaque élément (A_i, λ_i) est appelé *point pondéré*, avec $n \in \mathbb{N}^*$, $A_1, \ldots, A_n$ n points de E, et $\lambda_1, \ldots, \lambda_n$ n scalaires de $\mathbb{K}$.

• Avec les notations précédentes, on pose $\Lambda = \sum_{k=1}^{n} \lambda_k$.

(i) Si $\Lambda = 0$, alors le vecteur $\sum_{k=1}^{n} \lambda_k \overrightarrow{MA_k}$ ne dépend pas du point M.

(ii) Si $\Lambda \neq 0$, il existe un unique point G tel que $\sum_{k=1}^{n} \lambda_k \overrightarrow{GA_k} = 0$. Ce point est appelé le *barycentre* du système pondéré $(A_i, \lambda_i)_{i \in [\![1,n]\!]}$ et il vérifie $G = \dfrac{1}{\Lambda} \sum_{k=1}^{n} \lambda_k A_k$.

Démonstration. (i) Supposons $\Lambda = 0$. Soit $(M, N) \in E^2$. On a

$$\begin{aligned} \sum_{k=1}^{n} \lambda_k \overrightarrow{MA_k} &= \sum_{k=1}^{n} \lambda_k \overrightarrow{MA_k} + \sum_{k=1}^{n} \lambda_k \overrightarrow{NM} \\ &= \sum_{k=1}^{n} \lambda_k (\overrightarrow{NM} + \overrightarrow{MA_k}) \\ &= \sum_{k=1}^{n} \lambda_k \overrightarrow{NA_k} \end{aligned}$$

(ii) Supposons $\Lambda \neq 0$. On a successivement :

$$\begin{aligned} \sum_{k=1}^{n} \lambda_k \overrightarrow{GA_k} = 0 &\Leftrightarrow \sum_{k=1}^{n} \lambda_k (A_k - G) = 0 \\ &\Leftrightarrow \sum_{k=1}^{n} \lambda_k A_k - \left(\sum_{k=1}^{n} \lambda_k \right) G = 0 \\ &\Leftrightarrow G = \frac{1}{\Lambda} \sum_{k=1}^{n} \lambda_k A_k \end{aligned}$$

□

Définition 3.3.2.
Soit I un ensemble. On appelle *partition finie* de I tout k-uplet, pour $k \in \mathbb{N}$, $(I_1, \ldots, I_k)$ où les I_i sont des ensembles vérifiant $I_j \cap I_i = \varnothing$ si $i \neq j$ et $\bigcup_{1 \leqslant i \leqslant k} I_i = I$. Autrement dit, une partition est un ensemble de parties de I deux à deux disjointes, dont la réunion est I (on parle aussi de recouvrement de I par des parties deux à deux disjointes).

Exemple 3.3.3. — La partition de l'Europe par le traité de Verdun en 843 est une partition à trois éléments de l'ensemble des points de l'empire de Charlemagne.
— Notons C_0, C_1 et C_2 les parties de $\mathbb{Z}$ contenant respectivement les entiers congrus à 0, 1 et 2 modulo 3. Alors (C_0, C_1, C_2) est une partition de $\mathbb{Z}$.

Théorème 3.3.4 (Associativité du barycentre)**.** Soient I un ensemble non vide, $(A_i, \lambda_i)_{i\in I}$ un système de points pondérés de somme non-nulle, et soit $(I_1, \dots, I_n)$ une partition de I. Pour tout $k \in [\![1, n]\!]$, on note $\Lambda_k = \sum_{i\in I_k} \lambda_i$, on suppose que Λ_k est non-nul et on note alors G_k le barycentre du système pondéré $(A_i, \lambda_i)_{i\in I_k}$.

Alors le barycentre G de $(A_i, \lambda_i)_{i\in I}$ est aussi le barycentre du système pondéré $(G_k, \Lambda_k)_{k\in[\![1,n]\!]}$.

Démonstration.
On sait que $G = \frac{1}{\Lambda}\sum_{i\in I} \lambda_i A_i$ et $\Lambda_k G_k = \sum_{i\in I_k} \lambda_i A_i$, donc $G = \frac{1}{\Lambda}\sum_{k=1}^{n}(\sum_{i\in I_k} \lambda_i A_i) = \frac{1}{\Lambda}\sum_{k=1}^{n} \Lambda_k G_k$, et $\Lambda = \sum_{k=1}^{n} \Lambda_k$. □

Exercice 3.3.5.
En déduire :

1. que les médianes d'un triangle sont concourantes au centre de gravité ;
2. que droites reliant les milieux des arêtes opposées d'un tétraèdre et les droites reliant les centre de gravité des faces au sommet opposé sont toutes concourantes en un même point qu'on précisera.

Centre de gravité d'un triangle (ABC)= isobarycentre. Si I est le milieu de $[A, B]$, alors G =bar$((C, 1), (I, 2))$.

Théorème 3.3.6.
Un sea contient tous les barycentres obtenus à partir de ses points.

Démonstration.
Soit $\mathscr{F}$ un sea, $A_1 \dots A_n$ n points de $\mathscr{F}$, et $\lambda_1 \dots \lambda_n$ les poids correspondants, $\Lambda = \sum_{k=1}^{n} \lambda_k \neq 0$. On note $G =$ bar$((A_k, \lambda_k))$.
$A_1 \in \mathscr{F}$ donc $\mathscr{F} = A_1 + F$. Donc $G \in \mathscr{F}$ ssi $G - A_1 \in F$. Or $G - A_1 = \frac{1}{\Lambda}\sum_{k=1}^{n} \lambda_k(A_i - A_1)$, et tous les membres de cette somme sont dans F. □

Théorème 3.3.7.
Réciproquement, tout sous-ensemble non vide de E stable par barycentre (et même seulement par barycentre de deux points) est un sea.

Démonstration.
Soit $\mathscr{F}$ un sous-ensemble non vide de E et a un de ses points. Posons $F = \{\, b - a \mid b \in \mathscr{F} \,\}$. On a $\mathscr{F} = a + F$, il suffit donc de montrer que F est un sous-espace vectoriel de E.

F est une partie de E non vide car $0 \in F$.

Soit $x \in F$ et $\lambda \in \mathbb{K}$. Alors $a+x$ et a sont deux éléments de $\mathscr{F}$, donc leur barycentre $\lambda(a + x) + (1 - \lambda)a$ appartient aussi à $\mathscr{F}$. Or ce barycentre est $a + \lambda x$, donc $\lambda x \in F$. F est donc stable par multiplication externe.

Soit $(x, y) \in F$. Alors, $\mathscr{F}$ étant stable par barycentre, $\frac{1}{2}((a + x) + (a + y)) \in \mathscr{F}$, donc $a + \frac{1}{2}(x + y) \in \mathscr{F}$, donc $\frac{1}{2}(x + y) \in F$. D'après ce qui précède, on a alors $x + y = 2 \times \frac{1}{2}(x + y) \in F$. Donc F est stable par addition

Donc F est un sous-espace vectoriel de E. Donc $\mathscr{F}$ est un sous-espace affine de E. □

3.4 Convexité (hors programme)

Cette partie est laissée à titre culturel mais ne sera pas nécessairement traitée en cours.

Dans ce paragraphe, on prend $\mathbb{K} = \mathbb{R}$.

Définition 3.4.1.
On appelle *segment* de E tout ensemble de la forme $\{\lambda A + (1 - \lambda)B, \lambda \in [0, 1]\}$ avec $A, B \in E$. Ce segment est noté $[AB]$ ou $[A, B]$.

Remarque 3.4.2.
$[AB]$ est l'ensemble des barycentres de A et B avec des poids positifs (facultatif : dont la somme est 1). Faire un dessin.

Définition 3.4.3.
Soit $\mathscr{P}$ une partie de E. On dit que $\mathscr{P}$ est *convexe* si $\forall (A,B) \in \mathscr{P}^2 \quad [AB] \subset \mathscr{P}$.

Exemple 3.4.4.
Faire des dessins dans $\mathbb{R}^2$, puis dans $\mathbb{R}^3$.

Théorème 3.4.5.
Tout sea est convexe.

Démonstration.
Immédiat avec le théorème 3.3.6. □

Exemple 3.4.6.
On reprend un exemple ancien : pour montrer qu'un cercle n'est pas un sea (ou un sev), on peut montrer qu'il n'est pas convexe.

 La réciproque est fausse, même si le convexe contient 0. Par exemple, considérons $[-1,1]$ dans $\mathbb{R}$.

Exemple 3.4.7.
Dans $\mathbb{C}$, tout disque (fermé ou ouvert) est convexe. Se fait avec inégalité triangulaire en revenant à la définition.

Théorème 3.4.8.
Toute intersection de convexes est convexe.

Démonstration.
Soit I un ensemble et $(\mathscr{P}_i)_{i\in I}$ une famille de convexes.

Posons $\mathscr{P} = \bigcap_{i\in I} \mathscr{P}_i$ l'intersection de cette famille et montrons qu'elle est convexe, c'est-à-dire

$$\forall (A,B) \in \mathscr{P}^2 \quad [AB] \subset \mathscr{P}$$

Soit $(A,B) \in \mathscr{P}^2$. Il suffit de montrer que pour tout $i \in I$, $[AB] \subset \mathscr{P}_i$.

Soit $i \in I$. On a $A \in \mathscr{P}$, donc $A \in \mathscr{P}_i$. De même $B \in \mathscr{P}_i$. Donc $[AB] \subset \mathscr{P}_i$.

On a donc $\forall i \in I \quad [AB] \subset \mathscr{P}_i$, donc $[AB] \in \bigcap_{i\in I} \mathscr{P}_i$. □

4 Applications linéaires

Soient E_1 et E_2 deux $\mathbb{K}$-ev ($\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$).

4.1 Définitions

Définition 4.1.1.
On appelle *application linéaire* (ou *morphisme d'espaces vectoriels*) de E_1 dans E_2 toute application $\varphi : E_1 \to E_2$ vérifiant

$$\forall (x,y) \in E_1^2,\ \forall (\lambda,\mu) \in \mathbb{K}^2 \qquad \varphi(\lambda x + \mu y) = \lambda\varphi(x) + \mu\varphi(y). \quad \text{(XVIII.1)}$$

Autrement dit, l'image d'une combinaison linéaire est la combinaison linéaire des images : une application linéaire préserve les combinaisons linéaires.

- L'ensemble des applications linéaires de E_1 dans E_2 est noté $\mathscr{L}(E_1,E_2)$.
- Une application linéaire de E_1 dans E_1 est appelé *endomorphisme*. On note $\mathscr{L}(E_1,E_1) = \mathscr{L}(E_1)$.
- Une application linéaire bijective est appelée *isomorphisme*. L'ensemble des isomorphismes de E_1 dans E_2 est noté $\mathscr{GL}(E_1,E_2)$, appelé groupe linéaire.
- Un *automorphisme* est un endomorphisme qui est aussi un isomorphisme, on note $\mathscr{GL}(E_1) = \mathscr{GL}(E_1,E_1)$ l'ensemble des automorphismes de E_1.
- Une application linéaire de E_1 dans $\mathbb{K}$ est une *forme linéaire*.

Remarque 4.1.2.
Une application linéaire φ de E_1 dans E_2 est un morphisme *de groupes* de $(E_1,+)$ dans $(E_2,+)$, avec une propriété supplémentaire vis-à-vis de la loi externe.

Remarque 4.1.3.
La propriété fondamentale des applications linéaires se généralise aux combinaisons linéaires d'un nombre quelconque de vecteurs : si $x_1,\dots,x_n \in E$ et $\lambda_1,\dots,\lambda_n \in \mathbb{K}$ et $f \in \mathscr{L}(E,F)$, alors $f\left(\sum_{k=1}^{n} \lambda_i x_i\right) = \sum_{k=1}^{n} \lambda_i f(x_i)$.

De manière plus générale, pour toute famille

$(x_i)_{i\in I}$ et toute famille à support fini $(\lambda_i)_{i\in I}$, on a

$$f\left(\sum_{i\in I}\lambda_i x_i\right)=\sum_{i\in I}\lambda_i f(x_i)$$

Remarque 4.1.4 (Très utile en pratique)**.**
La propriété fondamentale des applications linéaires (XVIII.1) est équivalente à

$$\forall (x,y)\in E_1^2,\ \forall\lambda\in\mathbb{K}\qquad \varphi(\lambda x+y)=\lambda\varphi(x)+\varphi(y)\quad\text{(XVIII.2)}$$

ainsi qu'à

$$\forall (x,y)\in E_1^2, \varphi(x+y)=\varphi(x)+\varphi(y)\qquad \text{et } \forall(\lambda,x)\in\mathbb{K}\times E_1, \varphi(\lambda x)=\lambda\varphi(x).$$

La démonstration est analogue à celle pour les sev.

Exemple 4.1.5.
• Soit $u\in\mathbb{R}^3$. Alors $\varphi : \begin{array}{ccc}\mathbb{R}^3 & \to & \mathbb{R}\\ v & \mapsto & u\cdot v\end{array}$ est une forme linéaire (on dit que le produit scalaire est linéaire à droite).
• Soit $A\in\mathscr{M}_{n,p}(\mathbb{K})$. Alors $\varphi : \begin{array}{ccc}\mathscr{M}_{q,n}(\mathbb{K}) & \to & \mathscr{M}_{q,p}(\mathbb{K})\\ B & \mapsto & BA\end{array}$ estlinéaire (on dit que le produit matriciel est linéaire à gauche).

Exemple 4.1.6.
$\varphi : \begin{array}{ccc}\mathbb{R}^3 & \to & \mathbb{R}^3\\ (x,y,z) & \mapsto & (3x+y,2z,x-y+z)\end{array}$ est un endomorphisme.

Remarque 4.1.7.
Toute application polynomiale (en plusieurs variables) faisant intervenir des termes de degrés différents de 1 n'est pas linéaire.

Exemple 4.1.8.
$\varphi : \begin{array}{ccc}\mathbb{R}^2 & \to & \mathbb{R}\\ (x,y) & \mapsto & xy\end{array}$ n'est pas une application linéaire, idem avec x^2 et $3x+2y+2$.

Exemple 4.1.9.
On note $\ell_{\mathbb{N}}(\mathbb{R})$ l'ensemble des suites réelles convergentes, c'est un sev de $\mathbb{R}^{\mathbb{N}}$, et l'application $\varphi : \begin{array}{ccc}\ell_{\mathbb{N}}(\mathbb{R}) & \to & \mathbb{R}\\ (u_n) & \mapsto & \lim\limits_{n\to+\infty} u_n\end{array}$ est une forme linéaire.

Exemple 4.1.10.
Soit $E=\mathscr{F}(\mathbb{R},\mathbb{R})$ et $a\in\mathbb{R}$.
L'application $\mathrm{ev}_a : \begin{array}{ccc}E & \to & \mathbb{R}\\ f & \mapsto & f(a)\end{array}$ est une forme linéaire appelée *évaluation en a*.

Proposition 4.1.11.
Si $\varphi\in\mathscr{L}(E_1,E_2)$, alors $\varphi(0_{E_1})=0_{E_2}$.

Démonstration.
Comme pour les morphismes de groupes : $\varphi(0_{E_1})=\varphi(0_{E_1}+0_{E_1})=\varphi(0_{E_1})+\varphi(0_{E_1})$. □

4.2 Opérations sur les applications linéaires

Dans toute la suite, E_1, E_2 et E_3 sont des $\mathbb{K}$-ev.

Théorème 4.2.1.
1. $\mathscr{L}(E_1,E_2)$ est un sev de $(\mathscr{F}(E_1,E_2),+,\cdot)$.
2. Si $f\in\mathscr{L}(E_1,E_2)$ et $g\in\mathscr{L}(E_2,E_3)$, alors $g\circ f\in\mathscr{L}(E_1,E_3)$.
3. Soit $f\in\mathscr{L}(E_1,E_2)$. Alors les applications

$$\varphi:\left\{\begin{array}{ccc}\mathscr{L}(E_2,E_3) & \longrightarrow & \mathscr{L}(E_1,E_3)\\ g & \longmapsto & g\circ f\end{array}\right.$$

et

$$\psi:\left\{\begin{array}{ccc}\mathscr{L}(E_3,E_1) & \longrightarrow & \mathscr{L}(E_3,E_2)\\ g & \longmapsto & f\circ g\end{array}\right.$$

sont linéaires.

Démonstration.
Élémentaire. □

Remarque 4.2.2.
Ces résultats montrent, avec $E_1=E_2=E_3$, que $(\mathscr{L}(E_1),+,\circ)$ est un anneau.

 En général, cet anneau n'est pas commutatif.

Exemple 4.2.3.
On pose $E_1 = \mathscr{C}^{+\infty}(\mathbb{R},\mathbb{R})$: c'est un sev de $\mathscr{F}(\mathbb{R},\mathbb{R})$ (le montrer). On note

$$\varphi : \begin{array}{ccc} E_1 & \to & E_1 \\ f & \mapsto & f' \end{array} \quad \text{et } \psi : \begin{array}{ccc} E_1 & \to & E_1 \\ f & \mapsto & \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & xf(x) \end{array} \right. \end{array}$$

On constate alors que $\psi \circ \varphi \neq \varphi \circ \psi$.

4.3 Noyau et image

Théorème 4.3.1.
Soit $\varphi \in \mathscr{L}(E_1, E_2)$, A un sev de E_1 et B un sev de E_2.

1. L'image directe de A par φ est un sev de E_2.
2. L'image réciproque de B par φ est un sev de E_1.

Démonstration. 1. On a bien $\varphi(A) \subset E_2$ ainsi que $0_{E_2} \in \varphi(A)$, car $\varphi(0_{E_1}) = 0_{E_2}$ et $0_{E_1} \in A$.
Soit $(y_1, y_2) \in \varphi(A)^2$, soit $\lambda \in \mathbb{K}$ et soit $(x_1, x_2) \in A^2$ vérifiant $y_1 = \varphi(x_1)$ et $y_2 = \varphi(x_2)$. Alors, comme A est un sev de E_1, on a $x_1 + \lambda x_2 \in A$ et donc, par linéarité de φ, on a $y_1 + \lambda y_2 = \varphi(x_1) + \lambda\varphi(x_2) = \varphi(x_1 + \lambda x_2) \in \varphi(A)$. Ainsi, $\varphi(A)$ est un sev de E_2.

2. On a bien $\varphi^{-1}(B) \subset E_1$ ainsi que $0_{E_1} \in \varphi^{-1}(B)$, car $\varphi(0_{E_1}) = 0_{E_2}$ et $0_{E_2} \in B$.
Soit $(x_1, x_2) \in \varphi^{-1}(B)^2$, $\lambda \in \mathbb{K}$. Alors, $\varphi(x_1) \in B$ et $\varphi(x_2) \in B$ et, par linéarité de φ, $\varphi(x_1 + \lambda x_2) = \varphi(x_1) + \lambda\varphi(x_2) \in B$, car B est un sev de E_2. Ainsi, $x_1 + \lambda x_2 \in \varphi^{-1}(B)$ et donc $\varphi^{-1}(B)$ est un sev de E_1. □

Définition 4.3.2.
Soit $\varphi \in \mathscr{L}(E_1, E_2)$.

1. On appelle *noyau* de φ noté $\operatorname{Ker}\varphi$, l'ensemble $\{\, x \in E_1 \mid \varphi(x) = 0_{E_2} \,\}$
2. On appelle *image* de φ et on note $\operatorname{Im}\varphi$, l'ensemble $\{\, \varphi(x) \mid x \in E_1 \,\}$.

Remarque 4.3.3.
Le théorème 4.3.1 assure ainsi que $\operatorname{Ker}\varphi$ et $\operatorname{Im}\varphi$ sont des sev.

Remarque 4.3.4.
Pour montrer qu'un ensemble est muni d'une structure d'ev, on essaiera TOUJOURS de l'identifier comme noyau ou image d'une application linéaire. Sinon, on essaiera de l'identifier directement comme sev. d'un ev. de référence.
Rappel : on ne revient JAMAIS à la définition générale d'un ev.

Théorème 4.3.5.
Soit $\varphi \in \mathscr{L}(E_1, E_2)$.

1. φ est injective si et seulement si $\operatorname{Ker}\varphi = \{0\}$.
2. φ est surjective si et seulement si $\operatorname{Im}\varphi = E_2$.

Démonstration. 1. Deux méthodes : refaire comme la démo analogue pour les morphismes de groupes, ou utiliser directement ce théorème : on choisit la deuxième méthode. Il suffit alors remarquer que $\operatorname{Ker}\varphi$ est le même que l'on adopte le point de vue «groupe» ou le point de vue «espace vectoriel».
On peut aussi refaire la première méthode pour s'entraîner.
□

Remarque 4.3.6.
Les calculs de noyaux et d'images se ramènent souvent à des résolutions de systèmes linéaires.

Exemple 4.3.7.
Déterminer $\operatorname{Ker}\varphi$ et $\operatorname{Im}\varphi$, avec

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{R}^3 & \longrightarrow & \mathbb{R}^3 \\ \begin{pmatrix} x \\ y \\ z \end{pmatrix} & \longmapsto & \begin{pmatrix} x & + & 2y & + & 5z \\ & - & y & - & z \\ -x & + & y & - & 2z \end{pmatrix} \end{array} \right. .$$

Exemple 4.3.8.
Soit $\varphi : \begin{array}{ccc} \mathbb{R}^{\mathbb{R}} & \to & \mathbb{R}^{\mathbb{R}} \\ f & \mapsto & f \times \sin \end{array}$. On montre que φ est linéaire, puis que φ n'est pas injective, en trouvant une fonction f non nulle dans $\operatorname{Ker}\varphi$. Par exemple $f(x) = 0$ si $x \neq 0$ et $f(0) = 1$.
On montre enfin que $\psi = \varphi|_{\mathscr{C}^0(\mathbb{R})}$ est injective, en montrant que son noyau est réduit à $\{0\}$.

On peut maintenant unifier les résultats sur les structures des solutions de nombreux problèmes linéaires étudiés auparavant (systèmes linéaires, équations différentielles linéaires).

Proposition 4.3.9.
Soit $f \in \mathscr{L}(E_1, E_2)$ et $a \in E_2$. Alors $f^{-1}(\{a\})$ est soit vide, soit un sea de E_1 de direction $\operatorname{Ker} f$.

Remarque 4.3.10.
$f^{-1}(\{a\})$ est l'ensemble des solutions de l'équations $f(x) = a$, avec $x \in E_1$.

Démonstration.
Reprendre chaque preuve effectuée lorsque l'on a rencontré ce type de structure de solution. □

Exemple 4.3.11.
L'ensemble des suites réelles $(u_n)_{n_i n\mathbb{N}}$ vérifiant pour tout $n \in \mathbb{N}$, $u_{n+2} = 3u_{n+1} - 2u_n - 4$ est le sea de direction $\operatorname{Vect}((2^n)_{n\in\mathbb{N}}, 1)$ et passant par $(4n)_{n\in\mathbb{N}}$.

Remarque 4.3.12.
On retrouve ainsi que l'ensemble des solutions d'un système linéaire est soit vide soit un sea.

4.4 Isomorphismes

Un isomorphisme transporte la structure d'ev, comme pour les groupes.

 Dire que E_1 et E_2 sont isomorphes ne signifie pas que toute application linéaire de E_1 dans E_2 est un isomorphisme. On peut donner un exemple : $f : \mathbb{R}^2 \to \mathbb{R}^2$, $(x, y) \mapsto (x, 0)$.

Théorème 4.4.1.
Soit $\varphi \in \mathscr{L}(E_1, E_2)$.

1. Si φ est un isomorphisme, alors φ^{-1} aussi.
2. Une composée d'isomorphismes est un isomorphisme : si $\varphi \in \mathscr{GL}(E_1, E_2)$ et $\psi \in \mathscr{GL}(E_2, E_3)$, alors $\psi \circ \varphi \in \mathscr{GL}(E_1, E_3)$.
3. $(\mathscr{GL}(E_1), \circ)$ est un groupe appelé *groupe linéaire* (groupe des automorphismes).

Démonstration. 1. Soit $(y_1, y_2) \in E_2^2$, soit $\lambda \in \mathbb{K}$ et soit $(x_1, x_2) \in E_1^2$ vérifiant $x_1 = \varphi^{-1}(y_1)$ et $x_2 = \varphi^{-1}(y_2)$. On a alors, par linéarité de φ, $\varphi(x_1 + \lambda x_2) = \varphi(x_1) + \lambda\varphi(x_2) = y_1 + \lambda y_2$, donc $\varphi^{-1}(y_1 + \lambda y_2) = \varphi^{-1}(y_1) + \lambda\varphi^{-1}(y_2)$. Ainsi, φ^{-1} est linéaire.

2. On a déjà vu que $\psi \circ \varphi$ est bijective et linéaire : c'est fini !

3. Montrons que c'est un sous-groupe du groupe des permutations de E_1 : $(S_{E_1}, \circ)$. L'application identité est bijective et linéaire, donc $\mathrm{Id}_{E_1} \in \mathscr{GL}(E_1)$. Les deux résultats précédents montrent que $\mathscr{GL}(E_1)$ est stable par passage à l'inverse et composition, ce qui permet de conclure.

□

Remarque 4.4.2.
Notation : Si $n \in \mathbb{N}^*$, $\mathscr{GL}(\mathbb{K}^n)$ est noté $\mathscr{GL}_n(\mathbb{K})$.

Exemple 4.4.3.

$$\begin{array}{rccc} \varphi : & \mathbb{R}^2 & \to & \mathbb{R}^2 \\ & (x, y) & \mapsto & (x - y, x + 2y) \end{array} \in \mathscr{GL}_2(\mathbb{R})$$

On résout le système $\varphi(x, y) = (a, b)$, et cela montre que φ est bijective, et donne l'expression de φ^{-1}.

5 Familles de vecteurs

Dans cette partie, sauf mention expresse du contraire, I désigne un ensemble et $(x_i)_{i\in I}$ une famille de vecteurs de E indexée par cet ensemble.

Définition 5.0.1.
Étant donné deux familles de vecteurs $(x_i)_{i\in I}$ et $(y_j)_{j\in J}$, on note $(x_i)_{i\in I} \uplus (y_j)_{j\in J}$ leur concaténation.

Remarque 5.0.2.
Ce n'est pas une notation officielle et nous ne définirons pas formellement cette notion. On pourra aussi utiliser le symbole $\biguplus_{i=1}^{n}$ pour écrire la concaténation de n familles de vecteurs de E.

Exemple 5.0.3.
$(x_1, x_2, x_3) \uplus (y_1, y_2) = (x_1, x_2, x_3, y_1, y_2)$.

5.1 Image du sous-espace vectoriel engendré par une famille de vecteurs.

On utilisera beaucoup le résultat suivant.

Proposition 5.1.1.
Soit E et F deux espaces vectoriels. Soit $(x_i)_{i\in I}$ une famille de vecteurs d'un espace vectoriel E et $f : \mathscr{L}(E,F)$. Alors l'image directe du sous-espace de E engendré par la famille $(x_i)_{i\in I}$ est le sous-espace de F engendré par la famille $(f(x_i))_{i\in I}$:

$$f\big(\text{Vect}\left((x_i)_{i\in I}\right)\big) = \text{Vect}\left((f(x_i))_{i\in I}\right)$$

Démonstration.
Posons $V = \text{Vect}\left((x_i)_{i\in I}\right)$. $f(V)$ est un sous-espace vectoriel de F. Comme V contient tous les x_i pour $i \in I$, $f(V)$ contient tous les $f(x_i)$ pour $i \in I$. Donc il contient le sous-espace engendré par les $f(x_i)$: $\text{Vect}\left((f(x_i))_{i\in I}\right) \subset f(V)$.

Réciproquement, soit y un élément de $f(V)$. y est l'image d'un élément x de V. Alors x est une combinaison linéaire $\sum_{i\in I} \lambda_i x_i$ (où la famille $(\lambda_i)_{i\in I}$ est à support fini), donc on a

$$\begin{aligned} y &= f(x) \\ &= f\left(\sum_{i\in I} \lambda_i x_i\right) \\ &= \sum_{i\in I} \lambda_i f(x_i) \\ &\in \text{Vect}\left((f(x_i))_{i\in I}\right) \end{aligned}$$

Donc $f(V) \subset \text{Vect}\left((f(x_i))_{i\in I}\right)$. □

Exemple 5.1.2.
Soit $\varphi : \begin{array}{ccc} \mathbb{R}_3[X] & \to & \mathbb{R}_2[X] \\ P & \mapsto & P' + XP'' \end{array}$. Donner $\text{Im}\,\varphi$.

5.2 Sev engendré par une famille finie

Dans cette sous-partie, on s'intéressera exclusivement au cas où $I = [\![1,n]\!]$. La famille $(x_i)_{i\in I}$ est donc le n-uplet $(x_1,\dots,x_n)$.

Proposition 5.2.1.
$\text{Vect}(x_1,\dots,x_n) = \text{Im}\,\psi$ où ψ est l'application linéaire de $\mathbb{K}^n$ dans E

$$\begin{array}{rccc} \psi : & \mathbb{K}^n & \to & E \\ & (\lambda_1,\dots,\lambda_n) & \mapsto & \displaystyle\sum_{k=1}^{n} \lambda_k x_k \end{array}$$

Proposition 5.2.2.
1. $\text{Vect}(x_1,\dots,x_n)$ n'est pas modifié si l'on permute deux vecteurs de $(x_1,\dots,x_n)$.
2. si pour un $i \in [\![1,n]\!]$ on a x_i qui est combinaison linéaire des autres vecteurs (en particulier, si $x_i = 0$), alors $\text{Vect}(x_1,\dots,x_n) = \text{Vect}(x_1,\dots,x_{i-1},x_{i+1},\dots,x_n)$, c'est-à-dire que l'on peut ôter x_i de la famille sans modifier le sev engendré.
3. $\text{Vect}(x_1,\dots,x_n)$ n'est pas modifié si l'on remplace un des x_i par une combinaison linéaire en $x_1,\dots,x_n$ dont le coefficient en x_i est non nul.

Démonstration.
1. C'est une conséquence directe du fait que $\text{Vect}\,(x_1,\dots,x_n) = \text{Vect}\,\{x_1,\dots,x_n\}$.
2. C'est une conséquence du fait que pour toutes parties X et Y de E, si $X \subset Y \subset \text{Vect}(X)$, alors $\text{Vect}(X) \subset (Y) \subset \text{Vect}\,(\text{Vect}(X)) = \text{Vect}(X)$
3. Quitte à permuter les vecteurs, on peut supposer que $i = n$. Considérons un vecteur x' obtenu par combinaison linéaire des x_k pour $k \in [\![1,n]\!]$ dont le coefficient de x_n est non nul. Posons $V = \text{Vect}(x_1,\dots,x_n)$ et $V' = \text{Vect}(x_1,\dots,x_{n-1},x')$ et montrons $V = V'$. Posons $V'' = \text{Vect}(x_1,\dots,x_{n-1},x_n,x')$. x' étant combinaison linéaire des x_k pour $k \in [\![1,n]\!]$, on a $V'' = V$ d'après le point précédent.

   De plus, le coefficient de x_n dans cette combinaison linéaire est non nul, donc x_n peut s'exprimer comme combinaison linéaire de x_1, …, x_{n-1} et x'. Donc, toujours d'après le point précédent, $V'' = V'$. On a donc $V = V'' = V'$.

□

Remarque 5.2.3.
0_E est toujours combinaison linéaire de toute famille de vecteurs : on peut donc « l'enlever » d'une famille sans modifier le sev engendré par cette famille.

Exemple 5.2.4.
Dans $\mathbb{R}^3$, avec $u_1 = (1,0,0)$, $u_2 = (0,1,0)$ et $u_3 = (1,1,0)$.

1. $\text{Vect}\,(u_1,u_2,u_3) = \text{Vect}\,(u_1,u_2) = \text{Vect}\,(u_1,u_3)$.
2. Déterminer une CNS sur $w \in \mathbb{R}^3$ pour que $\text{Vect}\,(u_1,u_2,u_3,w) \neq \text{Vect}\,(u_1,u_2,u_3)$.

Exemple 5.2.5.
On veut construire une base à partir de la base canonique : $\text{Vect}\,((1,0),(0,1)) = \text{Vect}\,((2,3),(0,1)) = \text{Vect}\,((2,3),(1,2))$: la famille $((2,3),(1,2))$ est donc une base de $\mathbb{R}^2$.
C'est l'autre sens qui est le plus souvent utilisé, et qui fait apparaître un pivot de Gauss (encore et toujours) : $\text{Vect}\,((3,4),(1,5)) = \text{Vect}\,((0,-11),(1,5)) = \text{Vect}\,((0,1),(1,5)) = \text{Vect}\,((0,1),(1,0))$: la famille $((3,4),(1,5))$ est donc une base de $\mathbb{R}^2$.

5.3 Familles génératrices

Définition 5.3.1.
On dit que la famille $(x_i)_{i\in I}$ est *génératrice* ou qu'elle *engendre* le $\mathbb{K}$-espace vectoriel E si $E = \text{Vect}_{\mathbb{K}}\left((x_i)_{i\in I}\right)$.

Remarque 5.3.2.
Ainsi, dans le cas où $I = [\![1,n]\!]$, $(x_i)_{i\in I}$ est génératrice si et seulement si l'application ψ de la proposition 5.1.1 est surjective.

Proposition 5.3.3.
La famille $(x_i)_{i\in I}$ est *génératrice* si et seulement si tout élément de E peut s'écrire comme une combinaison linéaire des vecteurs de cette famille.

Démonstration.
On a $\text{Vect}_{\mathbb{K}}\left((x_i)_{i\in I}\right) \subset E$ puisque tous les éléments de $(x_i)_{i\in I}$ appartiennent à E. On a donc

$$E = \text{Vect}_{\mathbb{K}}\left((x_i)_{i\in I}\right) = E \iff E \subset \text{Vect}_{\mathbb{K}}\left((x_i)_{i\in I}\right)$$

Qui est exactement ce que dit la proposition. □

Exemple 5.3.4.
1. Dans $\mathbb{R}^3$, $\left\{\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix}\right\}$ est génératrice car $\begin{pmatrix}x\\y\\z\end{pmatrix} = xe_1 + ye_2 + ze_3$. Se généralise à $\mathbb{R}^n$ avec base canonique.
2. Dans $\mathbb{C}$ considéré comme un $\mathbb{R}$-ev, une famille génératrice est $\{1, i\}$.
3. Dans $\mathbb{C}$ considéré comme un $\mathbb{C}$-ev, une famille génératrice est $\{z\}$, pour n'importe quel $z \neq 0$. On peut noter $\mathbb{C} = \text{Vect}_{\mathbb{R}}(1,i) = \text{Vect}_{\mathbb{C}}(z)$.
4. Dans le $\mathbb{R}$-espace vectoriel $\mathbb{R}[X]$, la famille $\left(X^k\right)_{k\in\mathbb{N}}$ est une famille génératrice de $\mathbb{R}[X]$. Dans le $\mathbb{C}$-espace vectoriel $\mathbb{C}[X]$, la famille $\left(X^k\right)_{k\in\mathbb{N}}$ est une famille génératrice de $\mathbb{C}[X]$. En revanche, dans le $\mathbb{R}$-espace vectoriel $\mathbb{C}[X]$, la famille $\left(X^k\right)_{k\in\mathbb{N}}$ n'est pas génératrice de $\mathbb{C}[X]$ (car $\text{Vect}_{\mathbb{R}}\left(\left(X^k\right)_{k\in\mathbb{N}}\right) = \mathbb{R}[X] \neq \mathbb{C}[X]$.
5. Dans le $\mathbb{C}$-espace vectoriel $\mathbb{C}(X)$, d'après le cours sur la décomposition en élément simple, on obtient une famille génératrice de $\mathbb{C}(X)$ en regroupant les familles $\left(X^k\right)_{k\in\mathbb{N}}$ et $\left(\frac{1}{(X-\alpha)^k}\right)_{(\alpha,k)\in\mathbb{R}\times\mathbb{N}}$.

Remarque 5.3.5.
On a aussi la notion de famille génératrice d'un sev F de E.

Remarque 5.3.6.
On appelle *droite vectorielle* tout sev engendré par un seul vecteur (non nul), qui est alors *vecteur directeur*. Correspond bien à ce qui se passe dans $\mathbb{R}^2$ et $\mathbb{R}^3$.
Idem avec *plan vectoriel* et deux vecteurs.

Proposition 5.3.7.
Soit E, F deux $\mathbb{K}$-espaces-vectoriels, $f \in \mathscr{L}(E,F)$, soit $(x_i)_{i\in I}$ une famille génératrice de E. Alors, $(f(x_i))_{i\in I}$ est une famille génératrice de $\text{Im}\, f$.

Démonstration.
C'est juste une réécriture de la proposition 5.0.4 □

Corollaire 5.3.8.
Soit E et F deux $\mathbb{K}$-espaces vectoriels, $f \in$

$\mathscr{L}(E,F)$ avec f **surjective** et $(x_i)_{i\in I}$ **génératrice**. Alors l'image de cette famille par f est génératrice.

Démonstration.
C'est une conséquence directe de la proposition 5.0.4 :

$$\begin{aligned} F &= f(E) && \text{par surjectivité de } F \\ &= f\big(\text{Vect}\left((x_i)_{i\in I}\right)\big) && \text{car } (x_i)_{i\in I} \text{ génératrice} \\ &= \text{Vect}\left((f(x_i))_{i\in I}\right) && \text{par prop. 5.0.4} \end{aligned}$$

□

Exemple 5.3.9.
Soit

$$f : \begin{array}{ccc} \mathbb{R}^3 & \to & \mathbb{R}^3 \\ \begin{pmatrix} x \\ y \\ z \end{pmatrix} & \mapsto & \begin{pmatrix} 3x & - & y & & \\ 2x & + & y & + & z \\ x & + & 3y & + & 2z \end{pmatrix} \end{array}.$$

Alors,

$$\begin{aligned} \text{Im}(f) &= \text{Vect}(f(1,0,0), f(0,1,0), f(0,0,1)) \\ &= \text{Vect}((3,2,1),(-1,1,3),(0,1,2)) \\ &= \text{Vect}((0,5,10),(-1,1,3),(0,1,2)) \\ &= \text{Vect}((-1,1,3),(0,1,2)). \end{aligned}$$

Proposition 5.3.10. 1. Une famille génératrice à laquelle on ajoute des vecteurs est toujours génératrice.

2. On peut retirer tout vecteur qui est combinaison linéaire des autres vecteurs de la famille (c'est une condition suffisante mais elle est en fait aussi nécessaire).

Démonstration. 1. Découle du fait que l'inclusion de deux parties implique l'inclusion des sous-espaces engendrés.

2. Découle du fait que pour toutes parties X et Y de E, $X \subset Y \subset \text{Vect}(X)$ implique $\text{Vect}(X) = \text{Vect}(Y)$.

□

Exemple 5.3.11. 1. Dans $\mathbb{R}^4$, on considère $\mathscr{P}$ l'ensemble de $\mathbb{R}^4$ défini par

$$\mathscr{P} : \begin{cases} x - y + 2t &= 0 \\ x + y - z &= 0 \end{cases}$$

où (x,y,z,t) sont les coordonnées dans $\mathbb{R}^4$. On trouve

$$\mathscr{P} = \text{Vect}((1,0,1,-1/2),(0,1,1,1/2))$$

donc c'est bien un plan.

2. On considère l'ensemble S des suites réelles vérifiant $u_{n+2} + 2u_{n+1} - 3u_n = 0$. S est un sous-espace vectoriel de $\mathbb{R}^{\mathbb{N}}$ (le vérifier). On veut en donner une famille génératrice. On résout comme dans le cours, on trouve deux vecteurs générateurs. Ça marcherait pareil avec les solutions d'une équation différentielle.

Théorème 5.3.12.
Soient F et G deux sous-espaces vectoriels de E. Alors toute concaténation d'une famille génératrice de F et d'une famille génératrice de G est une famille génératrice de $F+G$.

Démonstration.
Soit $(x_i)_{i\in I_1}$ une famille génératrice de F et $(x_i)_{i\in I_2}$ une famille génératrice de G. Notons $(x_i)_{i\in I} = (x_i)_{i\in I_1} \uplus (x_i)_{i\in I_1}$

Toute combinaison linéaire d'éléments de la famille $(x_i)_{i\in I}$ est dans $F+G$.

Réciproquement, tout élément de $F+G$ s'écrit comme somme d'un élément de F et d'un élément de G. Le premier est une combinaison linéaire d'éléments de la famille $(x_i)_{i\in I_1}$ et le second de la famille $(x_i)_{i\in I_2}$. Donc leur somme est une combinaison linéaire d'éléments de la famille $(x_i)_{i\in I}$ □

5.4 Familles libres et liées

Définition 5.4.1.
On dit que la famille $(x_i)_{i\in I}$ est *libre* si toute combinaison linéaire d'éléments de $(x_i)_{i\in I}$ dont la valeur est 0_E est la combinaison triviale, c'est-à-dire n'a que des coefficients nuls. Formellement, la famille est libre si et seulement si, pour toute famille de scalaires $(\lambda_i)_{i\in I}$ à support fini, on a

$$\sum_{i\in I} \lambda_i x_i = 0 \Rightarrow \forall i \in I \ \lambda_i = 0$$

Dans le cas où $I = [\![1, n]\!]$, cette condition s'écrit : pour tout n-uplet $(\lambda_1, \dots, \lambda_n)$ de scalaires, on a

$$\sum_{i=1}^{n} \lambda_i x_i = 0 \Rightarrow (\lambda_1, \dots, \lambda_n) = (0, \dots, 0)$$

Une famille non libre est dite *liée*.

Remarque 5.4.2. — Une famille est donc liée si et seulement s'il existe une combinaison linéaire de valeur nulle à coefficients non tous nuls.
— Si l'un des x_i est nul, la famille est liée.
— Si la famille comporte deux fois le même vecteur, elle est liée.

Remarque 5.4.3.
Ainsi, dans le cas où $I = [\![1, n]\!]$, $(x_i)_{i\in I}$ est libre si et seulement si l'application ψ de la proposition 5.1.1 est injective.

Proposition 5.4.4.
La famille $(x_i)_{i\in I}$ est libre si et seulement si tout élément x de E s'écrit d'au plus une façon comme combinaison linéaire (à coefficients non nuls) d'éléments de E.

Démonstration.Sens direct Supposons que la famille $(x_i)_{i\in I}$ est libre et montrons que tout élément x de E s'écrit d'au plus une façon comme combinaison linéaire (à coefficients non nuls) d'éléments de E.

Soit x un élément de E. Supposons qu'il s'écrive à la fois $\sum_{i\in I} \lambda_i x_i$ et $\sum_{i\in I} \mu_x x_i$ où $(\lambda_i)_{i\in I}$ et $(\mu_i)_{i\in I}$ sont des familles de scalaires à support fini.

Alors on a

$$0 = x - x = \sum_{i\in I} (\lambda_i - \mu_i) x_i$$

Or la famille $(x_i)_{i\in I}$ est libre, donc pour tout $i \in I$, on a $\lambda_i - \mu_i = 0$.

Donc tout élément de E s'écrit d'au plus une façon comme combinaison linéaire (à coefficients non nuls) d'éléments de E.

Sens indirect Supposons que tout élément de E s'écrit d'au plus une façon comme combinaison linéaire (à coefficients non nuls) d'éléments de E et montrons que la famille $(x_i)_{i\in I}$ est libre.

Soit $(\lambda_i)_{i\in I}$ une famille de scalaires à support fini vérifiant

$$\sum_{i\in I} \lambda_i x_i = 0$$

Alors en posant $\mu_i = 0$ pour tout $i \in I$, on a aussi

$$\sum_{i\in I} \mu_i x_i = 0$$

0 s'écrit donc de deux façons comme combinaison linéaire de la famille $(x_i)_{i\in I}$: les deux familles $(\lambda_i)_{i\in I}$ et $(\mu_i)_{i\in I}$ sont donc la même famille :

$$\forall i \in I \quad \lambda_i = 0$$

La famille $(x_i)_{i\in I}$ est donc libre.

□

Proposition 5.4.5.
La famille $(x_i)_{i\in I}$ est *libre* si et seulement si aucun élément de cette famille ne peut s'exprimer comme combinaison linéaire des autres éléments de la famille.

Démonstration.
On fera ici la démonstration dans le cas où $I = [\![1, n]\!]$ qui est le cas qu'on rencontrera le plus fréquemment par la suite. La démonstration n'est pas plus compliquée dans le cas général.

Montrons que la famille considérée est liée, c'est-à-dire qu'il existe une combinaison linéaire non triviale valant 0, si et seulement si au moins un élément de la famille s'écrit comme combinaison linéaire des autres éléments de la famille.

Sens indirect Supposons qu'il existe une combinaison linéaire non triviale de $(x_1, \dots, x_n)$ valant 0. Notons $\lambda_1, \dots \lambda_n$ ses coefficients. L'un d'eux au moins étant non-nul, on peut supposer $\lambda_1 \neq 0$, quitte à permuter les vecteurs. Alors on a

$$\sum_{k=1}^{n} \lambda_k x_k = 0$$

donc

$$x_1 = \sum_{k=2}^{n} \Big(-\frac{\lambda_k}{\lambda_1}\Big) x_k$$

Donc x_1 est combinaison linéaire des autres vecteurs de la famille.

Sens direct Supposons que x_1 s'écrive

$$x_1 = \sum_{k=2}^{n} \lambda_k x_k$$

où $x_2, \ldots, x_n$ sont d'autres éléments de la famille et $\lambda_1, \ldots, \lambda_k$ sont des scalaires. Alors, en posant $\lambda_1 = -1$, on a

$$\sum_{k=1}^{n} \lambda_k u_k = 0$$

Et cette combinaison linéaire n'est pas triviale puisque λ_1 n'est pas nul, donc la famille est liée.

(le cas général fonctionne de même). □

Exemple 5.4.6. 1. Dans $\mathbb{R}^2$: une famille de deux vecteurs est liée si et seulement si les deux vecteurs sont colinéaires, donc une famille de deux vecteurs est libre si et seulement si c'est une base.

2. Dans $\mathbb{R}^3$, une famille de 3 vecteurs est liée si et seulement si les 3 vecteurs sont coplanaires, donc une famille de trois vecteurs est libre si et seulement si c'est une base.

Remarque 5.4.7.
Dans $\mathbb{R}^n$, si on utilise la définition pour chercher si une famille est libre, on est ramené à la résolution d'un système linéaire (une fois de plus).

Exemple 5.4.8.
• Montrer que $((1,0),(-1,2),(2,4))$ est liée dans $\mathbb{R}^2$.
• Montrer que $((1,0,0),(0,-1,1),(1,0,2))$ est libre dans $\mathbb{R}^3$.
• $(x \mapsto \sin x, x \mapsto \sin 2x, x \mapsto \sin 3x)$ est libre.

Définition 5.4.9.
Soit x, y deux vecteurs de E. On dit que
- x est colinéaire à y s'il existe $\lambda \in \mathbb{K}$ tel que $x = \lambda y$;
- x et y sont colinéaires s'il existe $\lambda \in \mathbb{K}^*$ tel que $x = \lambda y$.

Remarque 5.4.10.
- La relation « sont colinéaires » est une relation d'équivalence sur E, pas « est colinéaire à ».
- Si x et y sont tous les deux non nuls, x est colinéaire à y si et seulement si x et y sont colinéaires.

Proposition 5.4.11.
Soit x et y deux vecteurs de E. Alors (x, y) est libre si et seulement si aucun de ces vecteurs n'est colinéaire à l'autre.

Démonstration.
Élémentaire : à vous de le faire. □

 Cet argument n'est valable que pour deux vecteurs, comme nous l'avons vu plus haut.

Proposition 5.4.12.
Soit E et F deux $\mathbb{K}$-espaces vectoriels, $f \in \mathscr{L}(E,F)$ avec f **injective** et $(x_i)_{i\in I}$ une famille **libre** de E. Alors l'image de cette famille par f est libre.

Démonstration.
Soit $(\lambda_i)_{i\in I}$ une famille de scalaires à support fini tel que

$$\sum_{i\in I} \lambda_i f(x_i) = 0$$

Alors, par linéarité de f,

$$\sum_{i\in I} f(\lambda_i x_i) = 0.$$

Or f est injective donc

$$\sum_{i\in I} \lambda_i x_i = 0$$

Or $(x_i)_{i\in I}$ est libre, donc pour tout $i \in I$, $\lambda_i = 0$. □

Définition 5.4.13.
Soit $(x_i)_{i\in I}$ une famille de vecteurs de E. Pour tout $J \subset I$, on dit que $(x_i)_{i\in J}$ est une sous-famille de $(x_i)_{i\in I}$ et que $(x_i)_{i\in I}$ est une sur-famille de $(x_i)_{i\in J}$.

Théorème 5.4.14. 1. Toute sur-famille d'une famille liée est liée.

2. Toute sous-famille d'une famille libre est libre.

3. Si $(x_1, \dots, x_n)$ est une famille libre, alors $(x_1, \dots, x_n, x_{n+1})$ est libre si et seulement si x_{n+1} n'est pas combinaison linéaire des $x_1, \dots, x_n$.

Démonstration. 1. Il existe une combinaison linéaire nulle non triviale de la sous-famille. Il suffit de la compléter par des 0 pour en obtenir une pour la sur-famille.
2. C'est la contraposée du point précédent.
3. Le sens direct est évident. Pour l'autre sens, par contraposée supposons que $(x_1, \dots, x_n, x_{n+1})$ est liée. Alors il existe une combinaison linéaire nulle non triviale de $x_1, \dots x_n$, x_{n+1}. Si le coefficient de x_{n+1} est nul, il s'agit d'une combinaison linéaire des $x_1, \dots, x_n$. Sinon, on peut exprimer x_n comme combinaison linéaire de $x_1, \dots, x_n$.

□

Exemple 5.4.15.
Dans $\mathbb{R}^2$, toute famille de trois vecteurs ou plus est liée : si les deux premiers vecteurs sont liés, la famille l'est aussi. Sinon, le troisième vecteur est combinaison linéaire des deux premiers, car les deux premiers forment une base.
Idem dans $\mathbb{R}^3$ avec les familles de plus de 4 vecteurs.

Proposition 5.4.16.
Soient $F_1, \dots, F_n$ des sev d'un $\mathbb{K}$-ev E, et pour tout $i \in [\![1, n]\!]$, soit $\mathscr{F}_i$ une famille libre de F_i.
Si les F_i sont en somme directe, alors $\biguplus_{i=1}^{n} \mathscr{F}_i$ est une famille libre.

Enfin, terminons par un résultat bien pratique :

Définition 5.4.17.
Soit $n \in \mathbb{N}^*$ et $E = \mathbb{K}^n$. Soit $p \in [\![1, n]\!]$ et $(v_1, \cdots, v_p)$ une famille de vecteurs de E. Pour tout $i \in [\![1, p]\!]$, notons $(v_{i,j})_{j \in [\![1,n]\!]}$ les coordonnées du vecteur v_i. On dit que la famille $(v_1, \cdots, v_p)$ est *échelonnée* si :

1. pour tout $i \in [\![1, p]\!]$ il existe $r_i \in [\![0, n]\!]$ tel que $v_{i,r_i} \neq 0$ et pour tout $j \in [\![1, n]\!]$ tel que $j > r_i$, $v_{i,j} = 0$;
2. la suite des r_i est strictement croissante.

Exemple 5.4.18.
Dans $\mathbb{R}^5$, $\left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \\ 0 \\ -3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 2 \\ -5 \end{pmatrix} \right)$ est une famille échelonnée.
La famille $\left(\begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \\ 0 \\ -3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 2 \\ -5 \end{pmatrix} \right)$ n'en est pas une.

Remarque 5.4.19.
Avec les mêmes notations, si $0 \leqslant k < i \leqslant p$, alors $v_{k,r_i} = 0$.

Proposition 5.4.20.
Toute famille échelonnée sans vecteur nul est libre.

Démonstration.
Soit $n \in \mathbb{N}^*$ et $E = \mathbb{K}^n$. Soit $p \in [\![1, n]\!]$ et $(v_1, \cdots, v_p)$ une famille échelonnée de vecteurs de E.
Le résultat est assez intuitif et se voit facilement, par exemple en considérant le système $\sum_{i=1}^{p} \lambda_i v_i = 0$. En écrivant le système, on se rend compte qu'en remontant les lignes, les coefficients λ_i s'annulent les uns après les autres (le faire sur un exemple).
Donnons tout de même une démonstration propre, par récurrence sur le nombre de vecteurs. Pour tout $p \in [\![1, n]\!]$, posons (H_p) : toute famille échelonnée de E ayant p vecteurs non nuls est libre.
Un vecteur non nul formant à lui seul une famille libre, (H_1) est immédiate.
Soit $p \in [\![1, n-1]\!]$ tel que (H_p) soit vraie. Soit $(v_1, \cdots, v_{p+1})$ une famille échelonnée à vecteurs non nuls. Définissons les r_i comme dans la définition **??**. Soit $\lambda_1, \cdots, \lambda_{p+1}$ des scalaires tels que $\sum_{i=1}^{p+1} \lambda_i v_i = 0$. La r_{p+1}-ème ligne de ce système s'écrit $\lambda_{p+1} v_{p+1,r_{p+1}} = 0$, puisque pour tout $i \leqslant p$, $v_{i,r_{p+1}} = 0$, par définition d'une famille échelonnée. Mais comme $v_{p+1,r_{p+1}} \neq 0$, alors $\lambda_{p+1} = 0$. Il reste alors $\sum_{i=1}^{p} \lambda_i v_i = 0$. Mais $(v_1, \cdots, v_p)$ est échelonnée, donc par

hypothèse de récurrence elle est libre, ce qui implique que tous les λ_i sont nuls, d'où (H_{p+1}). □

Remarque 5.4.21.
Par abus, les familles de vecteurs présentant des blocs de zéros dans d'autres « coins » que le « coin inférieur gauche » peuvent aussi être dites échelonnées. En tout cas, avec la même démonstration, elles sont également libres. Par exemple les familles $\left(\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right)$, $\left(\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\right)$ et $\left(\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}\right)$ sont libres.

5.5 Bases

Définition 5.5.1.
Une famille $((x_i)_{i\in I})$ est une *base* de E si elle est libre et génératrice.

Remarque 5.5.2.
Ainsi, dans le cas où $I = [\![1, n]\!]$, $(x_i)_{i\in I}$ est une base si et seulement si l'application ψ de la proposition 5.1.1 est un isomorphisme.

Exemple 5.5.3.
Les bases canoniques des $\mathbb{R}^n$.

Remarque 5.5.4.
On a aussi la notion de base d'un sev de E.

Remarque 5.5.5.
Comme pour les familles libres et génératrices, on peut permuter l'ordre des vecteurs d'une base, et on a toujours une base.

Proposition 5.5.6.
Soit $\mathscr{B} = (x_i)_{i\in I}$ une famille de E. Alors $\mathscr{B}$ est une base si et seulement si pour tout $y \in E$, il existe une unique famille de scalaires $(\lambda_i)_{i\in I}$ à support fini telle que

$$y = \sum_{i\in I} \lambda_i x_i.$$

En particulier dans le cas où $I = [\![1, n]\!]$, $\mathscr{B}$ est une base si et seulement si pour tout $y \in E$, il existe un unique n-uplet $(\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n$ tel que

$$y = \sum_{k=1}^{n} \lambda_k x_k.$$

Démonstration.
On a déjà vu que cette famille de scalaires existe si et seulement si $(x_i)_{i\in I}$ est génératrice et est unique sous réserve d'existence si et seulement si $(x_i)_{i\in I}$ est libre. On en déduit le résultat. □

Définition 5.5.7.
Soit $\mathscr{B} = (x_i)_{i\in I}$ une base de E et $y \in E$. Alors l'unique famille de scalaire (à support fini) $(\lambda_i)_{i\in I}$ telle que $y = \sum_{i\in I} \lambda_i x_i$ est appelé *famille des coordonnées* de y dans $\mathscr{B}$.

Dans le cas où $I = [\![1, n]\!]$, cette famille est un n-uplet, appelé *n-uplet des coordonnées*.

Exemple 5.5.8.
Classique : montrer que $((1, 0, 1), (2, -1, 0), (0, 1, 1))$ est une base de $\mathbb{R}^3$, donner les coordonnées d'un vecteur dans cette base (mais attention, les coordonnées des vecteurs dans cette base et dans la base canonique ne sont pas les mêmes !).

Exemple 5.5.9.
Donner une base de $\mathscr{P} \subset \mathbb{R}^3$ où $\mathscr{P} = \{ (x, y, z) \in \mathbb{R}^3 \mid x + 2y - z = 0 \}$.

On a $(x, y, z) \in \mathscr{P}$ si et seulement si $x = x$, $y = y$ et $z = x + 2y$ si et seulement s'il existe $\alpha, \beta \in \mathbb{R}$ tel que $(x, y, z) = \alpha(1, 0, 1) + \beta(0, 1, 2)$ si et seulement si $(x, y, z) \in \mathrm{Vect}((1, 0, 1), (0, 1, 2))$. Et ces deux vecteurs sont libres.

Exemple 5.5.10.
Trouver une base de

$$\mathscr{E} = \left\{ (u_n) \in \mathbb{R}^{\mathbb{N}} \mid u_{n+2} + u_{n+1} - 2u_n = 0 \right\}.$$

Le polynôme caractéristique est $X^2 + X - 2$ de racine 1 et -2. Donc tout élément de $\mathscr{E}$ est combinaison linéaire de la suite $(v_n) = (1)$ et $(w_n) = ((-2)^n)$. Donc $((u_n), (v_n))$ est génératrice. On montre qu'elle est aussi libre.

Remarque 5.5.11.
Si E est un $\mathbb{K}$-ev admettant une base $\mathscr{B}$ à n vecteurs, alors l'application qui à un vecteur de E associe le n-uplet de ses coordonnées dans la base $\mathscr{B}$ est un ismorphisme de E dans $\mathbb{K}^n$. L'injectivité découle de l'unicité du n-uplet des coordonnées dans une base donnée.
Il est alors fréquent d'identifier un vecteur de E au n-uplet de ses coordonnées, et donc de l'identifier à un vecteur de $\mathbb{K}^n$. La proposition qui suit en est une illustration classique :

Proposition 5.5.12.
Une famille de polynômes non nuls de degrés distincts deux à deux est libre.

Démonstration.
Ce résultat peut très bien se démontrer en n'utilisant que des considérations de degré : c'est un bon exercice, classique, et laissé au lecteur.
Mais démontrons-le en utilisant des coordonnées.
Soit $\mathscr{F}$ une telle famille. Nous pouvons toujours supposer que les polynômes de cette famille sont classés de telle sorte que la suite de leurs degrés soit strictement croissante. Notons n le degré maximum de ces polynômes. Cette famille est donc une famille de $\mathbb{K}_n[X]$, dont $\mathscr{B} = (1, X, X^2, \cdots, X^n)$ est une base. La famille des $(n+1)$-uplets des coordonnées des polynômes de $\mathscr{F}$ dans la base $\mathscr{B}$ est donc une famille échelonnée de $\mathbb{K}^{n+1}$: elle est donc libre. Par conséquent, $\mathscr{F}$ aussi. □

Proposition 5.5.13.
L'image d'une base par une application linéaire injective est une base de l'image.

L'image d'une base par un isomorphisme est une base de l'espace d'arrivée.

Démonstration.
Vient directement des résultats des parties précédentes. □

Théorème 5.5.14.
Soient E_1 et E_2 deux ev, et soient $(f_i)_{i\in I}$ une base de E_1 et $(g_i)_{i\in I}$ une famille **quelconque** de E_2. Alors il existe une **unique** application linéaire $\varphi : E_1 \to E_2$ telle que pour tout $i \in [\![1, n]\!]$, $\varphi(f_i) = g_i$.

Démonstration. **Analyse** Soit φ une telle application. Soit $x \in E$. Alors x s'écrit $\sum_{i\in I} \lambda_i f_i$, donc

$$\begin{aligned}\varphi(x) &= \sum_{i\in I} \lambda_i \varphi(f_i)\\ &= \sum_{i\in I} \lambda_i g_i\end{aligned}$$

où $(\lambda_i)_{i\in I}$ est la famille des coordonnées de x dans la base $(f_i)_{i\in I}$.
$\varphi(x)$ est donc déterminé de façon unique.
Donc φ est déterminée de façon unique.

Synthèse Considérons l'application qui à tout élément x de E associe $\sum_{i\in I} \lambda_i g_i$, où $(\lambda_i)_{i\in I}$ est la famille des coordonnées de x dans la base $(f_i)_{i\in I}$.
On montre que φ est une application linéaire. De plus on peut montrer qu'elle vérifie les conditions demandées : $\forall i \in I\ f(f_i) = g_i$.

Conclusion Il existe bien une unique application répondant à la question posée.

□

Exemple 5.5.15.
Montrer qu'il existe une unique application linéaire $\varphi : \mathbb{R}_2[X] \to \mathbb{R}^2$ vérifiant les conditions suivantes :

$$\begin{aligned}\varphi(1) &= (1, 2)\\ \varphi(X+1) &= (2, 3)\\ \varphi(X^2+1) &= (0, 1)\end{aligned}$$

Théorème 5.5.16.
Soient $F_1, \ldots, F_n$ des sev d'un $\mathbb{K}$-ev E, et pour tout $i \in [\![1, n]\!]$, soit $\mathscr{B}_i$ une base de F_i.
Alors les F_i sont en somme directe si et seulement si $\biguplus_{i=1}^{n} \mathscr{B}_i$ est une base de $F_1 + \ldots + F_n$.
En particulier, les F_i sont supplémentaires si et seulement si $\biguplus_{i=1}^{n} \mathscr{B}_i$ est une base de E.

Démonstration. ($\Rightarrow$) Supposons que les F_i sont en somme directe. Alors, comme chaque $\mathscr{B}_i$ engendre F_i, leur union engendre $F_1 + \cdots + F_n$. Notons, avec un léger abus de notation, pour tout i, $\mathscr{B}_i = (x_i^j)_j$ et montrons donc que $\biguplus_{i=1}^{n} \mathscr{B}_i$ est libre. Soit une famille (λ_i^j) telle que $\sum_{i,j} \lambda_i^j x_i^j = 0_E$. Notons, pour tout i,

$u_i = \sum_j \lambda_i^j x_i^j \in F_i$. Donc, $u_1 + \cdots + u_n = 0_E$ et donc, comme les F_i sont en somme directe, pour tout i, $u_i = 0_E$. Par liberté de chaque famille $\mathscr{B}_i$, la famille (λ_i^j) est nulle, donc $\biguplus_{i=1}^{n} \mathscr{B}_i$ est libre.

($\Leftarrow$) Si $\biguplus_{i=1}^{n} \mathscr{B}_i$ est une base de $F_1 + \ldots + F_n$, soit $(y_1, \ldots, y_n) \in E_1 \times \cdots \times E_n$ tel que $y_1 + \cdots + y_n = 0_E$. Notons, pour chaque i, $(\lambda_i^j)_j$ les coordonnées de y_i dans $\mathscr{B}_i = (x_i^j)$. On a alors $\sum_{i,j} \lambda_i^j x_i^j = 0_E$. $\biguplus_{i=1}^{n} \mathscr{B}_i$ étant une base, la famille $(\lambda_i^j)_{i,j}$ est nulle, et donc a fortiori les $(y_i)_i$ le sont. Donc $F_1 + \cdots + F_n$ est directe.

□

5.6 Repère affine

On peut maintenant faire le lien entre les notions de base et de coordonnées vues dans les espaces vectoriels, et les notions géométriques de *repère* et de *coordonnées dans un repère* utilisées dans les petites classes.

Soit $\mathscr{F}$ un sous-espace affine de E, de direction F.

Définition 5.6.1.
Un repère de $\mathscr{F}$ est un couple $(O, \mathscr{B})$, où $O \in F$ et $\mathscr{B}$ est une base de F. Les coordonnées d'un point $x \in \mathscr{F}$ dans le repère $(O, \mathscr{B})$ sont les coordonnées de $x - O$ dans la base $\mathscr{B}$ (de F).

Remarque 5.6.2.
On dit souvent que O est l'origine du repère $(O, \mathscr{B})$.

Remarque 5.6.3.
À repère fixé, tout point de $\mathscr{F}$ est caractérisé par ses coordonnées (affines).

Exemple 5.6.4.
Revenir sur les études des solutions d'équations différentielles linéaires.

6 Endomorphismes particuliers

6.1 Homothéties

Définition 6.1.1.
Soit E un $\mathbb{K}$-ev. Soit $\lambda \in \mathbb{K}^*$. On appelle *homothétie de rapport* λ l'application

$$h_\lambda = \lambda \mathrm{Id}_E : \begin{array}{ccc} E & \to & E \\ x & \mapsto & \lambda x \end{array}$$

Remarque 6.1.2.
Cas particuliers : $\lambda = 1$: identité ; $\lambda = -1$, symétrie de centre 0.

Théorème 6.1.3.
Toute homothétie est un automorphisme de E, et $(h_\lambda)^{-1} = h_{\lambda^{-1}} = h_{1/\lambda}$.

Démonstration.
• Linéarité : simple.
• Bijectivité et réciproque : calculer $h_\lambda \circ h_{\lambda^{-1}}$ et $h_{\lambda^{-1}} \circ h_\lambda$. □

Proposition 6.1.4.
Soit $\mathscr{H}(E)$ l'ensemble des homothéties de E. Alors $(\mathscr{H}(E), \circ)$ est un sous-groupe de $\mathscr{GL}(E)$.

Démonstration.
• $\mathscr{H}(E) \subset \mathscr{GL}(E)$ d'après le théorème précédent.
• $\mathrm{Id} \in \mathscr{H}(E)$.
• Stable par passage à l'inverse d'après le théorème précédent.
• et on remarque que pour tout $\lambda, \mu \in \mathbb{K}^\star$, $h_\mu \circ h_\lambda = h_{\mu\lambda}$, donc on a la stabilité par produit. □

Remarque 6.1.5.
$\mathscr{GL}(E)$ n'est pas un sous-groupe commutatif, mais $\mathscr{H}(E)$ l'est. En fait il est isomorphe à $\mathbb{K}^\star$ via $\lambda \mapsto h_\lambda$.

6.2 Projecteurs

Dans toute la suite, on suppose que F et G sont deux sev supplémentaires, *i.e.* $E = F \oplus G$.

Définition 6.2.1.
On appelle *projection* sur F parallèlement à G l'endomorphisme p_F de $\mathscr{L}(E)$ défini par :

$$\forall y \in F,\ \forall z \in G \quad p_F(y+z) = y. \qquad \text{(XVIII.3)}$$

Remarque 6.2.2.
Voir le dessin sur la figure XVIII.1. Exemple dans $\mathbb{R}^3$ avec $F = \{x = 0\}$ et $G = \{x + y = 0, y + z = 0\}$.

Démonstration.
Il convient de montrer que cette définition est correcte, c'est-à-dire qu'il existe une unique application vérifiant les conditions demandées.

Analyse Soit p_F un endomorphisme vérifiant les conditions demandées. Alors pour tout $x \in E$, $p_F(x) = y$ où (y, z) est l'unique couple[4] de $F \times G$ tel que $x = y + z$. p_F est donc déterminé.

Synthèse Soit p_F l'application associant à tout $x \in E$ l'unique valeur[5] y telle que x s'écrive $y+z$ avec $y \in F$ et $z \in G$.

La proposition (XVIII.3) est manifestement vérifiée. On peut par ailleurs montrer que p_F est une application linéaire.

Conclusion Il existe une unique application vérifiant les conditions demandées

□

Théorème 6.2.3.
$p_F \in \mathscr{L}(E)$, $\operatorname{Ker} p_F = G$, $\operatorname{Im}(p_F) = F$.

Démonstration.
• Linéarité : élémentaire.
• Soit $x = y + z \in E$, $y \in F$, $z \in G$, donc $x \in \operatorname{Ker} p_F$ si et seulement si $y = 0$ si et seulement si $x = z$ si et seulement si $x \in G$.
$x \in \operatorname{Im} p_F$ si et seulement si il existe $x' = y' + z'$ tel que $x = y'$ si et seulement si $x \in F$. □

Remarque 6.2.4.
• Cas particuliers : $F = \{0_E\}$ et $G = E$: $p_F = 0_{\mathscr{L}(E)}$.
• $G = \{0_E\}$ et $F = E$: $p_F = \mathrm{Id}$. Hormis ce dernier cas, une projection n'est jamais injective, ni surjective.
• $p_F + p_G = \mathrm{Id}$, $p_F|_G = 0$, $p_F|_F = \mathrm{Id}_F$.

4. Il existe et est unique puisque $E = F \oplus G$.
5. Voir remarque précédente.

Définition 6.2.5.
On appelle *projecteur* tout endomorphisme f tel que $f \circ f = f$.

Théorème 6.2.6.
Toute projection est un projecteur.

Démonstration.
Il s'agit essentiellement d'utiliser que si $x = y + z$ $p_F(p_F(x)) = p_F(y) = p_F(y + 0_E) = y$. □

Théorème 6.2.7 (Réciproque)**.**
Soit f un projecteur. Alors $\operatorname{Ker} f \oplus \operatorname{Im} f = E$, et f est la projection sur $\operatorname{Im} f$ parallèlement à $\operatorname{Ker} f$.

Démonstration.
Soit $x \in \operatorname{Ker} f \cap \operatorname{Im} f$. Alors il existe y tel que $x = f(y)$. Or $f(x) = 0$ mais $f(x) = f(f(y)) = f(y) = x$, donc $x = 0$. $\operatorname{Ker} f$ et $\operatorname{Im} f$ sont donc en somme directe.
Montrons que $E = \operatorname{Ker} f + \operatorname{Im} f$.
Analyse : soient $y \in \operatorname{Im} f$ et $z \in \operatorname{Ker} f$ tels que $x = y + z$. Alors il existe u tel que $y = f(u)$. Donc $f(x) = f(f(u)) + f(z) = f(f(u)) = f(u) = y$. Donc on a $y = f(x)$ et donc $z = x - f(x)$.
Synthèse : on pose $y = f(x)$ et $z = x - f(x)$. Alors on a bien $x = y + z$. de plus $f(y) = f(f(x)) = f(x) = y$, donc $y \in \operatorname{Im} f$, et $f(z) = f(x - f(x)) = f(x) - f(f(x)) = f(x) - f(x) = 0$, et ainsi $z \in \operatorname{Ker} f$. On a bien le résultat voulu.
Mais si l'on note $x = y + z$ la décomposition associée à $\operatorname{Ker} f \oplus \operatorname{Im} f = E$, alors $\forall x$, $f(x) = y$, donc f est bien la projection sur $\operatorname{Im} f$ parallèlement à $\operatorname{Ker} f$. □

Remarque 6.2.8. 1. Si f est un projecteur, alors $\operatorname{Im} f = \operatorname{Ker}(f - \mathrm{Id})$: on utilise que $x \in \operatorname{Im} f$ si et seulement si $f(x) = x$ si et seulement si $f(x) - x = 0_E$ si et seulement si $(f - \mathrm{Id})(x) = 0_E$.

2. Si $E = F \oplus G$, alors $p_F + p_G = \mathrm{Id}$, et $p_F \circ p_G = p_G \circ p_F = 0_{\mathscr{L}(E)}$. En effet, si $x = y + z$, alors $p_F(x) = y$ et $p_G(x) = z$. Et $p_F(z) = p_G(y) = 0_E$.

Exercice 6.2.9.
Montrer que l'ensemble des fonctions paires et celui des fonctions impaires sont supplémentaires dans $\mathbb{R}^{\mathbb{R}}$. Donner l'expression des projections sur

l'un de ces deux ensembles parallèlement au second.

6.3 Symétries

Définition 6.3.1.
On appelle *symétrie par rapport à F et parallèlement à G* l'application $s_F : \begin{array}{ccc} E = F \oplus G & \to & E \\ x = y + z & \mapsto & y - z \end{array}$.

Remarque 6.3.2.
Voir le dessin sur la figure XVIII.1. Même exemple que pour la projection.

Théorème 6.3.3.
$s_F \in \mathscr{GL}(E)$, et on a $s_F = s_F^{-1}$: on dit que s_F est une *involution linéaire*.

Démonstration.
• Linéarité : élémentaire.
• $s_F(s_F(y+z)) = s_F(y-z) = y+z$. □

Théorème 6.3.4 (Réciproque)**.**
Toute involution linéaire est une symétrie, plus précisément, si f est une involution linéaire, on a :

1. $\mathrm{Ker}(f - \mathrm{Id}) \oplus \mathrm{Ker}(f + \mathrm{Id}) = E$.
2. f est la symétrie par rapport à $\mathrm{Ker}(f - \mathrm{Id})$ parallèlement à $\mathrm{Ker}(f + \mathrm{Id})$.

Démonstration. 1. • Soit $x \in \mathrm{Ker}(f-\mathrm{Id}) \cap \mathrm{Ker}(f+\mathrm{Id})$. Alors $f(x) = x$ et $f(x) = -x$, donc $x = -x$ donc $x = 0$.
• Analyse : si $x = y + z$ avec $y \in \mathrm{Ker}(f - \mathrm{Id})$ et $z \in \mathrm{Ker}(f + \mathrm{Id})$, alors $f(y) = y$ et $f(z) = -z$. Donc $f(x) = y - z$. D'où : $f(x) + x = 2y$ et $f(x) - x = 2z$. Donc $y = \frac{1}{2}(f(x) + x)$ et $z = \frac{1}{2}(f(x) - x)$.
• Synthèse.

2. On vient de voir que si la décomposition de x dans $\mathrm{Ker}(f-\mathrm{Id}) \oplus \mathrm{Ker}(f+\mathrm{Id})$ $x = y+z$, alors $f(x) = y-z$. CQFD.

□

Remarque 6.3.5.
On peut aussi montrer que $\mathrm{Ker}(s_F - \mathrm{Id}) = \mathrm{Im}(s_F + \mathrm{Id})$ et $\mathrm{Ker}(s_F + \mathrm{Id}) = \mathrm{Im}(s_F - \mathrm{Id})$. Montrons la première égalité :
• $x \in \mathrm{Im}(s_F + \mathrm{Id}) \Rightarrow x = s_F(x') + x'$. Donc $(s_F - \mathrm{Id})(x) = s_F(s_F(x') + x') - s_F(x') - x' = x' + s_F(x') - s_F(x') - x' = 0$.
• $x \in \mathrm{Ker}(s_F - \mathrm{Id}) \Rightarrow s_F(x) = -x$. On pose alors $x' = (s_F - \mathrm{Id})(-1/2x)$. Alors $x' = -\frac{1}{2}(-x - x) = x$, donc $x' = x$, or $x' \in \mathrm{Im}(s_F - \mathrm{Id})$.

Remarque 6.3.6.
On peut enfin montrer que $s_G + s_F = 0_{\mathscr{L}(E)}$, $s_F \circ s_G = -\mathrm{Id} = s_G \circ s_F$, et $p_F = \frac{1}{2}(s_F + \mathrm{Id})$. Faire un dessin.

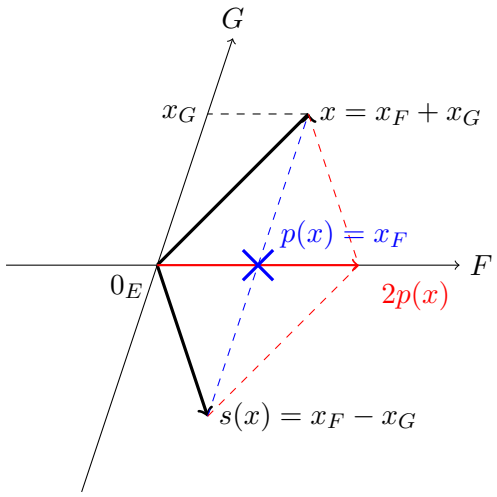


FIGURE XVIII.1 – Représentation de la projection et de la symétrie sur F, parallèlement à G.

Chapitre XIX

Intégration

Dans tout ce chapitre, a et b sont deux réels tels que $a \leqslant b$.

1 Continuité uniforme

Définition 1.0.1.
On dit que f est *uniformément continue sur I* si :

$$\forall \varepsilon > 0 \quad \exists \alpha > 0 \quad \forall (x,y) \in I^2 \quad |x-y| \leqslant \alpha \Rightarrow |f(x)-f(y)| \leqslant \varepsilon.$$

Remarque 1.0.2. 1. C'est une notion qui n'a de sens que sur un intervalle, jamais en un point.

2. Comparer cette expression avec celle de f continue sur I :

$$\forall x \in I \quad \forall \varepsilon > 0 \quad \exists \alpha > 0 \quad \forall y \in I \quad |x-y| \leqslant \alpha \Rightarrow |f(x)-f(y)| \leqslant \varepsilon.$$

La différence essentielle est l'inversion d'un $\forall$ avec un $\exists$.

Exemple 1.0.3.
La fonction $f : \begin{array}{ccc} \mathbb{R}_+^* & \to & \mathbb{R}_+^* \\ x & \mapsto & \dfrac{1}{x} \end{array}$ n'est pas uniformément continue. Montrons la négation d'uniforme continuité :

$$\exists \varepsilon > 0 \quad \forall \alpha > 0 \quad \exists (x,y) \in I^2 \quad |x-y| \leqslant \alpha \text{ et } |f(x)-f(y)| > \varepsilon.$$

Posons $\varepsilon = \frac{1}{2}$. Soit $\alpha > 0$. Posons $x = \min(\alpha, 1)$ et $y = \dfrac{x}{2}$. On a $|x-y| = \dfrac{x}{2} \leqslant \alpha/2 < \alpha$. De plus $|1/x - 1/y| = |1/x - 2/x| = 1/x \geqslant 1 > \varepsilon$.

Théorème 1.0.4. 1. Toute fonction uniformément continue sur I est continue sur I.

2. Toute application lipschitzienne sur I est uniformément continue sur I.

Démonstration. 1. Facile : on réécrit f uniformément continue en fixant $y = a$, et on trouve f continue en a.

2. On fixe ε, on pose $\alpha = \dfrac{\varepsilon}{K}$. Et on déroule les définitions.

□

Remarque 1.0.5.
Nous avons déjà vu que la fonction $f : \begin{array}{ccc} [1,+\infty[& \to & \mathbb{R} \\ x & \mapsto & \dfrac{1}{x} \end{array}$ est 1-lipschitzienne. Ce théorème n'est-il pas contradictoire avec ce dernier point et avec 1.0.9 ?

Théorème 1.0.6 (de Heine)**.**
Toute fonction continue sur un segment est uniformément continue sur ce segment.

Démonstration.
(non exigible). On pose $I = [a,b]$. Soit f continue sur I.

Par l'absurde, supposons que f n'est pas uniformément continue. Alors il existe $\varepsilon > 0$ vérifiant

$$\forall \alpha > 0 \ \exists (x,y) \in I^2 \quad |x-y| < \alpha \text{ et } |f(x)-f(y)| \geqslant \varepsilon. \tag{XIX.1}$$

Soit alors $n \in \mathbb{N}$. D'après la propriété (XIX.1), il existe $(x_n, y_n) \in I$ vérifiant

$$|x_n - y_n| < \frac{1}{n+1}, \tag{XIX.2}$$

$$|f(x_n) - f(y_n)| \geqslant \varepsilon. \tag{XIX.3}$$

Or, $(x_n)_{n\in\mathbb{N}}$ est une suite à valeurs dans le compact $[a,b]$, donc on peut extraire de $(x_n)_{n\in\mathbb{N}}$ une suite $\left(x_{\varphi(n)}\right)_{n\in\mathbb{N}}$ qui converge vers une limite $\ell \in [a,b]$.

Posons alors, pour $n \in \mathbb{N}$, $u_n = x_{\varphi(n)}$, $v_n = y_{\varphi(n)}$.

On a alors

$$u_n - v_n \xrightarrow[n\to+\infty]{} 0$$
$$\text{et} \qquad u_n \xrightarrow[n\to+\infty]{} \ell.$$

Donc, par somme de limites :

$$v_n \xrightarrow[n\to+\infty]{} \ell.$$

Or f est continue sur $[a,b]$ donc en ℓ, on a donc

$$f(u_n) \xrightarrow[n\to+\infty]{} f(\ell),$$
$$f(v_n) \xrightarrow[n\to+\infty]{} f(\ell).$$

Ainsi,

$$|f(u_n) - f(v_n)| \xrightarrow[n\to+\infty]{} 0.$$

Donc il existe $n \in \mathbb{N}$ vérifiant

$$|f(u_n) - f(v_n)| < \varepsilon/2,$$

ce qui est contradictoire avec (XIX.3). C'est donc absurde. □

Remarque 1.0.7.
Attention : ce résultat est faux si l'ensemble de départ considéré pour f n'est pas un segment. Ainsi $\begin{array}{ccc}]0,1] & \to & \mathbb{R} \\ x & \mapsto & \frac{1}{x} \end{array}$ est continue mais pas uniformément continue.

2 Construction de l'intégrale

2.1 Fonctions en escalier sur un segment

Définition 2.1.1.
On appelle *fonction en escalier* sur $[a,b]$ toute fonction $f : [a,b] \to \mathbb{R}$ telle qu'il existe $n \in \mathbb{N}$ et $n+1$ réels $x_0 \dots x_n$ tels que :

(i) $a = x_0 < x_1 < x_2 < \dots < x_n = b$;

(ii) pour tout $i \in [\![0, n-1]\!]$, $f|_{]x_i, x_{i+1}[}$ est constante.

L'ensemble $\{x_0, \dots, x_n\}$ est appelé une *subdivision* de $[a,b]$ *adaptée* à f. On note $\mathscr{E}([a,b])$ l'ensemble des fonctions en escalier sur $[a,b]$. Alors $\mathscr{E}([a,b])$ est un sev et un sous-anneau de $\mathbb{R}^{[a,b]}$.

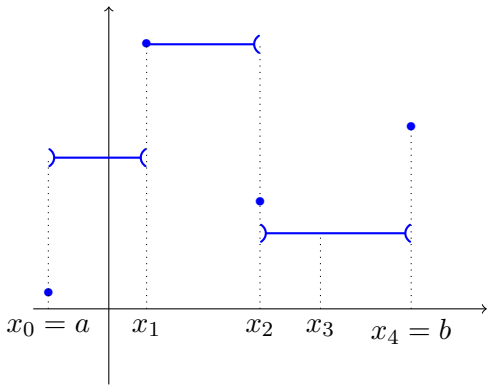


FIGURE XIX.1 – Illustration de la définition d'une fonction en escalier.

Remarque 2.1.2.
Attention aux valeurs prises aux points de la subdivision : elles peuvent valoir n'importe quoi. Si on rajoute des points à une subdivision adaptée, elle est toujours adaptée. Pas si on en ôte.

Remarque 2.1.3.
Si S et T sont deux subdivisions de $[a,b]$, alors :

1. Si S est adaptée à une application en escalier f et $S \subset T$, alors T est adaptée à f.
2. Si S et T sont des subdivisions adaptées à des applications en escalier respectivement f et g, alors $S \cup T$ est adaptée à la fois à f et à g.

Définition 2.1.4 (Intégrale d'une fonction en escalier)**.**
Soit $f \in \mathscr{E}([a,b])$ et $\{x_i\}_{i \in [\![0,n]\!]}$ une subdivision adaptée à f. Alors on appelle *intégrale de f sur $[a,b]$* et on note $\displaystyle\int_{[a,b]} f$ ou $\displaystyle\int_a^b f$ ou $\displaystyle\int_{[a,b]} f(t)\,\mathrm{d}t$ ou $\displaystyle\int_a^b f(t)\,\mathrm{d}t$ le réel

$$\sum_{i=0}^{n-1} v_i \times (x_{i+1} - x_i)$$

où, pour $i \in [\![0, n-1]\!]$, v_i est la valeur (constante) prise par f sur $]x_i, x_{i+1}[$ (on a en particulier $v_i = f\left(\frac{x_i + x_{i+1}}{2}\right)$).

Ce réel ne dépend pas de la subdivision choisie.

Démonstration.
La démonstration consiste à remarquer :

1. Que la valeur définie ci-dessus pour une subdivision S adaptée à f ne change pas si on ajoute un point à cette subdivision.
2. Que, par une récurrence immédiate, elle ne change pas si on rajoute un nombre fini de point et qu'en particulier, si on a deux subdivisions S et T avec $S \subset T$ et S adaptée à f, alors la valeur calculée pour S est la même que pour T.
3. Qu'enfin, si S et T sont deux subdivisions adaptées à f, alors la valeur calculée pour S est la même que pour $S \cup T$ et que celle calculée pour T est la même que pour $S \cup T$.

On se contentera de donner la démonstration du premier point : étant donné une subdivision $S = \{ x_0, \ldots, x_n \}$ adaptée à f en escalier sur $[a, b]$, et un point supplémentaire x', comparons la valeur calculée pour la subdivision S et pour la subdivision $S \cup \{ x' \}$. En notant i l'entier tel que $x_i < x' < x_{x+1}$ le terme $v_i(x_{i+1} - x_i)$ dans la somme pour la subdivision S est remplacée par la somme des deux termes $v_i(x' - x_i) + v_i(x_{i+1} - x')$ dans la somme obtenue pour la subdivision $S \cup \{ x' \}$. Or ces deux valeurs sont les mêmes. □

Remarque 2.1.5. 1. L'intégrale d'une fonction en escalier est bien la somme des aires algébriques des rectangles délimités par les subdivisions.

2. Changer la valeur de $f \in \mathscr{E}([a, b])$ en un point seulement ne change pas la valeur de l'intégrale : il suffit de rajouter ce point dans la subdivision.

3. L'intégrale de la fonction constante λ sur $[a, b]$ vaut $\lambda(b-a)$, en utilisant la subdivision adaptée $\{a, b\}$.

Proposition 2.1.6 (Propriétés de l'intégrale)**.** Soient $f, g \in \mathscr{E}([a, b])$, $\lambda \in \mathbb{R}$.

1. Linéarité : $\displaystyle\int_a^b (f + \lambda g) = \int_a^b f + \lambda \int_a^b g.$
2. Positivité : $f \geqslant 0 \Rightarrow \displaystyle\int_a^b f \geqslant 0.$
3. Croissance : $f \geqslant g \Rightarrow \displaystyle\int_a^b f \geqslant \int_a^b g.$
4. Relation de Chasles : si $c \in]a, b[$, $\displaystyle\int_a^b f = \int_a^c f + \int_c^b f.$

Démonstration. 1. Soit S une subdivision adaptée à f, T une subdivision adaptée à g, alors $S \cup T$ est adaptée à f et g. Notons $\{ z_i \mid i \in [\![0, q]\!] \}$ cette subdivision et exprimons $\displaystyle\int_a^b f$ et $\displaystyle\int_a^b g$:

$$\begin{aligned}
&\int_a^b (f + \lambda g) \\
&= \sum_{k=0}^{q-1} (f + \lambda g)\left(\frac{z_{i+1} + z_i}{2}\right) \times (z_{i+1} - z_i) \\
&= \sum_{k=0}^{q-1} f\left(\frac{z_{i+1} + z_i}{2}\right) \times (z_{i+1} - z_i) \\
&\quad + \lambda \sum_{k=0}^{q-1} g\left(\frac{z_{i+1} + z_i}{2}\right) \times (z_{i+1} - z_i) \\
&= \int_a^b f + \lambda \int_a^b g.
\end{aligned}$$

2. On exprime $\displaystyle\int_a^b f$ avec une subdivision adaptée à f : tous les termes sont positifs.
3. Appliquer le point précédent à $(f - g)$.
4. Soit S une subdivision adaptée à f. Ajoutons le point c et notons $\{ z_i \mid i \in [\![0, q]\!] \}$ la subdivision obtenue. Soit $s \in [\![1, q-1]\!]$ tel que $z_s = c$. Alors :

$$\begin{aligned}
\int_a^b f &= \sum_{k=0}^{q-1} f\left(\frac{z_{i+1} + z_i}{2}\right) \times (z_{i+1} - z_i) \\
&= \sum_{k=0}^{s-1} f\left(\frac{z_{i+1} + z_i}{2}\right) \times (z_{i+1} - z_i) \\
&\quad + \sum_{k=s}^{q-1} f\left(\frac{z_{i+1} + z_i}{2}\right) \times (z_{i+1} - z_i) \\
&= \int_a^c f + \int_c^b f.
\end{aligned}$$

□

2.2 Fonctions continues par morceaux sur un segment

Définition 2.2.1.
Soit $f : [a, b] \to \mathbb{R}$. On dit que f est continue par morceaux s'il existe une subdivision $\{x_0, \ldots, x_n\}$ de $[a, b]$ telle que

1. $a = x_0 < x_1 < \ldots < x_n = b$;
2. pour tout $i \in [\![0, n-1]\!]$, $f|_{]x_i, x_{i+1}[}$ est continue et prolongeable par continuité en x_i et en x_{i+1}.

L'ensemble $\{x_0, \dots, x_n\}$ est appelé une *subdivision* de $[a,b]$*adaptée* à f. On note $\mathscr{C}_m([a,b])$ l'ensemble des fonctions continues par morceaux sur $[a,b]$. Alors $\mathscr{C}_m([a,b])$ est un sev et un sous-anneau de $\mathbb{R}^{[a,b]}$.

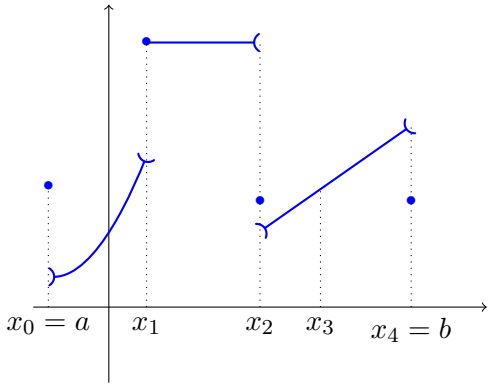


FIGURE XIX.2 – Illustration de la définition d'une fonction continue par morceaux.

Remarque 2.2.2.
Attention aux valeurs prises aux points de la subdivision : elles peuvent valoir n'importe quoi.

Exemple 2.2.3. 1. Dessiner des exemples de fonctions continues par morceaux.

2. La fonction tangente, prolongée en $\mathbb{R}$ en lui donnant la valeur 0 là où elle n'est pas définie, n'est pas continue par morceaux car elle n'est pas prolongeable par continuité en les points de discontinuité.
3. Idem pour $\begin{array}{ccc} \mathbb{R}^* & \to & \mathbb{R} \\ x & \mapsto & \sin 1/x \end{array}$.

On construit l'intégrale d'une fonction continue par morceaux en approchant celle-ci par des fonctions en escaliers.

Théorème 2.2.4.
Soit $f \in \mathscr{C}_m([a,b])$. Soit $\varepsilon > 0$. Alors il existe φ_ε^+ et $\varphi_\varepsilon^- \in \mathscr{E}([a,b])$ telles que $\varphi_\varepsilon^- \leqslant f \leqslant \varphi_\varepsilon^+$ et $0 \leqslant \varphi_\varepsilon^+ - \varphi_\varepsilon^- \leqslant \varepsilon$.

Démonstration.Première étape On suppose que f est continue sur $]a,b[$ et prolongeable par continuité en a et en b. On appelle $\tilde{f}$ ce prolongement. Alors f et $\tilde{f}$ coïncident sur $]a,b[$, mais pas forcément en a ni en b. On utilise le théorème de Heine : $\tilde{f}$ est uniformément continue sur $[a,b]$, donc il existe $\alpha > 0$ vérifiant

$$\forall x, y \in [a,b] \quad |x-y| \leqslant \alpha \Rightarrow |\tilde{f}(x) - \tilde{f}(y)| \leqslant \varepsilon$$

On choisit n tq $h = \dfrac{b-a}{n} \leqslant \alpha$ et on pose : $x_0 = a$, $x_1 = a + h \dots x_h = a + kh \dots x_n = a + nh = b$, donc $\{x_0 \dots x_n\}$ est une subdivision de $[a,b]$, et

$$\forall i \in [\![0, n-1]\!],\ \forall x, y \in [x_i, x_{i+1}],\ |\tilde{f}(x) - \tilde{f}(y)| \leqslant \varepsilon \ (\star).$$

Soit $i \in [\![0, n-1]\!]$, $\tilde{f}$ est continue, donc elle est bornée et atteint ses bornes sur $[x_i, x_{i+1}]$.
On pose

$$\varphi_i^+ = \max_{[x_i, x_{i+1}]} \tilde{f}$$

$$\varphi_i^- = \min_{[x_i, x_{i+1}]} \tilde{f}$$

$$\begin{array}{rccc} \varphi_\varepsilon^+ : & [a,b] & \to & \mathbb{R} \\ & x & \mapsto & \begin{cases} \varphi_i^+ & \text{si } x \in [x_i, x_{i+1}[\\ \varphi_{n-1}^+ & \text{si } x = b \end{cases} \end{array}$$

$$\begin{array}{rccc} \varphi_\varepsilon^- : & [a,b] & \to & \mathbb{R} \\ & x & \mapsto & \begin{cases} \varphi_i^- & \text{si } x \in [x_i, x_{i+1}[\\ \varphi_{n-1}^- & \text{si } x = b \end{cases} \end{array}.$$

On a bien $\varphi_\varepsilon^- \leqslant f \leqslant \varphi_\varepsilon^+$.
Puisque les max et min sont atteints, on a $\forall i \in [\![0, n-1]\!]$, $\exists y_i, z_i \in [x_i, x_{i+1}]$ tq $\varphi_i^+ = \tilde{f}(y_i)$ et $\varphi_i^- = \tilde{f}(z_i)$, donc $\forall i \in [\![0, n-1]\!]$, $0 \leqslant \varphi_i^+ - \varphi_i^- = \tilde{f}(y_i) - \tilde{f}(z_i) \leqslant \varepsilon$ (car $|y_i - z_i| \leqslant \alpha$), donc nécessairement $0 \leqslant \varphi_\varepsilon^+ - \varphi_\varepsilon^- \leqslant \varepsilon$.

 $\varphi_\varepsilon^\pm$ conviennent pour $\tilde{f}$ et non f : il suffit alors de changer leurs valeurs en a et b, en posant $\varphi_\varepsilon^+(a) = \varphi_\varepsilon^-(a) = f(a)$ et $\varphi_\varepsilon^+(b) = \varphi_\varepsilon^-(b) = f(b)$.

Deuxième étape Cas général : soient $f \in \mathscr{C}_m([a,b])$ et $\{x_i\}$ une subdivision adaptée. Alors on définit des $\varphi_\varepsilon^\pm$ sur chaque morceau de la subdivision, et on recolle. □

Définition 2.2.5 (Intégrale d'une fonction continue par morceaux)**.**
Soit $f \in \mathscr{C}_m([a,b])$. On note :
— $\mathscr{E}^+(f) = \{\, h \in \mathscr{E}([a,b]) \mid h \geqslant f \,\}$,
— $\mathscr{E}^-(f) = \{\, h \in \mathscr{E}([a,b]) \mid h \leqslant f \,\}$,
— $I^+(f) = \left\{ \int_a^b h \;\middle|\; h \in \mathscr{E}^+(f) \right\}$,

— $I^-(f) = \left\{ \int_a^b h \;\middle|\; h \in \mathscr{E}^-(f) \right\}$.

Alors $\sup I^-(f)$ et $\inf I^+(f)$ existent et sont égales. On appelle alors cette constante l'*intégrale de f sur $[a,b]$*, notée $\int_{[a,b]} f$ ou $\int_a^b f$ ou $\int_{[a,b]} f(t)\,\mathrm{d}t$ ou $\int_a^b f(t)\,\mathrm{d}t$.

Démonstration.
D'après le théorème d'approximation, il existe $\varphi^+ \in \mathscr{E}^+(f)$ et $\varphi^- \in \mathscr{E}^-(f)$, donc $\mathscr{E}^+(f)$ et $\mathscr{E}^-(f)$ ne sont pas vides, donc $I^\pm(f)$ non plus. De plus $I^+(f)$ est minorée par $\int_a^b \varphi^-$ et $I^-(f)$ est majorée par $\int_a^b \varphi^+$. Ainsi, avec le théorème de la borne sup, $\sup I^-(f)$ et $\inf I^+(f)$ existent, et $\sup I^-(f) \leqslant \int_a^b \varphi^+$.
Mais cette inégalité est valable pour tout $\varphi^+ \in \mathscr{E}^+(f)$, donc $\sup I^-(f) \leqslant \inf I^+(f)$.
Pour conclure, montrons l'inégalité inverse : soit $\varepsilon > 0$, alors il existe $\varphi_\varepsilon^+ \in \mathscr{E}^+(f)$ et $\varphi_\varepsilon^- \in \mathscr{E}^-(f)$ telles que $\varphi_\varepsilon^+ - \varphi_\varepsilon^- \leqslant \varepsilon$. Ainsi $\int_a^b \varphi_\varepsilon^+ \leqslant \int_a^b \varphi_\varepsilon^- + \int_a^b \varepsilon = \int_a^b \varphi_\varepsilon^- + (b-a)\varepsilon$. On obtient donc $\inf I^+(f) \leqslant \sup I^-(f) + (b-a)\varepsilon$ pour tout $\varepsilon > 0$, donc par passage à la limite, on a : $\inf I^+(f) \leqslant \sup I^-(f)$. □

Remarque 2.2.6.
Cette intégrale représente bien la notion « d'aire sous la courbe », même si la construction s'éloigne quelque peu d'une définition géométrique.

Remarque 2.2.7.
La notion d'intégrale de fonction continue par morceaux prolonge celle de fonction en escalier. En effet, si $f \in \mathscr{E}([a,b])$, alors $f \in \mathscr{E}^+(f) \cap \mathscr{E}^-(f)$, et l'on voit directement que $\int_a^b f \in I^+(f) \cap I^-(f)$.

Remarque 2.2.8.
Changer la valeur de $h \in \mathscr{E}([a,b])$ en un point seulement ne change pas la valeur de son intégrale : il suffit de rajouter ce point dans la subdivision. On peut en déduire que changer la valeur de $f \in \mathscr{C}_m([a,b])$ en un point seulement ne change pas la valeur de son intégrale.

Exercice 2.2.9.
Le démontrer.

Proposition 2.2.10.
Soient $f, g \in \mathscr{C}_m([a,b])$, $\lambda \in \mathbb{R}$.

1. Linéarité : $\int_a^b (f + \lambda g) = \int_a^b f + \lambda \int_a^b g$.
2. Positivité : $f \geqslant 0 \Rightarrow \int_a^b f \geqslant 0$.
3. Croissance : $f \geqslant g \Rightarrow \int_a^b f \geqslant \int_a^b g$.
4. Continuité (ou inégalité triangulaire) : $\left| \int_a^b f \right| \leqslant \int_a^b |f|$.
5. Inégalité de la moyenne : $\left| \int_a^b (fg) \right| \leqslant (\sup_{[a,b]} |f|) \times \int_a^b |g|$.
   Cas particulier : $\left| \int_a^b f \right| \leqslant (b-a) \sup_{[a,b]} |f|$.
6. Relation de Chasles : si $c \in]a,b[$, $\int_a^b f = \int_a^c f + \int_c^b f$.

Remarque 2.2.11.
On appelle *moyenne* de f sur $[a,b]$ la quantité $m = \dfrac{1}{b-a} \int_a^b f$. Faire un dessin avec les aires pour voir le rapport avec l'inégalité de la moyenne.

Démonstration. 1. (a) Montrons d'abord que pour tout $\lambda \in \mathbb{R}_+$, $\int_a^b \lambda f = \lambda \int_a^b f$.

Il suffit pour cela de montrer que pour tout $\varepsilon > 0$, on a

$$\left| \int_a^b \lambda f - \lambda \int_a^b f \right| \leqslant \lambda(b-a)\varepsilon$$

et d'en déduire le résultat par passage à la limite.

Considérons donc $\varepsilon > 0$. Choisissons φ^- et φ^+ des applications en escaliers encadrant f vérifiant $0 \leqslant \varphi^+ - \varphi^- \leqslant \varepsilon$. Alors λf est encadrée

par $\lambda\varphi^-$ et $\lambda\varphi^+$. On en déduit

$$\begin{aligned}\int_a^b \lambda f - \lambda\int_a^b f &\leqslant \int_a^b \lambda\varphi^+ - \lambda\int_a^b \varphi^- \\ &\leqslant \lambda\int_a^b \left(\varphi^+ - \varphi^-\right) \text{ (car } \varphi^+ \\ &\qquad \text{et } \varphi^- \text{ sont en escalier)} \\ &\leqslant \lambda(b-a)\varepsilon \ \left(\text{car } \varphi^+ - \varphi^- \leqslant \varepsilon\right).\end{aligned}$$

De même, on a

$$\int_a^b \lambda f - \lambda\int_a^b f \geqslant -\lambda(b-a)\varepsilon.$$

D'où le résultat.

(b) On procède de la même manière pour le cas $\lambda \in \mathbb{R}_-$, en faisant attention aux changements de sens dans les inégalités dûs au signe de λ.

(c) Montrons ensuite que $\displaystyle\int_a^b (f+g) = \int_a^b f + \int_a^b g$.

Il suffit de montrer que pour tout $\varepsilon > 0$, on a

$$\left|\int_a^b (f+g) - \left(\int_a^b f + \int_a^b g\right)\right| \leqslant 2\varepsilon(b-a)$$

Soit donc $\varepsilon > 0$. Choisissons φ_f^- et φ_f^+ encadrant f et φ_g^- et φ_g^+ encadrant g et vérifiant $\varphi_f^+ - \varphi_f^- \leqslant \varepsilon$ et $\varphi_g^+ - \varphi_g^- \leqslant \varepsilon$.

Alors on a :

$$\int_a^b f \geqslant \int_a^b \varphi_f^-$$

$$\int_a^b g \geqslant \int_a^b \varphi_g^-$$

$$\int_a^b (f+g) \leqslant \int_a^b \left(\varphi_f^+ + \varphi_g^+\right) \quad \left(\text{car } \varphi_f^+ + \varphi_g^- \in \mathscr{E}^+(f+g)\right)$$

$$\int_a^b (f+g) \leqslant \int_a^b \varphi_f^+ + \int_a^b \varphi_g^+ \quad \left(\text{ car } (\varphi_f^+, \varphi_g^+) \in \mathscr{E}([a,b])^2\right)$$

et finalement

$$\begin{aligned}&\int_a^b (f+g) - \left(\int_a^b f + \int_a^b g\right) \\ \leqslant &\int_a^b \varphi_f^+ - \int_a^b \varphi_f^- + \int_a^b \varphi_g^+ - \int_a^b \varphi_g^- \\ \leqslant &2\varepsilon(b-a).\end{aligned}$$

On montre de même

$$\int_a^b (f+g) - \left(\int_a^b f + \int_a^b g\right) \geqslant -2\varepsilon(b-a)$$

D'où le résultat.

2. Si $f \geqslant 0$, la fonction nulle est un élément de $\mathscr{E}^-(f)$ et donc $\displaystyle\int_a^b f \geqslant \int_a^b 0 = 0$.
3. La croissance découle directement de la positivité, appliquée à $f - g$.
4. Si f est continue par morceaux, alors $-f$, $|f|$ et $-|f|$. le sont aussi. Or $-|f| \leqslant f \leqslant |f|$, donc par croissance et linéarité de l'intégrale : $\displaystyle -\int_a^b |f| \leqslant \int_a^b |f|$, d'où $\displaystyle\left|\int_a^b f\right| \leqslant \int_a^b |f|$.
5. On a $|fg| = |f|\cdot|g|$ et donc $|fg| \leqslant (\sup|f|)\cdot|g|$, donc par continuité, croissance et linéarité de l'intégrale on a bien : $\displaystyle\left|\int_a^b (fg)\right| \leqslant (\sup_{[a,b]}|f|) \times \int_a^b |g|$.
   Le cas particulier s'obtient pour $g = 1$.
6. Soit $c \in]a,b[$.
   Il suffit de montrer que pour tout $\varepsilon > 0$, on a

$$\left|\int_a^c f + \int_a^c f - \int_a^b f\right| \leqslant \varepsilon(b-a).$$

Soit donc $\varepsilon > 0$. Notons $I_1 = [a,c]$ et $I_2 = [c,b]$.

Alors pour $i = 1, 2$, il existe φ_i^- et φ_i^+ des applications en escalier sur I_i encadrant la restriction de f à I_i vérifiant

$$\varphi_i^+ - \varphi_i^- \leqslant \varepsilon.$$

Posons alors

$$\begin{aligned}\varphi^- : \ [a,b] &\to \mathbb{R} \\ x &\mapsto \begin{cases}\varphi_1^-(x) & \text{si } x < c \\ \varphi_2^-(x) & \text{si } x \geqslant c\end{cases}\end{aligned}$$

$$\begin{aligned}\text{et } \varphi^+ : \ [a,b] &\to \mathbb{R} \\ x &\mapsto \begin{cases}\varphi_1^+(x) & \text{si } x < c \\ \varphi_2^+(x) & \text{si } x \geqslant c\end{cases}\end{aligned}$$

φ^- et φ^+ sont en escalier et on a :

$$\begin{aligned}&\int_a^c f + \int_c^b f \\ \leqslant &\int_a^c \varphi_1^+ + \int_c^b \varphi_2^+ \\ \leqslant &\int_a^c \varphi^+ + \int_c^b \varphi^+ \\ &\left(\varphi^+_{|[a,c]} \text{ et } \varphi_1^+ \text{ différent au plus en } c\right) \\ \leqslant &\int_a^b \varphi^+ \\ &\left(\varphi^+ \text{ est en escalier.}\right)\end{aligned}$$

Or $\displaystyle\int_a^b f \geqslant \int_a^b \varphi^- \text{ car } \left(\varphi^- \in \mathscr{E}^-(f)\right)$

Donc

$$\begin{aligned}
&\int_a^c f + \int_c^b f - \int_a^b f \\
\leqslant\ & \int_a^b \varphi^+ - \int_a^b \varphi^- \\
& \text{(par différence des inégalités précédentes)} \\
\leqslant\ & \int_a^b \left(\varphi^+ - \varphi^-\right) \\
& \left(\varphi^- \text{ et } \varphi^+ \text{ sont en escalier}\right) \\
\leqslant\ & (b-a)\varepsilon \\
& \left(\varphi^+ - \varphi^- \leqslant \varepsilon\right)
\end{aligned}$$

De la même façon on montre

$$\int_a^c f + \int_c^b f - \int_a^b f \geqslant -(b-a)\varepsilon$$

On en déduit le résultat.

□

Théorème 2.2.12.
Soit $f \in \mathscr{C}^0([a,b])$, vérifiant $f \geqslant 0$. Alors :

(i) s'il existe $x_0 \in [a,b]$ tel que $f(x_0) > 0$, alors $\int_a^b f > 0$;

(ii) si $\int_a^b f = 0$, alors $f = 0$.

Remarque 2.2.13.
Toutes les hypothèses sont indispensables : cherchez des contre-exemples !

Démonstration.
(ii) n'est que la contraposée de (i). Il suffit donc de montrer (i).

Si $f(x_0) > 0$ et f continue, alors il existe $\alpha > 0$ tel que $f > f(x_0)/2$ sur $[x_0-\alpha, x_0+\alpha] \cap [a,b]$. On note alors φ l'application prenant la valeur $f(x_0)/2$ sur $[x_0-\alpha, x_0+\alpha] \cap [a,b]$ et 0 ailleurs. φ est une fonction inférieure à f, donc $\int_a^b \varphi \leqslant \int_a^b f$. De plus elle φ est en escalier, elle est nulle sauf sur l'intervalle $[x_0-\alpha, x_0+\alpha] \cap [a,b]$ où elle a pour valeur $f(x_0)/2$. Son intégrale sur $[a,b]$ vaut donc $\ell \times f(x_0)/2$, où ℓ est la largeur de cet intervalle. Or celle-ci est non nulle (regarder les différents cas suivant que x_0 est intérieur à $[a,b]$ ou non), donc $\int_a^b \varphi > 0$, d'où le résultat. □

2.3 Extension au cas où $b \leqslant a$

Soit I un intervalle on dit qu'une application f est continue par morceaux sur I si elle est continue par morceaux sur tout segment non trivial de I.

Soit donc $f : I \to \mathbb{R}$ continue par morceaux.

Soit a et b deux réels quelconques de I. Si $a < b$, on a vu comment définir $\int_a^b f$.

Si $b < a$, alors on définit $\int_a^b f$ comme étant le réel $-\int_b^a f$.

Si $a = b$, on pose $\int_a^b f = 0$.

L'intérêt principal de cette définition est de généraliser la relation de Chasles aux cas où les points a, b et c sont dans un ordre quelconque.

Proposition 2.3.1 (Relation de Chasles)**.**
Soit I un intervalle et f continue par morceaux sur I. Alors, pour tout $(a,b,c) \in I^3$, on a

$$\int_a^b f = \int_a^c f + \int_c^b f.$$

Démonstration.
Remarquons tout d'abord que nous avons déjà démontré ce résultat proposition 2.2.9 dans le cas où $a < c < b$.

Notons que ce résultat est trivial si $a = c$ ou $c = b$. On a donc le résultat pour $a \leqslant c \leqslant b$.

Remarquons ensuite que pour tout m, x, y appartenant à I, avec $m \leqslant x$ et $m \leqslant y$, on a $\int_x^y f = \int_m^y f - \int_m^x f$.

En effet, si $x \leqslant y$, il suffit de remarquer $\int_m^y f = \int_m^x f + \int_x^y f$ et si $x \geqslant y$, de remarquer $\int_m^x f = \int_m^y f + \int_y^x f = \int_m^y f - \int_x^y f$.

En posant $m = \min(a,b,c)$ on a alors successivement :

$$\begin{aligned}
\int_a^c f + \int_c^b f &= \int_m^c f - \int_m^a f + \int_m^b f - \int_m^c f \\
&= \int_m^b f - \int_m^a f \\
&= \int_a^b f.
\end{aligned}$$

□

Exercice 2.3.2.
Que deviennent les résultats de la proposition 2.2.9 si on remplace les hypothèses $a < b$

et $f, g \in \mathscr{C}_m([a,b])$ par I est un intervalle, $f, g \in \mathscr{C}_m(I)$ et a et b sont des éléments quelconques de I ?

3 Le théorème fondamental de l'analyse

Dans toute la suite, I est un intervalle de $\mathbb{R}$.

3.1 Primitives

Définition 3.1.1.
Soit f une application de I dans $\mathbb{R}$. On appelle primitive de f sur I toute application $F \in \mathscr{D}(I,\mathbb{R})$ telle que $F' = f$.

Théorème 3.1.2.
Si $f : I \to \mathbb{R}$ a une primitive F, alors l'ensemble des primitives de f est $\{ F + \lambda \mid \lambda \in \mathbb{R} \}$.

Démonstration.
Déjà fait dans le chapitre sur les fonctions usuelles. □

Remarque 3.1.3.
Il ne faut donc JAMAIS parler de LA primitive de f, sous peine de se faire lourdement châtier.

3.2 Existence de primitives

Remarque 3.2.1.
Commençons par une première remarque : toutes les fonctions n'ont pas de primitive.

Exemple 3.2.2.
Posons

$$\begin{array}{rccl} f : & [-1,1] & \to & \mathbb{R} \\ & x & \mapsto & \begin{cases} 1 & \text{si } x = 0 \\ 0 & \text{sinon} \end{cases} \end{array} .$$

Par l'absurde supposons que f admet une primitive F. Alors $F' = 0$ sur $[-1,0[$ et $]0,1]$, donc $F = a$ sur $[-1,0[$ et b sur $]0,1]$. Mais F est dérivable donc continue, donc les limites à gauche et à droite en 0 doivent être égales, i.e. $a = b$. Mais alors F est constante sur $[-1,1]$, donc F' est nulle partout, et ainsi $F' \neq f$.

Remarque 3.2.3.
En revanche, la fonction f de l'exemple 3.2.2 a une **intégrale**, et l'application

$$\begin{array}{rccl} F : & [-1,1] & \to & \mathbb{R} \\ & x & \mapsto & \displaystyle\int_{-1}^{x} f(t)\,\mathrm{d}t \end{array}$$

est bien définie.

 Il ne faut donc pas confondre primitive et intégrale.

Remarque 3.2.4.
De manière plus générale, le théorème de Darboux (HP, mais c'est une conséquence simple du théorème de Rolle) montre qu'une fonction dérivée vérifie toujours la propriété des valeurs intermédiaires. Une fonction ne vérifiant pas cette propriété (comme celle de l'exemple 3.2.2) ne peut donc admettre de primitive.

Théorème 3.2.5 (Théorème fondamental de l'analyse)**.**
Soit $f \in \mathscr{C}^0(I,\mathbb{R})$, et $a \in I$.

1. f a une primitive, par exemple la fonction $\begin{array}{rccl} F : & I & \to & \mathbb{R} \\ & x & \mapsto & \displaystyle\int_a^x f(t)\,\mathrm{d}t \end{array}$.
2. Soit $A \in \mathbb{R}$. Alors f admet une unique primitive valant A en a. Il s'agit de la fonction $\begin{array}{rccl} F : & I & \to & \mathbb{R} \\ & x & \mapsto & \displaystyle\int_a^x f(t)\,\mathrm{d}t + A \end{array}$.
3. Soient $a, b \in I$ et $\tilde{F}$ une primitive de f sur I. Alors $\displaystyle\int_a^b f = \tilde{F}(b) - \tilde{F}(a)$. Cette quantité est aussi notée $[\tilde{F}]_a^b$, ou $[\tilde{F}(t)]_{t=a}^b$.

Remarque 3.2.6.
C'est souvent le deuxième ou le troisième point que l'on appelle théorème fondamental de l'analyse, mais en fait le point le plus important est le premier, les deux autres en découlent facilement.

Démonstration. 1. Montrons que F est dérivable et $F' = f$.
Soit $x_0 \in I$, montrons que F est dérivable en x_0, de dérivée $f(x_0)$.
Soit alors $\varepsilon > 0$. Puisque f est continue en x, alors on peut trouver $\alpha > 0$ tel que

$$\forall y \in I,\ |x_0 - y| \leqslant \alpha \Rightarrow |f(x_0) - f(y)| \leqslant \varepsilon$$

$|f - f(x_0)|$ est alors majorée par ε sur $[x_0 - \alpha, x_0 + \alpha]$.
Soit $x \in [x_0 - \alpha, x_0 + \alpha] \cap I \backslash \{x_0\}$.

$$\begin{aligned}\left|\frac{F(x) - F(x_0)}{x - x_0} - f(x_0)\right| &= \left|\frac{\displaystyle\int_a^x f - \int_a^{x_0} f}{x - x_0} - f(x_0)\right| \\ &= \left|\frac{\displaystyle\int_{x_0}^x f}{x - x_0} - \frac{\displaystyle\int_{x_0}^x f(x_0)}{x - x_0}\right| \\ &= \frac{\left|\displaystyle\int_{x_0}^x (f - f(x_0))\right|}{|x - x_0|} \\ &\leqslant \frac{|x - x_0|\varepsilon}{|x - x_0|} \\ &\leqslant \varepsilon.\end{aligned}$$

On a montré que pour ε fixé, il existe $\alpha > 0$ tel que

$$\forall x \in I \quad |x - x_0| \leqslant \alpha \Rightarrow \left|\frac{F(x) - F(x_0)}{x - x_0} - f(x_0)\right| \leqslant \varepsilon,$$

donc $\dfrac{F(x) - F(x_0)}{x - x_0} \xrightarrow[\substack{x \to x_0 \\ x \neq x_0}]{} f(x_0)$, d'où le résultat.

2. Facile.
3. Il existe K tel que $\tilde{F}(x) = \displaystyle\int_a^x f + K$, la suite est laissée en exercice.

□

Exemple 3.2.7. 1. Calculer l'intégrale $\displaystyle\int_1^2 \frac{1}{(x+1)^n}\,\mathrm{d}x$.

2. Calculer $\displaystyle\lim_{n \to +\infty} \int_0^1 \frac{t^n}{(2+t)^n}\,\mathrm{d}t$.

4 Méthodes de calcul

Se référer au chapitre sur les équations différentielles.

5 Formules de Taylor

Nous allons maintenant voir deux nouvelles formules de Taylor, mais qui sont cette fois des résultats *globaux*, alors que la formule de Taylor-Young est un résultat *local*.

Théorème 5.0.1 (Formule de Taylor avec reste intégral)**.**
Soient $n \in \mathbb{N}$ et $f \in \mathscr{C}^{n+1}(I, \mathbb{R})$ et $(a, b) \in I^2$. Alors :

$$f(b) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(b-a)^k + \int_a^b \frac{f^{(n+1)}(t)}{n!}(b-t)^n\,\mathrm{d}t. \quad (\star)$$

Remarque 5.0.2.
Si f est un polynôme de degré n, alors pour tout $k > n$, $f^{(k)} = 0$, et ainsi, en appliquant Taylor à un ordre supérieur à n, on retrouve la formule de Taylor pour les polynômes.

Démonstration.
Soit f une application de I dans $\mathbb{R}$ et $(a, b) \in I^2$. Pour $n \in \mathbb{N}$, on note $P(n)$ l'assertion «si $f \in \mathscr{C}^{n+1}(I, \mathbb{R})$, alors on a $(\star)$».

Alors :

— Montrons $P(0)$, c'est-à-dire si $f \in \mathscr{C}^1(I, \mathbb{R})$, alors $f(b) = f(a) + \displaystyle\int_a^b f'(t)\,\mathrm{d}t$. C'est tout simplement le théorème fondamental de l'analyse.

— Montrons $\forall n \in \mathbb{N}\ (P(n) \Rightarrow P(n+1))$.
Soit $n \in \mathbb{N}$. Supposons $P(n)$. Montrons $P(n+1)$. Pour cela, supposons $f \in \mathscr{C}^{n+2}(I, \mathbb{R})$. Alors $f \in \mathscr{C}^{n+1}(I, \mathbb{R})$ donc, puisqu'on a $P(n)$, on a

$$f(b) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(b-a)^k + \int_a^b \frac{f^{(n+1)}(t)}{n!}(b-t)^n\,\mathrm{d}t.$$

Calculons alors $\displaystyle\int_a^b \frac{f^{(n+1)}(t)}{n!}(b-t)^n\,\mathrm{d}t$ grâce à une intégration par parties. On dérive $f^{(n+1)}$ (qui est bien $\mathscr{C}^1$) et on intègre $\dfrac{(b-t)^n}{n!}$, qui est bien continue.

On obtient :

$$\begin{aligned}
&\int_a^b \frac{f^{(n+1)}(t)}{n!}(b-t)^n \,\mathrm{d}t \\
=&\left[f^{(n+1)}(t)\left(-\frac{(b-t)^{n+1}}{(n+1)!}\right)\right]_a^b \\
&-\int_a^b f^{(n+2)}(t)\left(-\frac{(b-t)^{n+1}}{(n+1)!}\right)\mathrm{d}t \\
=&0+\frac{f^{(n+1)}(a)}{(n+1)!}(b-a)^{n+1} \\
&+\int_a^b f^{(n+2)}(t)\frac{(b-t)^{n+1}}{(n+1)!}\,\mathrm{d}t.
\end{aligned}$$

On a donc bien $\forall n \in \mathbb{N}\ P(n) \Rightarrow P(n+1)$.
On a donc $P(0)$ et $\forall n \in \mathbb{N}\ P(n) \Rightarrow P(n+1)$, donc on a $\forall n \in \mathbb{N}\ P(n)$. On a donc le résultat cherché. □

Corollaire 5.0.3 (Inégalité de Taylor-Lagrange)**.**
Avec les mêmes notations et hypothèses, si $a < b$,

$$\left|f(b)-\sum_{k=0}^{n}\frac{f^{(k)}(a)}{k!}(b-a)^k\right| \leqslant \frac{|b-a|^{n+1}}{(n+1)!}\sup_{[a,b]}\left|f^{(n+1)}\right|.$$

Démonstration.
Faisons la démonstration dans le cas $a < b$ (le cas $a > b$ se traite de la même manière, en faisant attention au signe).
La formule de Taylor donne :

$$\underbrace{\left|f(b)-\sum_{k=0}^{n}\frac{f^{(k)}(a)}{k!}(b-a)^k\right|}_{A} = \left|\int_a^b \frac{f^{(n+1)}(t)}{n!}(b-t)^n\,\mathrm{d}t\right|$$

$$\leqslant \int_a^b \left|f^{(n+1)}(t)\right|\frac{|b-t|^n}{n!}\,\mathrm{d}t.$$

$f^{(n+1)}$ est continue sur le segment $[a,b]$, donc bornée, donc on a :

$$\begin{aligned}
A &\leqslant \int_a^b \sup_{[a,b]}\left|f^{(n+1)}\right|\frac{|b-t|^n}{n!}\,\mathrm{d}t \\
&\leqslant \sup_{[a,b]}\left|f^{(n+1)}\right|\int_a^b \frac{|b-t|^n}{n!}\,\mathrm{d}t \\
&\leqslant \sup_{[a,b]}\left|f^{(n+1)}\right|\left[\frac{-(b-t)^{n+1}}{(n+1)!}\right]_a^b \\
&\leqslant \sup_{[a,b]}\left|f^{(n+1)}\right|\frac{(b-a)^{n+1}}{(n+1)!}.
\end{aligned}$$

□

Exercice 5.0.4.
En appliquant l'inégalité de Taylor-Lagrange à la fonction exponentielle en zéro, montrer que pour tout $x \in \mathbb{R}$, $\displaystyle\sum_{k=0}^{n}\frac{x^k}{k!} \xrightarrow[n\to+\infty]{} \mathrm{e}^{\,x}$.

6 Cas des fonctions à valeurs complexes

Définition 6.0.1.
Soit $f : I \to \mathbb{C}$ telle que $g = \mathrm{Re}(f)$ et $h = \mathrm{Im}(f)$. Donc $g, h : I \to \mathbb{R}$ et $f = g + ih$. On suppose g et h de classe $\mathscr{C}_m$. Soient $a, b \in I$. On appelle *intégrale de f de a à b* , notée $\displaystyle\int_{[a,b]} f$ ou $\displaystyle\int_a^b f$ ou $\displaystyle\int_{[a,b]} f(t)\,\mathrm{d}t$ ou $\displaystyle\int_a^b f(t)\,\mathrm{d}t$, le **complexe** $\displaystyle\int_a^b f = \int_a^b g + i\int_a^b h$.

Remarque 6.0.2.

- On a donc $\mathrm{Re}\left(\displaystyle\int_a^b f\right) = \int_a^b \mathrm{Re}(f)$ et $\mathrm{Im}\left(\displaystyle\int_a^b f\right) = \int_a^b \mathrm{Im}(f)$.
- « L'aire sous la courbe » n'a plus aucun sens dans le cas d'une fonction à valeurs dans $\mathbb{C}$, et ne peut donc pas servir à interpréter l'intégrale d'une fonction à valeurs dans $\mathbb{C}$.

Théorème 6.0.3.
Soit $f \in \mathscr{C}^0(I, \mathbb{C})$ et $(a, b) \in I^2$ avec $a < b$.

1. La linéarité et la relation de Chasles sont toujours valables pour les fonctions à valeurs complexes.
2. Continuité : $\left|\displaystyle\int_a^b f\right| \leqslant \int_a^b |f|$.
3. Inégalité de la moyenne : $\left|\displaystyle\int_a^b (fg)\right| \leqslant (\sup_{[a,b]}|f|) \times \int_a^b |g|$.

Démonstration. 1. Se démontre comme pour les fonctions réelles.

2. On note $\theta = \arg\left(\int_a^b f\right)$, *i.e.* $\mathrm{e}^{-i\theta}\int_a^b f = \left|\int_a^b f\right|$.
On pose $F(x) = \int_a^x f$ et $G(x) = \mathrm{Re}\left(\mathrm{e}^{-i\theta}F(x)\right)$, $a, x \in I$.
Alors $G(b) = \mathrm{Re}(\mathrm{e}^{-i\theta}F(b)) = \mathrm{Re}\left(\mathrm{e}^{-i\theta}\int_a^b f\right) = \mathrm{Re}\left|\int_a^b f\right| = \left|\int_a^b f\right|$.
On a aussi $G(b) = \mathrm{Re}\left(\int_a^b \mathrm{e}^{-i\theta} f\right) = \int_a^b \mathrm{Re}(\mathrm{e}^{-i\theta}f) \leqslant \int_a^b |\mathrm{Re}(\mathrm{e}^{-i\theta}f)|$,
or $|\mathrm{Re}(\mathrm{e}^{-i\theta}f)| \leqslant |\mathrm{e}^{-i\theta}f|$ (classique), donc $\left|\int_a^b f\right| = G(b) \leqslant \int_a^b |\mathrm{e}^{-i\theta}f| = \int_a^b |f|$.
3. D'après ce qui précède, $\left|\int_a^b fg\right| \leqslant \int_a^b (|f| \times |g|)$. Il suffit alors d'utiliser les résultats sur les applications à valeurs réelles.

□

Exemple 6.0.4.

$$\begin{aligned}\int \frac{\mathrm{d}t}{1+it} &= \int \frac{1-it}{1+t^2}\,\mathrm{d}t \\ &= \int \frac{1}{1+t^2}\,\mathrm{d}t - i\int \frac{t}{1+t^2}\,\mathrm{d}t \\ &= \mathrm{Arctan}\, t - \frac{i}{2}\ln(1+t^2) + K, \qquad K \in \mathbb{C}.\end{aligned}$$

7 Approximation d'intégrales

On cherche maintenant à approcher des intégrales par des formes géométriques simples : rectangles à bases régulières d'abord, trapèzes ensuite.

7.1 Sommes de Riemann

Théorème 7.1.1 (Sommes de Riemann)**.**
Soient $a, b \in \mathbb{R}$ tels que $a < b$, $f \in \mathscr{C}^0([a,b],\mathbb{R})$ et $n \in \mathbb{N}^*$. On note alors, pour tout $k \in [\![0,n]\!]$, $x_k = a + k\dfrac{b-a}{n}$. Les $\{x_k\}_{k\in[\![0,n]\!]}$ forment alors une subdivision régulière de $[a,b]$ (*i.e.* tous les sous-intervalles sont de la même longueur).

En posant

$$S_n = \frac{b-a}{n}\sum_{k=0}^{n-1} f(x_k) \text{ et } S'_n = \frac{b-a}{n}\sum_{k=1}^{n} f(x_k),$$

$(S_n)_{n\in\mathbb{N}^*}$ et (S'_n) convergent toutes deux vers $\int_a^b f$.

Si de plus f est de classe $\mathscr{C}^1$, alors $\left|S_n - \int_a^b f\right| = O(1/n)$ et $\left|S'_n - \int_a^b f\right| = O(1/n)$, c'est-à-dire que dans les deux cas l'erreur de l'approximation est un $O(1/n)$.

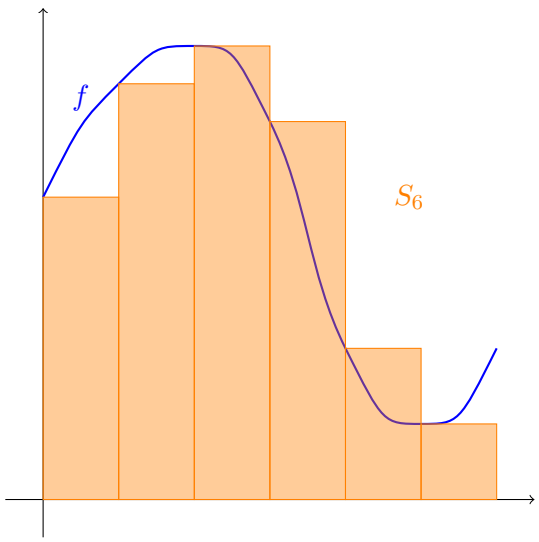


FIGURE XIX.3 – Exemple de somme de Riemann pour une fonction f, pour S_6.

Démonstration.
Traitons le cas de S'_n. Comme $S_n = S'_n + \dfrac{(b-a)}{n}(f(b) - f(a))$, les choses se passent exactement de la même manière pour S_n.

On a : $\int_a^b f = \int_{x_0}^{x_n} f \underset{\text{Chasles}}{=} \int_{x_0}^{x_1} f + \int_{x_1}^{x_2} f + \ldots + \int_{x_{n-1}}^{x_n} f = \sum_{k=1}^{n}\int_{x_{k-1}}^{x_k} f(t)\,\mathrm{d}t$.

Or $\int_{x_{k-1}}^{x_k} f(x_k)\,\mathrm{d}t = f(x_k)\int_{x_{k-1}}^{x_k} 1\,\mathrm{d}t = f(x_k)(x_k - x_{k-1}) = \dfrac{b-a}{n}f(x_k)$.

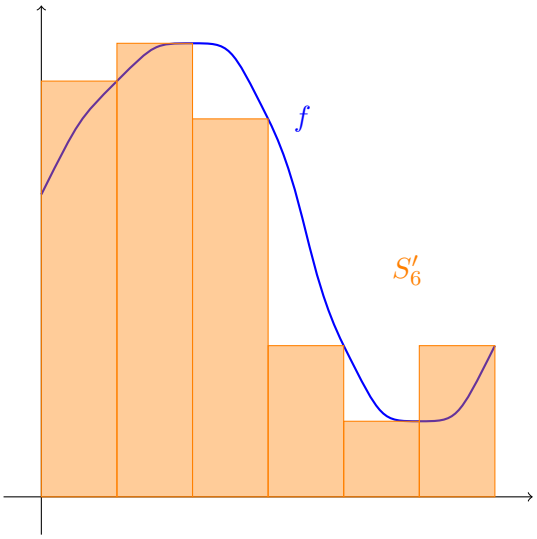


FIGURE XIX.4 – Exemple de somme de Riemann pour une fonction f, pour S'_6.

Donc $\left|\dfrac{b-a}{n}\sum_{k=1}^{n} f(x_k) - \int_a^b f(t)\,\mathrm{d}t\right| = \left|\sum_{k=1}^{n}\int_{x_{k-1}}^{x_k} (f(x_k)-f(t))\,\mathrm{d}t\right|$.

Ainsi $\left|S'_n - \int_a^b f\right| \leqslant \sum_{k=1}^{n}\int_{x_{k-1}}^{x_k} |f(x_k)-f(t)|\,\mathrm{d}t$ (♡).

Mais f est continue sur le segment $[a,b]$, donc d'après le théorème de Heine, elle y est uniformément continue, *i.e.* : soit $\varepsilon > 0$, alors il existe $\alpha > 0$ tel que $\forall x, y \in [a,b]$, $|x-y| < \alpha \Rightarrow |f(x)-f(y)| < \varepsilon$. Choisissons $N \in \mathbb{N}$ tel que $\dfrac{b-a}{N} < \alpha$, donc pour tout $n \geqslant N$, on a $\dfrac{b-a}{n} < \alpha$. Par conséquent, si $n \geqslant N$ et que l'on note encore $\{x_k\}$ la subdivision de l'énoncé associée à ce n, on a, pour tout $t \in [x_{k-1}, x_k]$, $|t - x_k| \leqslant |x_k - x_{k-1}| = \dfrac{b-a}{n} < \alpha$.

Dans ce cas, (♡) implique :

$$\begin{aligned}\left|S'_n - \int_a^b f\right| < \sum_{k=1}^{n}\int_{x_{k-1}}^{x^k} \varepsilon\,\mathrm{d}t &< \varepsilon\sum_{k=1}^{n}(x_k - x_{k-1})\\ &= \varepsilon\sum_{k=1}^{n}\frac{b-a}{n}\\ &= \varepsilon(b-a),\end{aligned}$$

et finalement $\left|S'_n - \int_a^b f\right| \xrightarrow[n\to+\infty]{} 0$.

Si de plus f est de classe $\mathscr{C}^1$, alors f' est continue et donc $|f'|$ est bornée par un certain réel $K > 0$ sur $[a,b]$. On en tire que f est K-lipschitzienne sur $[a,b]$. (♡) donne donc :

$$\begin{aligned}\left|S'_n - \int_a^b f\right| &\leqslant \sum_{k=1}^{n}\int_{x_{k-1}}^{x_k} K|x_k - t|\,\mathrm{d}t\\ &\leqslant K\sum_{k=1}^{n}\int_{x_{k-1}}^{x_k}(x_k - t)\,\mathrm{d}t\\ &\leqslant K\sum_{k=1}^{n}\left[-\frac{1}{2}(x_k-t)^2\right]_{x_{k-1}}^{x_k}\\ &\leqslant \frac{K}{2}\sum_{k=1}^{n}(x_k - x_{k-1})^2\\ &\leqslant \frac{K}{2}\sum_{k=1}^{n}\left(\frac{b-a}{n}\right)^2\\ &\leqslant \frac{K}{2}n\left(\frac{b-a}{n}\right)^2\\ &\leqslant \frac{K(b-a)^2}{2}\times\frac{1}{n},\end{aligned}$$

donc $\left|S'_n - \int_a^b f\right| = O\left(\dfrac{1}{n}\right)$. □

Remarque 7.1.2.
Pour la deuxième partie du résultat, il n'est pas nécessaire que f soit de classe $\mathscr{C}^1$: il suffit qu'elle soit lipschitzienne.

Exercice 7.1.3.
Montrer que la première partie du résultat reste vraie si on suppose seulement f de classe $\mathscr{C}_m$.

Remarque 7.1.4.
Quand f est continue, on peut toujours écrire

$$\begin{aligned}S_n &= \frac{b-a}{n}\sum_{k=1}^{n} f\left(a + k\frac{b-a}{n}\right)\\ &= (b-a)\times\frac{1}{n}\sum_{k=1}^{n} g\left(\frac{k}{n}\right)\\ &\xrightarrow[n\to+\infty]{} (b-a)\int_0^1 g,\end{aligned}$$

avec $g : [0,1] \to \mathbb{R}$, $t \mapsto f(a + t(b-a))$.

Exercice 7.1.5.
Faire apparaître une somme de Riemann dans

$$S_n = \sum_{k=1}^{n}\frac{n}{k^2 + 2n^2}$$

puis étudier la convergence de (S_n).

7.2 La méthode des trapèzes

La méthode d'approximation des sommes de Riemann est couramment appelée *méthode des rectangles*. Sa convergence n'est pas très rapide car elle est seulement en $O(1/n)$. Une amélioration possible est la méthode qui suit : la *méthode des trapèzes*.

Théorème 7.2.1.
On reprend les mêmes notations que dans le théorème 7.1.1, mais cette fois f est de classe $\mathscr{C}^2$. Alors :

$$\left|\frac{b-a}{n}\left(\frac{f(a)+f(b)}{2}+\sum_{k=1}^{n-1} f(x_k)\right)-\int_a^b f(t)\,\mathrm{d}t\right| = O(1/n^2).$$

Remarque 7.2.2.
Ce résultat est admis, mais remarquons tout de même les choses suivantes :

1. la somme des aires des trapèzes obtenus avec la subdivision $\{x_k\}$ vaut

$$\begin{aligned} T_n &= \sum_{k=0}^{n-1} \underbrace{\frac{b-a}{n}}_{\text{base}} \times \underbrace{\frac{f(x_{k+1})+f(x_k)}{2}}_{\text{moyenne des deux hauteurs}} \\ &= \frac{b-a}{2n}\left(\sum_{k=0}^{n-1} f(x_{k+1}) + \sum_{k=0}^{n-1} f(x_k)\right) \\ &= \frac{b-a}{2n}\left(\sum_{k=1}^{n} f(x_k) + \sum_{k=0}^{n-1} f(x_k)\right) \\ &= \frac{b-a}{2n}\left(f(x_0)+f(x_n)+2\sum_{k=1}^{n-1} f(x_k)\right) \\ &= \frac{b-a}{2n}\left(f(a)+f(b)+2\sum_{k=1}^{n-1} f(x_k)\right). \end{aligned}$$

2. il est aisé de voir que $(T_n)_{n\in\mathbb{N}^*}$ converge vers l'intégrale, et que la différence entre T_n et sa limite est un $O(1/n)$. En effet, pour tout $n \in \mathbb{N}^*$, $T_n = \frac{1}{2}(S_n + S'_n)$.

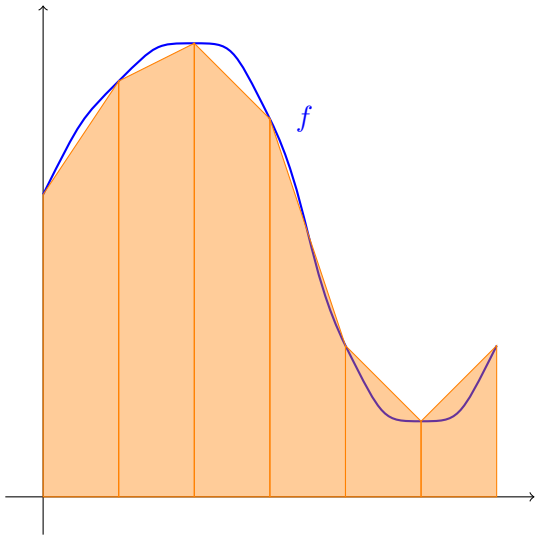


FIGURE XIX.5 – Exemple de la méthode des trapèzes pour une fonction f, avec 6 subdivision.

8 Comparaison série-intégrale

Proposition 8.0.1.
Soit $f : \mathbb{R}_+ \to \mathbb{R}_+$ une fonction continue par morceaux et décroissante.
Alors la suite $\left(\sum_{k=0}^{n} f(k)\right)_{n\in\mathbb{N}}$ converge si et seulement si la suite $\left(\int_0^n f(t)\,\mathrm{d}t\right)$ est convergente.
De plus la suite définie par $u_n = \sum_{k=0}^{n} f(k) - \int_0^n f(t)\,\mathrm{d}t$ converge.

Démonstration.
Soit $k \in \mathbb{N}$. Par décroissance de f, on a :

$$\forall t \in [k, k+1],\ 0 \leqslant f(k+1) \leqslant f(t) \leqslant f(k).$$

Puis, par intégration de cet encadrement sur $[k, k+1]$,

$$0 \leqslant f(k+1) \leqslant \int_k^{k+1} f(t)\,\mathrm{d}t \leqslant f(k) \qquad \text{(XIX.4)}$$

et, par sommation, pour $n \geqslant 1$,

$$0 \leqslant \sum_{k=0}^{n-1} f(k+1) \leqslant \int_0^n f(t)\,\mathrm{d}t \leqslant \sum_{k=0}^{n-1} f(k),$$

ou encore

$$0 \leqslant \sum_{k=0}^{n} f(k) - f(0) \leqslant \int_0^n f(t)\,\mathrm{d}t \leqslant \sum_{k=0}^{n} f(k) - f(n). \tag{XIX.5}$$

Les suites $\sum_{k=0}^{n} f(k)$ et $\int_0^n f(t)\,\mathrm{d}t$ ont donc la même nature.

De plus, il vient $0 \leqslant f(n) \leqslant \sum_{k=0}^{n} f(k) - \int_0^n f(t)\,\mathrm{d}t$, soit $0 \leqslant u_n$. Ainsi (u_n) est minorée. Enfin, on a

$$u_{n+1} - u_n = f(n+1) - \int_n^{n+1} f(t)\,\mathrm{d}t \leqslant 0.$$

La suite (u_n) est donc décroissante et minorée et converge donc. □

Remarque 8.0.2.
L'encadrement XXVI.1 est à rapprocher de la méthode des rectangles.

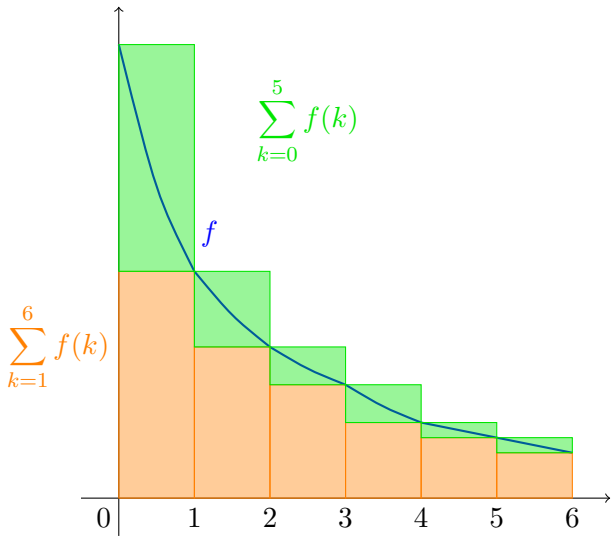


FIGURE XIX.6 – Exemple de comparaison série-intégrale pour une fonction f décroissante, positive.

Exercice 8.0.3.

Retrouver la nature de la suite $\left(\sum_{n=1}^{N} \frac{1}{n^\alpha}\right)_{N\in\mathbb{N}}$, pour $\alpha > 0$.

Exemple 8.0.4.
On pose $f : x \mapsto \frac{1}{1+x}$. On sait alors que la suite de terme général $u_n = \sum_{k=0}^{n} f(k) - \int_0^n f(t)\,\mathrm{d}t = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} - \ln n$ converge, vers une limite notée γ et nommée *constante d'Euler*.

9 Annexes

9.1 Règles de Bioche

Ces règles sont explicitement hors-programme et ne sont pas exigibles.

Soit f une expression rationnelle en $\sin t$ et $\cos t$, c'est-à-dire qu'il existe deux polynômes P et Q tels que $f(t) = \frac{P(\sin t, \cos t)}{Q(\sin t, \cos t)}$. Les régles de Bioche indiquent suivant certains cas, quel changement de variable poser pour pouvoir calculer $\int f(t)\,\mathrm{d}t$. On pose $W(t) = f(t)\,\mathrm{d}t$. Alors, si :

1. W est pair [1], un changement de variable judicieux est $u = \cos t$.
2. $W(\pi - t) = W(t)$, un changement de variable judicieux est $u = \sin t$.
3. $W(\pi + t) = W(t)$, un changement de variable judicieux est $u = \tan t$.
4. Si 2 des 3 relations précédentes sont vraies (dans ce cas les 3 relations sont vraies), un changement de variable judicieux est $u(t) = \cos(2t)$.
5. Dans les autres cas, le changement de variable $u(t) = \tan(t/2)$ s'avère souvent judicieux.

Exemple 9.1.1.
Calculer $\int \frac{\sin t}{1+\cos^2 t}\,\mathrm{d}t$ et $\int \frac{1}{\cos^2 t(1+\tan t)}\,\mathrm{d}t$.

9.2 Fonctions dont la variable intervient dans les bornes d'une intégrale (cas particulier d'intégrales dépendant d'un paramètre)

1. Attention : W n'est pas une application, on considère que $W(-t) = f(-t)\,\mathrm{d}(-t) = -f(-t)\,\mathrm{d}t$.

Théorème 9.2.1.
Soit $\varphi, \psi \in \mathscr{C}^1(I, J)$ où I et J sont deux intervalles de $\mathbb{R}$, et soit $f \in \mathscr{C}^0(J, \mathbb{R})$. Alors la fonction

$$\Gamma \ : \ \left\{ \begin{array}{ccc} I & \to & \mathbb{R} \\ x & \mapsto & \displaystyle\int_{\varphi(x)}^{\psi(x)} f(t)\,\mathrm{d}t \end{array} \right.$$

est de classe $\mathscr{C}^1$, et sa dérivée est

$$\gamma \ : \ \left\{ \begin{array}{ccc} J & \to & \mathbb{R} \\ x & \mapsto & \psi'(x) \times (f \circ \psi)(x) \\ & & -\varphi'(x) \times (f \circ \varphi)(x) \end{array} \right. .$$

Démonstration.
f étant continue, elle admet une primitive F. On a alors, pour tout $x \in I$:

$$\begin{aligned} \Gamma(x) &= \int_{\varphi(x)}^{\psi(x)} f(t)\,\mathrm{d}t = F(\psi(x)) - F(\varphi(x)) \\ &= F \circ \psi(x) - F \circ \varphi(x). \end{aligned}$$

Mais F, ψ et φ étant de classe $\mathscr{C}^1$, Γ l'est aussi et on a

$$\begin{aligned} \Gamma' &= (F \circ \psi - F \circ \varphi)' \\ &= \psi' \times (F' \circ \psi) - \varphi' \times (F' \circ \varphi) \\ &= \psi' \times (f \circ \psi) - \varphi' \times (f \circ \varphi) \\ &= \gamma. \end{aligned}$$

□

Chapitre XX

Dénombrement

Soient E, F et G trois ensembles.

Définition 0.0.1.
On dit que E et F sont *équipotents* s'il existe une bijection de E dans F. Dans ce cas, on notera $E \cong F$ (notation non officielle), et si φ est une bijection de E dans F, on notera $\varphi : E \xrightarrow{\sim} F$.

Proposition 0.0.2.
La relation d'équipotence est une relation d'équivalence.

1 Cardinal d'un ensemble fini

Le programme stipule que parmi les propriétés de la partie 1, les plus intuitives seront admises sans démonstration ; il stipule également que l'utilisation systématique de bijections dans les problèmes de dénombrement n'est pas un attendu du programme.

Définition 1.0.1.
On dit que E est *fini* s'il est vide ou s'il existe $n \in \mathbb{N}^*$ tel que $E \cong [\![1, n]\!]$.
Dans le cas contraire, E est dit *infini*.

Le résultat qui donne un sens à ce que l'on appelle intuitivement *le nombre d'éléments d'un ensemble fini* est alors le suivant.

Théorème 1.0.2. (i) Soient n, m deux entiers naturels non nuls. Si $[\![1, n]\!] \cong [\![1, m]\!]$, alors $n = m$.

(ii) Cela assure que si un ensemble est fini et équipotent à $[\![1, n]\!]$ pour un certain $n \in \mathbb{N}^*$, alors ce n est unique et est appelé le *cardinal* de E, et est noté $\operatorname{Card} E$, $\#E$ ou $|E|$. Par convention, $\operatorname{Card} \varnothing = 0$.

Démonstration.
La démonstration du premier point se fait par récurrence sur n en posant l'hypothèse (P_n) : pour tout $m \in \mathbb{N}^*$, si $[\![1, m]\!] \cong [\![1, n]\!]$, alors $m = n$.
La démonstration est tout à fait du même style que les démonstrations des résultats 1.0.8 et , et est laissée en exercice. □

Exemple 1.0.3. 1. Pour tout $n \in \mathbb{N}$, $[\![1, n]\!]$ est évidemment fini et de cardinal n.

2. Soient $n, m \in \mathbb{N}$, $n < m$.
Alors $\operatorname{Card}[\![n, m]\!] = m - n + 1$. En effet, l'application $[\![1, m-n+1]\!] \to [\![n, m]\!]$, $a \mapsto a+n-1$ est une bijection.

Dans toute la suite on supposera que E est fini de cardinal n.

Théorème 1.0.4.
E est équipotent à F si et seulement si (F est aussi fini et $\operatorname{Card} E = \operatorname{Card} F$).

Démonstration.
Si E est vide, F aussi.
Sinon, soit $\varphi : [\![1, n]\!] \xrightarrow{\sim} E$, et $\psi : E \xrightarrow{\sim} F$. Alors $\psi \circ \varphi : [\![1, n]\!] \xrightarrow{\sim} F$. □

Lemme 1.0.5.
Supposons E non vide, et $a \in E$. Alors $E \backslash \{a\}$ est fini de cardinal $n - 1$.

Démonstration.
Le cas où $E = \{a\}$ est évident. Supposons donc que $E\backslash\{a\}$ est non vide.
Soit $\varphi : [\![1, n]\!] \xrightarrow{\sim} E$.
Si $\varphi(n) = a$, posons $\psi = \varphi$.
Si $\varphi(n) = b$ pour b un élément de E différent de a, notons p l'antécédent de a. Donc $p < n$. Posons alors $\psi = \varphi \circ \tau_{p,n}$, où $\tau_{p,n}$ est la transposition de S_n échangeant p et n.
Alors dans tous les cas, $\psi : [\![1, n]\!] \xrightarrow{\sim} E$, et $\psi(n) = a$.
Ainsi, $\psi|_{[\![1,n-1]\!]} : [\![1, n-1]\!] \xrightarrow{\sim} E\backslash\{a\}$, d'où le résultat. □

Théorème 1.0.6.
Soit $A \subset E$. Alors A est fini et $\operatorname{Card} A \leqslant \operatorname{Card} E$. De plus, $\operatorname{Card} A = \operatorname{Card} E$ si et seulement si $A = E$.

Démonstration.
Par récurrence sur $n = \operatorname{Card} E$.
Si $n = 0$, $E = A = \varnothing$, et le résultat est évident.
Soit $n \in \mathbb{N}$ tel que pour tout ensemble E de cardinal n, et pour tout $A \subset E$, on A soit fini et $\operatorname{Card} A \leqslant \operatorname{Card} E$.
Soit E de cardinal $n+1$, et $A \subset E$. Si $A = E$, alors A est fini et $\operatorname{Card} A = \operatorname{Card} E$.
Sinon, soit $a \in E \backslash A$. Posons $\tilde{E} = E \backslash \{a\}$. Alors $\operatorname{Card} \tilde{E} = n-1$ d'après le lemme précédent, et $A \subset \tilde{E}$. Par hypothèse de récurrence, A est fini, et $\operatorname{Card} A \leqslant n-1$. En particulier, $\operatorname{Card} A < \operatorname{Card} E$, donc $A \neq E$, ce qui prouve au passage que $\operatorname{Card} A = \operatorname{Card} E$ si et seulement si $A = E$. □

Remarque 1.0.7.
Grâce à ce résultat, pour montrer l'égalité de deux ensembles finis, on peut montrer la double inclusion, mais aussi se contenter d'une inclusion et montrer l'égalité des cardinaux.
Ce résultat est à rapprocher du résultat assurant que deux espaces vectoriels de dimension finie sont égaux si et seulement si l'un est inclus dans l'autre et ils ont même dimension.

Lemme 1.0.8.
Soit f une application surjective de F dans G. Alors il existe une injection de G dans F.

Démonstration.
Soit $y \in G$. Alors y a un (ou plusieurs) antécédent(s) par f. Choisissons un de ces antécédents, par exemple le plus petit, puisque $f^{-1}(\{y\})$ est une partie non vide de $\mathbb{N}$, et notons-le $g(y)$. On définit ainsi une application $g : G \to F$, tel que pour tout $y \in G$, $f(g(y)) = y$. Ainsi, $f \circ g$ est injective, et on sait alors que g est injective de G dans F. □

Exercice 1.0.9.
Montrer que s'il existe une injection $f : F \to G$, alors il existe une surjection $g : G \to F$.

Théorème 1.0.10.
Soit f une application de F dans G.

(i) Si G est fini et f est injective, alors F est fini également, et $\operatorname{Card} F \leqslant \operatorname{Card} G$.

(ii) Si F est fini et f est surjective, alors G est fini également, et $\operatorname{Card} F \geqslant \operatorname{Card} G$.

(iii) Si F et G sont finis et $\operatorname{Card} F = \operatorname{Card} G$, alors :

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

Remarque 1.0.11.
La relation « F a moins d'éléments que G » correspond donc à « F s'injecte dans G » (au moins pour des ensembles finis).

De même, la relation « F a plus d'éléments que G » correspond donc à « F se surjecte sur G » (au moins pour des ensembles finis).

Concernant des ensembles quelconques, le lecteur intéressé pourra étudier le théorème de Cantor-Bernstein.

Remarque 1.0.12.
Une fois encore, ce résultat est à rapprocher des résultats sur les espaces vectoriels et les applications linéaires en dimension finie.

Démonstration. (i) f étant injective, elle établit une bijection de F dans $f(F)$. Or $f(F) \subset G$, donc $f(F)$ est fini et $\operatorname{Card} f(F) \leqslant \operatorname{Card} G$. Ainsi, puisque $F \cong f(F)$, F est fini et $\operatorname{Card} F \leqslant \operatorname{Card} G$.

(ii) En utilisant 1.0.11, soit g injective de G dans F. En appliquant le premier point, G est donc fini et $\operatorname{Card} G \leqslant \operatorname{Card} F$.

(iii) Il suffit de démontrer : f est injective $\Leftrightarrow$ f est surjective, le reste étant alors facile.
Pour le sens direct, si f est injective, f est une bijection de F dans $f(F)$, donc $\operatorname{Card} F = \operatorname{Card} f(F)$. Mais $\operatorname{Card} G = \operatorname{Card} F$, donc $\operatorname{Card} f(F) = \operatorname{Card} G$, et comme $f(F) \subset G$, nous avons $f(F) = G$, ce qui signifie bien que f est surjective.
Pour le sens indirect, soient $x, y \in F$ tels que $f(x) = f(y)$ et $x \neq y$. Alors $f(y) \in f(F \backslash \{y\})$, et donc $f(F \backslash \{y\}) = G$. Par conséquent, $f|_{F\backslash\{y\}}$ est surjective à valeurs dans G, donc avec le point (ii), $\operatorname{Card} F\backslash\{y\} \geqslant \operatorname{Card} G$. Mais $\operatorname{Card} F\backslash\{y\} = \operatorname{Card} F - 1 = \operatorname{Card} G - 1$, ce qui est absurde. Par conséquent, f est aussi injective.

□

Exercice 1.0.13.
Soient $(G, \star)$ un groupe et A une partie ***finie*** non vide de G stable par $\star$. Soit $x \in A$.

1. Soit $\varphi : \mathbb{N}^* \to G$ l'application définie par $\varphi(n) = x^n$. Montrer que φ n'est pas injective.
2. En déduire que $x^{-1} \in A$, puis que A est un sous-groupe de $(G, \star)$.

Corollaire 1.0.14 (Principe des tiroirs, ou *Pigeonhole Principle* en anglais)**.**
Si $m < n$, il est impossible de ranger n paires de chaussettes dans m tiroirs sans en mettre au moins deux dans le même tiroir.

Exercice 1.0.15.
1. On prend un Rubik's Cube fini sur lequel on effectue la même manipulation encore et toujours. Démontrer que l'on finit par se retrouver avec ce Rubik's Cube de nouveau terminé [1].
2. Les membres d'une société internationale sont originaires de six pays différents. La liste des membres contient 1978 noms numérotés de 1 à 1978. Montrer qu'il y a un membre dont le numéro vaut la somme des numéros de deux autres membres venant du même pays ou le double du numéro d'un compatriote.

2 Dénombrement

2.1 Réunion, intersection et complémentaire

Définition 2.1.1.
Lorsque deux ensembles A et B sont disjoints, la réunion de A et B est appelée *union disjointe* de A et B, et est notée $A \sqcup B$.

Théorème 2.1.2.
Soient A et B deux parties de E.

(i) Si A et B sont disjoints, alors $\mathrm{Card}(A \sqcup B) = \mathrm{Card}\, A + \mathrm{Card}\, B$;

(ii) $\mathrm{Card}(A \backslash B) = \mathrm{Card}\, A - \mathrm{Card}(A \cap B)$;

(iii) $\mathrm{Card}(A \cup B) = \mathrm{Card}\, A + \mathrm{Card}\, B - \mathrm{Card}(A \cap B)$.

(iv) $\mathrm{Card}\left(\complement_E^A\right) = \mathrm{Card}\, E - \mathrm{Card}\, A$.

Démonstration. (i) Soient m, p les cardinaux de A et B, et $\varphi : [\![1, m]\!] \xrightarrow{\sim} A$ et $\psi : [\![1, p]\!] \xrightarrow{\sim} B$.
Soit $\chi : \begin{array}{ccc} [\![1, m+p]\!] & \to & A \sqcup B \\ x & \mapsto & \begin{cases} \varphi(x) & \text{si } x \leqslant m \\ \psi(x-m) & \text{si } x > m \end{cases} \end{array}$.
Cette application est bien définie et il est facile de voir qu'elle est surjective. De plus, A et B étant disjoints, elle est injective, donc $A \sqcup B \cong [\![1, m+p]\!]$, donc $\mathrm{Card}(A \sqcup B) = m + p = \mathrm{Card}\, A + \mathrm{Card}\, B$.

(ii) Il suffit d'écrire que $A = (A \cap B) \sqcup (A \backslash B)$ et d'utiliser le premier point.

(iii) Là encore, on remarque que $A \cup B = B \sqcup (A \backslash B)$ et on utilise les deux premiers points.

(iv) Remarquer que $\complement_E^A = E \backslash A$.

□

Remarque 2.1.3.
Il existe une formule qui généralise le résultat précédent à la réunion d'une famille finie d'ensembles finis : c'est la *formule de Poincaré*, aussi appelée *formule du crible*. Elle est hors-programme et sera vue en TD.

2.2 Produit cartésien

Théorème 2.2.1.
Soient E et F deux ensembles finis. Alors $E \times F$ est fini et

$$\mathrm{Card}(E \times F) = (\mathrm{Card}\, E) \times (\mathrm{Card}\, F).$$

 Il existe beaucoup d'analogies entre la dimension d'un espace vectoriel et le cardinal d'un ensemble, mais $\dim(E \times F) = \dim E + \dim F$.

Démonstration.
On note :

$$n = \mathrm{Card}\, E,\ p = \mathrm{Card}\, F,$$
$$E = \{ e_1, \cdots, e_n \},\ F = \{ f_1, \cdots, f_p \}.$$

1. Pour mémoire, il y a plus de 43.10^{12} combinaisons possibles sur un Rubik's Cube classique.

Donc $E \times F = \{ (e_i, f_j),\ i \in [\![1,n]\!],\ j \in [\![1,p]\!] \}$.
Donc en notant $A_i = \{ e_i \} \times F$ pour $i \in [\![1,n]\!]$, on a :

$$E \times F = \bigsqcup_{i=1}^{n} A_i,$$

ainsi

$$\begin{aligned} \operatorname{Card} E \times F &= \sum_{i=1}^{n} \operatorname{Card} A_i \\ &= \sum_{i=1}^{n} \operatorname{Card} F \\ &= n \operatorname{Card} F \\ &= \operatorname{Card} E \times \operatorname{Card} F. \end{aligned}$$

□

Remarque 2.2.2.
Ce résultat se généralise facilement par récurrence à un produit de q ensembles finis, $q \in \mathbb{N}^*$:

$$\operatorname{Card}\left(\prod_{i=1}^{q} E_i\right) = \prod_{i=1}^{q} \operatorname{Card} E_i.$$

Exercice 2.2.3.
Combien y a-t'il de possibilités de tirer neuf cartes avec remise dans un jeu de 32 cartes ?

2.3 Applications entre ensembles finis

Théorème 2.3.1.
Soient E et F deux ensembles finis. Alors F^E est fini et

$$\operatorname{Card}\left(F^E\right) = (\operatorname{Card} F)^{\operatorname{Card} E}.$$

Démonstration.
On pose $\varphi : [\![1,n]\!] \xrightarrow{\sim} E$, et :

$$\begin{array}{rccc} \mu : & F^E & \to & F^n \\ & f & \mapsto & (f \circ \varphi(1), \cdots, f \circ \varphi(n)) = (f \circ \varphi(i))_{i \in [\![1,n]\!]} \end{array}$$

$$\begin{array}{rccc} \nu : & F^n & \to & F^E \\ & (f_1, \cdots, f_n) = (f_i)_{i \in [\![1,n]\!]} & \mapsto & \left\{ \begin{array}{ccc} E & \to & F \\ x & \mapsto & f_{\varphi^{-1}(x)} \end{array} \right. \end{array}.$$

On vérifie que $\nu \circ \mu = \mathrm{Id}_{F^E}$ et $\mu \circ \nu = \mathrm{Id}_{F^n}$, donc ce sont des bijections. Ainsi $F^E \cong F^n$ et l'on peut conclure avec 1.0.7. □

Définition 2.3.2.
Soit $p \in [\![1,n]\!]$. On appelle *p-arrangement de E* toute injection de $[\![1,p]\!]$ dans E. Autrement dit, un p-arrangement est une manière de choisir p éléments distincts de E **en tenant compte de l'ordre dans lequel on choisit ces éléments** ; c'est donc aussi un p-uplet de E, ou encore une liste de p éléments de E.

Exemple 2.3.3.
Si $E = [\![1,5]\!]$ et $p = 2$, les applications φ et ψ de $[\![1,2]\!]$ dans E telles que $\varphi(1) = 3$, $\varphi(2) = 5$, $\psi(1) = 5$ et $\psi(2) = 3$, sont deux p-arrangements **différents** de E.

On peut aussi les identifier aux couples $(3,5)$ et $(5,3)$.

Théorème 2.3.4.
Si $\operatorname{Card} E = n$, il y a exactement $\dfrac{n!}{(n-p)!}$ p-arrangements de E.

Démonstration.
Pour construire une injection f de $[\![1,p]\!]$ dans E, il y a n choix possibles pour $f(1)$. Il reste alors $n-1$ choix possibles pour $f(2)$ et ainsi de suite, jusqu'aux $n-p+1$ choix possibles pour $f(p)$: il y a donc $n \times (n-1) \times \cdots \times (n-p+1)$ injections possibles. □

Remarque 2.3.5.
Les arrangements sont utilisés pour modéliser des tirages **successifs** et **sans remise**.

Exercice 2.3.6.
Vous jouez « au hasard » au tiercé lors d'une course avec 10 partants : combien avez-vous de chance d'avoir le tiercé dans l'ordre ?

Corollaire 2.3.7.
Le groupe S_n des permutations sur n éléments est fini de cardinal $n!$.

Démonstration.
S_n correspond à l'ensemble des n-uplets de $[\![1,n]\!]$. □

2.4 Parties d'une ensemble fini

Définition 2.4.1.
Soit $p \in [\![0, n]\!]$. On appelle p-combinaison de E toute partie de E de cardinal p. Autrement dit, une p-combinaison est une manière de choisir p éléments distincts de E **sans tenir compte de l'ordre dans lequel on choisit ces éléments**. On note alors $\binom{n}{p}$ le nombre de p-combinaisons de E ; ce nombre se lit « p parmi n ».

Remarque 2.4.2.
Les combinaisons sont utilisées pour modéliser des tirages **simultanés**.

Remarque 2.4.3.
On étend cette définition à $p \in \mathbb{Z}$ par $\binom{n}{p} = 0$ lorsque $p \notin [\![0, n]\!]$.

Théorème 2.4.4.
Si $n \in \mathbb{N}$ et $p \in [\![0, n]\!]$, alors $\binom{n}{p} = \dfrac{n!}{(n-p)!p!}$.

Remarque 2.4.5.
Nous venons donc de donner une nouvelle définition du coefficient binomial $\binom{n}{p}$, défini en début d'année, et que nous avions interprétré comme le nombre de chemin réalisant p succès lors de n répétitions d'une même expérience aléatoire. Remarquons à nouveau qu'il s'agit d'un entier, ce qui n'est absolument pas évident avec la formule du théorème 2.4.4.

Démonstration.
Commençons par remarquer qu'ordonner (totalement) un ensemble à n éléments revient à numéroter ses éléments de 1 à n. Par conséquent, un ordre sur E peut être vu comme une bijection de $[\![1, n]\!]$ dans E, ou encore comme une permutation de E. Il y a donc $n!$ façons d'ordonner un ensemble à n éléments.
Ainsi, pour chaque choix de p éléments parmi n, il existe $p!$ p-arrangements contenant ces p-éléments : il y a donc exactement $p!$ fois plus de p-arrangements que de p-combinaisons. Ainsi, $\binom{n}{p} = \dfrac{1}{p!} \times \dfrac{n!}{(n-p)!}$. □

Exercice 2.4.6.
Vous jouez au hasard au tiercé lors d'une course avec 10 partants : combien avez-vous de chance d'avoir le tiercé dans le désordre ?

Proposition 2.4.7 (Formule du triangle de Pascal)**.**
Si $n \in \mathbb{N}$ et si $p \in \mathbb{N}$, $\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p}$.

Démonstration.
On donne ici une preuve combinatoire. Le cas où $p \notin [\![1, n-1]\!]$ est évident. Sinon, soit E de cardinal n et $a \in E$. Notons F_p l'ensemble des parties de E a p éléments, alors

$$F_p = \underbrace{\{A \subset E | \#A = p \text{ et } a \in A\}}_{A_p} \sqcup \underbrace{\{A \subset E | \#A = p \text{ et } a \notin A\}}_{B_p}.$$

Il est évident *(sinon, détaillez le !)* que A_p est en correspondance bijective avec l'ensemble des parties de $E \setminus \{a\}$ ayant $p-1$ éléments (par $A \mapsto A \setminus \{a\}$) et possède donc $\binom{n-1}{p-1}$ éléments. De même, B_p est en correspondance bijective avec l'ensemble des parties de $E \setminus \{a\}$ ayant p éléments (par $A \mapsto A$) et possède donc $\binom{n-1}{p}$ éléments. Cela permet donc de conclure, car $\#F_p = \#A_p + \#B_p$. □

Proposition 2.4.8 (Formule du binôme de Newton)**.**
Soit x et y deux éléments d'un anneau $(A, +, \cdot)$ commutant l'un avec l'autre ($xy = yx$), soit $n \in \mathbb{N}$. Alors

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

Démonstration.
En voici une preuve combinatoire. On montre d'abord aisément par récurrence que toutes les puissances de x et de y commutent. Ensuite, lorsque l'on développe le produit

$$(x+y)^n = \underbrace{(x+y)\cdots(x+y)}_{n \text{ fois}}$$

on obtient des termes qui sont des produits de k facteurs valant x, et de $n-k$ facteurs valant y, pour k allant de 0 à n. Or, pour chacun de ces k, il y a k parmi n possibilités d'obtenir un produit de k facteurs valant x, et de $n-k$ facteurs valant y, d'où le résultat. □

Théorème 2.4.9.
Si E est fini, l'ensemble $\mathscr{P}(E)$ des parties l'est aussi et

$$\operatorname{Card} \mathscr{P}(E) = 2^{\operatorname{Card} E}.$$

Démonstration.
Pour tout $i \in [\![0, n]\!]$, notons P_i l'ensemble des parties de E ayant i éléments. Nous avons alors $\mathscr{P}(E) = \bigsqcup_{i=0}^{n} P_i$. Or chaque P_i est de cardinal $\binom{n}{i}$, donc $\mathscr{P}(E)$ est fini et :

$$\begin{aligned}\operatorname{Card} \mathscr{P}(E) &= \sum_{i=0}^{n} \binom{n}{i} \\ &= (1+1)^n \quad \text{(binôme de Newton)} \\ &= 2^n.\end{aligned}$$

On peut aussi voir qu'il y a une correspondance bijective entre les parties de E et les applications à variables dans E et à valeurs dans $\{0,1\}$, par $\mathscr{P}(E) \to \{0,1\}^E$, $A \mapsto \mathbf{1}_A$. □

Exercice 2.4.10.
Dans une urne, on place quatre boules rouges (numérotées 1 à 4) et quatre boules vertes (numérotées 5 à 8). On réalise trois tirages avec remise, un résultat est le triplet des boules tirées.

Combien y a-t-il de résultats contenant exactement une boule rouge ? Au moins une boule rouge ? Et si les tirages se font sans remise ?

Chapitre XXI

Espaces vectoriels de dimension finie

Dans tout ce chapitre, sauf mention expresse du contraire, E désigne un espace vectoriel sur un corps $\mathbb{K}$, valant $\mathbb{R}$ ou $\mathbb{C}$.

1 Notion de dimension

1.1 Définition

Définition 1.1.1.
On dit que E est *de dimension finie* si E admet une famille génératrice finie.

Exemple 1.1.2.
1. $\mathbb{K}^n$ est de dimension finie car engendré notamment par la famille des $\Big((\delta_{ij})_{i\in[\![1,n]\!]}\Big)_{j\in[\![1,n]\!]}$.
2. $\mathbb{K}[X]$ n'est pas de dimension finie. En effet, considérons une famille finie de polynômes $(P_i)_{i\in[\![1,n]\!]}$. Alors toute combinaison linéaire de cette famille a un degré borné par le maximum des degrés des P_i. Or les éléments de $\mathbb{K}[X]$ ont des degrés arbitrairement élévés, donc la famille considérée ne peut être génératrice.
3. Soit A un ensemble. L'espace vectoriel $\mathbb{K}^A$ est de dimension finie si et seulement si A est fini [1].
4. Soit E un $\mathbb{K}$-espace vectoriel (pas nécessairement de dimension fini). Soit $n \in \mathbb{N}$ et $x_1, \dots, x_n$, n vecteurs de E. Alors le sous-espace vectoriel de E $\mathrm{Vect}\,(x_1, \dots, x_n)$ est un espace vectoriel de dimension finie.

Remarque 1.1.3.
Cas particulier : l'espace vectoriel $\{0\}$ est de dimension finie. En effet, toute famille en est génératrice (y compris la famille vide).

1.2 Théorème fondamental

Dans toute la suite du chapitre, E est un $\mathbb{K}$-ev de dimension finie.

1. Le «si» est facile à voir, le «seulement si» est beaucoup plus difficile à démontrer ; on pourra utiliser le résultat 1.2.1

Théorème 1.2.1.
Soit $n \in \mathbb{N}$ tel que E admette une famille génératrice à n éléments. Alors toute famille de E contenant strictement plus de n vecteurs est liée.

Démonstration.
Remarquons d'abord qu'il suffit de montrer que toute famille de E contenant $n+1$ vecteurs est liée. En effet, une famille contenant strictement plus de n vecteurs, en contient au moins $n+1$. Elle contient donc une sous-famille liée, donc est liée elle-même.
Montrons le résultat par récurrence sur n, en posant pour tout $n \in \mathbb{N}$:

(H_n) : pour tout $\mathbb{K}$-ev E admettant une famille génératrice à n éléments, toute famille de E contenant strictement plus de n vecteurs est liée.

• Le cas $n = 0$ est celui où $E = \{0\}$, et le résultat est alors vrai.
• Supposons (H_n) vraie pour un entier $n \in \mathbb{N}$. Soient $(g_1, \dots, g_{n+1})$ une famille génératrice d'un $\mathbb{K}$-ev E, et $(v_1, \dots, v_{n+2})$ une famille de vecteurs de E.
Pour tout $i \in [\![1, n+2]\!]$, on note $v_i = \sum_{k=1}^{n+1} \alpha_{i,k} g_k$. Distinguons deux cas :
1er cas : si pour tout i, $\alpha_{i,1} = 0$, alors pour tout i, $v_i \in \mathrm{Vect}(g_2, \dots, g_{n+1})$. Si l'on note $F = \mathrm{Vect}(g_2, \dots, g_{n+1})$, on peut appliquer l'hypothèse de récurrence à F, qui admet une famille génératrice à n éléments, et à $(v_1, \dots, v_{n+2})$: $(v_1, \dots, v_{n+2})$ est liée dans F, donc aussi dans E, dont F est un sev, et (H_{n+1}) est vraie.
2ème cas : il existe $i \in [\![1, n+2]\!]$ tel que $\alpha_{i,1} \neq 0$, par exemple $\alpha_{1,1} \neq 0$.
Alors

$$g_1 = \frac{1}{\alpha_{1,1}} \left(v_1 - \sum_{k=2}^{n+1} \alpha_{1,k} g_k \right),$$

d'où

$$\text{pour tout } i \in [\![2, n+2]\!], \quad v_i = \frac{\alpha_{i,1}}{\alpha_{1,1}} \left(v_1 - \sum_{k=2}^{n+1} \alpha_{1,k} g_k \right) + \sum_{k=2}^{n+1} \alpha_{i,k} g_k.$$

Si l'on pose $w_i = v_i - \dfrac{\alpha_{i,1}}{\alpha_{1,1}} v_1$, alors pour tout $i \in [\![2, n+2]\!]$ $w_i \in \mathrm{Vect}(g_2, \dots, g_{n+1})$. Par hypothèse de récurrence, $(w_2, \dots, w_{n+2})$ est liée. Il existe donc une combinaison linéaire nulle en les w_i, à coefficients non tous nuls. Il est facile de voir que cette combinaison linéaire est aussi une combinaison linéaire nulle en les $v_1, \dots, v_{n+2}$, à coefficients non tous nuls. Ainsi (H_{n+1}) est vraie. □

Remarque 1.2.2.
On notera que l'idée de la démonstration précédente est très proche de celle de l'algorithme du pivot de Gauss.

Exemple 1.2.3.
• Dans $\mathbb{R}^2$, toute famille de trois vecteurs est liée. Mais une famille de strictement moins de trois vecteurs n'est pas forcément libre !
• Dans $\mathbb{R}^3$, toute famille de quatre vecteurs est liée.
• Dans $\mathbb{R}_n[X]$, toute famille de $n+2$ polynômes est liée.
• Dans $\mathbb{C}_n[X]$, vu comme $\mathbb{C}$-espace vectoriel, toute famille de $n+2$ polynômes est liée.
• Dans $\mathbb{C}_n[X]$, vu comme $\mathbb{R}$-espace vectoriel, toute famille de $2n+3$ polynômes est liée, tandis que la famille de $2n+2$ polynômes $(1, i, X, iX, \dots, X^n, iX^n)$ est libre.

Nous verrons dans la partie **? ?** que ce résultat (fondamental !) mène directement au corollaire suivant.

Corollaire 1.2.4.
Dans un espace vectoriel de dimension finie, toutes les bases sont finies et de même cardinal.

1.3 Existence de bases

On peut développer une première idée afin d'obtenir une base dans un espace vectoriel de dimension finie, idée d'ailleurs déjà ébauchée dans le cours sur les espaces vectoriels. On part d'une famille génératrice finie de E :
- si cette famille est libre, c'est une base ;
- sinon, un de ses vecteurs et « redondant », soit combinaison linéaire des autres, et on peut l'enlever pour obtenir une famille génératrice strictement plus petite.

En itérant, on obtient une suite de familles génératrices strictement décroissante (en taille) : on s'arrête donc et l'on obtient une base.

Nous allons voir un résultat plus fin qui nous permet de retrouver ceci : le théorème de la base incomplète.

Lemme 1.3.1.
Soit $p \in \mathbb{N}$ et $(x_i)_{i\in[\![1,p]\!]}$ une famille de vecteurs de E.

La famille $(x_i)_{i\in[\![1,p]\!]}$ est liée si et seulement s'il existe $k \in [\![1,p]\!]$ vérifiant

$$x_k \in \mathrm{Vect}\,(x_1, \dots, x_{k-1}).$$

Autrement dit si et seulement si l'un des vecteurs de la famille est combinaison linéaire des précédents.

Démonstration.
Supposons que la famille est liée. Alors il existe une combinaison linéaire $\sum_{i=1}^{p} \lambda_i x_i$ non triviale de valeur 0. On note k le plus grand entier i tel que $\lambda_i \neq 0$. Alors on a successivement :

$$\sum_{i=1}^{k} \lambda_i x_i = 0,$$

$$x_k = \frac{1}{\lambda_k} \sum_{i=1}^{k-1} \lambda_i x_i,$$

$$x_k \in \mathrm{Vect}\,(x_1, \dots, x_{k-1}).$$

L'implication réciproque est évidente. □

Corollaire 1.3.2.
Soit
- $p \in \mathbb{N}$,
- $(x_1, \dots, x_p)$ une famille libre de vecteurs de E,
- x un vecteur de E.

Alors

$$(x_1, \dots, x_p, x) \text{ est liée } \iff x \in \mathrm{Vect}(x_1, \dots, x_p).$$

Démonstration.
Supposons $(x_1, \dots, x_p, x)$ liée, et posons $x_{p+1} = x$. D'après le lemme, il existe $k \in 1, p+1$ vérifiant $x_k \in \mathrm{Vect}\,(x_1, \dots, x_{k-1})$. On ne peut avoir $k \leqslant p$ puisque la famille $(x_1, \dots, x_p)$ est libre. Donc $k = p+1$ et on a $x \in \mathrm{Vect}\,(x_1, \dots, x_p)$.

□

Théorème 1.3.3 (de la base incomplète)**.**
Soient E un $\mathbb{K}$-espace vectoriel engendré par une famille $\mathscr{G}$ finie, et $\mathscr{L}$ une famille libre de E. Alors on peut compléter $\mathscr{L}$ en une base de E en lui rajoutant des vecteurs de $\mathscr{G}$.

Remarque 1.3.4.
Ce théorème est vrai pour tout espace vectoriel E et non seulement pour ceux de dimension finie. La démonstration est relativement délicate dans le cas général (on utilise en général le lemme de Zorn, équivalent à l'axiome du choix), nous nous contenterons de la donner dans le cas de la dimension finie.

Démonstration.
Une démonstration possible est de considérer l'algorithme suivant :

$\mathscr{B} \leftarrow \mathscr{L}$
Invariant de boucle : $\mathscr{B}$ *est libre et* $\mathscr{L} \subset \mathscr{B}$
Variant : $\operatorname{Card}\mathscr{G} - \operatorname{Card}\mathscr{B}$
TantQue $\mathscr{G} \not\subset \operatorname{Vect}\mathscr{B}$ **Faire**
  `Choisir v` $\in (\mathscr{G} \setminus \operatorname{Vect}\mathscr{B})$
  $\mathscr{B} \leftarrow \mathscr{B} \cup \{$ `v` $\}$
FinTantQue

$\mathscr{L}$ est libre et l'invariant est clairement vérifié avant l'entrée dans la boucle.

Si l'invariant est vérifié, au début d'un tour de boucle, $\mathscr{B}$ est libre et $\mathscr{G} \setminus \operatorname{Vect}\mathscr{B} \neq \varnothing$, donc on peut effectivement choisir `v` dans $\mathscr{G} \setminus \operatorname{Vect}\mathscr{B}$.

Alors puisque $\mathscr{B}$ est libre, d'après le lemme 1.3.1, $\mathscr{B} \cup \{$ `v` $\}$ est libre également.

À la fin du tour de boucle, $\mathscr{B}$ est donc toujours libre, est toujours un sur-ensemble de $\mathscr{L}$ et un sous-ensemble de $\mathscr{G}$, l'invariant est donc encore vérifié.

Par ailleurs, $\mathscr{B}$ est libre et $\mathscr{G}$ est génératrice, donc, avec le lemme fondamental, $\operatorname{Card}\mathscr{B} \geqslant \operatorname{Card}\mathscr{G}$. Ainsi $\operatorname{Card}\mathscr{G} - \operatorname{Card}\mathscr{B}$ est un entier naturel. De plus, à chaque étape de la boucle, on ajoute à $\mathscr{B}$ un élément de $\mathscr{G}$ qui n'est pas déjà dans $\operatorname{Vect}\mathscr{B}$, donc pas déjà dans $\mathscr{B}$, donc le cardinal de $\mathscr{B}$ augmente strictement. Donc à chaque tour de boucle $\operatorname{Card}\mathscr{G} - \operatorname{Card}\mathscr{B}$ décroît strictement, donc l'algorithme termine.

À la fin de l'exécution de l'algorithme, $\mathscr{B}$ est une famille libre, et $\mathscr{G} \subset \operatorname{Vect}\mathscr{B}$. Donc $\mathscr{B}$ est une base de E. De plus, on a $\mathscr{L} \subset \mathscr{B} \subset \mathscr{G}$ donc on a bien construit $\mathscr{B}$ en rajoutant à $\mathscr{L}$ des vecteurs de $\mathscr{G}$. □

Exemple 1.3.5.
Compléter $((1,2,0,0),(1,0,1,0))$ en une base de $\mathbb{R}^4$.

Le théorème de la base incomplète a deux corollaires. Le premier est fondamental.

Corollaire 1.3.6.
Tout espace vectoriel de dimension finie admet une base finie.

Démonstration.
Il suffit d'appliquer le théorème de la base incomplète avec la famille vide et une famille génératrice finie. □

Remarque 1.3.7.
Cas particulier : l'espace vectoriel $\{0\}$ a pour base la famille vide. C'est la seule famille libre (donc la seule base) de cet espace vectoriel, puisque toute famille d'au moins un élément contient le vecteur nul et est donc liée.

Il peut sembler étonnant (au premier abord) que le résultat qui suit soit un corollaire du théorème de la base incomplète.

Corollaire 1.3.8.
De toute famille génératrice finie on peut extraire une base.

Démonstration.
Lorsque la famille génératrice considérée est finie, il suffit là encore d'appliquer le théorème de la base incomplète avec la famille vide et une famille génératrice finie : en complétant la famille vide avec des vecteurs de la famille génératrice considérée, on obtient bien une base extraite de la famille génératrice de départ.

Lorsque la famille génératrice considérée est infinie, on peut montrer le résultat en utilisant l'algorithme donné pour la démonstration du théorème de la base incomplète mais un problème se pose, celui de la terminaison. Celle-ci peut être justifiée par le théorème fondamental 1.2.1 : dans un espace de dimension finie, le nombre d'éléments d'une famille libre est majoré par un entier p, où p est par exemple le cardinal d'une famille génératrice finie de E. Or le nombre d'éléments de la famille $\mathscr{B}$ croît strictement à chaque tour de boucle, p moins ce nombre d'éléments est donc un variant de l'algorithme, donc celui-ci termine.
□

1.4 Existence de la dimension

Théorème 1.4.1 (de la dimension)**.**
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Alors toutes les bases ont même nombre d'éléments.

Démonstration.
E étant de dimension finie, il admet une base $\mathscr{B}_1$ finie.
Soit $\mathscr{B}_2$ une seconde base de E. Étant libre, elle a moins d'éléments que $\mathscr{B}_1$.
Mais réciproquement, $\mathscr{B}_2$ est génératrice et $\mathscr{B}_1$ est libre, donc $\mathscr{B}_1$ a moins d'éléments que $\mathscr{B}_2$, ce qui montre que toutes les bases de E ont le même nombre d'éléments que $\mathscr{B}_1$. D'où le résultat. □

Définition 1.4.2.
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. On appelle *dimension du $\mathbb{K}$-espace vectoriel E* et on note $\dim_{\mathbb{K}} E$ (voire $\dim E$ si le contexte permet de savoir clairement ce qu'est $\mathbb{K}$) le nombre d'éléments commun à toutes les bases de E.

On notera parfois $\dim_{\mathbb{K}} E < +\infty$ l'assertion «le $\mathbb{K}$-espace vectoriel E est de dimension finie».

Remarque 1.4.3.
Pour que cette définition ait un sens il est nécessaire et suffisant d'être assuré :
- d'une part que toutes les bases d'un espace vectoriel de dimension finie ont toutes le même nombre d'éléments
- d'autre part que tout espace vectoriel de dimension finie possède bien au moins une base.

Ce qu'on a bien vérifié plus haut.

Remarque 1.4.4.
Cas particulier : $\dim\{0\} = 0$.

Exemple 1.4.5.
Soit $n, p \in \mathbb{N}$.
- $\dim_{\mathbb{K}} \mathbb{K}^n = n$
- $\dim_{\mathbb{R}} \mathbb{C}^n = 2n$
- $\dim_{\mathbb{K}} \mathbb{K}_n[X] = n+1$
- $\dim_{\mathbb{R}} \mathbb{C}_n[X] = 2(n+1)$
- $\dim_{\mathbb{K}} \mathscr{M}_{n,p}(\mathbb{K}) = np$
- $\dim_{\mathbb{R}} \mathscr{M}_{n,p}(\mathbb{C}) = 2np$

Proposition 1.4.6.
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie.
- Toute famille libre de E a au plus $\dim_{\mathbb{K}} E$ éléments.
- Toute famille génératrice de E a au moins $\dim_{\mathbb{K}} E$ éléments.

Démonstration.
C'est une conséquence directe du théorème fondamental 1.2.1. □

Proposition 1.4.7.
1. Toute famille libre maximale d'éléments de E est une base de E.
2. Toute famille génératrice de E minimale est une base de E.

Remarque 1.4.8.
Par famille libre maximale, il faut entendre : «famille libre à laquelle on ne peut rajouter un vecteur sans la rendre liée». Symétriquement, par famille génératrice minimale, il faut entendre «famille génératrice à laquelle on ne peut enlever un vecteur sans lui faire perdre son caractère générateur».

Démonstration.
Le résultat est vrai même si on est dans le cadre d'un espace vectoriel qui n'est pas de dimension finie (auquel cas les familles considérées sont infinies).

1. Soit $\mathscr{F}$ une famille libre maximale. D'après le théorème de la base incomplète, on peut la compléter en une base $\mathscr{B}$. La famille $\mathscr{B}$ est libre. Or la famille $\mathscr{F}$ est maximale, donc $\mathscr{F} = \mathscr{B}$.
2. Soit $\mathscr{G}$ une famille génératrice minimale. D'après le théorème de la base extraite, on peut en extraire une base $\mathscr{B}$. La famille $\mathscr{B}$ est génératrice. Or la famille $\mathscr{G}$ est minimale, donc $\mathscr{G} = \mathscr{B}$.

□

Proposition 1.4.9 (Caractérisation des bases)**.**
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. et soit $\mathscr{F}$ une famille constituée d'exactement $\dim_{\mathbb{K}} E$ vecteurs de E.

Alors les trois propositions suivantes sont équivalentes.

1. $\mathscr{F}$ est une base de E.
2. $\mathscr{F}$ est une famille génératrice de E.
3. $\mathscr{F}$ est une famille libre de E.

Démonstration.
Il est clair que si $\mathscr{F}$ est une base alors elle est libre et génératrice.

Supposons que $\mathscr{F}$ est génératrice. Toute famille génératrice ayant au moins $\dim E$ vecteurs, on ne peut enlever le moindre vecteur à $\mathscr{F}$ sans lui faire perdre son caractère générateur. Donc elle est génératrice minimale, c'est donc une base.

De même, supposons que $\mathscr{F}$ est libre. Toute famille libre ayant au plus $\dim E$ vecteurs, on ne peut ajouter le moindre vecteur à $\mathscr{F}$ sans la rendre liée. Donc elle est libre maximale, donc c'est une base. □

Exemple 1.4.10.
Soient $a, b, c, d \in \mathbb{K}$ deux à deux distincts et

$$\begin{aligned} A &= (X-b)(X-c)(X-d),\\ B &= (X-a)(X-c)(X-d),\\ C &= (X-a)(X-b)(X-d),\\ D &= (X-a)(X-b)(X-c). \end{aligned}$$

Montrer que (A, B, C, D) est une base de $\mathbb{K}_3[X]$.

1.5 Classification en dimension finie

Proposition 1.5.1.
Soit $n \in \mathbb{N}$ et E un $\mathbb{K}$-espace vectoriel de dimension finie n. Alors E est isomorphe à $\mathbb{K}^n$.

Démonstration.
On a $\dim E = n$, donc on peut trouver une base $(e_1, \dots, e_n)$ de E.

Posons alors

$$\begin{array}{rccc} \varphi : & \mathbb{K}^n & \to & E \\ & (\lambda_1, \dots, \lambda_n) & \mapsto & \displaystyle\sum_{k=1}^{n} \lambda_k e_k \end{array}.$$

On peut alors remarquer que

1. φ est une application linéaire,
2. φ est injective (car la famille $(e_1, \dots, e_n)$ est libre),
3. φ est surjective (car la famille $(e_1, \dots, e_n)$ est génératrice de E).

La fonction φ est donc un isomorphisme de $\mathbb{K}^n$ sur E. E et $\mathbb{K}^n$ sont donc isomorphes. □

Proposition 1.5.2.
Soit E et F deux $\mathbb{K}$-espaces vectoriels. Supposons que E est de dimension finie.

Alors E et F sont isomorphes si et seulement si F est aussi de dimension finie et $\dim E = \dim F$.

Démonstration.
Notons tout d'abord n la dimension de E et choisissons $(e_1, \dots, e_n)$ une base de E.

Supposons E et F isomorphes. On peut alors trouver un isomorphisme φ de E sur F. $(\varphi(e_1), \dots, \varphi(e_n))$ est alors une base de F. Donc F est de dimension finie et $\dim F = n = \dim E$.

Réciproquement, supposons que F soit de dimension finie, égale à celle de E. Alors d'après la proposition 1.5.1 E et F sont tous les deux isomorphes à $\mathbb{K}^n$, donc sont isomorphes. □

Corollaire 1.5.3.
En particulier, tout espace vectoriel E est de dimension finie n si et seulement si E est isomorphe à $\mathbb{K}^n$.

Proposition 1.5.4.
Soit E un $\mathbb{K}$-espace vectoriel. Notons L l'ensemble des entiers n tels qu'il existe au moins une famille libre de E à n éléments. Alors

— ou bien E est de dimension finie et alors $L = [\![0, \dim E]\!]$.
— ou bien E n'est pas de dimension finie et alors $L = \mathbb{N}$.

En particulier, E est de dimension finie si et seulement si L est majoré.

Démonstration.
Si E est de dimension finie, on a nécessairement $L \subset [\![0, \dim E]\!]$. Notons alors $\mathscr{B}$ une base. $\mathscr{B}$ est une famille libre à $\dim E$ élément et toute sous-famille de $\mathscr{B}$ est encore libre. Donc $[\![0, \dim E]\!] \subset L$. D'où l'égalité.

Supposons désormais que E n'est pas de dimension finie. Montrons qu'alors L n'est pas majoré.

Par l'absurde supposons que L possède un majorant. Comme L est un ensemble d'entier non vide (il contient 0), il admet alors un maximum M. Soit alors $\mathscr{F}$ une famille libre à M éléments. Si on rajoute un élément à $\mathscr{F}$ on

obtient une famille à $M+1$, or $M+1 \notin L$ donc cette sur-famille ne peut être libre. Donc $\mathscr{F}$ est maximale, donc c'est une base de E, donc E est de dimension finie ce qui est absurde.

L n'est donc pas majoré, donc pour tout entier n il existe $p \in L$ vérifiant $p \geqslant n$. On peut donc trouver une famille libre à p éléments. Toute sous-famille de cette famille en est libre, en prenant une sous-famille arbitraire à n élément, on voit donc qu'on a $n \in L$.

Donc $L \subset \mathbb{N}$, donc $L = \mathbb{N}$. □

1.6 Exemples avancés

Exemple 1.6.1.

• Les solutions d'une équation différentielle linéaire homogène du premier ordre forment un espace vectoriel de dimension 1.

• Les solutions d'une équation différentielle linéaire homogène du second ordre à coefficients constants forment un espace vectoriel de dimension 2.

Proposition 1.6.2.

Soit E et F deux $\mathbb{K}$-espaces vectoriels de dimensions finies.

Alors $E \times F$ est de dimension finie et

$$\dim_{\mathbb{K}}(E \times F) = \dim_{\mathbb{K}} E + \dim_{\mathbb{K}} F.$$

Plus précisément, posons $n = \dim E$ et $p = \dim F$ et choisissons $(e_1, \dots, e_n)$ une base de E et $(f_1, \dots, f_p)$ une base de F. Alors $(b_i)_{i \in [\![1, n+p]\!]}$ est une base de $E \times F$, où

$$\begin{cases} b_i = (e_i, 0_F) & \text{pour } i \in [\![1, n]\!], \\ b_{n+i} = (0_E, f_i) & \text{pour } i \in [\![1, p]\!]. \end{cases}$$

Démonstration.

Un vecteur $z \in E_1 \times E_2$ s'écrit de manière unique $(x, y) = (x, 0_F) + (0_E, y)$. De plus, x (resp. y) s'écrit de manière unique comme combinaison linéaire des e_i (resp. f_i).

L'existence assure l'aspect générateur de la famille. L'unicité assure la iberté. □

Remarque 1.6.3.

Ce résultat assure qu'il existe un isomorphisme entre $E \times F$ et $\mathbb{K}^{n+p}$. Donnons un tel isomorphisme.

— Dans le cas où $E = \mathbb{K}^n$ et $F = \mathbb{K}^p$, on dispose de l'isomorphisme évident

$$\varphi : \begin{array}{ccc} \mathbb{K}^{n+p} & \to & \mathbb{K}^n \times \mathbb{K}^p \\ (x_1, \dots, x_{n+p}) & \mapsto & ((x_1, \dots, x_n), (x_1, \dots, x_p)) \end{array}.$$

— Dans le cas général, il est assez naturel également : on peut utiliser cette remarque et la proposition 1.5.1.

On a $E \cong \mathbb{K}^n$ et $F \cong \mathbb{K}^p$, d'où $E \times F \cong \mathbb{K}^n \times \mathbb{K}^p \cong \mathbb{K}^{n+p}$.

Plus précisément, posons

$$\psi : \begin{array}{ccc} \mathbb{K}^{n+p} & \to & E \times F \\ (x_1, \dots, x_{n+p}) & \mapsto & \left(\displaystyle\sum_{k=1}^{n} x_k e_k, \sum_{k=1}^{p} x_{n+k} f_k \right) \end{array}.$$

Remarquons successivement :

1. ψ est linéaire,
2. ψ est injective (les familles $(e_i)_{i \in [\![1,n]\!]}$ et $(f_i)_{i \in [\![1,p]\!]}$ étant libres),
3. ψ est surjective (les familles $(e_i)_{i \in [\![1,n]\!]}$ et $(f_i)_{i \in [\![1,p]\!]}$ étant génératrice).

Donc $E \times F$ est isomorphe à $\mathbb{K}^{n+p}$. En particulier, d'une part $\dim E \times F = n + p$ et d'autre part l'image de la base canonique de $\mathbb{K}^{n+p}$ est une base de $E \times F$. Or cette image n'est autre que la famille $(b_i)_{i \in [\![1,n+p]\!]}$ donnée dans l'énoncé de la proposition.

Proposition 1.6.4.

Soient E et F deux $\mathbb{K}$-ev de dimension finie. Alors $\mathscr{L}(E, F)$ est un $\mathbb{K}$-ev de dimension finie, et $\dim \mathscr{L}(E, F) = \dim E \times \dim F$.

Démonstration.

Soit $n \in \mathbb{N}$ et $(e_1, \dots, e_n)$ une base de E.

On considère $\varphi : \begin{array}{ccc} \mathscr{L}(E, F) & \to & F^n \\ u & \mapsto & (u(e_k))_{1 \leqslant k \leqslant n} \end{array}$.

Il est aisé de vérifier que φ est linéaire.

En se souvenant que pour toute famille $f_1, \dots, f_n$ de F il existe une unique application linéaire $u \in \mathscr{L}(E, F)$ tel que pour tout $k \in [\![1, n]\!]$, $u(e_k) = f_k$, on constate que φ est bijective.

Par conséquent $\mathscr{L}(E, F)$ et F^n sont isomorphes, ils ont donc même dimension. En utilisant la proposition 1.6.2 et une récurrence sans difficulté, F^n a pour dimension $n \dim F = \dim E \times \dim F$, d'où le résultat. □

2 Sous-espaces vectoriels en dimension finie

2.1 Dimension d'un sous-espace vectoriel

Proposition 2.1.1.
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et F un sous-espace vectoriel de E.

Alors F est de dimension finie et $\dim F \leqslant \dim E$.

De plus $\dim F = \dim E$ si et seulement si $F = E$.

Démonstration.
Toute famille libre de F est une famille libre d'éléments de E et a donc un nombre d'élément majoré par $\dim E$. Donc d'après la proposition 1.5.4, F est de dimension finie, et $\dim F \leqslant \dim E$.

En outre on a trivialement $F = E \Rightarrow \dim F = \dim E$.

Réciproquement, supposons $\dim F = \dim E$ et montrons $F = E$. Alors on peut trouver une base $\mathscr{B}$ de F comportant $\dim E$ éléments. On a $\text{Vect}(\mathscr{B}) = F$. En outre, $\mathscr{B}$ est une famille libre de F donc de E or elle comporte $\dim E$ éléments, donc d'après 1.4.8, c'est une famille génératrice de E, donc $\text{Vect}(\mathscr{B}) = E$. On a donc $F = E$. □

Définition 2.1.2.
Soit E un $\mathbb{K}$-espace vectoriel (non nécessairement de dimension fini). Soit $n \in \mathbb{N}$ et $(x_1, \dots, x_n)$ une famille de n vecteurs. On appelle *rang de la famille* $(x_1, \dots, x_n)$ et on note $\text{rg}(x_1, \dots, x_n)$ la dimension de l'espace vectoriel qu'ils engendrent :

$$\text{rg}(x_1, \dots, x_n) = \dim \text{Vect}(x_1, \dots, x_n).$$

Remarque 2.1.3.
$\text{Vect}(x_1, \dots, x_n)$ étant engendré par la famille de n vecteurs $(x_i)_{i\in[\![1,n]\!]}$, il s'agit d'un espace vectoriel de dimension finie, et sa dimension est au plus n.

Donc le rang de $(x_i)_{i\in[\![1,n]\!]}$ est bien défini et $\text{rg}(x_1, \dots, x_n) \leqslant n$.

De manière directe, ce rang vaut n si et seulement si la famille est libre.

De plus, $(x_i)_{i\in[\![1,n]\!]}$ est génératrice si et seulement si E est de dimension finie et $(x_i)_{i\in[\![1,n]\!]}$ est de rang $\dim E$.

De plus, si E est de dimension finie p, alors $\text{rg}(x_1, \dots, x_n) \leqslant p$.

2.2 Existence de supplémentaires

Théorème 2.2.1 (Existence de supplémentaires)**.**
Soit E un $\mathbb{K}$-espace vectoriel et F un sous-espace vectoriel de E.

Alors F admet un supplémentaire S dans E.

Remarque 2.2.2.
Ce théorème est vrai pour tout espace vectoriel E et non seulement pour ceux de dimension finie. Nous nous contenterons de donner la démonstration dans le cas de la dimension finie, mais la généralisation aux cas infini est relativement immédiate.

Démonstration.
Supposons que E soit de dimension finie. Alors, on peut choisir une base $(b_1, \dots, b_p)$ de F où $p = \dim F$.

Cette base de F est une famille libre de vecteurs de F, donc de E. On peut donc la compléter en une famille $(b_1, \dots, b_n)$ de E, avec $n = \dim E \geqslant p$.

Posons alors $S = \text{Vect}(b_{p+1}, \dots, b_n)$. La famille $(b_{p+1}, \dots, b_n)$, sous-famille d'une base de E, est une famille libre. De plus, elle est génératrice de S, donc c'est une base de S.

On a donc trouvé une base de F et une base de S dont la réunion est une base de E. F et S sont donc supplémentaires. □

 Ne parlez jamais **du** supplémentaire : en effet tout sev admet en fait une infinité de supplémentaires ! Regardez l'exercice suivant pour vous convaincre que dans la démonstration précédente, il existe une infinité de choix pour compléter une famille libre en une base, ce qui mène à une infinité de supplémentaires à un sev, sans rien supposer sur l'espace vectoriel de départ.

Exercice 2.2.3.
Soit F et G deux sous-espaces supplémentaires d'un $\mathbb{K}$-ev E. Soit x un vecteur non nul de F et $(y_1, y_2, \dots, y_p)$ une base de G.

1. Montrer que les vecteurs $x+y_1, x+y_2, \dots, x+y_p$ engendrent un sous-espace supplémentaire

de F, noté G_x.

2. Montrer que si $x, x' \in F$ tel que $x \neq x'$ alors $G_x \neq G_{x'}$. En déduire que F admet une infinité de sous-espaces supplémentaires distincts (sauf dans des cas triviaux : lesquels ?)

Exemple 2.2.4.
Déterminer un supplémentaire de $F = \text{Vect}\left((1,2,0,0),(1,0,0,-3)\right)$ dans $\mathbb{R}^4$.

2.3 Dimension d'une somme de sous-espaces vectoriels

Proposition 2.3.1 (Formule de Grassmann)**.**
Soit E un $\mathbb{K}$-espace vectoriel. Soit F et G deux sous-espaces de dimensions finies de E. Alors $F + G$ est de dimension finie et

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

En particulier

$$\dim(F+G) \leqslant \dim F + \dim G$$

et l'égalité a lieu si et seulement si F et G sont en somme directe.

Démonstration. 1. Montrons tout d'abord le résultat dans le cas où la somme $F + G$ est directe : On peut alors choisir une base de F et une base de G, elles ont respectivement $\dim F$ et $\dim G$ éléments. Leur réunion possède donc $\dim F + \dim G$ éléments et est une base de $F \oplus G$. Donc $F \oplus G$ est de dimension finie et

$$\dim(F \oplus G) = \dim F + \dim G$$

(c'est bien un cas particulier car alors $\dim(F \cap G) = \dim\{0\} = 0$).

2. Montrons maintenant le résultat dans le cas général. Remarquons tout d'abord que $F \cap G$ est un sous-espace vectoriel de F qui est de dimension finie. Donc $F \cap G$ possède un supplémentaire S dans F et $\dim F = \dim(F \cap G) + \dim S$, d'où

$$\dim S = \dim F - \dim(F \cap G)$$

De plus

$$\begin{aligned} S \cap G &= (S \cap F) \cap G \\ &= S \cap (F \cap G) \\ &= \{0\}. \end{aligned}$$

Comme $F \cap G \subset G$, on a $F + G = (S + (F \cap G)) + G = S + G$, donc S et G sont supplémentaires dans $F + G$. Donc $F + G$ est de dimension finie et

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

□

Exercice 2.3.2.
Soit $\mathscr{P}_1$ et $\mathscr{P}_2$ deux plans distincts de $\mathbb{R}^3$ (sev de dimension 2). Montrer que $\mathscr{P}_1 + \mathscr{P}_2 = \mathbb{R}^3$. Que peut-on dire de $\mathscr{P}_1 \cap \mathscr{P}_2$?

Proposition 2.3.3.
Soit E un $\mathbb{K}$-espace vectoriel et F et G deux sous-espaces vectoriels de dimensions finies.

Alors si F et G sont supplémentaires, les trois propositions suivantes sont vraies :

1. $F \cap G = \{0\}$,
2. $F + G = E$,
3. $\dim E < +\infty$ et $\dim F + \dim G = \dim E$.

Réciproquement il suffit que deux de ces propositions soient vraies pour que F et G soient supplémentaires.

Démonstration.
Pour le sens direct, les deux premières propositions sont des conséquences connues, la troisième est la conséquence de la formule de Grassmann.

Pour le sens réciproque, étudions les différentes possibilités :

1. Supposons 1 et 2. Alors F et G sont supplémentaires dans E.
2. Supposons 1 et 3. Alors

$$\begin{aligned} \dim(F+G) &= \dim F + \dim G - \dim(F \cap G) \\ &= \dim F + \dim G \\ &= \dim E. \end{aligned}$$

Or $F + G$ est un sous-espace vectoriel de E donc $F + G = E$. Donc F et G sont supplémentaires.

3. Supposons 2 et 3. Alors

$$\dim E = \dim F + \dim G - \dim(F \cap G)$$
$$\text{et } \dim E = \dim F + \dim G.$$

Ainsi, $\dim(F \cap G) = 0$, et donc $F \cap G = \{0\}$. F et G sont donc supplémentaires.

□

Corollaire 2.3.4.
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et F un sous-espace vectoriel de E. Alors tous les supplémentaires de F ont même dimension : $\dim E - \dim F$.

Démonstration.
E est de dimension finie donc F et tous ses supplémentaires également. D'après ce qui précède tout supplémentaire S de F vérifie $\dim F + \dim S = \dim E$, donc $\dim S = \dim E - \dim F$. □

Exemple 2.3.5.
Regarder tous ces points de vue dans $\mathbb{R}^3$ avec $\mathscr{P} = \left\{ (x,y,z) \in \mathbb{R}^3 \;\middle|\; x - y + z = 0 \right\}$ et $\mathscr{D} = \text{Vect}((1,-1,1))$.

Proposition 2.3.6.
Soit $n \in \mathbb{N}$ et $F_1, \dots, F_n$, n sous-espaces vectoriels de dimension finie. Alors

$$\dim \sum_{k=1}^{n} F_k \leqslant \sum_{k=1}^{n} \dim F_k$$

et on a l'égalité si et seulement si la somme des F_k pour $k = 1, \dots, n$ est directe.

Démonstration.
L'inégalité se déduit directement de la formule de Grassmann par récurrence. Montrons le cas de l'égalité. Notons, pour $n \in \mathbb{N}$, $P(n)$ l'assertion «Toute famille $F_1, \dots, F_n$ de sous-espaces vectoriels de dimension finie vérifiant

$$\dim \sum_{k=1}^{n} F_k = \sum_{k=1}^{n} \dim F_k$$

est en somme directe» et montrons $\forall n \in \mathbb{N} \quad P(n)$.

Montrons $P(2)$ (on pourrait en fait montrer $P(0)$ ou $P(1)$, le plus long est de comprendre ce que dit l'énoncé dans ce cas). Soit F_1 et F_2 deux sous-espaces vectoriels de dimension finie vérifiant $\dim(F_1 + F_2) = \dim F_1 + \dim F_2$. On a déjà vu qu'alors, F_1 et F_2 sont en somme directe.

Montrons $\forall n \in \mathbb{N} \quad P(n) \Rightarrow P(n+1)$.

Soit $n \in \mathbb{N}$. Supposons $P(n)$ et montrons $P(n+1)$. Soit $F_1, \dots, F_{n+1}$ des sous-espaces vectoriels de dimension finie vérifiant

$$\dim \sum_{k=1}^{n+1} F_k = \sum_{k=1}^{n+1} \dim F_k. \qquad \text{(XXI.1)}$$

On a

$$\dim \sum_{k=1}^{n+1} F_k \leqslant \dim \sum_{k=1}^{n} F_k + \dim F_{n+1}$$
$$\text{et } \dim \sum_{k=1}^{n} F_k \leqslant \sum_{k=1}^{n} \dim F_k.$$

Si l'une au moins de ces inégalités était stricte, on ne pourrait avoir l'égalité (XXI.1). On a donc

$$\dim \sum_{k=1}^{n} F_k = \sum_{k=1}^{n} \dim F_k.$$

D'après l'hypothèse de récurrence, les F_k pour $k \in [\![1,n]\!]$ sont en somme directe. De plus

$$\dim \left(\bigoplus_{k=1}^{n} F_k + F_{n+1} \right) = \dim \bigoplus_{k=1}^{n} F_k + \dim F_{n+1},$$

donc $\bigoplus_{k=1}^{n} F_k$ et F_{n+1} sont en somme directe, donc F_1, …, F_{n+1} sont en somme directe.

On a donc $P(n+1)$.

On a donc $\forall n \in \mathbb{N} \quad P(n)$. □

3 Applications linéaires en dimension finie

3.1 Expression d'une application linéaire en dimension finie

Proposition 3.1.1.
Soit E et F deux $\mathbb{K}$-espaces vectoriels de dimensions finies respectives n et p et soit $\varphi \in \mathscr{L}(E,F)$.

Soit alors $\mathscr{E} = (e_1, \dots, e_n)$ une base de E et $\mathscr{F} = (f_1, \dots, f_p)$ une base de F.

Pour $k \in [\![1,n]\!]$, notons $a_{1k}, \dots, a_{pk}$ les coordonnées de $\varphi(e_k)$ dans la base $\mathscr{F}$.

Soit $u \in E$. Notons $x_1, \dots, x_n$ ses coordonnées dans la base $\mathscr{E}$, et $y_1, \dots, y_p$ les coordonnées de $\varphi(u)$ dans la base $\mathscr{F}$.

Alors, pour tout $i \in [\![1,p]\!]$, on a

$$y_i = \sum_{k=1}^{n} a_{ik} x_k.$$

Démonstration.
On a :

$$\begin{aligned}\varphi(u) &= \varphi\left(\sum_{k=1}^{n} x_k e_k\right)\\ &= \sum_{k=1}^{n} x_k \varphi(e_k)\\ &= \sum_{k=1}^{n}\left(x_k \sum_{i=1}^{p} a_{ik} f_i\right)\\ &= \sum_{i=1}^{p}\left(\sum_{k=1}^{n} x_k a_{ik}\right) f_i.\end{aligned}$$

Pour tout $i \in [\![1,p]\!]$, la i^{e} coordonnée de $\varphi(u)$ est donc $\sum_{k=1}^{n} a_{ik}x_k$. □

Remarque 3.1.2.
On sait par ailleurs que pour tout choix d'une famille de scalaires $(a_{ij})_{(i,j)\in[\![1,p]\!]\times[\![1,n]\!]}$, il existe une application $\varphi \in \mathscr{L}(E,F)$ telle que pour tout $k \in [\![1,n]\!]$, les coordonnées de $\varphi(e_k)$ dans la base $\mathscr{F}$ soient $a_{1k},\dots,a_{pk}$.

3.2 Théorème du rang

Proposition 3.2.1.
Soit E et F deux $\mathbb{K}$-espaces vectoriels et $u \in \mathscr{L}(E,F)$.

Supposons qu'il existe un supplémentaire S de $\operatorname{Ker} u$ dans E.

Alors u réalise un isomorphisme de S sur $\operatorname{Im} u$ (ou, si l'on préfère, $u|_S^{\operatorname{Im} u} : S \to \operatorname{Im} u$ est un isomorphisme).

Démonstration.
Notons φ la restriction de u à S au départ et à $\operatorname{Im} u$ à l'arrivée. Il est clair que φ est bien définie et que c'est une application linéaire de S dans $\operatorname{Im} u$.

— Montrons que φ est surjective. Soit $y \in \operatorname{Im} u$. Montrons qu'il existe $s \in S$ vérifiant $\varphi(s) = y$.
Pour cela, remarquons tout d'abord qu'il existe $x \in E$ vérifiant $u(x) = y$. Comme S et $\operatorname{Ker} u$ sont supplémentaires dans E, il existe $s \in S$ et $k \in \operatorname{Ker} u$ vérifiant $x = s + k$. On a alors $u(x) = u(s) + u(k) = u(s) + 0$. Donc $\varphi(s) = u(s) = y$.
φ est donc surjective.

— Montrons que φ est injective. Pour cela, il suffit de montrer $\operatorname{Ker}\varphi \subset \{0\}$.
Soit $k \in \operatorname{Ker}\varphi$. On a $\varphi(k) = 0$, donc $u(k) = 0$, donc $k \in \operatorname{Ker} u$. Or $k \in S$, donc $k \in \operatorname{Ker} u \cap S$. Or $\operatorname{Ker} u$ et S sont supplémentaires, donc $k = 0$.
Ainsi, φ est injective.

Finalement, φ est donc bijective. □

Remarque 3.2.2.
Ce théorème est fondamental pour comprendre comment «fonctionne» une application linéaire. De nombreuses questions (dont des exercices) se résolvent aisément grâce à lui ou grâce aux idées contenues dans sa démonstration.

Théorème 3.2.3 (Théorème du rang)**.**
Soit E et F deux $\mathbb{K}$-espaces vectoriels, avec E de dimension finie et $u \in \mathscr{L}(E,F)$.

Alors $\operatorname{Im} u$ est de dimension finie et

$$\dim \operatorname{Im} u = \dim E - \dim \operatorname{Ker} u.$$

La dimension de $\operatorname{Im} u$ est appelée *rang de l'application linéaire* u et notée $\operatorname{rg} u$.

Démonstration.
On sait que $\operatorname{Ker} u$ possède un supplémentaire S dans E. On a donc $\dim S + \dim \operatorname{Ker} u = \dim E$. De plus S et $\operatorname{Im} u$ sont isomorphes d'après 3.2.1, donc $\dim S = \dim \operatorname{Im} u$. On en déduit immédiatement le résultat. □

Exemple 3.2.4.
• Le rang d'une forme linéaire non nulle vaut 1, celui d'une forme linéaire nulle vaut 0.
• Calculer de deux manières le rang de l'application u :

$$\begin{array}{ccc}\mathbb{R}^3 & \to & \mathbb{R}^3\\ \begin{pmatrix}x\\y\\z\end{pmatrix} & \mapsto & \begin{pmatrix}2x-y\\x+z\\x-y-z\end{pmatrix}\end{array}.$$

Corollaire 3.2.5.
Soient E et F deux $\mathbb{K}$-ev de dimension finie, et $u \in \mathscr{L}(E,F)$. Alors,

(i) u est surjective si et seulement si $\operatorname{rg} u = \dim F$;

(ii) u est injective si et seulement si $\operatorname{rg} u = \dim E$.

Corollaire 3.2.6.
Soit E un $\mathbb{K}$-espace vectoriel et $u \in \mathscr{GL}(E)$. Alors, pour tout sous-espace vectoriel F de E, si F est de dimension finie, $u(F)$ l'est également et $\dim u(F) = \dim F$.

Démonstration.
Notons $u_{|F}$ la restriction de u au départ à F. Autrement dit, notons $u_{|F}$ l'application de F dans E, $x \mapsto u(x)$.

Alors $\operatorname{Im} u_{|F}$ est de dimension finie et $\dim \operatorname{Im} u_{|F} = \dim F - \dim \operatorname{Ker} u_{|F}$. Or $\operatorname{Ker} u_{|F} \subset \operatorname{Ker} u = \{0\}$ et $\operatorname{Im} u_{|F} = u(F)$. On en déduit le résultat. □

Corollaire 3.2.7.
Soient E et F deux $\mathbb{K}$-ev de dimension fine, et $u \in \mathscr{L}(E, F)$.
Alors $\operatorname{rg} u \leqslant \min(\dim E, \dim F)$.
En particulier :
• si $\dim E < \dim F$, u ne peut être surjective ;
• si $\dim E > \dim F$, u ne peut être injective.

Théorème 3.2.8 (d'invariance du rang)**.**
Soit E et F deux espaces vectoriels avec E de dimension finie. Soit $u \in \mathscr{L}(E, F)$. Alors :

(i) soit $v \in \mathscr{GL}(F)$, alors $\operatorname{rg}(v \circ u) = \operatorname{rg} u$;

(ii) soit $w \in \mathscr{GL}(E)$, alors $\operatorname{rg}(u \circ w) = \operatorname{rg} u$.

Démonstration. (i) Il suffit de remarquer $\operatorname{Im}(v \circ u) = v(\operatorname{Im} u)$. E étant de dimension finie, $\operatorname{Im} u$ aussi. Or $v \in \mathscr{GL}(F)$, donc $v(\operatorname{Im} u)$ est de dimension finie égale à celle de $\operatorname{Im} u$, donc à $\operatorname{rg} u$.

(ii) Il suffit de remarquer $\operatorname{Im}(u \circ w) = u(w(E)) = u(E) = \operatorname{Im} u$.

□

Remarque 3.2.9.
Pour le point (i) l'injectivité de v suffit, tandis que pour le point (ii), la surjectivité de w suffit.

Proposition 3.2.10 (Caractérisation des isomorphismes)**.**
Soit E et F deux $\mathbb{K}$-espaces vectoriels de dimension finie. Soit $\varphi \in \mathscr{L}(E, F)$.

Alors si φ est un isomorphisme, on a les trois propriétés suivantes :

1. φ est injective,
2. φ est surjective,
3. $\dim E = \dim F$.

Réciproquement, il suffit que deux de ces trois propositions soient vraies pour que u soit un isomorphisme.

Démonstration.
On a déjà montré que si φ était un isomorphisme les trois propositions étaient vraies. Montrons que si deux sont vraies, alors l'autre l'est aussi.

D'après le théorème du rang, $\dim \operatorname{Im} \varphi = \dim E - \dim \operatorname{Ker} \varphi$.

Par ailleurs, on sait que φ est injective si et seulement si son noyau est de dimension 0 et que φ est surjective si et seulement si $\operatorname{Im} \varphi$ est de dimension $\dim F$.

On peut alors remarquer :
— que si les deux premières propriétés sont vraies, alors φ est un isomorphisme ;
— que si φ est injective et $\dim E = \dim F$, alors $\dim \operatorname{Im} \varphi = \dim E = \dim F$, donc φ est surjective donc bijective.
— que si φ est surjective et $\dim E = \dim F$, alors $\dim \operatorname{Ker} \varphi = \dim E - \dim \operatorname{Im} \varphi = \dim E - \dim F = 0$, donc φ est injective donc bijective.

□

Exemple 3.2.11.
Soit $n \in \mathbb{N}^*$, $x_0, \dots, x_n \in \mathbb{K}$ des scalaires tous distincts et $\varphi : \begin{array}{ccc} \mathbb{K}_n[X] & \to & \mathbb{K}^{n+1} \\ P & \mapsto & (P(x_0), \dots, P(x_n)) \end{array}$.
Alors φ est un isomorphisme.
φ est aisément linéaire, et l'égalité $\dim \mathbb{K}_n[X] = n + 1 = \dim \mathbb{K}^{n+1}$ assure qu'il suffit de montrer l'injectivité OU la surjectivité de φ, mais pas les deux.
Il s'agit de faire le bon choix : l'injectivité se démontre sans peine en utilisant qu'un polynôme de degré au plus n ayant $(n+1)$ racines distinctes ne peut être que le polynôme nul. La surjectivité quant à elle peut se démontrer en utilisant les polynômes de Lagrange, ce qui est nettement moins immédiat.

Le résultat précédent s'exprime simplement dans le cas des endomorphismes.

Corollaire 3.2.12 (Éléments inversibles de $\mathscr{L}(E)$)**.**
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Soit $\varphi \in \mathscr{L}(E)$.

Alors les trois propositions suivantes sont équivalentes :

1. φ est injective,
2. φ est surjective,
3. φ est bijective.

Corollaire 3.2.13.
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Soit φ un élément de l'anneau $(\mathscr{L}(E), +, \circ)$. Alors les trois propositions suivantes sont équivalentes :

1. φ est inversible à gauche,
2. φ est inversible à droite,
3. φ est inversible.

 L'hypothèse de dimension finie est indispensable.
Considérer par exemple les applications

$$\begin{array}{rccc} \varphi : & \mathbb{R}^{\mathbb{N}} & \to & \mathbb{R}^{\mathbb{N}} \\ & (u_n)_{n\in\mathbb{N}} & \mapsto & (u_{n+1})_{n\in\mathbb{N}} \\ \psi : & \mathbb{R}^{\mathbb{N}} & \to & \mathbb{R}^{\mathbb{N}} \\ & (u_n)_{n\in\mathbb{N}} & \mapsto & (u_{p(n)})_{n\in\mathbb{N}} \end{array}$$

où $p : \mathbb{N} \to \mathbb{N}$

$$n \mapsto \begin{cases} 0 & \text{si} \quad n = 0, \\ n-1 & \text{si} \quad n \neq 0. \end{cases}$$

Remarque 3.2.14.
De la même manière que le corollaire 3.2.13, on peut montrer que si E et F sont deux $\mathbb{K}$-espaces vectoriels de dimension finie tels que $\dim E = \dim F$, et si φ est un élément de $\mathscr{L}(E, F)$, alors les trois propositions suivantes sont équivalentes :

1. il existe $\psi \in \mathscr{L}(F, E)$ telle que $\psi \circ \varphi = \mathrm{Id}_E$,
2. il existe $\chi \in \mathscr{L}(F, E)$ telle que $\varphi \circ \chi = \mathrm{Id}_F$,
3. φ est bijective.

4 Formes linéaires et hyperplans

Donnons une première définition générale :

Définition 4.0.1.
Soit E un $\mathbb{K}$-espace vectoriel. On appelle *droite vectorielle* de E tout sous-espace vectoriel de dimension 1 et *hyperplan* de E tout sous-espace vectoriel de E admettant une droite pour supplémentaire.

Dans le cas des espaces vectoriels de dimension finie, cette définition se récrit :

Définition 4.0.2.
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n. On appelle *hyperplan* de E tout sous-espace vectoriel de dimension $n-1$.

Exemple 4.0.3.
• Les droites vectorielles sont les hyperplans de $\mathbb{R}^2$.
• Les plans vectoriels sont les hyperplans de $\mathbb{R}^3$.
• L'espace est un hyperplan de l'espace-temps.
• $\mathbb{K}_n[X]$ est un hyperplan de $\mathbb{K}_{n+1}[X]$.
• $\mathbb{K}^n$ peut être vu comme un hyperplan de $\mathbb{K}^{n+1}$, si l'on considère que $\mathbb{K}^n$ est isomorphe à $\mathbb{K}^n \times \{0\}$, qui est un hyperplan de $\mathbb{K}^{n+1}$.

Proposition 4.0.4.
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et H un hyperplan de E. Alors toute droite vectorielle D non contenue dans H est supplémentaire de H dans E.

Démonstration.
Soit D une droite vectorielle non contenue dans H. Alors $D \cap H$ est strictement inclus dans D, donc $\dim D \cap H < \dim D = 1$, donc $D \cap H = \{0\}$, donc D et H sont en somme directe. De plus $\dim D + \dim H = \dim E$. Donc D et H sont supplémentaires. □

Proposition 4.0.5.
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et $F \subset E$.

Alors F est un hyperplan de E si et seulement si c'est le noyau d'une forme linéaire non nulle.

Démonstration.
Notons n la dimension de E.

Supposons que F est un hyperplan. Soit alors S un supplémentaire de F dans E. F est de dimension $n-1$ donc S est une droite vectorielle. Soit e un vecteur directeur de S. Tout élément de x de E s'écrit donc de façon unique sous la forme $f + \lambda e$, où $f \in F$ et $\lambda \in \mathbb{K}$.

Notons $u(x)$ ce scalaire λ. u est une application linéaire de E dans F. Elle est non nulle car $u(e) \neq 0$.

De plus, pour tout $x \in E$, on a $x \in \operatorname{Ker} u$ si et seulement si x s'écrit sous la forme $f + 0e$, où $f \in \mathbb{F}$. Donc $\operatorname{Ker} u = F$.

Réciproquement soit u une forme linéaire non nulle. Alors $\operatorname{Im} u = \mathbb{K}$, donc $\dim \operatorname{Im} u = 1$, donc d'après le théorème du rang, $\dim \ker u = \dim E - 1$. Donc $\ker u$ est un hyperplan. □

Remarque 4.0.6.
Soit H un hyperplan d'un espace vectoriel E et soit e un vecteur non nul n'appartenant pas à H. Alors pour toute forme linéaire u de noyau H, on a $u = \lambda\varphi$, où $\lambda = u(e)$ et φ est l'application associant α à tout vecteur de la forme $h + \alpha e$.

Démonstration.
Posons $D = \operatorname{Vect}(e)$. L'application φ est bien définie car $E = H \oplus D$ et elle est linéaire. Soit $u \in \mathscr{L}(E, \mathbb{K})$ vérifiant $\operatorname{Ker} u = H$. Alors soit $x \in E$. x s'écrit sous la forme $h + \alpha e$ et on a $u(x) = u(h) + \alpha u(e) = 0 + \alpha\lambda = \lambda\varphi(x)$.

Donc $\forall x \in E u(x) = \lambda\varphi(x)$. Donc $u = \lambda\varphi$. De plus, $\lambda \neq 0$ (sinon $\ker u = E \neq H$). □

Proposition 4.0.7.
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n. Soit $(e_1, \ldots, e_n)$ une base de E.

Soit H un hyperplan de E. Alors les éléments de H sont les points dont les coordonnées $(x_1, \ldots, x_n)$ sont les solutions d'une équation de la forme $a_1x_1 + \ldots + a_nx_n = 0$, où $a_1, \ldots, a_n$ sont des scalaires fixés non tous nuls.

Réciproquement, toute équation de cette forme est celle d'un hyperplan.

De plus pour un même hyperplan, les coefficients $a_1, \ldots, a_n$ sont uniques à multiplication près par un scalaire non nul.

Démonstration.
Soit H un hyperplan de E. Alors d'après 4.0.19, il existe une application linéaire φ dont H est le noyau. Or d'après 3.1.1, pour tout élément $x \in E$, la valeur de $\varphi(x)$ (qui est la coordonnée de $\varphi(x)$ dans la base canonique de $\mathbb{K}$) s'exprime sous la forme $a_1x_1 + \ldots + a_nx_n$. $\operatorname{Ker}\varphi$ est donc l'ensemble des points dont les coordonnées vérifient $a_1x_1 + \ldots a_nx_n = 0$.

Réciproquement, pour tout n-uplet de scalaires $(a_1, \ldots, a_n)$ non tous nuls, l'application φ qui à tout vecteur de E de coordonnées $(x_1, \ldots, x_n)$ associe $a_1x_1 + \ldots + a_nx_n$ est une forme linéaire, à l'évidence non nulle (considérer le vecteur de E dont toutes les coordonnées sont nulles, exceptées la i^{e}, où $i \in [\![1, n]\!]$ est tel que $a_i \neq 0$), les points dont les coordonnées sont solutions de l'équation $a_1x_1 + \ldots + a_nx_n = 0$ sont donc les éléments du noyau de $\operatorname{Ker}\varphi$, qui est un hyperplan.

De plus d'après la remarque précédente, deux formes linéaires ayant le même noyau sont proportionnelles, d'où la remarque sur l'unicité à un facteur multiplicatif près. □

Lemme 4.0.8.
Soit H un hyperplan d'un espace vectoriel E de dimension finie n. Soit F un sous-espace vectoriel de E de dimension p. Alors $H \cap F$ est de dimension $p-1$ ou p.

Démonstration.
Si $H \cap F = F$, le résultat est évident.

Sinon, considérons un supplémentaire S de $H \cap F$ dans F. $H \cap F \neq F$, donc $\dim S \geqslant 1$. On a $S \subset F$, donc $S \cap H = (S \cap F) \cap H = S \cap (H \cap F) = \{ 0 \}$. Donc S et H sont en somme directe, donc $\dim H \oplus S \geqslant n - 1 + 1 = n$. Donc $H \oplus S = E$, donc $\dim S = n - (n-1) = 1$, donc $\dim H \cap F = \dim F - \dim S = p - 1$. □

Proposition 4.0.9.
Soit $H_1, \ldots, H_m$ m hyperplans d'un espace vectoriel E de dimension finie n. Alors $\bigcap_{k=1}^{m} H_k$ est de dimension au moins $n - m$.

Réciproquement soit F un sous-espace vectoriel de dimension $n - m$ d'un espace vectoriel de E de dimension finie n, où $m \in \mathbb{N}$. Alors F est l'intersection de m hyperplans.

Démonstration.
Le premier point se démontre par une récurrence immédiate en utilisant le lemme 4.0.22.

Pour la réciproque, considérons un supplémentaire S de F dans E. Alors $\dim S = m$. Choisissons une base $(e_1, \dots, e_m)$ de S. Notons p la projection sur S parallèlement à F. Pour tout $k \in [\![1, m]\!]$, notons f_k la forme linéaire qui à $x \in E$ associe la k^{e} coordonnée de $p(x)$.

Soit $x \in E$. On a $x \in F$ si et seulement si $x \in \operatorname{Ker} p$ si et seulement si pour tout $k \in [\![1, m]\!]$, $f_k(x) = 0$ si et seulement si $x \in \bigcap_{k=1}^{m} \operatorname{Ker} f_k$. Donc on a

$$F = \bigcap_{k=1}^{m} \operatorname{Ker} f_k$$

Donc F est l'intersection de m hyperplans. □

Chapitre XXII

Probabilités sur un univers fini

La théorie des probabilités cherche à modéliser des phénomènes faisant intervenir le hasard. Puisqu'il s'agit d'une modélisation, il conviendra, pour chaque définition que nous allons donner, d'une part d'apprendre sa définition mathématique et d'autre part de comprendre en quoi cette définition modélise un phénomène aléatoire.

1 Événements, probabilités

1.1 Expérience aléatoire et univers

a Introduction

On parlera d'expérience aléatoire pour modéliser un processus dont le résultat est incertain. Exemple : tirage au sort d'une boule dans une urne, tirage à pile ou face avec une pièce de monnaie, lancer d'un ou plusieurs dés, choix au hasard d'une personne dans la population française, tirage de trois cartes à jouer au hasard dans un paquet, etc.

On appellera généralement *univers des possibles* ou *univers*, l'ensemble des résultats possibles d'une expérience aléatoire. Cet univers dépend bien évidemment de la modélisation choisie : par exemple pour un tirage à pile ou face, on peut modéliser l'univers comme étant l'ensemble $\{ \text{pile}, \text{face} \}$ ou comme $\{ \text{pile}, \text{face}, \text{tranche} \}$.

Il arrive parfois qu'on s'intéresse à une expérience aléatoire donnant plusieurs résultats. Par exemple, si on tire une carte à jouer dans un jeu, on peut s'intéresser à la couleur de la carte, auquel cas on considérera l'univers $\Omega_1 = \{ \heartsuit, \diamondsuit, \spadesuit, \clubsuit \}$ ou à sa valeur, auquel cas on s'intéressera à l'univers $\Omega_2 = \{ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \text{Valet}, \text{Dame}, \text{Roi} \}$. Si on s'intéresse aux deux simultanément, on prendra plutôt comme univers $\Omega = \Omega_1 \times \Omega_2$.

De manière générale, on prendra pour univers un ensemble nous permettant de représenter simultanément tous les résultats qui nous intéresseront.

Sur l'exemple précédent, on peut s'intéresser à l'*événement* qui consiste à tirer une carte rouge et de valeur trois ou quatre. Cet événement est modélisé comme une partie de Ω, en l'espèce la partie $\{ (\heartsuit, 3), (\heartsuit, 4), (\diamondsuit, 3), (\diamondsuit, 4) \}$.

Dans toute la suite de ce chapitre, on utilisera souvent des expériences imagées : tirages de dés, de boules dans une urne *etc.* On adoptera les conventions suivantes, sauf mention du contraire :

- les dés sont équilibrés, à six faces ;
- les urnes sont opaques, les boules sont indiscernables au toucher et, si une urne contient n boules, ces dernières sont numérotées de 1 à n ;
- les jeux de cartes sont parfaitement mélangés.

b Univers, événements

Définition 1.1.1 (Univers)**.**
On appelle *univers* un ensemble non vide Ω.

Cette année, on se limitera au cas où Ω est fini.

Dans ce cas [1], on appelle *événement* toute partie de l'univers, c'est-à-dire tout élément de $\mathscr{P}(\Omega)$ et on appelle *événement élémentaire* ou *éventualité* les événements singletons, c'est-à-dire de la forme $\{ \omega \}$, pour $\omega \in \Omega$ (selon le contexte, le terme événement élémentaire peut parfois désigner les éléments de Ω et non les singletons).

Un événement est dit *impossible* s'il désigne la partie vide ($\varnothing$) et *certain* s'il désigne la partie pleine (Ω).

Étant donnés deux événements A et B, on définit

— l'*événement contraire de* A : $\Omega \setminus A$, noté $\bar{A}$.
— l'événement «A et B» (conjonction de A et B) : $A \cap B$.
— l'événement «A ou B» (disjonction de A et B) : $A \cup B$.

On dit que A et B sont incompatibles si $A \cap B = \varnothing$, autrement dit si leur conjonction est impossible.

On dit que des événements $A_1, \ldots, A_n$ sont *mutuellement incompatibles* si leur conjonction est impossible. On dit qu'ils sont *deux à deux incompatibles* si pour tout i et j, $i \neq j$ implique A_i et A_j incompatibles. Dans ce dernier cas, on dit que leur union $A_1 \cup \ldots \cup A_n$ est une *union disjointe*.

Remarque 1.1.2.
L'incompatibilité deux à deux de n événements (avec $n \geqslant 2$) implique l'incompatibilité mutuelle mais la réciproque est fausse. Considérons par exemple $\Omega = \{ 1, 2, 3, 4, 5, 6 \}$ l'univers des résultats d'un tirage d'un dé à six faces. Alors les trois événements «le résultat est pair», «le résultat est divisible par 3» et «le résultat est un nombre premier» ne sont pas deux à deux incompatibles mais sont mutuellement incompatibles.

Remarque 1.1.3.
Dans le cas où Ω n'est pas fini ni dénombrable, modéliser les événements par les éléments de $\mathscr{P}(\Omega)$ pose des problèmes techniques. Pour les résoudre, on impose aux événements d'être des élément d'un sous-ensemble $\mathscr{T}$ de $\mathscr{P}(\Omega)$, cet ensemble $\mathscr{T}$ devant former ce qu'on appelle une *tribu*. Dans le cas fini ou dénombrable, $\mathscr{P}(\Omega)$ est une tribu.

Exemple 1.1.4.
Pour modéliser les tirages successifs, sans remise, de deux boules dans une urne contenant n boules numérotées de 1 à n, on peut utiliser l'univers $[\![1, n]\!]^2$.

Ici, l'événement $\{(i, k)\}$ modélise « on tire d'abord la boule i, puis la boule k » Les événements du type $\{(i, i)\}$ n'ont pas d'interprétation dans notre modèle. Ce n'est pas grave : on leur attribuera plus tard une probabilité nulle.

c Système complet d'événements

Définition 1.1.5.
On dit qu'une famille $(A_i)_{i\in I}$ d'événements dans un univers Ω est un *système complet d'événements* si ces événements sont deux à deux incompatibles et que leur union (disjointe) est certaine : $\Omega = \bigsqcup_{i\in I} A_i$.

Exemple 1.1.6.
Si A est un événement, $\left\{A, \overline{A}\right\}$ est un système complet d'événements.

1. Dans le cas infini, la définition est un peu plus subtile. La cas dénombrable sera traité en seconde année.

Exemple 1.1.7.
Pour l'exemple du tirage d'une carte donné plus haut, la famille (A_1, A_2, A_3), où A_1 est l'événement «la carte tirée est rouge», A_2 l'événement «la carte tirée est un sept noir» et A_3 l'événement «la carte tirée est noire mais n'est pas un sept» constitue un système complet d'événements.

Remarque 1.1.8.
La notion de système complet d'événements est très proche de celle de partition. Les différences sont les suivantes :

1. un système complet d'événements est une famille de parties de Ω alors qu'une partition est un ensemble de parties de Ω ;
2. la notion de système complet d'événements ne s'utilise qu'en probabilités ;
3. rien dans la définition de système complet d'événements n'impose aux A_i d'être non vides.

Proposition 1.1.9.
Soit $(A_i)_{i\in I}$ un système complet d'événements sur un univers Ω, soit B un événement. Alors, B peut s'écrire comme l'union suivante :

$$B = \bigcup_{i\in I} B \cap A_i$$

et cette union est une union disjointe (les $(B \cap A_i)_{i\in I}$ sont deux à deux incompatibles).

Démonstration.
Montrons tout d'abord que B est inclus dans cette réunion. Soit $b \in B$. On a $b \in \Omega$ et la réunion des A_i pour $i \in I$ est égale à Ω, donc il existe un $i_0 \in I$ vérifiant $b \in A_{i_0}$. On a alors $b \in B \cap A_{i_0}$. On a donc

$$b \in \bigcup_{i\in I} B \cap A_i$$

Ce qui montre cette première inclusion.

L'inclusion réciproque est immédiate : pour tout $i \in I$, on a $B \cap A_i \subset B$, donc

$$\bigcup_{i\in I} B \cap A_i \subset B$$

On a donc l'égalité voulue.

On peut aussi montrer cela par calcul sur les ensembles : par la relation de De Morgan,

$$B = B \cap \Omega = B \cap \bigcup_{i\in I} A_i = \bigcup_{i\in I} B \cap A_i.$$

Le fait que l'union soit disjointe est immédiat : soit $(i,j) \in [\![1,n]\!]^2$ vérifiant $i \neq j$. Alors $(B \cap A_i) \cap (B \cap A_j) \subset A_i \cap A_j = \varnothing$. □

1.2 Espaces probabilisés finis

a Définition

À tout événement, on veut associer sa *probabilité*, qui modélise la « probabilité de réalisation » de cet événement lors de la réalisation de cette expérience aléatoire. Mais que veut dire cette phrase ? On peut le voir comme la fréquence de la réalisation de cet événement au bout d'un « grand » nombre de répétitions « indépendantes » de cette expérience. La loi des grands nombres (sa version faible dans le cas dénombrable sera vue en seconde année) justifie la consistance de la définition suivante avec son interprétation concrète.

Définition 1.2.1.
Une *probabilité* (ou *mesure de probabilité*) sur un univers fini Ω est une application P de $\mathscr{P}(\Omega)$ dans $\mathbb{R}$ vérifiant les trois propriétés suivantes :

1. Pour tout événement A, $0 \leqslant P(A) \leqslant 1$.
2. $P(\Omega) = 1$.
3. Pour tout couple (A,B) d'événements, si A et B sont incompatibles alors $P(A \sqcup B) = P(A) + P(B)$.

Un *espace probabilisé fini* est un couple (Ω, P), où Ω est un univers fini et P une probabilité.

Pour tout événement A d'un espace probabilisé (Ω, P), la valeur $P(A)$ est appelée probabilité de l'événement A.

On dit qu'un événement A est *presque sûr* (ou *quasi certain*) si $P(A) = 1$ et est *négligeable* (ou *quasi impossible*) si $P(A) = 0$.

Remarque 1.2.2. 1. Dans le cas où l'univers est infini, il faut adapter un peu la définition : l'ensemble de départ de P est alors la tribu des événements et on donne au troisième axiome une forme plus générale. Comme on ne verra cette année que le cas fini, on s'autorisera à omettre la précision « fini » quand on parlera d'espaces probabilisés.

2. L'intérêt de la notion de quasi certitude ou quasi impossibilité n'est pas évidente quand il s'agit de probabilités sur un univers fini. Donnons un exemple intuitif dans le cas d'un univers infini : si on tire un réel au hasard dans $[0,1]$, il n'est pas impossible d'obtenir exactement le réel $1/3$ mais la probabilité de cet événement est nulle (la probabilité d'obtenir un réel situé dans un intervalle donné est proportionnelle au diamètre de cet intervalle). C'est donc un événement quasi-impossible mais non impossible.

3. Il est important de retenir que la notion de quasi impossibilité ne veut pas dire «probabilité faible». Un physicien dirait qu'un événement de probabilité 10^{-100} est impossible (le nombre d'atomes dans l'univers est de l'ordre de 10^{80}) mais pour un mathématicien, un tel événement n'est même pas un événement quasi impossible.

Définition 1.2.3.
Un prédicat défini sur Ω vrai sur un événement de probabilité 1 sera dit « presque-sûr ».

Exemple 1.2.4.
Reprenons l'exemple **??** : on tire successivement, sans remise, deux boules dans une urne contenant $n \geqslant 2$ boules numérotées de 1 à n. Il est pratique de considérer comme univers $\Omega = [\![1,n]\!]^2$. On prend alors une probabilité P telle que l'événement $\{\, (i,i) \mid 1 \leqslant i \leqslant n \,\}$ est négligeable.

Sur cet univers, presque-sûrement on aura « $i \neq k$ » pour $1 \leqslant i,k \leqslant n$.

b Probabilité uniforme

Définition 1.2.5 (probabilité uniforme)**.**
Soit Ω un univers fini. L'application

$$\begin{array}{rccc} P: & \mathscr{P}(\Omega) & \to & \mathbb{R} \\ & A & \mapsto & \frac{\operatorname{Card} A}{\operatorname{Card} \Omega} \end{array}$$

est une probabilité, appelée *probabilité uniforme*.

Démonstration.
Remarquons que Ω est un ensemble fini, donc ses parties sont finies également donc ont des cardinaux entiers. Comme de plus $\Omega \neq \varnothing$, son cardinal est non nul, donc on peut diviser par $\operatorname{Card}\Omega$. P est donc bien définie sur $\mathscr{P}(\Omega)$.

Pour montrer que P est une probabilité, il suffit de vérifier les trois propriétés de la définition :

1. Soit $A \in \mathscr{P}(\Omega)$, alors $0 \leqslant \operatorname{Card} A \leqslant \operatorname{Card}(\Omega)$ donc $0 \leqslant P(A) \leqslant 1$.
2. On a bien $P(\Omega) = 1$.
3. Soit (A, B) deux événements incompatibles. Alors $A \cap B = \varnothing$ donc $\operatorname{Card}(A \cup B) = \operatorname{Card} A + \operatorname{Card} B$, donc $P(A \cup B) = P(A) + P(B)$.

□

Remarque 1.2.6.
Cette probabilité modélise souvent l'expression « au hasard », prise dans son acceptation courante (tirer une boule au hasard dans une urne, etc.).

Exemple 1.2.7.
Continuons l'exemple **??** : la probabilité que l'on considérera sur Ω n'est pas uniforme, mais sa restriction à $\{\,(i,k) \mid 1 \leqslant i,k \leqslant n \text{ et } i \neq k\,\}$ le sera.

c Propriétés élémentaires

Proposition 1.2.8.
Soit (Ω, P) un espace probabilisé. Soit A et B deux événements. Alors on a

1. $P(\varnothing) = 0$;
2. $A \subset B \Rightarrow P(A) \leqslant P(B)$;
3. $P(A \cup B) = P(A) + P(B) - P(A \cap B)$;
4. $P(A) = 1 - P(\bar{A})$.

Démonstration.
1. $\varnothing = \varnothing \sqcup \varnothing$ donc $P(\varnothing) = P(\varnothing) + P(\varnothing) = 0$, d'où le résultat.
2. Supposons $A \subset B$. Alors $B = A \cup (B \setminus A)$. De plus, A et $B \setminus A$ sont incompatibles, donc $P(B) = P(A) + P(B \setminus A) \geqslant P(A)$.
3. On a $A \cup B = A \cup (B \setminus A \cap B)$ et $B \setminus A \cap B$ et A sont incompatibles, donc $P(A \cup B) = P(A) + P(B \setminus (A \cap B))$. Or $B = (B \setminus (A \cap B)) \cup (A \cap B)$ et $B \setminus (A \cap B)$ et $A \cap B$ sont incompatibles, donc $P(B) = P(B \setminus (A \cap B)) + P(A \cap B)$. On en déduit le résultat.
4. $\Omega = A \cup \bar{A}$ et A et $\bar{A}$ sont incompatibles, donc $1 = P(\Omega) = P(A) + P(\bar{A})$ d'où le résultat.

□

Remarque 1.2.9.
La formule donnée en **??** se généralise en la formule du *crible de Poincaré*, comme pour le cardinal : pour des événements $A_1, \ldots, A_n$:

$$P\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{k=1}^{n} (-1)^k \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} P(A_{i_1} \cap \cdots \cap A_{i_k}).$$

Proposition 1.2.10.
Soit (Ω, P) un espace probabilisé. Soit $n \in \mathbb{N}$ et $A_1, \ldots, A_n$ des événements *deux à deux incompatibles*. Alors la probabilité de leur union (appelée union disjointe) est la somme de leurs probabilités :

$$P\left(\bigsqcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} P(A_i).$$

Démonstration.
Pour $k \in [\![0, n]\!]$, notons $E(k)$ la proposition

$$P\left(\bigsqcup_{i=1}^{k} A_i\right) = \sum_{i=1}^{k} P(A_i)$$

Montrons $\forall k \in [\![0,n]\!] \quad E(k)$ par récurrence :

— On a $P\left(\bigsqcup_{i=1}^{0} A_i\right) = P(\varnothing) = 0 = \sum_{i=1}^{0} P(A_i)$.

— Montrons $\forall k \in [\![0, n-1]\!] \quad P(k) \Rightarrow P(k+1)$. Soit $k \in [\![0, n-1]\!]$ vérifiant $P(k)$. Alors, comme les événements A_i pour $i \in [\![1,n]\!]$ sont deux à deux incompatibles, on a $\forall i \in 1,k \quad A_i \cap A_{k+1} = \varnothing$. Donc

$$\left(\bigsqcup_{i=1}^{k} A_i\right) \cap A_{k+1} = \varnothing$$

On a donc

$$P\left(\left(\bigsqcup_{i=1}^{k} A_i\right) \sqcup A_{k+1}\right) = P\left(\bigsqcup_{i=1}^{k} A_i\right) + P(A_{k+1})$$

Or on a $E(k)$, donc

$$P\left(\bigsqcup_{i=1}^{k+1} A_i\right) = \left(\sum_{i=1}^{k} P(A_i)\right) + P(A_{k+1})$$

On a donc $E(k+1)$.
On a donc $\forall k \in [\![0, n]\!] \quad E(k)$. □

Proposition 1.2.11 (Formule des probabilités totales, première forme)**.**
Soit (Ω, P) un espace probabilisé, $n \in \mathbb{N}^*$, $(A_i)_{i\in[\![1,n]\!]}$ un système complet d'événements et B un événement. Alors

$$P(B) = \sum_{i=1}^{n} P(A_i \cap B).$$

Démonstration.
D'après la proposition 1.1.9, on a

$$B = \bigcup_{i=1}^{n} A_i \cap B.$$

et cette union est une union disjointe. Donc d'après la proposition 1.2.7, on a le résultat. □

d Détermination par les images des singletons

Dans cette partie, on considère un univers fini $\Omega = \{\omega_1, \ldots, \omega_n\}$ de cardinal $n \in \mathbb{N}^*$.

Proposition 1.2.12.
Soit P une probabilité sur Ω. Alors pour tout événement A, on a

$$P(A) = \sum_{\omega\in A} P(\{\,\omega\,\}). \qquad \text{(XXII.1)}$$

Démonstration.
Il suffit de remarquer que pour tout événement A, A est l'union disjointe des $\{\,\omega\,\}$ pour $\omega \in A$ et d'utiliser la proposition 1.2.7. □

Corollaire 1.2.13.
En particulier, des réels $p_1, \ldots, p_n$ étant donnés, il existe au plus une probabilité sur Ω vérifiant $\forall i \in [\![1, n]\!] \quad P(\{\,\omega_i\,\}) = p_i$.

Démonstration.
En effet, considérons deux probabilités P_1 et P_2 vérifiant cette condition. Alors, d'après la proposition, pour tout événement A, $P_1(A) = P_2(A)$. □

Remarque 1.2.14.
Remarquons que pour qu'une probabilité vérifiant cette condition existe, il est nécessaire que les p_i soit tous positifs ou nuls (car ce sont des probabilités) et que leur somme soit égale à 1 (car d'après l'égalité (XXII.1) c'est la probabilité de Ω). La proposition suivante montre que ces deux conditions sont suffisantes.

Proposition 1.2.15.
Soit $p_1, \ldots, p_n$, n réels positifs ou nuls de somme égale à 1. Alors il existe une (unique) fonction P de probabilité sur Ω telle que pour tout $i \in [\![1, n]\!]$, on a $P(\{\,\omega_i\,\}) = p_i$.

Démonstration.
On a déjà vu l'unicité sous réserve d'existence. Montrons l'existence. Notons P l'application de $\mathscr{P}(\Omega)$ dans $\mathbb{R}$ qui à tout événement A associe

$$P(A) = \sum_{i\in[\![1,n]\!],\omega_i\in A} p_i$$

Il est clair que pour tout $i \in [\![1, n]\!]$, on a $P(\{\,\omega_i\,\}) = p_i$. Montrons que P est une probabilité sur Ω.

1. Soit A un événement. Les p_i pour $i \in [\![1, n]\!]$ étant positifs ou nuls, on a pour tout A, $P(A) \geqslant 0$. De plus, $P(A)$ est inférieur ou égal à la somme des p_i, qui vaut 1, donc $0 \leqslant P(A) \leqslant 1$.
2. On a $P(\Omega) = \sum_{i=1}^{n} p_i = 1$.
3. Pour tout couple (A, B) d'événements incompatibles, comme $\{\, i \in [\![1, n]\!] \mid \omega_i \in A \cup B \,\}$ et la réunion disjointe de $\{\, i \in [\![1, n]\!] \mid \omega_i \in A \,\}$ et

$\{ i \in [\![1,n]\!] \mid \omega_i \in B \}$, on a

$$\begin{aligned} P(A \cup B) &= \sum_{i \in [\![1,n]\!], \omega_i \in A \cup B} p_i \\ &= \sum_{i \in [\![1,n]\!], \omega_i \in A} p_i + \sum_{i \in [\![1,n]\!], \omega_i \in B} p_i \\ &= P(A) + P(B). \end{aligned}$$

Ainsi, P est donc bien une probabilité. □

Exemple 1.2.16.
Nous pouvons maintenant définir des mesures de probabilités de la manière suivante : « la probabilité P est définie sur $[\![0,5]\!]$ par

k	0	1	2	3	4	5
$P(\{k\})$	1/4	0	1/2	1/12	1/12	1/12

».

Exemple 1.2.17.
Étant donné des points $A_1, \dots, A_n$ dans un ensemble (fini) Ω, on définit la (mesure de) probabilité empirique par rapport à $A_1, \dots, A_n$ par

$$\forall x \in \Omega,\ P_n(\{x\}) = \frac{1}{n} \mathrm{Card} \{ i \in [\![1,n]\!] \mid A_i = x \}.$$

1.3 Probabilités conditionnelles

a Définition

Le résultat d'une expérience aléatoire dépend parfois du résultat d'une autre. Par exemple, en prenant pour univers l'ensemble des jours de l'année 2017 muni de la probabilité uniforme P, si on appelle A l'événement «j'attrape un rhume aujourd'hui» et B l'événement «il fait un temps froid et humide aujourd'hui», on aimerait pouvoir exprimer que lorsque B est réalisé, A a une plus grande probabilité d'être réalisé.

Pour cela, on peut restreindre notre univers Ω à l'ensemble des jours où B est réalisé et regarder quelle est la probabilité de l'événement «attraper un rhume» dans cet univers restreint. On appellera cette probabilité la probabilité de A sachant B.

Dans l'univers Ω, l'événement A est l'ensemble des jours où j'attrape un rhume, B est l'ensemble des jours froids et humides. Notre univers restreint est B et l'événement «j'attrape un rhume» dans cet univers est l'ensemble $A \cap B$. Sa probabilité, si on le munit de la probabilité uniforme est $\mathrm{Card}(A \cap B)/\mathrm{Card}\, B = P(A \cap B)/P(B)$.

Cet exemple nous conduit à la définition suivante.

Définition 1.3.1 (Probabilité conditionnelle)**.**
Soit (Ω, P) un espace probabilisé et A et B deux événements, avec B de probabilité non nulle. On appelle probabilité de A sachant B, et on note $P_B(A)$ ou $P(A|B)$, le réel $\dfrac{P(A \cap B)}{P(B)}$.

Remarque 1.3.2.
Même si l'exemple donné concernait une probabilité uniforme, la définition donnée s'applique à toute probabilité.

Proposition 1.3.3.
Sous les hypothèses de la définition ci-dessus, l'application $P_B : \mathscr{P}(\Omega) \to \mathbb{R}$ est une probabilité sur Ω.

Démonstration.
En effet, elle est bien définie car $P(B) > 0$. Elle est à valeurs positives ou nulles et pour tout $A \in \mathscr{P}(\Omega)$, on a $A \cap B \subset B$ donc $P(A \cap B) \leqslant P(B)$ donc $P_B(A) \leqslant 1$. De plus $P_B(\Omega) = P(B)/P(B) = 1$. Enfin, pour tout couple (A, C) d'événements incompatibles, $A \cap B$ et $C \cap B$ sont incompatibles, donc

$$\begin{aligned} P_B(A \cup C) &= \frac{P((A \cap B) \cup (C \cap B))}{P(B)} \\ &= \frac{P(A \cap B) + P(C \cap B)}{P(B)} \\ &= P_B(A) + P_B(C) \end{aligned}$$

□

Remarque 1.3.4.
Dans les exercices de probabilités, l'un des points délicats (et donc intéressant) est souvent de traduire correctement l'énoncé en termes de probabilités conditionnelles. En effet, les énoncés ne sont pas toujours donnés de manière mathématisée et vous avez alors un (petit) travail de modélisation à effectuer. On pourra commencer par s'entraîner sur les exercices **??** et **??**.

Exercice 1.3.5.
Dans une urne, on place deux boules blanches et une boule noire. On effectue un premier tirage dans l'urne, dans laquelle on remet la boule tirée en y rajoutant une boule de même couleur. On effectue un second tirage dans l'urne.

Modéliser (*i.e.* traduire l'énoncé mathématiquement, ici en termes de probabilités conditionnelles).

b Probabilités composées, probabilités totales

Proposition 1.3.6 (Formule des probabilités composées)**.**
Soit A et B deux événements, avec $P(A) > 0$. Alors

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

Démonstration.
C'est une simple réécriture de la définition. □

Remarque 1.3.7.
On généralise cela au cas de plusieurs événements. Soit par exemple A, B, C et D quatre événements tels que $P(A \cap B \cap C \cap D) \neq 0$. Alors

$$P(A \cap B \cap C \cap D) = P(A) \times P(B|A) \times P(C|A \cap B) \times P(D|A \cap B \cap C).$$

Exercice 1.3.8.
Soit $(A_1, \dots, A_n)$ des événements dont la probabilité de l'intersection est non nulle. Exprimer $P\left(\bigcap_{i=1}^{n} A_i\right)$ à l'aide de la formule des probabilités composées.

Proposition 1.3.9 (Formule des probabilités totales, deuxième forme)**.**
Soit $n \in \mathbb{N}^*$, $(A_i)_{i\in[\![1,n]\!]}$ un système complet d'événements de probabilités toutes non nulles et B un événement. Alors

$$P(B) = \sum_{i=1}^{n} P(B|A_i) \times P(A_i).$$

Démonstration.
C'est une conséquence immédiate de la première forme (proposition 1.2.8) et de la formule des probabilités composées. □

Remarque 1.3.10.
On adopte souvent la convention suivante, fort utile dans l'utilisation de la formule des probabilités totales : si $P(A_i) = 0$, on pose $P(B|A_i) \times P(A_i) = 0$. Ainsi, la formule est valide pour tout système complet d'événements, ce qui peut éviter certaines contorsions particulièrement douloureuses ...

Attention : cette convention n'est pas au programme de la filière MP (mais elle l'est en PSI). Si vous voulez l'utiliser, rappelez la *clairement* avant. Ou mieux : revenez à la formule utilisant les intersections.

Exercice 1.3.11.
On considère une urne contenant quatre boules blanches et trois boules noires. On tire successivement et sans remise trois boules.

Calculer la probabilité de tirer exactement deux boules noires.

Note : il peut être intéressant de dessiner un arbre des possibilités pour raisonner. Mais un tel arbre n'est en *aucun cas* une justification.

Exercice 1.3.12.
On effectue $N \geqslant 2$ tirages successifs dans une urne, contenant initialement une boule blanche et une boule noire.

Chaque fois que l'on tire une boule blanche, on la remet et on rajoute une boule blanche supplémentaire dans l'urne.

Chaque fois que l'on tire une boule noire, on la remet dans l'urne.

On suppose que cette expérience est modélisée par un espace probabilisé fini (Ω, P). Quelle est la probabilité p_N d'obtenir la première boule noire au N^{e} tirage ?

Remarque 1.3.13. — Un des points attendus est de justifier rigoureusement l'utilisation d'une certaine formule ...

— L'exercice précédent est souvent modifié en « si l'on tire une boule noire, on s'arrête ». Cela change-t-il la modélisation ?
— L'année prochaine, vous pourrez modéliser cela en considérant une suite infinie de tirages. Comme nous ne considérons que des espaces probabilisés finis, nous nous limitons à N tirages successifs ... avec N quelconque.
— Que vaut $\sum_{n=1}^{+\infty} p_n$? Pouvez-vous l'interpréter, au moins intuitivement ?

c Formule de Bayes

Exercice 1.3.14 (fondamental)**.**
On effectue un test de dépistage d'une maladie. Le test rend un résultat binaire : positif ou négatif. La probabilité que le test rende un résultat positif pour une personne si cette personne a contracté la maladie est appelé *sensibilité* du test et est notée p_1. La probabilité que le test rende un résultat négatif pour une personne qui n'a pas contracté cette maladie est appelée *spécificité* et est notée p_2.

Une personne prise au hasard dans la population française effectue le test et celui-ci rend un résultat positif. Quelle est la probabilité que cette personne soit malade ?

On donne : $p_1 = 0,99$, $p_2 = 0,98$, population française : $N = 6 \times 10^7$ personnes, nombre de personnes ayant contracté la maladie dans la population française : $m = 10^3$.

Proposition 1.3.15 (Formule de Bayes, cas particulier)**.**
Soit A et B deux événements tels que $P(A) > 0$ et $P(B) > 0$. Alors

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}.$$

Démonstration.
Il suffit de remplacer $P(A|B)$ et $P(B|A)$ par leurs définitions pour constater le résultat. □

Remarque 1.3.16.
Le théorème de Bayes dit, que pour deux événements A et B de probabilité non nulle, la probabilité d'avoir l'événement A, sachant qu'on a observé B (appelée probabilité *a posteriori*) est la probabilité d'avoir B sachant A multipliée par le rapport de la probabilité d'avoir A (probabilité *a priori*) et de la probabilité d'avoir B.

Proposition 1.3.17 (Formule de Bayes, cas général)**.**
Soit $(A_i)_{i\in[\![1,n]\!]}$ un système complet d'événements de probabilités toutes non nulles et B un événement de probabilité non nulle. Alors pour tout $j \in [\![1, n]\!]$, on a

$$P(A_j|B) = \frac{P(B|A_j)P(A_j)}{\sum_{i=1}^{n} P(B|A_i)P(A_i)}.$$

Démonstration.
Soit $j \in [\![1, n]\!]$. Alors en utilisant la version précédente du théorème de Bayes, on obtient

$$P(A_j|B) = \frac{P(B|A_j)P(A_j)}{P(B)}$$

Or d'après le théorème des probabilités totales, on a

$$P(B) = \sum_{i=1}^{n} P(B|A_i)P(A_i)$$

□

Remarque 1.3.18.
Il est essentiel d'avoir compris ce que dit cette formule et d'être capable de la redémontrer rapidement.

Exercice 1.3.19.
Monsieur C. vient au lycée à pied, à cheval ou en voiture avec des probabilités respectives 9/100, 9/10 et 1/100. Quand il vient à pied, il met des chaussures de sport avec probabilité 9/10 ; à cheval, avec probabilité 5/10 et en voiture avec probabilité 1/10. Aujourd'hui, vous constatez qu'il a mis des chaussures de sport. Quelle est la probabilité qu'il soit venu à cheval ?

Remarque 1.3.20.
Remarquez l'abus de langage de l'exercice ci-dessus : en réalité, si on se place aujourd'hui et que Monsieur C. est déjà au lycée, ou bien il est venu à cheval ou bien il est venu par un autre moyen et parler de probabilité n'a plus de sens. En réalité, ce que signifie la formulation, c'est : « si on se place dans l'univers de tous les jours possibles, quelle est la probabilité que M. C. soit venu à cheval sachant qu'il a mis des chaussures de sport ». Cet abus de langage est typique de nombreux problèmes de probabilités et modéliser correctement le problème n'est pas toujours chose facile (voir le problème des trois portes).

1.4 Événements indépendants

a Couple d'événements indépendants

Définition 1.4.1.
Soit A et B deux événements. On dit que A et B sont indépendants si et seulement si $P(A \cap B) = P(A) \times P(B)$.

Remarque 1.4.2.
1. Si $P(B) > 0$, alors cette condition est équivalente à $P(A|B) = P(A)$. Autrement dit, de façon informelle, savoir B ne modifie pas la probabilité de A.
2. Si $P(B) > 0$ et $P(\bar{B}) > 0$, elle est également équivalente à $P(A|B) = P(A|\bar{B})$.
3. Il arrive que l'on démontre l'indépendance de deux événements mais le plus souvent, il s'agit d'une hypothèse de modélisation du problème considéré.
4. Dans tout exercice de probabilités, il est primordial de bien repérer dans l'énoncé les hypothèses d'indépendance.

Exercice 1.4.3.
Quels sont les événements indépendants d'eux-mêmes ?

Exemple 1.4.4.
Si on lance deux fois un dé à six faces et qu'on note A et B les événements «obtenir un 6» respectivement au premier et deuxième tirage, on aura tendance à modéliser le problème en disant que les deux événements sont indépendants ce qui correspond à l'intuition physique : le fait qu'on obtienne un 6 au deuxième tirage ne dépend pas du fait qu'on a obtenu un 6 au tirage précédent, le dé n'ayant pas de «mémoire» de ce qui s'est passé. Attention : même si le dé est pipé, il est raisonnable de considérer que les deux événements sont indépendants.

Si au lieu de considérer deux lancers d'un même dé, on considère plutôt le lancer simultané d'un dé rouge et d'un dé vert, il est encore raisonnable de penser que les deux événements sont indépendants, même si les dés sont pipés et même s'ils sont pipés de deux façons différentes. À moins par exemple que les dés soient aimantés, auquel cas les résultats des deux dés pourraient être reliés.

Exercice 1.4.5.
Le jeu de la roulette russe à deux joueurs consiste à placer une unique balle dans un revolver à 6 coups puis à faire tourner le barillet de façon aléatoire. Chacun à son tour, chaque joueur pointe le revolver sur sa propre tempe avant d'actionner la détente. La partie s'arrête dès le chien percute la cartouche (le perdant est celui qui tenait le revolver).

On note A l'événement «le premier joueur perd dès son premier essai», B l'événement «le deuxième joueur perd dès son premier essai».

Modéliser le problème et calculer $P(A)$ et $P(B)$. Peut-on raisonnablement penser que A et B sont indépendants ?

Variante : on fait tourner de nouveau le barillet à chaque tour. Calculer $P(A)$ et $P(B)$.

NB : Bien qu'il soit rare de développer une addiction à ce jeu, y jouer est fortement déconseillé.

Exercice 1.4.6.
On considère une urne contenant 10 boules noires et 10 boules blanches. On tire successivement deux boules, sans remise. On note A (resp. B) l'événement «la première (resp. seconde) est blanche».

Modéliser ce problème.

A et B sont-elles indépendantes ? Calculer $P(A)$ et $P(B)$. Que vaut $P(A|B)$? Que vaut $P(B|A)$?

Mêmes questions si on tire maintenant simul-

tanément deux boules, l'une de la main gauche, l'autre de la main droite et qu'on note A (resp. B) l'événement «la boule tirée par la main gauche (resp. droite) est blanche».

b Famille finie d'événements mutuellement indépendants

Définition 1.4.7.
Soit n un entier. On dit que des événements A_1, …, A_n sont *mutuellement indépendants* si pour toute partie I de $[\![1, n]\!]$, on a

$$P\left(\bigcap_{i\in I} A_i\right) = \prod_{i\in I} P(A_i).$$

On dit qu'ils sont *deux à deux indépendants* si et seulement si pour tout $(i, j) \in [\![1, n]\!]^2$, avec $i \neq j$, A_i et A_j sont indépendants.

Remarque 1.4.8. 1. L'ordre des éléments n'a aucune importance.

2. L'indépendance mutuelle entraîne l'indépendance deux à deux.
3. La réciproque est fausse. Considérer par exemple deux tirages d'un dé et les événements «le premier tirage donne un nombre pair», «le second tirage donne un nombre pair» et «la somme des deux nombres obtenus est paire».
4. Il ne suffit pas de vérifier que la probabilité de l'intersection des A_i est égale au produit des $P(A_i)$ pour l'ensemble de tous les indices mais bien de le vérifier pour tous les ensembles d'indices possibles. Considérer par exemple l'univers $\Omega = [\![1, 8]\!]$ des résultats possibles d'un dé équilibré à 8 faces, et les événements $A_1 = \{ 1, 2, 3, 4 \}$, $A_2 = \{ 1, 2, 3, 4 \}$ et $A_3 = \{ 1, 5, 6, 7 \}$.
5. Le plus souvent, l'indépendance mutuelle est une hypothèse faite lors de la modélisation du problème. Le problème, c'est que dans de nombreux énoncés, cette hypothèse n'est écrite nulle part : c'est le mathématicien qui analyse le problème [2] qui doit se poser la question de l'indépendance des événements.
6. Lorsqu'il s'agit de montrer l'indépendance mutuelle de plusieurs événements, il faut vérifier autant de conditions que de sous-ensembles de $[\![1, n]\!]$, soit 2^n, dont $n + 1$ sont trivialement vérifiées (celles pour lesquelles I possède 0 ou 1 élément).

Proposition 1.4.9.
Remplacer, dans une famille d'événements mutuellement indépendants, certains événements par leurs contraires donne une nouvelle famille d'événements mutuellement indépendants. En d'autres termes, soit n un entier et A_1, …, A_n n événements indépendants. On se donne n événements B_1, …, B_n tels que pour tout $i \in [\![1, n]\!]$, B_i est égal à A_i ou à $\bar{A}_i$. Alors la famille B_1, …, B_n est une famille d'événements indépendants.

Démonstration.
Il suffit de montrer le cas où $B_i = A_i$ pour $i = 1, \ldots, n-1$ et où $B_n = \bar{A}_n$. En effet, on peut alors en déduire que si, dans une famille d'événements mutuellement indépendants, on change l'un des événements en son contraire, on obtient de nouveau une famille d'événements mutuellement indépendants. Par une récurrence immédiate, il vient alors que si on change p événements en leurs contraires, on obtient de nouveau une famille d'événements mutuellement indépendants.

Posons donc $B_i = A_i$ pour $i \in [\![1, n-1]\!]$ et $B_n = \bar{A}_n$.

Soit alors I une partie de $[\![1, n]\!]$, montrons qu'on a

$$P\left(\bigcap_{i\in I} B_i\right) = \prod_{i\in I} P(B_i)$$

Si I ne contient pas n, c'est évident.

Si I contient n, alors posons $J = I \setminus \{ n \}$. On a succes-

2. Donc vous en particulier !

sivement :

$$\begin{aligned}
P\left(\bigcap_{i\in I} B_i\right) &= P\left(\bar{A_n} \cap \bigcap_{i\in J} A_i\right)\\
&= P\left((\Omega \setminus A_n) \cap \bigcap_{i\in J} A_i\right)\\
&= P\left(\bigcap_{i\in J} A_i \setminus \left(A_n \cap \bigcap_{i\in J} A_i\right)\right)\\
&= P\left(\bigcap_{i\in J} A_i\right) - P\left(\bigcap_{i\in I} A_i\right)\\
&= \prod_{i\in J} P(A_i) - \prod_{i\in I} P(A_i)\\
&= (1 - P(A_n)) \prod_{i\in J} P(A_i)\\
&= P(B_n) \prod_{i\in J} P(B_i)\\
&= \prod_{i\in I} P(B_i).
\end{aligned}$$

□

2 Variables aléatoires

2.1 Définitions

Définition 2.1.1.
Une *variable aléatoire* (v.a.) X est une application définie sur l'univers Ω à valeurs dans un ensemble E. Lorsque $E \subset \mathbb{R}$, la variable aléatoire est dite *réelle*. On appelle parfois *univers image* l'image directe de Ω par X.

Exemple 2.1.2.
Intuitivement, X représente une valeur associée à une expérience aléatoire : si l'on prend l'exemple du cas d'une personne jouant au loto, la valeur X, exprimée en euros, de son gain au loto lors du tirage qui aura lieu à une certaine date peut être modélisée par une variable aléatoire à valeurs réelles (l'univers Ω étant l'ensemble des tirages de loto possible).

Remarque 2.1.3.
Une variable aléatoire modélise donc un « objet aléatoire ». Si l'on considère une matrice aléatoire, on manipulera donc des variables aléatoires à valeurs matricielles, tandis que si l'on considère des triangles aléatoires on manipulera des variables aléatoires à valeurs dans l'ensemble des triangles du plan.

Par exemple, si $X_1, \dots, X_n$ sont des variables aléatoires à valeurs dans un ensemble A, si P_n est la (mesure de) probabilité empirique par rapport à $X_1, \dots, X_n$, alors P_n est une variable aléatoire à valeurs dans l'ensemble des (mesures de) probabilités sur A.

Remarque 2.1.4.
En toute généralité, la définition de variable aléatoire est plus subtile. On se place ici dans un cadre très simplifié (univers fini).

Définition 2.1.5.
Soit X une variable aléatoire à valeurs dans un ensemble E.

Pour toute partie A de E, on note $\{ X \in A \}$ ou $(X \in A)$, (voire $[X \in A]$) l'événement $X^{-1}(A)$.

Si $E \subset \mathbb{R}$, et $x \in \mathbb{R}$, X est dite *réelle* et on note $(X = x)$, $(X \leqslant x)$, $(X < x)$, $(X \geqslant x)$, $(X > x)$ respectivement les événements $X^{-1}(\{ x \})$, $X^{-1}(]-\infty, x])$, ...

On note $P(X \in A)$, $P(X = x)$, $P(X \leqslant x)$, ... les probabilités de ces événements.

Exemple 2.1.6.
Pour reprendre l'exemple précédent, $(X \geqslant 1000)$ représente l'événement «le gain du joueur au loto est supérieur ou égal à mille euros» et $P(X \geqslant 1000)$ représente la probabilité de cet événement.

Proposition 2.1.7.
Soit X une variable aléatoire à valeurs dans un ensemble fini E. Alors $([X = x])_{x\in E}$ est un système complet d'événements.

Démonstration.
Soit $\omega \in \Omega$, alors $\omega \in [X = X(\omega)]$ donc $\cup_{x\in E}[X = x] = \Omega$. Soit $(x, y) \in E^2$, avec $x \neq y$. Si $\omega \in [X = x] \cap [X = y]$, alors $X(\omega) = x = y$, ce qui est impossible, donc $[X = x] \cap [X = y] = \varnothing$. □

Remarque 2.1.8.
C'est souvent ce type de système complet d'événements que l'on utilisera.

2.2 Loi d'une variable aléatoire

Définition 2.2.1.
Soit X une variable aléatoire à valeurs dans un ensemble E.

On appelle *loi de la variable aléatoire* X la loi de probabilité $P_X : \mathscr{P}(X(\Omega)) \to \mathbb{R}$ qui à tout élément x de $X(\Omega)$ associe la probabilité de l'événement $X = x$:

$$\forall x \in X(\Omega) \quad P_X(\{x\}) = P(X = x).$$

et associe 0 aux autres éléments de $\mathscr{P}(E)$.

Proposition 2.2.2.
Soit X une variable aléatoire définie sur un espace probabilisé fini (Ω, P). Alors $X(\Omega)$ est fini et P_X est une probabilité sur $X(\Omega)$.

Démonstration.
Par la caractérisation d'une loi par l'image de ses singletons, il suffit de remarquer que

$$\sum_{x \in X(\Omega)} P(X = x) = 1.$$

□

Corollaire 2.2.3.
Si $A \subset X(\Omega)$, $P_X(A) = P(X \in A)$.

Remarque 2.2.4.
On peut donc définir la loi d'une variable aléatoire en précisant la probabilité que cette v.a. soit égale à chaque élément de son image. Par exemple, on peut dire « la v.a. X à valeurs dans $[\![0, 5]\!]$ dont la loi est déterminée par

k	0	1	2	3	4	5
$P(X = k)$	1/4	0	1/2	1/12	1/12	1/12

».

Remarque 2.2.5.
Pour déterminer la loi d'une variable aléatoire X, on procédera *systématiquement* de la manière suivante :
• on détermine l'image de X ;
• pour chaque $k \in X(\Omega)$, on calcule $P(X = k)$;
• si on obtient une loi connue, on la nomme.

Exercice 2.2.6.
Soit X à valeurs dans $\{-1; 0; 1\}$ dont la loi est déterminée par

$$P(X = -1) = P(X = 0) = P(X = 1) = \frac{1}{3}.$$

Comment s'appelle la loi de X ? Quelle est la loi de $-X$? A-t-on $X = -X$?

Remarque 2.2.7.
La définition ci-dessus pose problème dans le cas où X est une variable aléatoire réelle continue (hors-programme mais vu en terminale) : la probabilité d'avoir $P(X = x)$ ne donne aucune information puisque pour tout x fixé, $P(X = x) = 0$.

C'est pourquoi on trouve parfois une autre définition de P_X : P_X est alors l'application de $\mathscr{P}(E)$ dans $\mathbb{R}$ qui, à une partie A de E, associe $P(X \in A)$. Dans ce cas, P_X a la propriété d'être une probabilité sur E (lorsque E est fini) et est déterminée de façon unique par les valeurs des $P(X = x)$ pour $x \in E$ puisqu'on a $P(X \in A) = \sum_{x \in A} P(X = x)$.

Cette deuxième définition pose également des problèmes dans le cas des variables continues mais ils sont plus facilement réparables (on ne peut plus définir P_X sur $\mathscr{P}(E)$ mais seulement sur une partie).

Définition 2.2.8.
Soit E et F deux ensembles. Soit X une variable aléatoire à valeurs dans un ensemble E. Soit $f : E \to F$. L'application $f \circ X : \Omega \to F$ est une variable aléatoire à valeurs dans F appelée *image de X par f* et parfois notée $f(X)$.

Remarque 2.2.9.
Le terme «image d'une variable aléatoire» vient

du fait que pour tout $\omega \in \Omega$, $f(X)(\omega)$ est l'image de $X(\omega)$ par f.

Exemple 2.2.10.
Si X est une v.a. réelle, on pourra considérer les v.a. réelles X^2, $|X|$ *etc.*

Proposition 2.2.11.
La loi associée à la variable aléatoire $f(X)$ introduite ci-dessus est

$$\begin{array}{rccc} P_{f(X)} : & f(X(\Omega)) & \to & \mathbb{R} \\ & y & \mapsto & P(X \in f^{-1}(\{\, y \,\})) \end{array} .$$

Démonstration.
Il suffit de remarquer

$$\begin{aligned} (X \in f^{-1}(\{\, y \,\})) &= \left\{ \omega \in \Omega \;\middle|\; X(\omega) \in f^{-1}(\{\, y \,\}) \right\} \\ &= \{\, \omega \in \Omega \mid f(X(\omega)) \in \{\, y \,\} \,\} \\ &= \{\, \omega \in \Omega \mid f(X)(\omega) \in \{\, y \,\} \,\} \\ &= \left\{ \omega \in \Omega \;\middle|\; \omega \in (f(X))^{-1}(\{\, y \,\}) \right\} \\ &= (f(X) = y). \end{aligned}$$

□

Exemple 2.2.12.
Soit X un v.a. à valeurs dans $\{-1, 0, 1\}$ telle que $P(X = -1) = P(X = 0) = P(X = 1) = \dfrac{1}{3}$. Déterminer les lois de X^2 et de X^3.

Définition 2.2.13 (Fonction de répartition)**.**
Soit X une variable aléatoire réelle. On appelle *fonction de répartition* de X la fonction

$$\begin{array}{rccc} F_X : & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & P(X \leqslant x) \end{array} .$$

Exemple 2.2.14.
S'il faut retenir une chose, c'est le dessin de la fonction de répartition, figure XXII.1.

Proposition 2.2.15.
La fonction de répartition d'une variable réelle X sur un univers Ω *fini* est une fonction en escalier. Plus précisément, Ω étant fini, $X(\Omega)$ est fini et s'écrit $\{\, x_1, \ldots, x_n \,\}$ avec $n \geqslant 1$, où $x_1 < \ldots < x_n$. Alors F_X est constante sur les intervalles $]-\infty, x_1[$, $[x_1, x_2[$, $[x_2, x_3[$, $\ldots$, $[x_{n-1}, x_n[$, $[x_n, +\infty[$, prend pour valeur 0 sur le premier de ces intervalles, 1 sur le dernier et pour tout $i \in [\![1, n-1]\!]$ prend la valeur $\displaystyle\sum_{k=1}^{i} P(X = x_k)$ sur $[x_i, x_{i+1}[$.

Démonstration.
Il suffit de constater que pour tout $i \in [\![1, n-1]\!]$, et tout $t \in [x_i, x_{i+1}[$, l'événement $(X \leqslant t)$ n'est autre que l'union des événements deux à deux disjoints $(X = x_k)$ pour $k \leqslant i$, d'où

$$F_X(t) = \sum_{k=1}^{i} P(X = x_k).$$

De même on a $F_X(t) = 0$ pour $t \in]-\infty, x_1[$ et $F_X(t) = \displaystyle\sum_{k=1}^{n} P(X = x_k) = 1$ pour $t \in [x_n, +\infty[$. On en déduit que F_X est en escalier. □

Proposition 2.2.16.
La fonction de répartition d'une v.a. réelle est croissante et continue à droite. Elle a pour limite 0 en $-\infty$ et 1 en $+\infty$.

Remarque 2.2.17.
Cette propriété est vraie même pour les v.a. réelles définies sur un univers infini (programme de seconde année).

Démonstration.
C'est un corollaire immédiat de ce qui précède. □

Proposition 2.2.18.
La fonction de répartition caractérise la loi d'une variable X, au sens où pour tout réel t $P(X = t) > 0$ si et seulement si F_X n'est pas continue en t, et $P(X = t) = F_X(t) - \lim\limits_{t-} F_X$.

Démonstration.
Là encore, cela découle de ce qui précède. □

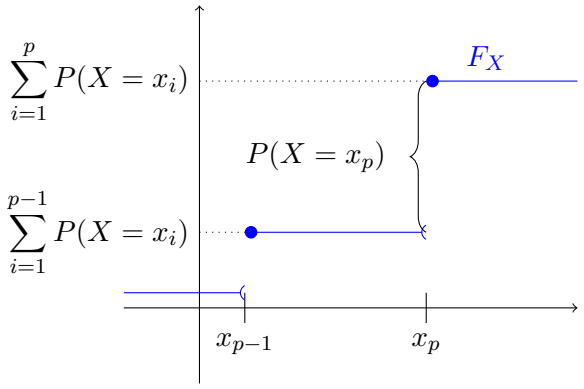


FIGURE XXII.1 – Illustration de la fonction de répartition d'une variable aléatoire X à valeurs dans $\{x_1, \dots, x_n\}$ avec $x_1 < \cdots < x_n$.

2.3 Loi usuelles

Dans cette partie, on étendra automatiquement les définitions données en commettant l'abus de notation suivant. Soit X une variable aléatoire X à valeurs dans E, $A \subset E$ tel que $\forall x \in E \backslash A, P(X = x) = 0$ et $\forall a \in A, P(X = a) > 0$ (on dit que A est le support de la loi de X). Formellement, $X(\Omega) = E$, mais on étendra les définitions suivantes comme si $X(\Omega) = A$.

Exemple 2.3.1.
Si $X : \Omega \to \{1, 2, 3, 4\}$, avec $P(X = 1) = P(X = 2) = P(X = 3) = \frac{1}{3}$ et $P(X = 4) = 0$, on s'autorisera à dire que X suit une loi uniforme sur $\{1, 2, 3\}$.

a Loi uniforme

Définition 2.3.2.
Soit E un ensemble fini, non vide. On dit qu'une variable aléatoire réelle X suit *la loi uniforme* sur E et on note $X \hookrightarrow \mathscr{U}(E)$ (voire $X \equiv \mathscr{U}(E)$) si $X(\Omega) = E$ et P_X est la probabilité uniforme sur E (autrement dit, pour tout $x \in E$, $P(X = x) = 1/\#E$).

En particulier pour tout couple (a, b) d'entiers relatifs avec $a \leqslant b$, on a $X \hookrightarrow \mathscr{U}(\llbracket a, b \rrbracket)$ si et seulement si

$$\forall x \in \llbracket a, b \rrbracket \quad P(X = x) = \frac{1}{b - a + 1}.$$

Exemple 2.3.3. — La variable aléatoire modélisant le nombre obtenu par tirage d'un dé équilibré à 6 faces suit la loi uniforme sur $\llbracket 1, 6 \rrbracket$.
— Pour modéliser le numéro d'une boule tirée dans une urne contenant n boules numérotées de 1 à n on prendra une variable aléatoire suivant la loi uniforme sur $\llbracket 1, n \rrbracket$.

Exercice 2.3.4.
On tire deux boules *sans remise* dans une urne. Montrer que le couple des numéros tirés (dans l'ordre) suit une loi uniforme dans l'ensemble des 2-arrangements de $\llbracket 1, n \rrbracket$.

b Loi de Bernoulli

Définition 2.3.5.
Soit $p \in [0, 1]$. On dit qu'une variable aléatoire X est une variable de Bernoulli (ou suit la loi de Bernoulli) de paramètre p et on note $X \hookrightarrow \mathscr{B}(p)$ si X est à valeurs dans $\{ 0, 1 \}$ et $P(X = 1) = p$.

Exemple 2.3.6. — Modélisons le tirage d'une pièce à pile ou face par la variable X valant 0 si l'on obtient pile et 1 si l'on obtient face. Si la pièce est supposée équilibrée, on supposera que X suit la loi uniforme sur $\{ 0, 1 \}$; que ce soit le cas ou non, il s'agit d'une variable de Bernoulli de paramètre la probabilité d'obtenir face.
— Si X est à valeurs dans $\{0, 1\}$, alors $X \hookrightarrow \mathscr{B}(P(X = 1))$.
— De manière générale, notons A un événement sur un espace probabilisé Ω. Alors χ_A, la fonction indicatrice de A, définie par

$$\chi_A : \left\{ \begin{array}{ccc} \Omega & \longrightarrow & \{ 0, 1 \} \\ \omega & \longmapsto & \begin{cases} 1 \text{ si } \omega \in A, \\ 0 \text{ si } \omega \notin A. \end{cases} \end{array} \right.$$

est une variable de Bernoulli de paramètre $P(A)$.

Très souvent, on s'intéressera à un événement A lors d'une expérience aléatoire et on dira que l'expérience est un succès si A est réalisé et un échec si A ne l'est pas. χ_A est alors la variable de Bernoulli prenant la valeur 1 en cas de succès et 0 en cas d'échec.

Exercice 2.3.7.
Montrer que toute variable aléatoire réelle définie sur un espace probabilisé fini peut s'écrire comme une combinaison linéaire de variables aléatoires suivant des lois de Bernoulli.

c Loi binomiale

Définition 2.3.8.
Soit $n \in \mathbb{N}$ et $p \in [0,1]$. On dit qu'une variable aléatoire X suit la loi binomiale de paramètres n et p et on note $X \hookrightarrow \mathscr{B}(n,p)$ si X est à valeurs dans $[\![0,n]\!]$ et pour tout $k \in [\![0,n]\!]$, on a

$$P(X=k) = \binom{n}{k} p^k (1-p)^{n-k}.$$

Exemple 2.3.9.
- Considérons n expériences aléatoires mutuellement indépendantes toutes de probabilité de succès p. On modélisera le nombre de succès par une variable binomiale de paramètres n et p. On verra dans la proposition 2.5.11 une justification mathématique à cette modélisation.
- En particulier considérons une urne opaque contenant B boules blanches et N boules noires indiscernables au toucher ($B \in \mathbb{N}^*$, $N \in \mathbb{N}^*$), dans laquelle on tire n fois une boule, *avec* remise. Alors on modélisera le nombre de fois où l'on tire une boule noire par une variable aléatoire suivant la loi binomiale de paramètres n et $N/(B+N)$.

Exercice 2.3.10.
On considère un joueur jouant au jeu suivant :
- Il mise un euro. Cette mise est définitivement perdue.
- Il lance quatre pièces de monnaie.
- Si exactement trois des pièces tombent sur pile, il perçoit un euro. Si les quatre pièces tombent sur pile, il perçoit dix euros.

On note X le gain du joueur (mise incluse, le gain peut donc être négatif). Donner la loi de X.

2.4 Couples de variables aléatoires

Dans cette partie, on considère Ω un espace probabilisé fini et deux variables aléatoires X et Y.

On écrira $X(\Omega)$ sous la forme $\{ x_1, \dots, x_N \}$ et $Y(\Omega)$ sous la forme $\{ y_1, \dots, y_P \}$ où N et P sont des entiers.

Remarque 2.4.1.
On peut considérer, en commettant un léger abus de notation, que (X,Y) est une variable aléatoire, à valeurs dans $\{ x_1, \dots, x_N \} \times \{ y_1, \dots, y_P \}$.

Proposition 2.4.2.
La famille $((X=x_i) \cap (Y=y_j))_{(i,j) \in [\![1,N]\!] \times [\![1,P]\!]}$ est un système complet d'événements.

Démonstration.
Soit $(i,j) \in [\![1,N]\!] \times [\![1,P]\!]$, il suffit de remarquer que $[(X,Y)=(x_i,y_j)] = [X=x_i] \cap [Y=y_j]$ et d'utiliser la proposition 2.1.6. □

Remarque 2.4.3.
On notera souvent l'événement $[X=x] \cap [Y=y]$ par $[X=x, Y=y]$.

Définition 2.4.4 (Loi conjointe)**.**
On appelle *loi conjointe de X et Y* la loi du couple (X,Y), soit la loi $P_{X,Y} : \mathscr{P}(X(\Omega) \times Y(\Omega)) \to \mathbb{R}$ vérifiant $\forall (x,y) \in X(\Omega) \times Y(\Omega)$, $P_{X,Y}(\{(x,y)\}) = P((X=x) \cap (Y=y)) = P(X=x, Y=y)$.

Exercice 2.4.5.
On tire un dé équilibré à six faces et on lance une pièce de monnaie équilibrée. On note X la variable de Bernoulli associée à l'événement «obtenir pile» et Y la valeur tirée sur le dé.

Donner la loi conjointe de X et Y.

Exercice 2.4.6.
On tire deux dés équilibrés à quatre faces, un vert et un rouge. On appelle X la valeur obtenue sur le dé vert, Y la valeur obtenue sur le dé rouge et Z la somme des deux. Donner la loi conjointe de X et Y puis de X et Z.

Définition 2.4.7.
On appelle *première (resp. seconde) loi marginale du couple* (X, Y) la loi de X (resp. de Y).

Proposition 2.4.8.
Les lois marginales du couple (X, Y) sont déterminées de façon unique par la loi du couple $P_{X,Y}$. Plus précisément, on a pour tout $x \in X(\Omega)$

$$\begin{aligned} P(X = x) = P_X(\{x\}) &= \sum_{y \in Y(\Omega)} P_{X,Y}(\{(x, y)\}) \\ &= \sum_{y \in Y(\Omega)} P(X = x, Y = y). \end{aligned}$$

Symétriquement, pour tout $y \in Y(\Omega)$, on a

$$\begin{aligned} P(Y = y) = P_Y(\{y\}) &= \sum_{x \in X(\Omega)} P_{X,Y}(\{(x, y)\}) \\ &= \sum_{x \in X(\Omega)} P(X = x, Y = y). \end{aligned}$$

En revanche, les lois marginales ne suffisent pas à déterminer la loi du couple.

Démonstration.
Pour le premier point, considérons $x \in X$ et remarquons alors qu'on a

$$(X = x) = \bigcup_{y \in Y(\Omega)} (X = x) \cap (Y = y).$$

Or cette union est une union disjointe, d'où l'égalité

$$P(X = x) = \sum_{y \in Y(\Omega)} P((X = x) \cap (Y = y)).$$

D'où le premier point. Autrement dit : la famille des $(Y = y)$ pour $y \in Y(\Omega)$ constitue un système complet d'événements et le résultat se déduit immédiatement de la formule des probabilités totales.

Pour le second point, il suffit de montrer que deux couples peuvent avoir des lois différentes bien qu'ayant les mêmes lois marginales. On peut par exemple considérer, sur l'univers $\Omega = \{ 1, 2 \}$ muni de la probabilité uniforme, les variables de Bernoulli X et Y définies par $X(1) = 1$, $X(2) = 0$, $Y(1) = 0$ et $Y(2) = 1$. Alors les variables X et Y ont même loi, les deux couples de variables aléatoires (X, X) et (X, Y) ont donc mêmes lois marginales. Cependant, ils ont des lois conjointes différentes puisque $P_{X,X}(1, 1) = \frac{1}{2}$ et $P_{X,Y}(1, 1) = 0$. □

Exemple 2.4.9.
On lance deux dés à 6 faces et l'on note X et Y le résultat de chacun. Alors (après avoir modélisé cela), les lois jointes de (X, X) et de (X, Y) sont différentes alors que (X, X) et (X, Y) ont les mêmes lois marginales.

Définition 2.4.10 (Loi conditionnelle)**.**
Soit X et Y deux variables aléatoires respectivement à valeurs dans des ensembles E et F. Soit $x \in X(\Omega)$ vérifiant $P_X(x) \neq 0$. Alors on appelle loi conditionnelle de Y sachant $(X = x)$ la loi de la variable Y sur l'univers Ω muni de la probabilité $P_{X=x}$. C'est donc la fonction $P_{Y|X=x} : \mathscr{P}(Y(\Omega)) \to \mathbb{R}$ vérifiant :

$$\forall y \in Y(\Omega),\ P_{Y|X=x}(y) = P(Y = y | X = x).$$

Remarque 2.4.11.
On définit de même, pour $y \in Y(\Omega)$ vérifiant $P_Y(y) \neq 0$, la loi conditionnelle de X sachant $(Y = y)$.

Exercice 2.4.12.
Un joueur possède six dés : le dé n° 1 a 4 faces, le n° 2 en a 6, le n° 3 8, le n° 4 10, le n° 5 12 et le n° 6 20. Il lance un dé à 6 faces, obtient i, lance le dé n° i et note X le résultat obtenu.

Quelle est la loi de X ?

Remarque 2.4.13.
La loi de Y conditionnellement à $X = x$ ne dépend que de la loi jointe de X et de Y :

$$P(Y = y | X = x) = \frac{P(X = x, Y = y)}{\sum_{z \in Y(\Omega)} P(X = x, Y = z)}.$$

On peut généraliser de la même manière ces notions sur les couples de variables aléatoires et définir la loi conjointe d'un n-uplet de variables aléatoires, les n lois marginales de ce n-uplet ainsi que la loi conditionnelle d'une variable, par exemple X_n, sachant $X_1 = x_1$, … et $X_{n-1} = x_{n-1}$.

2.5 Variables aléatoires indépendantes

Dans ces parties, sauf mention expresse du contraire, X et Y sont des variables aléatoires à valeurs respectivement dans des ensembles E et F.

Définition 2.5.1.
On dit que X et Y sont indépendantes si pour tout $x \in E$ et tout $y \in F$ on a

$$P([X = x] \cap [Y = y]) = P(X = x)P(Y = y). \tag{XXII.2}$$

On dira que deux variables aléatoires sont *indépendantes et identiquement distribuées* (i.i.d.) si elles sont indépendantes et de même loi.

Remarque 2.5.2.
On écrira souvent cela comme

$$P(X = x, Y = y) = P(X = x)P(Y = y).$$

Deux v.a. sont donc indépendantes si et seulement si leur loi jointe se factorise en le produit de leurs lois.

Exemple 2.5.3.
Si l'on tire deux dés ou si l'on effectue deux tirages avec remise dans une urne, on modélisera les deux résultats comme des v.a. indépendantes.

Exercice 2.5.4.
On effectue deux tirages sans remise dans une urne contenant n boules. Modéliser. Les numéros tirés sont-ils indépendants ?

Proposition 2.5.5.
X et Y sont indépendantes si et seulement si pour tout $A \subset E$ et tout $B \subset F$, on a

$$P((X, Y) \in A \times B) = P(X \in A)P(Y \in B). \tag{XXII.3}$$

Démonstration.
Pour le sens indirect, c'est-à-dire pour montrer l'égalité (XXII.2), sous l'hypothèse que l'égalité (XXII.3) est vérifiée pour tout A et tout B, il suffit de choisir $A = \{ x \}$ et $B = \{ y \}$.

Montrons le sens direct : supposons donc qu'on a (XXII.2) pour tout $(x, y) \in E \times F$ et montrons que pour tout $(A, B) \in \mathscr{P}(E) \times \mathscr{P}(F)$, on a (XXII.3). Quitte à remplacer A par $A \cap X(\Omega)$ et B par $B \cap Y(\Omega)$, on peut supposer que A et B sont des ensembles finis. On a alors

$$[X \in A] = \bigcup_{x \in A} [X = x]$$
$$[Y \in B] = \bigcup_{y \in B} [Y = y]$$
$$[(X, Y) \in A \times B] = \bigcup_{(x,y) \in A \times B} [X = x] \cap [Y = y]$$

Or ces trois unions sont des unions disjointes, donc :

$$\begin{aligned} P((X, Y) \in A \times B) &= P\left(\bigcup_{(x,y) \in A \times B} [X = x] \cap [Y = y] \right) \\ &= \sum_{(x,y) \in A \times B} P([X = x] \cap [Y = y]) \\ &= \sum_{(x,y) \in A \times B} P(X = x) \times P(Y = y) \\ &= \left(\sum_{x \in A} P(X = x) \right) \times \left(\sum_{y \in B} P(Y = y) \right) \\ &= P\left(\bigcup_{x \in A} [X = x] \right) \times P\left(\bigcup_{y \in B} [Y = y] \right) \\ &= P(X \in A) \times P(Y \in B). \end{aligned}$$

□

Exercice 2.5.6.
Soit X, Y indépendantes de loi uniforme sur $[\![1, n]\!]$. Calculer $P(X \leqslant Y)$.

Proposition 2.5.7.
Soit E, E', F et F' quatre ensembles. Soit $f : E \to E'$ et $g : F \to F'$. Soit alors X et Y deux variables aléatoires indépendantes. Alors $f(X)$ et $g(Y)$ sont des variables aléatoires indépendantes.

Démonstration.
Soit $A' \subset E'$ et $B' \subset F'$. D'après la proposition qui précède, il suffit de montrer

$$P\big((f(X), g(Y)) \in A' \times B'\big) = P(f(X) \in A') \times P(f(Y) \in B').$$

Or on a

$$\big[(f(X), g(Y)) \in A' \times B'\big] = \big[f(X) \in A'\big] \cap \big[g(Y) \in B'\big].$$

Et d'autre part, on a

$$\begin{aligned}\big[f(X) \in A'\big] &= \big\{\, \omega \in \Omega \;\big|\; f(X(\omega)) \in A' \,\big\} \\ &= \big\{\, \omega \in \Omega \;\big|\; X(\omega) \in f^{-1}(A') \,\big\} \\ &= \big[X \in f^{-1}(A')\big]\end{aligned}$$

et de la même façon, on obtient :

$$\big[g(Y) \in B'\big] = \big[Y \in g^{-1}(B')\big].$$

On en déduit

$$\begin{aligned}&\big[(f(X), g(Y)) \in A' \times B'\big] \\ =\ &\big[f(X) \in A'\big] \cap \big[g(Y) \in B'\big] \\ =\ &\big[X \in f^{-1}(A')\big] \cap \big[Y \in g^{-1}(B')\big] \\ =\ &\big[(X, Y) \in f^{-1}(A') \times g^{-1}(B')\big].\end{aligned}$$

Puis :

$$\begin{aligned}&P\big((f(X), g(Y)) \in A' \times B'\big) \\ =\ &P\big((X, Y) \in f^{-1}(A') \times g^{-1}(B')\big) \\ =\ &P\big(X \in f^{-1}(A')\big) \times P\big(Y \in g^{-1}(B')\big) \\ =\ &P\big(f(X) \in A'\big) \times P\big(g(Y) \in B'\big),\end{aligned}$$

qui est ce qu'on voulait démontrer. □

Définition 2.5.8.
Soit n un entier et $X_1, \ldots, X_n$ des variables aléatoires à valeurs dans des ensembles respectifs $E_1, \ldots, E_n$. On dit que les variables $X_1, \ldots, X_n$ sont mutuellement indépendantes si pour tous $x_1, \ldots, x_n$ appartenant respectivement à $X_1(\Omega), \ldots, X_n(\Omega)$, on a

$$P\left(\bigcap_{i=1}^{n} (X_i = x_i)\right) = \prod_{i=1}^{n} P(X_i = x_i). \quad \text{(XXII.4)}$$

On dira que des variables aléatoires sont *indépendantes et identiquement distribuées* (i.i.d.) si elles sont mutuellement indépendantes et de même loi.

Remarque 2.5.9.
On montrera bientôt que des variables aléatoires mutuellement indépendantes le sont deux à deux.


Comme le montre l'exemple **??**, des v.a. indépendantes deux à deux ne le sont pas forcément mutuellement.

Exemple 2.5.10.
Soit X, Y i.i.d. de loi de Rademacher : $P(X = 1) = P(X = -1) = \dfrac{1}{2}$, soit $Z = XY$. Montrer que X, Y et Z sont indépendantes deux à deux, mais pas mutuellement.

Proposition 2.5.11.
Les variables aléatoires $X_1, \ldots, X_n$ à valeurs dans des ensembles respectifs $E_1, \ldots, E_n$ sont mutuellement indépendantes si et seulement pour tous sous ensembles respectifs $A_1, \ldots, A_n$ de $E_1, \ldots, E_n$, on a

$$P\left(\bigcap_{i=1}^{n} (X_i \in A_i)\right) = \prod_{i=1}^{n} P(X_i \in A_i). \quad \text{(XXII.5)}$$

Démonstration.
La démonstration est similaire à celle du cas de deux variables.

Pour le sens indirect, c'est-à-dire pour montrer l'égalité (XXII.5), sous l'hypothèse que l'égalité (XXII.6) est vérifiée pour tous ensembles $A_1, \ldots, A_n$, il suffit de choisir $A_i = \{\, x_i \,\}$ pour $i = 1, \ldots n$.

Montrons le sens direct : supposons donc qu'on a (XXII.5) pour tous $x_1, \ldots, x_n$ appartenant respectivement à $E_1, \ldots, E_n$ et montrons que pour tous sous ensembles respectifs $A_1, \ldots A_n$ de $E_1, \ldots, E_n$, on a (XXII.6). Quitte à remplacer chaque A_i par $A_i \cap X_i(\Omega)$, on peut supposer que les A_i sont des ensembles finis. On a alors, si $1 \leqslant i \leqslant n$,

$$(X_i \in A_i) = \bigcup_{x_i \in A_i} (X_i = x_i).$$

Ainsi,

$$P\left(\bigcap_{i=1}^{n}(X_i \in A_i)\right) = P\left(\bigcap_{i=1}^{n}\bigcup_{x_i\in A_i}(X_i = x_i)\right)$$
$$= P\left(\bigcup_{(x_1,\dots,x_n)\in A_1\times\dots\times A_n}\bigcap_{i=1}^{n}(X_i = x_i)\right).$$

Or, cette réunion est disjointe, donc

$$P\left(\bigcap_{i=1}^{n}(X_i \in A_i)\right) = \sum_{(x_1,\dots,x_n)\in A_1\times\dots\times A_n} P\left(\bigcap_{i=1}^{n}(X_i = x_i)\right).$$

Par indépendance mutuelle,

$$P\left(\bigcap_{i=1}^{n}(X_i \in A_i)\right) = \sum_{(x_1,\dots,x_n)\in A_1\times\dots\times A_n}\prod_{i=1}^{n} P(X_i = x_i)$$
$$= \prod_{i=1}^{n}\sum_{x_i\in A_i} P(X_i = x_i)$$
$$= \prod_{i=1}^{n} P(X_i \in A_i),$$

d'où le résultat. □

Remarque 2.5.12.
Notez la différence entre la définition d'événements mutuellement indépendants et celle de variables mutuellement indépendantes : dans ce dernier cas, la définition ne demande pas de regarder pour tous les sous-ensembles de $[\![1, n]\!]$, pour une bonne raison : le résultat suivant assure que si l'égalité (XXII.5) est vérifiée, alors elle est vraie aussi si l'on effectue le produit et l'intersection seulement pour un sous-ensemble de $[\![1, n]\!]$.

Proposition 2.5.13.
Toute sous-famille d'une famille de variables aléatoires mutuellement indépendantes est constituée de variables mutuellement indépendantes : soit $X_1, \dots, X_n$ des variables aléatoires mutuellement indépendantes et $I \subset [\![1, n]\!]$; alors les X_i pour $i \in I$ sont mutuellement indépendantes.

Démonstration.
D'après la proposition 2.5.5, il suffit de montrer que pour toute famille d'événements A_i pour $i \in I$, on a

$$P\left(\bigcap_{i\in I}(X_i \in A_i)\right) = \prod_{i\in I} P(X_i \in A_i).$$

Considérons donc une telle famille quelconque, et posons $A_i = E_i$ pour $i \in [\![1, n]\!] \setminus I$. Alors, pour tout $i \in [\![1, n]\!] \setminus I$, l'événement $X_i \in A_i$ est certain, c'est-à-dire est égal à Ω. Donc

$$P\left(\bigcap_{i\in I}(X_i \in A_i)\right) = P\left(\bigcap_{i=1}^{n}(X_i \in A_i)\right)$$
$$= \prod_{i=1}^{n} P(X_i \in A_i)$$
$$= \prod_{i\in I} P(X_i \in A_i).$$

□

Corollaire 2.5.14 (Lemme des coalitions)**.**
Soit $(X_1, \dots, X_n)$ des variables aléatoires mutuellement indépendantes, I et J deux sous-ensembles disjoints de $\{1, \dots, n\}$.

Alors les variables aléatoires $(X_i)_{i\in I}$ et $(X_j)_{j\in J}$ sont indépendantes.

Démonstration.
Direct, par indépendance mutuelle de la famille $(X_k)_{k\in I\cup J}$. □

Remarque 2.5.15.
Ce lemme se généralise directement à l'indépendance mutuelle de m « paquets » de variables aléatoires pris sur m sous-ensembles disjoints deux à deux de $\{1, \dots, n\}$.

Proposition 2.5.16.
Si $X_1, \dots, X_n$ sont des variables aléatoires mutuellement indépendantes et $f_1, \dots, f_n$ sont des fonctions définies sur $X_1(\Omega), \dots, X_n(\Omega)$, alors $f_1(X_1), \dots, f_n(X_n)$ sont mutuellement indépendantes.

Démonstration.
Exactement comme pour deux v.a. □

Exemple 2.5.17.
Si X, Y, Z, T sont quatre v.a. réelles mutuellement indépendantes, alors $(X, Y), Z, T$ sont aussi mutuellement indépendantes, tout comme $X + Y, \mathrm{e}^{Z}$ et T^2.

Proposition 2.5.18.
Soit $n \in \mathbb{N}$, $A_1, \ldots, A_n$ n événements et $X_1, \ldots, X_n$ les variables de Bernoulli respectivement associées à ces événements. Alors les événements $A_1, \ldots, A_n$ sont indépendants si et seulement si les variables aléatoires $X_1, \ldots, X_n$ sont indépendantes.

Démonstration.
Supposons que les événements $A_1, \ldots, A_n$ sont indépendants. Soit alors $x_1, \ldots, x_n$ n éléments de $\{ 0, 1 \}$. Notons B_i l'événement $X_i = x_i$ pour $i \in [\![1, n]\!]$. Alors pour tout i, on a $B_i = A_i$ ou $B_i = \bar{A}_i$. Donc les événements B_1, $\ldots$, B_n sont mutuellement indépendants. On en déduit successivement :

$$\begin{aligned} P\left(\bigcap_{i=1}^{n}(X_i = x_i)\right) &= P\left(\bigcap_{i=1}^{n} B_i\right) \\ &= \prod_{i}^{n} P(B_i) \\ &= \prod_{i}^{n} P(X_i = x_i). \end{aligned}$$

Ainsi, les variables aléatoires $X_1, \ldots, X_n$ sont mutuellement indépendantes.

Réciproquement, supposons que les variables aléatoires $X_1, \ldots, X_n$ sont mutuellement indépendantes et montrons que les événements $A_1, \ldots, A_n$ le sont aussi. Soit $I \subset [\![1, n]\!]$. Alors les X_i pour $i \in I$ sont mutuellement indépendantes, en particulier, on a

$$P\left(\bigcap_{i \in I}(X_i = 1)\right) = \prod_{i \in I} P(X_i = 1)$$

Or pour tout $i \in I$, l'événement $(X_i = 1)$ n'est autre que A_i. On en déduit donc le résultat. □

Remarque 2.5.19.
Si $X_1, \ldots, X_n$ sont des variables aléatoires suivant des loi de Bernoulli, alors

$$\sum_{i=1}^{n} X_i = \operatorname{Card} \{ i \in [\![1, n]\!] \mid X_i = 1 \}.$$

On remarquera, sans s'émouvoir, que $\{ i \in [\![1, n]\!] \mid X_i = 1 \}$ est une variable aléatoire à valeurs dans $\mathscr{P}([\![1, n]\!])$.

Proposition 2.5.20.
Soit $p \in [0, 1]$ et $n \in \mathbb{N}$. Soit $X_1, \ldots, X_n$ n variables aléatoires suivant toutes la loi de Bernoulli de paramètre p et mutuellement indépendantes. Alors la variable X à valeurs dans $[\![0, n]\!]$ définie par

$$X = X_1 + \ldots + X_n$$

suit la loi binomiale de paramètres n et p.

Démonstration.
On a, pour tout $i \in [\![1, n]\!]$, $X_i(\Omega) = \{ 0, 1 \}$, donc $X(\Omega) \subset [\![0, n]\!]$.

Posons $E = \{ 0, 1 \}^n$, et pour tout élément $(x_1, \ldots, x_n)$ de E, on note $A_{(x_1,\ldots,x_n)}$ l'événement $\bigcap_{i=1}^{n}(X_i = x_i)$. La famille $(A_x)_{x \in E}$ est un système complet d'événements. Donc on a, pour tout $k \in [\![0, n]\!]$

$$\begin{aligned} (X = k) &= \bigcup_{x \in E} (X = k) \cap A_x \\ &= \bigcup_{\substack{(x_1,\ldots,x_n) \in E \\ x_1 + \cdots + x_n = k}} A_{(x_1,\ldots,x_n)}. \end{aligned}$$

Or les A_x forment un système complet d'événements. On a donc

$$\begin{aligned} P(X = k) &= \sum_{(x_1,\ldots,x_n) \in E} P(A_{(x_1,\ldots,x_n)} \cap [X = k]) \\ &= \sum_{\substack{(x_1,\ldots,x_n) \in E \\ x_1 + \cdots + x_n = k}} P(A_{(x_1,\ldots,x_n)}). \end{aligned}$$

Or, les X_i étant mutuellement indépendantes, pour tout $(x_1, \ldots, x_n) \in E$, on a

$$P(A_{(x_1,\ldots,x_n)}) = \prod_{i=1}^{n} P(X_i = x_i).$$

Or pour tout $i \in [\![1, n]\!]$, X_i est une variable de Bernoulli de paramètre p, donc si $x_i = 1$, $P(X_i = x_i)$ vaut p et si $x_i = 0$, $P(X_i = x_i)$ vaut $(1 - p)$. Donc si k est le nombre de membres du n-uplet $(x_1, \ldots, x_n)$ valant 1, on a

$$P(A_{(x_1,\ldots,x_n)}) = p^k (1 - p)^{n-k}$$

D'où

$$\begin{aligned} P(X = k) &= \sum_{\substack{(x_1,\ldots,x_n) \in E \\ x_1 + \cdots + x_n = k}} p^k (1 - p)^{n-k} \\ &= \binom{n}{k} p^k (1 - p)^{n-k}. \end{aligned}$$

On peut aussi le montrer par récurrence sur n. En notant $S_n = \sum_{k=1}^{n} X_k$, alors naturellement $S_1 \hookrightarrow \mathscr{B}(1, p)$.

Supposons que $S_{n-1} \hookrightarrow \mathscr{B}(n-1,p)$. Alors X_n est indépendante de $(X_1,\dots,X_{n-1})$ donc de S_{n-1}. Il ne reste plus qu'à montrer que si $Y \hookrightarrow \mathscr{B}(n-1,p)$ est indépendante de X_n, alors $S = X_n + Y \hookrightarrow \mathscr{B}(n,p)$.

Comme $X_1(\Omega) = \{0,1\}$ et $Y(\Omega) = [\![0,n-1]\!]$, alors $S(\Omega) \subset [\![0,n]\!]$. Soit $k \in [\![0,n]\!]$, calculons $P(S=k)$.

— Si $k=0$, $P(S=0) = P([X_n=0]\cap[Y=0])$ et donc par indépendance de X_n et de Y, $P(S=0) = P(X_n=0)P(Y=0) = (1-p)\cdot(1-p)^{n-1} = (1-p)^n$.

— De même, si $k=n$, $P(S=n) = P([X_n=1]\cap[Y=n-1])$ et donc $P(S=n) = P(X_n=1)P(Y=n-1) = p\cdot p^{n-1} = p^n$.

— Si $0<k<n$, alors $([X_n=0],[X_n=1])$ est un système complet d'événements, donc par la formule des probabilités totales

$$\begin{aligned}
P(S=k) &= P([S=k]\cap[X_n=0]) \\
&\quad + P([S=k]\cap[X_n=1]) \\
&= P([Y=k]\cap[X_n=0]) \\
&\quad + P([Y=k-1]\cap[X_n=1]) \\
\text{ind.} &= P(Y=k)P(X_n=0) \\
&\quad + P(Y=k-1)P(X_n=1) \\
&= \binom{n-1}{k} p^k (1-p)^{n-1-k}\cdot(1-p) \\
&\quad + \binom{n-1}{k-1} p^{k-1}(1-p)^{n-1-(k-1)}\cdot p \\
&= p^k(1-p)^{n-k}\left[\binom{n-1}{k} + \binom{n-1}{k-1}\right] \\
&= p^k(1-p)^{n-k}\binom{n}{k}
\end{aligned}$$

par la formule du triangle de Pascal, ce qui permet de conclure.

□

Remarque 2.5.21.
Dans le dernier calcul, on pouvait aussi écrire

$$\begin{aligned}
P(S=k) &= P(S=k|X=0)P(X=0) \\
&\quad + P(S=k|X=1)P(X=1) \\
&= P(Y=k|X=0)P(X=0) \\
&\quad + P(Y=k-1|X=1)P(X=1)
\end{aligned}$$

puis de voir, par indépendance de X et de Y, que $P(Y=k|X=0) = P(Y=k)$ ainsi que $P(Y=k-1|X=1) = P(Y=k-1)$.

Nous n'avons fait que démontrer ceci.

2.6 Espérance

Définition 2.6.1.
Soit X une variable aléatoire réelle. On appelle espérance de X et on note $\mathrm{E}(X)$ la somme

$$\sum_{x\in X(\Omega)} P(X=x)x.$$

On dit qu'une variable aléatoire X est *centrée* si son espérance est nulle.

Remarque 2.6.2.
1. L'espérance est la moyenne des valeurs prises par X, pondérées par leurs probabilités.
2. L'espérance de X ne dépend que de la loi de X, donc deux variables ayant même loi ont même espérance.

Exercice 2.6.3.
On lance deux dés et on note X la somme des deux résultats. Calculer l'espérance de X.

Proposition 2.6.4.
Soit X une variable aléatoire réelle. Alors on a

$$\mathrm{E}(X) = \sum_{\omega\in\Omega} P(\{\,\omega\,\})X(\omega).$$

Démonstration.
Il suffit de remarquer que pour tout $x \in X(\Omega)$, on a $\{\,X=x\,\} = \{\,\omega\in\Omega \mid X(\omega)=x\,\}$, donc

$$P(X=x) = \sum_{\substack{\omega\in\Omega \\ X(\omega)=x}} P(\{\,\omega\,\})$$

On a alors successivement :

$$\begin{aligned}
\mathrm{E}(X) &= \sum_{x\in X(\Omega)} \left(\sum_{\substack{\omega\in\Omega \\ X(\omega)=x}} P(\{\,\omega\,\})\right) x \\
&= \sum_{x\in X(\Omega)} \left(\sum_{\substack{\omega\in\Omega \\ X(\omega)=x}} P(\{\,\omega\,\})X(\omega)\right) \\
&= \sum_{\omega\in\Omega} P(\{\,\omega\,\})X(\omega)
\end{aligned}$$

□

Proposition 2.6.5.
L'espérance est linéaire et positive, donc croissante. Plus précisément, soit X et Y deux variables aléatoires réelles et α et β deux réels.

Alors

$$\mathrm{E}(\alpha X + \beta Y) = \alpha \mathrm{E}(X) + \beta \mathrm{E}(Y)$$

De plus si X est presque sûrement à valeurs positives ($P(X \geqslant 0) = 1$) alors $\mathrm{E}(X) \geqslant 0$.

Enfin, si l'événement $X \leqslant Y$ est presque sûr, alors $\mathrm{E}(X) \leqslant \mathrm{E}(Y)$.

Démonstration.
Les deux premiers points se déduisent immédiatement de la proposition 2.6.3 (pour le second on utilise que pour $x < 0$, on a $P(X = x) \leqslant P(X < 0) = 1 - P(X \geqslant 0) = 0$).

Le troisième se déduit du fait que $\mathrm{E}(Y) = \mathrm{E}(Y - X) + \mathrm{E}(X)$ et que $P(Y - X \leqslant 0) = P(X \leqslant Y) = 1$. □

Remarque 2.6.6.
La propriété précédente s'étend naturellement, par récurrence, à toute combinaison linéaire (finie !) de variables aléatoires.

Remarque 2.6.7.
Si X est une v.a. réelle, alors $X - \mathrm{E}(X)$ est centrée.

Proposition 2.6.8.
Une variable aléatoire positive d'espérance nulle est nulle presque-sûrement.

Démonstration.
On a une somme de termes positifs qui est nulle. □

Proposition 2.6.9 (Espérance des lois usuelles.)**.**
Soit $C \in \mathbb{R}$, $p \in [0,1]$, $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$.

1. L'espérance d'une variable aléatoire constante de valeur C est égale à C.
2. L'espérance d'une variable aléatoire suivant la loi de Bernoulli de paramètre p est p.
3. L'espérance d'une variable aléatoire suivant la loi binomiale de paramètres n et p vaut np.
4. L'espérance d'une variable aléatoire suivant la loi uniforme sur $[\![a, b]\!]$, avec $a < b$, vaut $\dfrac{a+b}{2}$.

Démonstration.
Les deux premiers points se déduisent directement de la définition. Pour le troisième, on sait que l'espérance d'une variable aléatoire ne dépend que de sa loi. Étant donné une variable X sur un espace probabilisé Ω suivant la loi binomiale de paramètres n et p où $n \in \mathbb{N}$ et $p \in [0,1]$, on construit une variable aléatoire Y, sur un autre espace de probabilité Ω', de façon à ce que d'une part Y suive la loi binomiale de paramètres n et p et d'autre part Y s'écrive comme somme de de variables $Y_1, \ldots, Y_n$ de Bernoulli indépendantes, toutes de paramètre p. On a alors

$$\begin{aligned}
\mathrm{E}(X) &= \mathrm{E}(Y) \\
&= \mathrm{E}\left(\sum_{i=1}^{n} Y_i\right) \\
&= \sum_{i=1}^{n} \mathrm{E}(Y_i) \\
&= \sum_{i=1}^{n} p \\
&= np.
\end{aligned}$$

Voici comment construire Ω' et Y. On pose $\Omega' = \{0,1\}^n$ et pour tout $\omega = (\omega_1, \ldots, \omega_n) \in \Omega'$, on pose $p_\omega = \prod_{i=1}^{n} \alpha(\omega_i)$, où $\alpha(0) = 1 - p$ et $\alpha(1) = p$.

On a

$$\begin{aligned}
\sum_{\omega \in \Omega'} p_\omega &= \sum_{(\omega_1, \ldots, \omega_n) \in \{0,1\}^n} \prod_{i=1}^{n} \alpha(\omega_i) \\
&= \prod_{i=1}^{n} \sum_{\omega_i \in \{0,1\}} \alpha(\omega_i) \\
&= \prod_{i=1}^{n} (1 - p + p).
\end{aligned}$$

Ainsi, il existe une probabilité sur Ω' vérifiant pour tout $\omega \in \Omega'$, $P(\{\omega\}) = p_\omega$.

On définit alors, pour $i \in I$, Y_i la variable aléatoire de Bernoulli vérifiant $Y_i(\omega_1, \ldots, \omega_n) = \omega_i$. Alors les Y_i, pour $i = 1, \ldots, n$ sont des variables aléatoires mutuellement indépendantes. En effet, soit x_i pour $i = 1, \ldots, n$ des éléments de $\{0,1\}$.

Soit $i \in [\![1, n]\!]$, on a alors

$$\begin{aligned} P(Y_i = x_i) &= \sum_{\substack{(\omega_1,\dots,\omega_n)\in\{0,1\}^n \\ \omega_i = x_i}} \prod_{j=1}^{n} \alpha(\omega_j) \\ &= \alpha(x_i) \prod_{\substack{j=1 \\ j\neq i}}^{n} \sum_{\omega_j \in \{0,1\}} \alpha(\omega_j) \\ &= \alpha(x_i) \prod_{\substack{j=1 \\ j\neq i}}^{n} (1-p+p) \\ &= \alpha(x_i). \end{aligned}$$

Par ailleurs, on a

$$\begin{aligned} P\left(\bigcap_{i=1}^{n} \{ Y_i = x_i \}\right) &= P(\{ (x_1, \dots, x_n) \}) \\ &= \prod_{i=1}^{n} \alpha(x_i), \end{aligned}$$

donc

$$P\left(\bigcap_{i=1}^{n} \{ Y_i = x_i \}\right) = \prod_{i=1}^{n} P(Y_i = x_i).$$

Concernant le dernier point, il suffit de voir que si $X \hookrightarrow \mathscr{U}([\![a, b]\!])$, alors $X - a \hookrightarrow \mathscr{U}([\![0, b-a]\!])$. Soit donc $n \in \mathbb{N}$ et $Y \hookrightarrow \mathscr{U}([\![0, n]\!])$, alors

$$\mathrm{E}Y = \sum_{k=0}^{n} kP(Y = k) = \frac{1}{n+1} \sum_{k=0}^{n} k = \frac{n}{2},$$

ce qui permet de conclure par $\mathrm{E}X = \mathrm{E}[X - a] + a = \dfrac{b-a}{2} + a = \dfrac{a+b}{2}$. □

Proposition 2.6.10 (Formule de transfert)**.**
Soit X une variable aléatoire à valeur dans E et $f : X(\Omega) \to \mathbb{R}$. Alors

$$\mathrm{E}[f(X)] = \sum_{x \in X(\Omega)} P(X = x) f(x)$$

Démonstration.
On a déjà noté que pour tout $x \in X(\Omega)$, on a

$$P(X = x) = \sum_{\substack{\omega\in\Omega \\ X(\omega)=x}} P(\{ \omega \}).$$

En posant $s = \sum_{x \in X(\Omega)} P(X = x) f(x)$, on a alors successivement :

$$\begin{aligned} s &= \sum_{x \in X(\Omega)} \left(\sum_{\substack{\omega\in\Omega \\ X(\omega)=x}} P(\{ \omega \}) \right) f(x) \\ &= \sum_{x \in X(\Omega)} \left(\sum_{\substack{\omega\in\Omega \\ X(\omega)=x}} P(\{ \omega \}) f(X(\omega)) \right) \\ &= \sum_{\omega \in \Omega} P(\{ \omega \}) f(X)(\omega) \\ &= \mathrm{E}[f(X)]. \end{aligned}$$

□

Remarque 2.6.11.
La formule de transfert montre que $\mathrm{E}[f(X)]$ dépend juste de la loi de X et de f. Pour calculer cette espérance, nul besoin d'obtenir la loi de $f(X)$!

Exercice 2.6.12.
Si $X \hookrightarrow \mathscr{U}([\![0, n]\!])$, calculer $\mathrm{E}[X^2]$.

Proposition 2.6.13 (Espérance de variables indépendantes)**.**
Soit X et Y deux variables à valeurs réelles indépendantes. Alors $\mathrm{E}(XY) = \mathrm{E}(X)\mathrm{E}(Y)$.

Démonstration.
On a, par la formule de transfert (appliquée à (X, Y) et à $(x, y) \mapsto xy$),

$$\begin{aligned} \mathrm{E}(XY) &= \sum_{(x,y)\in X(\Omega)\times Y(\Omega)} P((X, Y) = (x, y))xy \\ &= \sum_{(x,y)\in X(\Omega)\times Y(\Omega)} P(X = x)P(Y = y)xy \\ &= \sum_{x\in X(\Omega))} P(X = x)x \times \sum_{y\in Y(\Omega)} P(Y = y)y \\ &= \mathrm{E}(X)\mathrm{E}(Y) \end{aligned}$$

□

Remarque 2.6.14.
La réciproque est bien entendu fausse. Considérez par exemple la variable $X \hookrightarrow \mathscr{U}(-1, 0, 1)$ et $Y = X^2$.

Remarque 2.6.15.
Cela se généralise : si $X_1, \dots, X_n$ sont des v.a. réelles mutuellement indépendantes, alors $\mathrm{E}[X_1 \dots X_n] = \mathrm{E}[X_1] \dots \mathrm{E}[X_n]$.

Proposition 2.6.16 (Inégalité de Markov)**.**
Soit X une variable aléatoire réelle à *valeurs positives* presque-sûrement. Soit $t \in \mathbb{R}_+^*$. On a :

$$P(X \geqslant t) \leq \frac{\mathrm{E}(X)}{t}.$$

Démonstration.
On a

$$\begin{aligned}
\mathrm{E}(X) &= \sum_{\omega \in \Omega} P(\{\,\omega\,\})X(\omega) \\
&= \sum_{\substack{\omega \in \Omega \\ X(\omega) \geqslant t}} P(\{\,\omega\,\})X(\omega) + \sum_{\substack{\omega \in \Omega \\ X(\omega) < t}} P(\{\,\omega\,\})X(\omega) \\
&\geqslant \sum_{\substack{\omega \in \Omega \\ X(\omega) \geqslant t}} P(\{\,\omega\,\})X(\omega) \\
&\geqslant \sum_{\substack{\omega \in \Omega \\ X(\omega) \geqslant t}} P(\{\,\omega\,\})t \\
&\geqslant tP(\{\,\omega \in \Omega \mid X(\omega) \geqslant t\,\}) \\
&\geqslant tP(X \geqslant t)
\end{aligned}$$

Sinon, il suffit de voir que $t\mathbf{1}_{X \geqslant t}$ est une variable aléatoire inférieure à X p.s, puis de considérer son espérance ... □

Remarque 2.6.17.
C'est une inégalité fondamentale en probabilité, vous la retrouverez de nombreuses fois : retenez la bien !

Exemple 2.6.18.
n étudiants ont travaillé au mois de juillet dernier. En moyenne, leur travail leur a rapporté 750 euros chacun. Donner un majorant de la proportion d'étudiants ayant gagné au moins 1000 euros.

2.7 Variance, écart type et covariance

Définition 2.7.1 (Moments)**.**
Soit X une variable aléatoire réelle. Soit $r \in \mathbb{N}^*$.

On appelle moment d'ordre r de X et on note $m_r(X)$ l'espérance de X^r :

$$m_r(X) = \mathrm{E}(X^r).$$

On appelle moment centré d'ordre r de X et on note $\mu_r(X)$ le moment d'ordre r de $X - \mathrm{E}(X)$:

$$\mu_r(X) = \mathrm{E}((X - \mathrm{E}(X))^r).$$

On appelle variance de X et on note $V(X)$ son moment centré d'ordre 2 :

$$V(X) = \mathrm{E}\Big((X - \mathrm{E}(X))^2\Big).$$

On appelle écart-type de X et on note $\sigma(X)$ la racine carrée de la variance :

$$\sigma(X) = \sqrt{V(X)}.$$

On dit que X est une variable aléatoire *réduite* si sa variance est 1.

Remarque 2.7.2.
1. Les moments et les moments centrés ne dépendent que de la loi de X.
2. Intuitivement la variance mesure la « moyenne » du carré des écarts à la « moyenne ». C'est donc une mesure de la dispersion des valeurs autour de la valeur moyenne prise par la variable aléatoire X. Si la variable X est exprimée dans une unité u, la variance sera exprimée dans l'unité u^2 (et l'écart-type dans l'unité u).

Proposition 2.7.3 (Formule de König-Huygens)**.**
Soit X une variable aléatoire réelle. Alors la variance est la différence entre l'espérance de son carré et le carré de son espérance :

$$V(X) = \mathrm{E}(X^2) - \mathrm{E}(X)^2.$$

Démonstration.
Il suffit d'utiliser la définition, la linéarité de l'espérance

et le résultat sur l'espérance d'une variable constante pour obtenir successivement :

$$\begin{aligned} V(X) &= \mathrm{E}\big((X-\mathrm{E}(X))^2\big) \\ &= \mathrm{E}\big(X^2 - 2\mathrm{E}(X)X + \mathrm{E}(X)^2\big) \\ &= \mathrm{E}\big(X^2\big) - 2\mathrm{E}(X)\mathrm{E}(X) + \mathrm{E}(X)^2 \\ &= \mathrm{E}\big(X^2\big) - \mathrm{E}(X)^2. \end{aligned}$$

□

Proposition 2.7.4.
Soit X une variable aléatoire réelle, et a et b deux réels.

Alors

$$\begin{aligned} \mathrm{E}(aX+b) &= a\mathrm{E}(X) + b, \\ V(aX+b) &= a^2 V(X), \\ \sigma(aX+b) &= |a|\sigma(X). \end{aligned}$$

En particulier, si $\sigma(X) \neq 0$, la variable Y définie par

$$Y = \frac{X - \mathrm{E}(X)}{\sigma(X)}$$

est une variable centrée réduite.

Démonstration.
On connaît déjà le premier point. Il suffit de remplacer par les définitions et de calculer pour conclure pour les autres. □

Proposition 2.7.5 (Variance des lois usuelles)**.**
Soit $p \in [0,1]$ et $n \in \mathbb{N}^*$.

1. Toute variable aléatoire constante p.s. est de variance nulle.
2. Toute variable aléatoire réelle suivant la loi de Bernoulli de paramètre p a pour variance $p(1-p)$.
3. Toute variable aléatoire réelle suivant la loi binomiale de paramètres p et n a pour variance $np(1-p)$.
4. Toute variable aléatoire rélle suivant la loi uniforme sur $[\![1,n]\!]$, a pour variance $\dfrac{n^2-1}{12}$.

Démonstration. 1. Direct.

2. Considérons X une variable aléatoire réelle suivant la loi de Bernoulli de paramètre p. Alors $V(X) = E(X^2) - E(X)^2$. Or $P(X^2 = 1) = P(X = 1) = p$ et donc $E(X^2) = p$. Donc $V(X) = p - p^2 = p(1-p)$.
3. Soit X une variable aléatoire réelle suivant la loi binomiale de paramètres p et n. Alors on peut construire une variable aléatoire réelle Y de même loi que X, donc de même variance, de façon que Y soit la somme de n variables de Bernoulli $Y_1, \ldots, Y_n$ de paramètre p mutuellement indépendantes.

   On verra plus loin que *dans le cas particulier de variables deux à deux indépendantes*, la variance de la somme est égale à la somme des variances. on a donc ici :

$$V(Y) = \sum_{i=1}^{n} V(Y_i) = np(1-p)$$

4. Faisons le calcul dans le cas général $X \hookrightarrow \mathscr{U}([\![a,b]\!])$, avec $a < b$. $X - a \hookrightarrow \mathscr{U}([\![0, b-a]\!])$ et $V(X-a) = V(X)$. Soit $Y \hookrightarrow \mathscr{U}([\![0,n]\!])$, avec $n \in \mathbb{N}$, calculons $V(Y)$. Par la formule de König-Huygens, $V(Y) = \mathrm{E}\left[Y^2\right] - \mathrm{E}\left[Y\right]^2 = \mathrm{E}\left[Y^2\right] - \dfrac{n^2}{4}$. De plus, par la formule de transfert,

$$\begin{aligned} \mathrm{E}\left[Y^2\right] &= \sum_{k=0}^{n} k^2 P(Y=k) \\ &= \frac{1}{n+1}\sum_{k=0}^{n} k^2 \\ &= \frac{n(2n+1)}{6}. \end{aligned}$$

   Ainsi,

$$V(Y) = \frac{2n(2n+1)}{12} - \frac{3n^2}{12} = \frac{n(n+2)}{12}.$$

   Donc $V(X) = \dfrac{(b-a)(b-a+2)}{12}$ et l'on retrouve bien l'énoncé avec $b = n$ et $a = 1$.

□

Théorème 2.7.6 (Inégalité de Bienaymé-Tchebychev)**.**
Soit X une variable aléatoire réelle, $V(X)$ sa variance, soit $\varepsilon > 0$. Alors

$$P(|X - \mathrm{E}X| \geqslant \varepsilon) \leqslant \frac{V(X)}{\varepsilon^2}.$$

Démonstration.
Il suffit de constater que $(X - \mathrm{E}X)^2$ est une v.a. positive, donc d'après l'inégalité de Markov :

$$\begin{aligned} P(|X - \mathrm{E}X| \geqslant \varepsilon) &= P\big((X - \mathrm{E}X)^2 \geqslant \varepsilon^2\big) \\ &\leqslant \frac{\mathrm{E}\left[(X - \mathrm{E}X)^2\right]}{\varepsilon^2} \\ &\leqslant \frac{V(X)}{\varepsilon^2}. \end{aligned}$$

□

Remarque 2.7.7.
Cette inégalité contrôle la déviation d'une variable aléatoire par rapport à sa moyenne. C'est un résultat fondamental !

Corollaire 2.7.8.
Une variable aléatoire de variance nulle est constante presque-sûrement.

Démonstration.
Remarquons que $(X - \mathrm{E}[X])^2$ est positive, donc si $V(X) = 0$ alors p.s. $(X - \mathrm{E}[X])^2 = 0$, en utilisant le résultat **??**. Ainsi p.s. $X = \mathrm{E}[X]$. □

Définition 2.7.9 (Covariance)**.**
Soit X et Y deux variables aléatoires réelles. On appelle covariance de X et Y et on note $\mathrm{Cov}(X, Y)$ le réel

$$\mathrm{Cov}(X, Y) = \mathrm{E}((X - \mathrm{E}X)(Y - \mathrm{E}Y)).$$

Si $\mathrm{Cov}(X, Y) = 0$, on dit que X et Y sont décorrélées.

Remarque 2.7.10.
$\mathrm{Cov}(X, X)$ n'est autre que $V(X)$ et $\mathrm{Cov}(X, Y) = \mathrm{Cov}(Y, X)$.

Remarque 2.7.11.
Si $\sigma(X) = 0$, nous avons vu que $X = \mathrm{E}[X]$ p.s, donc $\mathrm{Cov}(X, Y) = 0$.

Si $\sigma(X)$ et $\sigma(Y)$ ne sont pas nuls, on définit le *coefficient de corrélation* de X et de Y par

$$\rho(X, Y) = \frac{\mathrm{Cov}(X, Y)}{\sigma(X)\sigma(Y)}.$$

L'inégalité de Cauchy-Schwarz (que nous verrons bientôt) permet de montrer deux résultats intéressants :

- $\rho(X, Y) \in [-1, 1]$;
- si $|\rho(X, Y)| = 1$, alors il existe $a, b, c \in \mathbb{R}$ tels que $aX + bY = c$ p.s, *i.e.* X et Y sont p.s. en relation affine.

On montre aussi facilement que, si l'on résout le *problème de régression affine de Y sur X par moindres carrés*, *i.e.* si l'on minimise en $a, b \in \mathbb{R}$ la quantité :

$$\mathrm{E}\left[(Y - aX - b)^2\right],$$

alors le coefficient a optimal (c'est la pente de la droite de régression de Y sur X) est

$$a = \frac{\mathrm{Cov}(X, Y)}{V(X)} = \rho(X, Y) \times \frac{\sigma(Y)}{\sigma(X)}.$$

Remarquons que, dans ce cas, effectuer la régression de Y sur X n'est pas la même chose que d'effectuer la régression de X sur Y !

Si X et Y sont centrées-réduites (en pratique, il convient souvent de centrer-réduire ses données avant d'effectuer un traitement statistique dessus), on s'aperçoit que

$$a = \rho(X, Y).$$

Exercice 2.7.12.
Soit (Ω, P) un espace probabilisé fini, X une variable aléatoire réelle définie sur Ω et f une fonction réelle croissante.

Montrer que $\mathrm{Cov}(X, f(X)) \geqslant 0$.

Proposition 2.7.13.
Soit X et Y deux variables aléatoires réelles. Alors on a

$$\mathrm{Cov}(X, Y) = \mathrm{E}(XY) - \mathrm{E}(X)\mathrm{E}(Y).$$

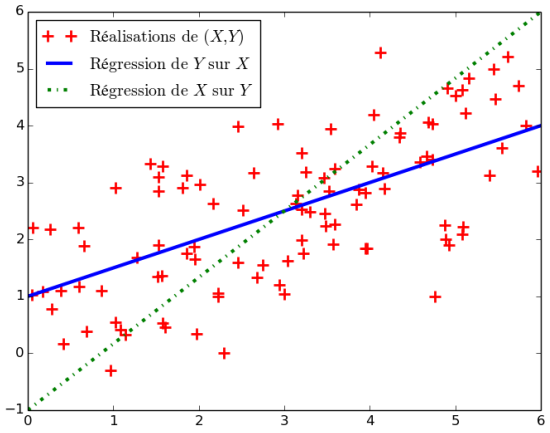


FIGURE XXII.2 – Exemple de régression affine par moindres carrés, ici $\rho(X,Y) = \sqrt{\frac{3}{7}} \approx 0,65$.

Démonstration.
Comme pour la formule de König-Huygens :

$$\begin{aligned}\mathrm{Cov}(X,Y) &= \mathrm{E}(X-\mathrm{E}X)(Y-\mathrm{E}Y)\\ &= \mathrm{E}(XY - X\mathrm{E}Y - Y\mathrm{E}X + \mathrm{E}X\mathrm{E}Y)\\ &= \mathrm{E}(XY) - \mathrm{E}(X)\mathrm{E}(Y) - \mathrm{E}(X)\mathrm{E}(Y) + \mathrm{E}(X)\mathrm{E}(Y)\\ &= \mathrm{E}(XY) - \mathrm{E}(X)\mathrm{E}(Y).\end{aligned}$$

□

Remarque 2.7.14.
Par la formule de transfert,

$$\mathrm{E}[XY] = \sum_{x\in X(\Omega),\ y\in Y(\Omega)} xyP(X=x, Y=y).$$

Corollaire 2.7.15.
Deux variables aléatoires indépendantes ont une covariance nulle.

Remarque 2.7.16.
Comme montré par l'exemple $X \hookrightarrow \mathscr{U}(-1,0,1)$ et $Y = X^2$, deux variables peuvent être non corrélées mais sans être indépendantes.

Proposition 2.7.17.
Soit $n \in \mathbb{N}$ et $X_1, \ldots, X_n$ n variables aléatoires réelles. Alors on a

$$V(\sum_{i=1}^{n} X_i) = \sum_{i=1}^{n} V(X_i) + 2 \sum_{1\leqslant i<j\leqslant n} \mathrm{Cov}(X_i, X_j).$$

Démonstration.
Posons, pour $i = 1, \ldots, n$, $Y_i = X_i - \mathrm{E}(X_i)$ et $X = \sum_{i=1}^{n} X_i$.
On a :

$$\begin{aligned}V(X) &= \mathrm{E}\left(\left(\sum_{i=1}^{n} Y_i\right)^2\right)\\ &= \mathrm{E}\left(\sum_{i=1}^{n} Y_i^2 + 2\sum_{1\leqslant i<j\leqslant n} Y_iY_j\right)\\ &= \sum_{i=1}^{n} \mathrm{E}\left(Y_i^2\right) + 2\sum_{1\leqslant i<j\leqslant n} \mathrm{E}(Y_iY_j)\\ &= \sum_{i=1}^{n} V(X_i) + 2\sum_{1\leqslant i<j\leqslant n} \mathrm{Cov}(X_i, X_j).\end{aligned}$$

□

Corollaire 2.7.18.
Dans le cas particulier où les variables $X_1, \ldots, X_n$ sont deux à deux décorrélées, la variance de leur somme est égale à la somme de leurs variances.

Remarque 2.7.19.
On déduit de ce résultat la variance de la loi binomiale, comme on l'a vu plus haut.

Chapitre XXIII

Calcul matriciel

Dans tout ce chapitre et sauf mention expresse du contraire, n, m, p, q, r et t désignent des entiers naturels non nuls, et $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

1 Structure de $\mathscr{M}_{n,p}(\mathbb{K})$

1.1 Rappels

a Définitions élémentaires

Définition 1.1.1.
On appelle *matrice de taille* $n \times p$ (ou à n lignes et p colonnes), à valeurs (ou coefficients) dans $\mathbb{K}$, toute famille de np éléments de $\mathbb{K}$, ces éléments étant notés $(a_{ij})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant p}$, et présentés sous la forme d'un tableau de la manière suivante :

$$A = \begin{pmatrix} a_{1,1} & \dots & a_{1,p} \\ \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,p} \end{pmatrix}.$$

On note $A = (a_{ij})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant p}$, les $(a_{i,j})$ étant les *coefficients* de la matrice A, $a_{i,j}$ étant le coefficient de la i^{e} ligne et de la j^{e} colonne.

La matrice $(a_{i,j})_{1\leqslant j\leqslant n}$ est la i^{e} ligne de A, parfois notée $a_{i,*}$.

La matrice $(a_{i,j})_{1\leqslant i\leqslant n}$ est la j^{e} colonne de A, parfois notée $a_{*,j}$.

Remarque 1.1.2.
Le premier indice indique toujours la ligne et le second indice indique toujours la colonne. En général (mais attention quand même), on les note respectivement i et j.

Exemple 1.1.3.
Donner la matrice $(i \times j)_{1\leqslant i\leqslant 3, 1\leqslant j\leqslant 5}$.

Définition 1.1.4.
- L'ensemble des matrices de taille $n \times p$ est noté $\mathscr{M}_{n,p}(\mathbb{K})$.
- On appelle *matrice carrée d'ordre* n toute matrice de taille $n \times n$. L'ensemble des matrices carrées d'ordre n est noté $\mathscr{M}_n(\mathbb{K})$.
- On appelle *matrice nulle d'ordre* n la matrice carrée d'ordre n dont tous les coefficients sont nuls. On la note simplement 0_n, ou 0 sans référence à sa taille s'il n'y a pas d'ambiguïté.
- On appelle *matrice identité d'ordre* n la matrice $(\delta_{i,j})_{1\leqslant i,j\leqslant n}$. On la note I_n, ou Id_n.
- On appelle *matrice diagonale* toute matrice carrée $(a_{ij})_{1\leqslant i,j\leqslant n}$ telle que pour tous $i, j \in [\![1, n]\!]$, $i \neq j \Rightarrow a_{i,j} = 0$.
- On appelle *matrice triangulaire supérieure* (resp. *inférieure*) toute matrice carrée $(a_{ij})_{1\leqslant i,j\leqslant n}$ telle que pour tous $i, j \in [\![1, n]\!]$ tells que $i > j$ (resp. $i < j$), $a_{ij} = 0$.

Remarque 1.1.5.
1. On note généralement les matrices par des lettres majuscules, et la famille des coefficients par la lettre minuscule correspondante.
2. On identifie les matrices colonnes de $\mathscr{M}_{n,1}(\mathbb{K})$ avec les éléments de $\mathbb{K}^n$.
3. On se gardera d'identifier les matrices lignes avec les éléments de $\mathbb{K}^n$ car on préfère les identifier avec d'autres objets mathématiques (on verra cela plus tard).

b Opérations sur les matrices

Définition 1.1.6.
Soient $A = (a_{ij})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant p}$ et $B = (b_{ij})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant p}$ deux matrices **de même taille**, et $\lambda \in \mathbb{K}$ un scalaire.

Addition On appelle *somme* de A et B la matrice $(a_{ij} + b_{ij})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant p}$, notée $A + B$.

Produit par un scalaire On note λA la matrice $(\lambda a_{ij})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant p}$.

 Attention aux tailles des matrices : on ne peut additionner n'importe quoi avec n'importe quoi.

Exemple 1.1.7.
$\begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} + 2\begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 1 \\ 1 & 8 \end{pmatrix}$.

Définition 1.1.8 (Produit matriciel)**.**
Soient $A \in \mathscr{M}_{n,p}(\mathbb{K})$ et $B \in \mathscr{M}_{p,q}(\mathbb{K})$. On appelle *produit de A par B noté AB* la matrice de $\mathscr{M}_{n,q}(\mathbb{K})$ de coefficients $\left(\sum_{k=1}^{p} a_{ik}b_{kj}\right)$.

 Gare aux dimensions, on ne peut pas multiplier n'importe quelle matrices.

Exemple 1.1.9. — On tâchera d'organiser les produits comme suit :

$$\begin{array}{cc} & \overbrace{\begin{pmatrix} 1 & 0 & 2 \\ -1 & 3 & 2 \end{pmatrix}}^{B} \\ \underbrace{\begin{pmatrix} 2 & 1 \\ 1 & 0 \\ 4 & 2 \end{pmatrix}}_{A} & \underbrace{\begin{pmatrix} 1 & 3 & 6 \\ 1 & 0 & 2 \\ 2 & 6 & 12 \end{pmatrix}}_{=AB} \end{array}$$

— Le produit impossible :

$$\begin{pmatrix} 1 & 3 & 0 \\ 2 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix}.$$

 Ce produit comporte plein de pièges :
• Il n'est pas commutatif, par exemple : $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Et même pire, AB peut exister mais pas BA.
• Le produit de deux matrices non nulles peut valoir la matrice nulle. Exemple : $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, alors $AA = 0$, $AB = 0$ et $BA \neq 0$.
• On ne peut pas « simplifier » dans un produit. Ici : $A \times A = A \times B$ mais $A \neq B$.

Proposition 1.1.10.
Le produit matriciel est :

Associatif : si $A \in \mathscr{M}_{n,p}(\mathbb{K})$, $B \in \mathscr{M}_{p,q}(\mathbb{K})$, $C \in \mathscr{M}_{q,r}(\mathbb{K})$, alors $(AB)C$ et $A(BC)$ sont dans $\mathscr{M}_{n,r}(\mathbb{K})$ et sont égales, notées ABC.

Bilinéaire : si A, B, C, D sont des matrices de taille convenable, et si $\lambda \in \mathbb{K}$, alors $(A + \lambda B)C = AC + \lambda BC$ et $A(C + \lambda D) = AC + \lambda AD$.

Les matrices nulles et identité jouent un rôle bien particulier. Si $A \in \mathscr{M}_{n,p}(\mathbb{K})$ et $q \in \mathbb{N}^*$, alors

Neutre à gauche : $I_n A = A$

Neutre à droite : $AI_p = A$

Mult. par 0 à gauche : $0_{q,n}A = 0_{q,p}$

Mult. par 0 à droite : $A0_{p,q} = 0_{n,q}$

Démonstration.
Bien qu'un peu technique, nous donnons ici la démonstration ; nous en verrons plus tard une autre.

1. $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij})$. Ainsi,
$$BC = \left(\sum_{k=1}^{q} b_{ik}c_{kj}\right)_{1\leqslant i\leqslant p, 1\leqslant j\leqslant r}$$
et
$$A(BC) = \left(\sum_{\ell=1}^{p} a_{i\ell} \times \left(\sum_{k=1}^{q} b_{\ell k}c_{kj}\right)\right)_{1\leqslant i\leqslant n, 1\leqslant j\leqslant r}.$$
Or, si $1 \leqslant i \leqslant n$ et $1 \leqslant j \leqslant r$,
$$\begin{aligned} \sum_{\ell=1}^{p} a_{i\ell} \times \left(\sum_{k=1}^{q} b_{\ell k}c_{kj}\right) &= \sum_{\ell=1}^{p} a_{i\ell} \times \sum_{k=1}^{q} b_{\ell k}c_{kj} \\ &= \sum_{\ell=1}^{p}\sum_{k=1}^{q} a_{i\ell}b_{\ell k}c_{kj} \\ &= \sum_{k=1}^{q}\sum_{\ell=1}^{p} a_{i\ell}b_{\ell k}c_{kj} \\ &= \sum_{k=1}^{q}\left(\sum_{\ell=1}^{p} a_{i\ell}b_{\ell k}\right) \times c_{kj}, \end{aligned}$$
qui est le coefficient i, j de $(AB)C$. D'où l'égalité voulue.
2. *idem*
3. $I_n A = \left(\sum_{k=1}^{n} \delta_{ik}a_{kj}\right) = (\delta_{ii}a_{ij}) = (a_{ij}) = A$.

4. Direct.

□

Remarque 1.1.11.
Par associativité, il y a 5 manières de calculer $ABCD$ qui conduisent toutes au même résultat : $((AB)C)D = (A(BC))D = A((BC)D) = A(B(CD)) = (AB)(CD)$. Mais le temps de calcul est-il le même dans les 5 cas ? C'est le problème de la *multiplication matricielle enchaînée* (Matrix chain multiplication ou Matrix Chain Ordering Problem (MCOP) en anglais). Plus généralement, le problème est de savoir dans quel ordre effectuer les produits pour calculer le plus efficacement possible un produit de matrices $M_1.M_2.\cdots.M_n$. Ce problème peut se résoudre par programmation dynamique, ce qui est au programme en option informatique, mais même si ce n'est pas toujours la solution optimale, il vaut mieux commencer par les produits qui font apparaître des « petites » matrices.

Précisément, le produit d'une matrice $n \times p$ par une matrice $p \times q$ nécessite de l'ordre de $n \times p \times q$ opérations. Ainsi, si $A \in \mathscr{M}_{10,100}(\mathbb{K})$, $B \in \mathscr{M}_{100,5}$ et $C \in \mathscr{M}_{5,50}$, le calcul de $(AB)C$ demande de l'ordre de $(10 \times 100 \times 5) + 10 \times 5 \times 50 = 7\,500$ opérations, alors que celui de $A(BC)$ en demande de l'ordre de $100 \times 5 \times 50 + 10 \times 100 \times 50 = 75\,000$.

c Matrices carrées

Théorème 1.1.12.
$(\mathscr{M}_n(\mathbb{K}), +, \times)$ est un anneau, et le neutre de $\times$ est I_n.

Démonstration.
On a déjà vu que $\mathscr{M}_n(\mathbb{K})$ était un groupe abélien. Or on a de plus les propriétés suivantes :

1. $(\mathscr{M}_n(\mathbb{K}), \times)$ est un monoïde (le produit est une loi de composition interne associative et la matrice identité est neutre pour cette loi).
2. la multiplication est distributive à gauche et à droite par rapport à l'addition.

□

 Rappel :

1. cet anneau n'est pas commutatif ;
2. il n'est pas intègre, d'une part parce qu'il n'est pas commutatif et d'autre part aussi parce qu'on peut trouver des matrices non-nulles dont le produit est nul.

Maintenant que l'on sait que $(\mathscr{M}_n(\mathbb{K}), +, \times)$ est un anneau, on peut utiliser les résultats démontrés dans le chapitre sur les anneaux.

Définition 1.1.13 (Puissances d'une matrice carrée)**.**
On les définit par récurrence : si $M \in \mathscr{M}_n(\mathbb{K})$, alors, $M^0 = \mathrm{I}_n$, $M^1 = M$, et pour tout $k \in \mathbb{N}$, $M^{k+1} = M \times M^k$ (on a donc, pour tout $k \in \mathbb{N}^*$, $M^k = \underbrace{M \times M \ldots \times M}_{k \text{ fois}}$. Ainsi pour tout $k \in \mathbb{N}$, on a $M^n \in \mathscr{M}_n(\mathbb{K})$.

Remarque 1.1.14.
On remarque que les puissances d'une même matrice commutent entre elles :

$$\begin{aligned} M^k \times M^j &= \underbrace{M \times M \ldots \times M}_{k \text{ fois}} \times \underbrace{M \times M \ldots \times M}_{j \text{ fois}} \\ &= \underbrace{M \times M \ldots \times M}_{(k+j) \text{ fois}} \\ &= \underbrace{M \times M \ldots \times M}_{j \text{ fois}} \times \underbrace{M \times M \ldots \times M}_{k \text{ fois}} \\ &= M^j \times M^k. \end{aligned}$$

Théorème 1.1.15 (Formule du binôme de Newton)**.**
Elle est valable pour les matrices *carrées qui* ***commutent***.

 Il s'agit de ne jamais oublier de vérifier que deux matrices cummutent avant de pouvoir utiliser cette formule.

Exemple 1.1.16.
Calculer A^2 avec

$$\begin{aligned} A &= \begin{pmatrix} 1 & 1 & 1 \\ 2 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 1 \\ 2 & -1 & 0 \\ 0 & -2 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 2 & 0 \end{pmatrix} \\ &= B + C. \end{aligned}$$

Calculer A^3 avec

$$\begin{aligned} A &= \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 4 & 6 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 1 & 2 \end{pmatrix} + \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 3 & 4 \end{pmatrix} \\ &= B + C. \end{aligned}$$

La définition d'inversibilité donnée en début d'année est exactement celle qu'on a donnée dans le chapitre sur les anneaux.

Définition 1.1.17.
Soit $A \in \mathscr{M}_n(\mathbb{K})$. On dit que A est *inversible* s'il existe une matrice $B \in \mathscr{M}_n(\mathbb{K})$ telle que $AB = BA = \mathrm{I}_n$.
Dans ce cas B est unique, est appelée *l'inverse de* A et est notée A^{-1}.

Il est utile de connaître le résultat suivant.

Proposition 1.1.18 (Critère et formule d'inversibilité d'une matrice 2×2)**.**
$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est inversible si et seulement si son *déterminant* est non nul, *i.e.* $ad - bc \neq 0$. Alors, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \dfrac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Démonstration.
On a déjà fait la preuve par le calcul, par exemple en se fondant sur la relation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 - (a+d) \begin{pmatrix} a & b \\ c & d \end{pmatrix} + (ad - bc) I_2 = 0.$$

On en verra une preuve plus générale dans le chapitre traitant les déterminants. □

Exemple 1.1.19.
À vous de construire votre exemple !

On a déjà vu que l'ensemble des inversibles, muni de la multiplication, constituait un groupe.

Définition 1.1.20.
Le groupe des inversibles de $\mathscr{M}_n(\mathbb{K})$ est appelé *le groupe linéaire d'ordre* n et est noté $\mathscr{GL}_n(\mathbb{K})$.

1.2 Structure d'espace vectoriel

Théorème 1.2.1.
$(\mathscr{M}_{n,p}(\mathbb{K}), +, .)$ est un $\mathbb{K}$-espace vectoriel de base $(E_{i,j})_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]}$, avec $E_{i,j} = (\delta_{ki} \times \delta_{\ell j})_{(k,\ell)}$. En particulier

$$\dim_{\mathbb{K}} \mathscr{M}_{n,p}(\mathbb{K}) = np.$$

La base $(E_{i,j})_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]}$ est la *base canonique* de $\mathscr{M}_{n,p}(\mathbb{K})$.

Démonstration.
On a déjà vu qu'il s'agissait d'un $\mathbb{K}$-ev puisque :

1. $(\mathscr{M}_{n,p}(\mathbb{K}), +)$ est un groupe abélien ($+$ est une loi de composition interne, associative, commutative, admettant un élément neutre — la matrice nulle — et pour laquelle tout élément admet un opposé — la matrice de coefficients opposés).
2. Pour toute $M \in \mathscr{M}_{n,p}(\mathbb{K})$, $1 \cdot M = M$.
3. Le produit externe est distributif à droite par rapport à l'addition.
4. Le produit externe est distributif à gauche par rapport à l'addition.
5. On a la propriété d'associativité mixte.

Il reste à montrer que la famille des $(E_{i,j})_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]}$ en est une base.

Pour cela, il suffit de remarquer que pour toute matrice M, de coefficients $(m_{ij})_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]}$, on a

$$M = \sum_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]} m_{ij}E_{ij}.$$

On en déduit donc :

— d'une part que toute matrice M s'écrit d'au moins une façon comme combinaison linéaire des E_{ij} pour $(i,j) \in [\![1,n]\!] \times [\![1,p]\!]$ et que la famille (E_{ij}) est génératrice ;

— d'autre part que toute combinaison linéaire des (E_{ij}) est égale à une matrice dont les coefficients sont ceux de la combinaison linéaire, qu'en conséquence toute combinaison linéaire $\sum_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]}\lambda_{ij}E_{ij}$ de valeur nulle est aussi égale à la matrice des $(\lambda_{ij})_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]}$ qui ne peut donc avoir que des coefficients tous nuls et que la famille des (E_{ij}) est donc libre.

□

1.3 Remarques sur le produit

a Produit par un vecteur colonne

Remarque 1.3.1.
Soit $M \in \mathscr{M}_{n,p}(\mathbb{K})$ et

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}.$$

Alors, en notant $C_1,\ldots,C_p$ les colonnes de M, on a

$$MX = \sum_{k=1}^{p} x_k C_k.$$

En particulier :

— la matrice MX est une combinaison linéaire des C_k, pour $k \in [\![1,p]\!]$,

— pour tout $i \in [\![1,p]\!]$, le produit ME_i où E_i est le i^{e} vecteur de la base canonique de $\mathscr{M}_{p,1}(\mathbb{K})$ est exactement C_i. En effet

$$ME_i = M\begin{pmatrix} \delta_{1i} \\ \vdots \\ \delta_{pi} \end{pmatrix} = \sum_{k=1}^{p} \delta_{ki}C_k = C_i.$$

b Colonnes d'un produit

Proposition 1.3.2.
Soient $A \in \mathscr{M}_{n,p}(\mathbb{K})$ et $B \in \mathscr{M}_{p,q}(\mathbb{K})$. Soit $\alpha \in [\![1,q]\!]$. Notons C_α la α^{e} colonne de B. Alors la α^{e} colonne de AB est la matrice AC_α.

Démonstration.
Le produit AB est la matrice de coefficients

$$\left(\sum_{k=1}^{p} a_{ik}b_{kj}\right)_{(i,j)\in[\![1,n]\!]\times[\![1,q]\!]},$$

qui possède q colonnes, comme B. La α^{e} colonne de cette matrice existe donc et a pour coefficients

$$\left(\sum_{k=1}^{p} a_{ik}b_{k\alpha}\right)_{i\in[\![1,n]\!]}.$$

Notons $c_1,\ldots,c_p$ les coefficients de C_α. La matrice AC_α est la matrice colonne de coefficients

$$\left(\sum_{k=1}^{p} a_{ik}c_k\right)_{i\in[\![1,n]\!]}.$$

Or C_α est la α^{e} colonne de B, donc pour tout $k \in [\![1,p]\!] c_k = b_{k\alpha}$.

AC_α a donc même coefficients que la α^{e} colonne de AB, elle lui est donc égale. □

c Application canoniquement associée

Définition 1.3.3.
Soit $M \in \mathscr{M}_{n,p}(\mathbb{K})$. On appelle *application linéaire canoniquement associée à M* l'application

$$u : \left\{ \begin{array}{ccc} \mathscr{M}_{p,1}(\mathbb{K}) & \longrightarrow & \mathscr{M}_{n,1}(\mathbb{K}) \\ X & \longmapsto & MX \end{array} \right.$$

ou, en identifiant $\mathbb{K}^p$ avec $\mathscr{M}_{p,1}(\mathbb{K})$ et $\mathbb{K}^n$ avec $\mathscr{M}_{n,1}(\mathbb{K})$:

$$u : \left\{ \begin{array}{ccc} \mathbb{K}^p & \longrightarrow & \mathbb{K}^n \\ (x_1,\ldots,x_p) & \longmapsto & M\begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \end{array} \right..$$

Proposition 1.3.4.
Cette application est bien une application linéaire.

Démonstration.
Pour tout $(X,Y)\in\mathscr{M}_{p,1}(\mathbb{K})$ et tout $\lambda\in\mathbb{K}$, on a

$$\begin{aligned}u(\lambda X+Y)&=M(\lambda X+Y)\\&=\lambda(MX)+MY\\&=\lambda u(X)+u(Y).\end{aligned}$$

□

Définition 1.3.5.
On appelle noyau (resp. image) de M et on note $\operatorname{Ker}M$ (resp. $\operatorname{Im}M$) le noyau (resp. l'image) de l'application linéaire canoniquement associée à M.

d Produit d'éléments des bases canoniques

Proposition 1.3.6.
Notons
- $(E_{ij})_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]}$ la base canonique de $\mathscr{M}_{n,p}(\mathbb{K})$;
- $\left(E'_{ij}\right)_{(i,j)\in[\![1,p]\!]\times[\![1,q]\!]}$ celle de $\mathscr{M}_{p,q}(\mathbb{K})$.
- $\left(E''_{ij}\right)_{(i,j)\in[\![1,n]\!]\times[\![1,q]\!]}$ celle de $\mathscr{M}_{n,q}(\mathbb{K})$.

Soit
- $(i,j)\in[\![1,n]\!]\times[\![1,p]\!]$;
- $(k,h)\in[\![1,p]\!]\times[\![1,q]\!]$.

Alors

$$\begin{aligned}E_{ij}\times E'_{kh}&=\delta_{jk}E''_{ih}\\&=\begin{cases}E''_{ih} & \text{si } j=k,\\ 0_{nq} & \text{sinon.}\end{cases}\end{aligned}$$

Remarque 1.3.7.
Dessiner les matrices pour voir de quoi il retourne. La démonstration suivante n'est que la description du dessin.

Démonstration.
Soit $\alpha\in[\![1,q]\!]$. La α^{e} colonne de $E_{ij}\times E'_{kh}$ est $E_{ij}C_\alpha$ où C_α est la α^{e} colonne de E'_{kh}. Si $\alpha\neq h$, $C_\alpha=0_{p1}$, donc toutes les colonnes de $E_{ij}\times E'_{kh}$ sont nulles sauf peut-être la h^{e}.

Cette h^{e} colonne de E_{kh} est égale à $E_{ij}C_h$. C_h étant le k^{e} vecteur de la base canonique de $\mathscr{M}_{p,1}(\mathbb{K})$, $E_{ij}C_h$ est la k^{e} colonne de E_{ij}. Celle-ci est nulle si $j\neq k$. Sinon, il s'agit du i^{e} vecteur de la base canonique de $\mathscr{M}_{n,1}(\mathbb{K})$.

On en déduit le résultat.

On peut également adopter une démonstration purement calculatoire. Notons $(m_{ab})_{(a,b)\in[\![1,n]\!]\times\in[\![1,q]\!]}$ les coefficients du produit $E_{ij}E'_{kh}$. Alors, soit $(a,b)\in[\![1,n]\!]\times[\![1,q]\!]$. On a

$$\begin{aligned}m_{ab}&=\sum_{c=1}^{p}(\delta_{ai}\delta_{cj})(\delta_{ck}\delta_{bh})\\&=(\delta_{ai}\delta_{cc})(\delta_{jk}\delta_{bh})\\&=\delta_{jk}(\delta_{ai}\delta_{bh})\end{aligned}$$

m_{ab} est donc le coefficient de la ligne a, colonne b de $\delta_{jk}E''_{ih}$. □

2 Matrices, familles de vecteurs et applications linéaires

2.1 Matrice d'une famille de vecteurs relativement à une base

Définition 2.1.1.
Soit $\mathscr{B}=(e_1,\dots,e_n)$ une base d'un $\mathbb{K}$-ev E de dimension finie n. Soient $v_1,\dots,v_p$ p vecteurs de E. On note a_{ij} la i^{e} coordonnées de v_j dans $\mathscr{B}$, *i.e.* $v_j=\sum_{i=1}^{n}a_{ij}e_i$.
Alors, la matrice $A=(a_{ij})\in\mathscr{M}_{n,p}(\mathbb{K})$ est appelée *matrice de la famille $(v_1,\dots,v_p)$ dans la base $\mathscr{B}$ (ou relativement à la base $\mathscr{B}$)* , et elle est notée $\operatorname{Mat}_{\mathscr{B}}(v_1,\dots,v_p)$ (parfois $\mathscr{M}_{\mathscr{B}}(v_1,\dots,v_p)$).

Exemple 2.1.2. 1. Dans $\mathbb{R}^2$, notons $\mathscr{B}$ la base canonique et $\mathscr{B}'$ la base $((0,1);(1,1))$. Avec $\mathscr{F}=((1,2);(0,3);(-1,1))$, on a

$$\operatorname{Mat}_{\mathscr{B}}(\mathscr{F})=\begin{pmatrix}1&0&-1\\2&3&1\end{pmatrix},$$

$$\operatorname{Mat}_{\mathscr{B}'}(\mathscr{F})=\begin{pmatrix}1&3&2\\1&0&-1\end{pmatrix}.$$

2. Dans $\mathbb{R}_3[X]$ muni de la base canonique $\mathscr{B}$, avec la famille $\mathscr{F} = (1+X^2; 1+X+X^2+X^3; X^3-2)$, on a
$$\mathrm{Mat}_{\mathscr{B}}(\mathscr{F}) = \begin{pmatrix} 1 & 1 & -2 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$
3. Matrice d'une famille de vecteurs de $\mathbb{K}^n$ dans la base canonique.
4. La matrice d'une famille de vecteurs colonnes $C_1, \ldots, C_p$ éléments de $\mathscr{M}_{n,1}(\mathbb{K})$ dans la base canonique est la matrice dont les colonnes sont $C_1, \ldots, C_p$.

Théorème 2.1.3.
Soit $\mathscr{B} = (e_1, \ldots, e_n)$ une base d'un $\mathbb{K}$-ev E de dimension finie n. Alors l'application
$$\varphi : \left\{ \begin{array}{ccc} (E,+,.) & \to & (\mathscr{M}_{n,1}(\mathbb{K}),+,.) \\ x & \mapsto & \mathrm{Mat}_{\mathscr{B}}(x) \end{array} \right.$$
est un isomorphisme d'espaces vectoriels.

Démonstration.
Soient $x, y \in E$ tels que $x = \sum_{k=1}^{n} x_k e_k$ et $y = \sum_{k=1}^{n} y_k e_k$. Soit $\lambda \in \mathbb{K}$. Alors $\varphi(x+\lambda y) = (x_i + \lambda y_i)_{1\leqslant i\leqslant n} = (x_i)_{1\leqslant i\leqslant n} + \lambda(y_i)_{1\leqslant i\leqslant n} = \varphi(x) + \lambda\varphi(y)$. D'où la linéarité de φ.
De plus, soit $M = (m_i)_{1\leqslant i\leqslant n} \in \mathscr{M}_{n,1}(\mathbb{K})$. Alors $\varphi(x) = M$ si et seulement si pour tout i, $m_i = x_i$, d'où la bijectivité de φ. □

2.2 Matrice associée à une application linéaire relativement à deux bases

Définition 2.2.1.
Soient E un $\mathbb{K}$-ev de dimension finie p et F un $\mathbb{K}$-ev de dimension finie n. Soient $\mathscr{B} = (e_1, \ldots, e_p)$ et $\mathscr{C} = (f_1, \ldots, f_n)$ des bases de E et F respectivement. Soit $u \in \mathscr{L}(E,F)$. On appelle *matrice de u relativement à $\mathscr{B}$ et $\mathscr{C}$*, notée $\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)$ (parfois $\mathscr{M}_{\mathscr{B},\mathscr{C}}(u)$), la matrice $\mathrm{Mat}_{\mathscr{C}}(u(e_1), \ldots, u(e_p)) \in \mathscr{M}_{n,p}(\mathbb{K})$.

Autrement dit, cette matrice contient les coordonnées des images des vecteurs de la base de départ décomposés dans la base d'arrivée.

Remarque 2.2.2.
Si $\mathscr{B} = \mathscr{C}$, on note $\mathrm{Mat}_{\mathscr{B}}(u) = \mathrm{Mat}_{\mathscr{B},\mathscr{B}}(u)$.

Remarque 2.2.3.
On pourra représenter f et sa matrice dans un schéma comme représenté dans la figure **? ?**.

$$E, \mathscr{B} \xrightarrow[\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(f)]{f} F, \mathscr{C}$$

FIGURE XXIII.1 – Représentation schématique de la matrice d'une application linéaire.

Exemple 2.2.4.
Soit $u : \mathbb{R}^2 \to \mathbb{R}^2$, $(x,y) \mapsto (x-y, 3x+2y)$, $\mathscr{B} = (e_1, e_2)$ la base canonique $\mathscr{B}$ de $\mathbb{R}^2$ On a $u(e_1) = (1,3) = e_1 + 3e_2$ et $u(e_2) = (-1,2) = -e_1 + 2e_2$. Ainsi, la matrice associée à u relativement à $\mathscr{B}$ est
$$\mathrm{Mat}_{\mathscr{B}}(u) = \begin{pmatrix} 1 & -1 \\ 3 & 2 \end{pmatrix}.$$
Avec $\mathscr{C}$ la base $(f_1, f_2) = \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}; \begin{pmatrix} 0 \\ -1 \end{pmatrix} \right)$, on a $u(e_1) = f_1 - 2f_2$ et $u(e_2) = -f_1 - 3f_2$. Ainsi,
$$\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u) = \begin{pmatrix} 1 & -1 \\ -2 & -3 \end{pmatrix}.$$

Exercice 2.2.5.
1. Avec les mêmes u, $\mathscr{B}$ et $\mathscr{C}$, calculer $\mathrm{Mat}_{\mathscr{C},\mathscr{B}}(u)$.
2. Réciproquement, trouver l'application linéaire associée à $M = \begin{pmatrix} 0 & 3 \\ -1 & 2 \end{pmatrix}$ relativement aux bases canoniques de $\mathbb{R}^2$.
3. Notons $\varphi : \mathbb{R}_3[X] \to \mathbb{R}_4[X]$, $P \mapsto P' + 3XP$, $\mathscr{B} = (1, X, X^2, X^3)$ et $\mathscr{C} = (X^3, X, X^2, 1, X^4)$ Trouver la matrice de φ relativement aux bases $\mathscr{B}$ et $\mathscr{C}$.

4. Réciproquement, avec les mêmes bases, notons φ l'unique application linéaire telle que

$$\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(\varphi) = \begin{pmatrix} 0 & 0 & 3 & 0 \\ 3 & 0 & 2 & 0 \\ 0 & 3 & 0 & 3 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

retrouver l'expression de φ.

5. Donner la matrice de $\begin{array}{ccc} \mathbb{R}_3[X] & \to & \mathbb{R}_3[X] \\ P & \mapsto & P' \end{array}$ dans les bases canoniques.

6. Donner la matrice de $\begin{array}{ccc} \mathbb{R}_3[X] & \to & \mathbb{R} \\ P & \mapsto & P(\pi) \end{array}$ dans les bases canoniques.

Théorème 2.2.6.
Soient E un $\mathbb{K}$-ev de dimension finie p et F un $\mathbb{K}$-ev de dimension finie n. Soient $\mathscr{B} = (e_1, \dots, e_p)$ et $\mathscr{C} = (f_1, \dots, f_n)$ des bases de E et F respectivement. Soit $M \in \mathscr{M}_{n,p}(\mathbb{K})$. Il existe une unique application $u \in \mathscr{L}(E,F)$ telle que $M = \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)$: c'est l'unique application linéaire associant, pour tout $i \in [\![1,p]\!]$, au i^{e} vecteur de la base $\mathscr{B}$ le vecteur dont le vecteur des coordonnées dans la base $\mathscr{C}$ est la i^{e} colonne de M.

Démonstration.
Notons $(m_{ij})_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]}$ les coefficients de M et C_1, …, C_p les colonnes de M. Pour $j \in [\![1,p]\!]$, on note v_j l'unique vecteur de E tel que $\mathrm{Mat}_{\mathscr{C}}(v_j) = C_j$ (il s'agit du vecteur $m_{1j}f_1 + \dots m_{nj}f_n$).

Soit alors $u \in \mathscr{L}(E,F)$. On a $M = \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)$ si et seulement si

$$\mathrm{Mat}_{\mathscr{C}}(v_1, \dots, v_p) = \mathrm{Mat}_{\mathscr{C}}(u(e_1), \dots, u(e_p)),$$

c'est-à-dire si et seulement si $\forall i \in [\![1,p]\!] v_i = u(e_i)$, or on sait qu'il existe une unique application linéaire u vérifiant cette dernière condition.

Il existe donc une unique application linéaire u vérifiant $M = \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)$. □

Remarque 2.2.7.
Dans le cas où les espaces vectoriels de départ et d'arrivée sont le même, la matrice de l'identité est I_n *si on considère* ***la même base*** *au départ et à l'arrivée.*

 dans des bases différentes, la matrice de l'identité n'est pas l'identité ! Exemple : calculer $\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(\mathrm{Id}_{\mathbb{R}^2})$ où $\mathscr{C} = (\overrightarrow{\imath}, \overrightarrow{\jmath})$ est la base canonique de $\mathbb{R}^2$ et $\mathscr{B} = (\overrightarrow{\imath} + \overrightarrow{\jmath}, \overrightarrow{\imath} - \overrightarrow{\jmath})$.

Proposition 2.2.8.
Soit $M \in \mathscr{M}_{n,p}(\mathbb{K})$. La matrice de l'*application linéaire canoniquement associée à M* dans les bases canoniques de $\mathscr{M}_{n,1}(\mathbb{K})$ et $\mathscr{M}_{p,1}(\mathbb{K})$ est M.

Démonstration.
Notons u l'application canoniquement associée à M. D'après la remarque 1.3.1, pour tout $k \in [\![1,p]\!]$, l'image par u du k^{e} vecteur de la base canonique est la k^{e} colonne de M. Donc la matrice de u est la matrice des vecteurs colonnes de M dans la base canonique : c'est donc M. □

Théorème 2.2.9.
On garde les mêmes notations. On considère l'application

$$\varphi : \left\{ \begin{array}{ccc} (\mathscr{L}(E,F),+,.) & \longrightarrow & (\mathscr{M}_{n,p}(\mathbb{K}),+,.) \\ u & \longmapsto & \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u) \end{array} \right. .$$

Alors, φ est un isomorphisme d'espaces vectoriels.

Démonstration.
On a déjà vu que cette application était bijective. Voir pourquoi elle est linéaire est laissé en exercice au lecteur.

Remarquons que, puisqu'on sait que les deux espaces vectoriels considérés sont de dimension finie et de même dimension, on aurait pu se dispenser de montrer précédemment qu'elle était injective ou se dispenser de montrer qu'elle était surjective. □

Remarque 2.2.10. 1. Ceci justifie l'identification forme linéaire sur $\mathbb{K}^p$ / matrice ligne à p colonnes. Exemple.

2. Ce résultat permet au passage de dire que si $M \in \mathscr{M}_{p,n}(\mathbb{K})$ et $\forall X \in \mathscr{M}_{n,1}(\mathbb{K})$, $MX = 0$, alors $M = 0$. En effet, les applications $X \mapsto MX$ et $X \mapsto 0_n X$ sont alors égales, donc les matrices M et 0_n le sont.

Proposition 2.2.11.
Avec les mêmes notations qu'en 2.2.1, on a

$$\forall x \in E \quad \mathrm{Mat}_{\mathscr{C}}(u(x)) = \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u) \times \mathrm{Mat}_{\mathscr{B}}(x).$$

Démonstration.
Soit $x \in E$. Posons $M = \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)$ et $X = \mathrm{Mat}_{\mathscr{B}}(x)$. Notons $(m_{ij})_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]}$ les coefficients de M, $(x_j)_{j\in[\![1,p]\!]}$ ceux de X, $(y_i)_{i\in[\![1,n]\!]}$ ceux de MX, $(e_j)_{j\in[\![1,p]\!]}$ les vecteurs de la base $\mathscr{B}$ et $(f_i)_{i\in[\![1,n]\!]}$ ceux de $\mathscr{C}$.

Alors, par définition du produit matriciel, on a

$$\forall i \in [\![1,n]\!] \quad y_i = \sum_{j=1}^{p} m_{ij}x_j.$$

Alors on a $x = \sum_{j=1}^{p} x_j e_j$, donc $u(x) = \sum_{j=1}^{p} x_j u(e_j)$.

Par ailleurs, pour tout $j \in [\![1,p]\!]$, $u(e_j) = \sum_{i=1}^{n} m_{ij} f_i$.

On a donc

$$\begin{aligned} u(x) &= \sum_{j=1}^{p}\sum_{i=1}^{n} x_j m_{ij} f_i \\ &= \sum_{i=1}^{n}\sum_{j=1}^{p} x_j m_{ij} f_i \\ &= \sum_{i=1}^{n} y_i f_i. \end{aligned}$$

Ainsi, $\mathrm{Mat}_{\mathscr{C}}(u(x))$ a pour coefficients la famille $(y_i)_{i\in[\![1,n]\!]}$. □

Exemple 2.2.12.
Reprendre les deux premiers exemple de la série d'exemples précédente avec le vecteur $(17, 42)$.

Remarque 2.2.13.
On pourra représenter schématiquement ce résultat comme dans la figure **??** : avec $M = \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)$ et $\mathrm{Mat}_{\mathscr{B}}(x)$, on a $\mathrm{Mat}_{\mathscr{C}}(u(x)) = MX$.

Théorème 2.2.14.
Soient E, F, G trois $\mathbb{K}$-ev de bases $\mathscr{B}, \mathscr{C}, \mathscr{D}$. Soient $f \in \mathscr{L}(F,G)$, $g \in \mathscr{L}(E,F)$. Alors $\mathrm{Mat}_{\mathscr{B},\mathscr{D}}(f \circ g) = \mathrm{Mat}_{\mathscr{C},\mathscr{D}}(f) \times \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(g)$.

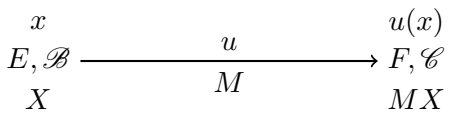


FIGURE XXIII.2 – Matrice de l'image d'un vecteur par une application linéaire.

Alors : $\mathrm{Mat}_{\mathscr{C}}(g(x)) = BX$, et $\mathrm{Mat}_{\mathscr{B},\mathscr{D}}(f \circ g)X = \mathrm{Mat}_{\mathscr{D}}((f \circ g)(x)) = A(BX) = (AB)X$. Soit $\varphi \in \mathscr{L}(E,G)$ de matrice $N = \mathrm{Mat}_{\mathscr{B},\mathscr{D}}(f \circ g) - AB$. Alors pour tout x, $NX = 0$, donc $\varphi(x) = 0$, ainsi $\varphi = 0$. Mais par unicité de la matrice (théorème précédent), on a $N = 0$, d'où $\mathrm{Mat}_{\mathscr{B},\mathscr{D}}(f \circ g) = AB$.

Démonstration.
Notons n, p et q les dimensions respectives de E, F, et G et $(e_1, \ldots, e_n)$ les vecteurs de la base $\mathscr{B}$. Posons $A = \mathrm{Mat}_{\mathscr{C},\mathscr{D}}(f)$, $B = \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(g)$ et $C = \mathrm{Mat}_{\mathscr{B},\mathscr{D}}(f \circ g)$.

AB et C sont toutes deux des matrices $q \times n$. Montrons qu'elles ont mêmes colonnes, ce qui montrera le résultat voulu : elles sont égales.

Soit $k \in [\![1,n]\!]$. Notons X_k la k^{e} colonne de AB. Alors, d'après la proposition 1.3.2, $X_k = AY_k$ où Y_k est la k^{e} colonne de B.

Or la Y_k est la matrice des coordonnées de $g(e_k)$ dans la base $\mathscr{C}$, donc AY_k est la matrice des coordonnées de $f(g(e_k))$ dans la base $\mathscr{D}$. Donc X_k est la matrice des coordonnées de $f(g(e_k))$ dans $\mathscr{D}$.

Or $f(g(e_k)) = (f \circ g)(e_k)$ et $f \circ g$ a pour matrice C dans les bases $\mathscr{B}$ et $\mathscr{D}$. Donc X_k est la k^{e} colonne de C.

AB et C ont donc les mêmes colonnes, donc sont égales. □

Remarque 2.2.15.
Ce résultat peut être vu comme LA raison pour laquelle le produit matriciel est associatif. On peut en effet en tirer une démonstration non-calculatoire de l'associativité du produit matriciel : étant donné trois matrices A, B, C telles que le produit $A(BC)$ soit bien défini, il suffit de choisir quatre espaces vectoriels, des bases de ces espaces vectoriels et trois applications f, g et h telles que les matrices A, B et C soient respectivement celles de f, g et h. Alors $A(BC)$ est la matrice de $f \circ (g \circ h)$ et $(AB)C$ est celle de $(f \circ g) \circ h$. Or la composition d'application est associative donc ces deux applications sont égales, donc $A(BC) = (AB)C$.

On laisse au lecteur le soin de vérifier que la propriété d'associativité du produit matriciel n'a pas été utilisée dans la démonstration ci-dessus ni dans les résultats ou définitions qu'elle utilise.

Remarque 2.2.16.
On pourra représenter schématiquement ce résultat comme dans la figure **??** : avec $M = \mathrm{Mat}_{\mathscr{C},\mathscr{D}}(f)$ et $N = \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(g)$, on a $\mathrm{Mat}_{\mathscr{B},\mathscr{D}}(f \circ g) = MN$. On réalise alors ce que l'on peut appeler un *diagramme de composition commutatif* : les applications obtenues en composant plusieurs flèches ayant même départ et même origine sont identiques.

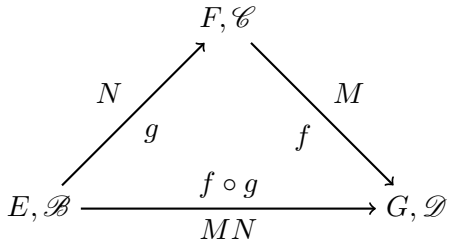


FIGURE XXIII.3 – Diagramme de composition d'applications linéaires et de leurs représentations matricielles.

Exemple 2.2.17.
Choisir deux applications $f : \mathbb{R}^3 \to \mathbb{R}^3$ et $g : \mathbb{R}^2 \to \mathbb{R}^3$, faire les calculs.

Définition 2.2.18.
Soient $(A_1, +, \times)$ et $(A_2, +, \times)$ deux anneaux, et $\varphi : A_1 \to A_2$. On dit que φ est un morphisme d'anneaux si c'est un morphisme de groupes pour la loi $+$ et $\varphi(1_{A_1}) = 1_{A_2}$ et $\forall x, y \in A_1 \quad \varphi(x \times y) = \varphi(x) \times \varphi(y)$

Remarque 2.2.19.
Ne pas oublier la condition $\varphi(1_{A_1}) = 1_{A_2}$. L'application suivante, qui vérifie toutes les autres conditions, n'est en effet pas un morphisme d'anneau :

$$\begin{array}{ccc} \mathbb{Z}/2\mathbb{Z} & \to & \mathbb{Z}/6\mathbb{Z} \\ 0 & \mapsto & 0 \\ 1 & \mapsto & 3 \end{array}$$

Corollaire 2.2.20.
Soit E un $\mathbb{K}$-ev de dim n, et $\mathscr{B}$ une base de E. Alors, l'application

$$\varphi : \left\{ \begin{array}{ccc} (\mathscr{L}(E), +, \circ) & \to & (\mathscr{M}_n(\mathbb{K}), +, \times) \\ u & \mapsto & \mathrm{Mat}_{\mathscr{B}}(u) \end{array} \right.$$

est un isomorphisme d'anneaux.

Démonstration.
Le théorème 2.2.9 assure que c'est un isomorphisme de groupes pour la loi $+$, le théorème 2.2.11 montre que l'image du produit est le produit des images et l'image du neutre de $\mathscr{L}(E)$ pour la composition (qui est l'application identité sur E) est le neutre de $\mathscr{M}_n(\mathbb{K})$ pour le produit (qui est I_n). □

2.3 Inversibilité

Proposition 2.3.1.
La matrice d'une application linéaire est inversible si et seulement si cette application linéaire est un isomorphisme. Dans ce cas, l'inverse de la matrice considérée est la matrice de l'application réciproque de l'isomorphisme considéré.

Démonstration.
Soit E et F deux espaces vectoriels de dimension finies respectives p et n. Soit $\mathscr{B}$ une base de E et $\mathscr{C}$ une base de F. Soit $u \in \mathscr{L}(E, F)$ et $v \in \mathscr{L}(F, E)$. Posons $A = \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)$ et $B = \mathrm{Mat}_{\mathscr{C},\mathscr{B}}(v)$.

On a :

$$\begin{aligned} u \circ v = \mathrm{Id}_F &\iff \mathrm{Mat}_{\mathscr{C},\mathscr{C}}(u \circ v) = \mathrm{I}_n \\ &\iff \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u) \times \mathrm{Mat}_{\mathscr{C},\mathscr{B}}(v) = \mathrm{I}_n \\ &\iff AB = \mathrm{I}_n \end{aligned}$$

De même

$$v \circ u = \mathrm{Id}_E \iff BA = \mathrm{I}_p$$

En particulier, si u est un isomorphisme, d'isomorphisme réciproque v, alors $AB = \mathrm{I}_n$ et $BA = \mathrm{I}_p$. De plus, on a alors $\dim E = \dim F$, donc $n = p$. Donc A est une matrice carrée et B est son inverse.

Réciproquement, si $u \in \mathscr{L}(E, F)$ possède une matrice inversible A, alors en notant v l'unique application linéaire telle que $A^{-1} = \mathrm{Mat}_{\mathscr{C},\mathscr{B}}(v)$, on a $u \circ v = \mathrm{Id}_F$ et $v \circ u = \mathrm{Id}_E$. □

Remarque 2.3.2.
Soit M une matrice carrée, u l'endomorphisme qui lui est canoniquement associé. On peut utiliser la proposition précédente pour montrer que M est inversible et déterminer, le cas échéant, son inverse.

- On commence par prendre X, Y deux vecteurs colonne ayant autant de lignes que M.
- On résout en X le système $MX = Y$.
- S'il y a toujours existence et unicité de la solution, on lit $X = M^{-1}Y$.

Cela correspond bien à ce qui était fait auparavant, la proposition précédente justifie bien que l'on puisse conclure à l'inversibilité de M directement, et obtenir son inverse.

Exemple 2.3.3.
Montrer que la matrice

$$M = \begin{pmatrix} 4 & 2 & -1 \\ 1 & 0 & 1 \\ 3 & -1 & 2 \end{pmatrix}$$

est inversible et déterminer son inverse.

Corollaire 2.3.4.
Soit A et B deux matrices carrées de taille n. Alors $AB = \mathrm{I}_n$ si et seulement si A et B sont inversibles et sont inverses l'une de l'autre.

Il est donc équivalent pour une matrice (carrée) d'être :

1. inversible ;
2. inversible à gauche ;
3. inversible à droite.

Démonstration.
Pour montrer cette équivalence, il suffit de montrer le sens direct, l'autre découlant directement de la définition d'inverse.

Supposons donc $AB = \mathrm{I}_n$.

Notons u et v les applications linéaires canoniquement associées respectivement à A et B relativement à la base canonique.

En reprenant la démonstration précédente, on peut remarquer que $u \circ v = \mathrm{Id}_F$, donc v est un endomorphisme injectif et u un endomorphisme surjectif.

La dimension de $\mathbb{K}^n$ étant finie, on u et v sont donc des automorphismes et on a $v = u^{-1} \circ u \circ v = u^{-1} \circ \mathrm{Id}_F = u^{-1}$.

Donc d'après la proposition précédente A et B sont inversibles et sont inverses l'une de l'autre. □

Corollaire 2.3.5.
Dans un espace vectoriel E de dimension finie n, la matrice d'une famille de vecteurs est inversible si et seulement si cette famille de vecteurs est une base.

Démonstration.
Pour que la matrice soit inversible, il est nécessaire qu'elle soit carrée. Pour que la famille de vecteur soit une base, il est nécessaire qu'elle possède exactement n vecteurs. On peut donc se restreindre au cas d'une famille de n vecteurs $v_1, \ldots, v_n$ et de la matrice M associée relativement à une base $\mathscr{B}$ de E. Notons $(e_1, \ldots, e_n)$ les vecteurs de $\mathscr{B}$.

Notons u l'unique endomorphisme de E tel que $\mathrm{Mat}_{\mathscr{B}}(u) = M$.

M est inversible si et seulement si u est un automorphisme. E étant de dimension finie, cela est équivalent à u surjective, c'est-à-dire à $\mathrm{rg}\, u = n$. Or $\mathrm{rg}\, u = \mathrm{rg}(u(e_1), \ldots, u(e_n)) = \mathrm{rg}(v_1, \ldots, v_n)$. Donc M est inversible si et seulement si $(v_1, \ldots, v_n)$ est génératrice. Or $\dim E = n$ donc cela est équivalent à $(v_1, \ldots, v_n)$ est une base. □

Remarque 2.3.6.
Ainsi, s'il y a une relation de dépendance entre les colonnes de M, M n'est pas inversible.

Exemple 2.3.7.
$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ -1 & 1 & 0 \end{pmatrix}$ n'est pas inversible.

Remarque 2.3.8.
Retour sur $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, qui est inversible si et seulement si $ad - bc \neq 0$, *i.e.* si et seulement si les colonnes $\begin{pmatrix} a \\ b \end{pmatrix}$ et $\begin{pmatrix} c \\ d \end{pmatrix}$ sont linéairement indépendantes.

2.4 Matrices de passage

Dans cette section E est un $\mathbb{K}$-ev de dimension finie n, et $\mathscr{B}, \mathscr{B}', \mathscr{B}''$ sont des bases de E.

Une question se pose maintenant naturellement : peut-on relier les matrices d'un vecteur

ou d'une application linéaire exprimées dans des bases différentes ?

Définition 2.4.1.
On appelle *matrice de passage de $\mathscr{B}$ dans $\mathscr{B}'$* la matrice $\mathrm{Mat}_{\mathscr{B}}(\mathscr{B}')$. On la note parfois $P_{\mathscr{B}}^{\mathscr{B}'}$.

Exemple 2.4.2.
$E = \mathbb{R}^2$: $\mathscr{B} = ((0,1),(1,1)) = (f_1, f_2), \mathscr{B}' = ((1,-1),(0,1)) = (g_1, g_2)$.
$g_1 = f_2 - 2f_1$ et $g_2 = f_1$, donc $\mathrm{Mat}_{\mathscr{B}}(\mathscr{B}') = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}$.

Théorème 2.4.3.
On note $P = \mathrm{Mat}_{\mathscr{B}}(\mathscr{B}')$ et $P' = \mathrm{Mat}_{\mathscr{B}'}(\mathscr{B}'')$.

1. $P = \mathrm{Mat}_{\mathscr{B}',\mathscr{B}}(\mathrm{Id}_E)$.
2. P est inversible est son inverse est $\mathrm{Mat}_{\mathscr{B}'}(\mathscr{B})$ (matrice de passage de $\mathscr{B}'$ dans $\mathscr{B}$).
3. La matrice de passage de $\mathscr{B}$ dans $\mathscr{B}''$ est $\mathrm{Mat}_{\mathscr{B}}(\mathscr{B}'') = PP' = \mathrm{Mat}_{\mathscr{B}}(\mathscr{B}') \times \mathrm{Mat}_{\mathscr{B}'}(\mathscr{B}'')$ (« transitivité »).

Remarque 2.4.4.
On pourra représenter schématiquement le point **??** comme dans la figure **??**. Ce schéma

$$E, \mathscr{B} \xleftarrow[P_{\mathscr{B}}^{\mathscr{B}'}]{\mathrm{Id}_E} E, \mathscr{B}'$$

FIGURE XXIII.4 – Application linéaire représentée par une matrice de passage.

sera le bloc fondamental de tous les schémas que nous écrirons lors de changements de base : retenez-le bien !

Remarque 2.4.5.
On pourra représenter schématiquement le point **??** comme dans la figure **??**.

Remarque 2.4.6.
On pourra représenter schématiquement le point **??** comme dans la figure **??**.

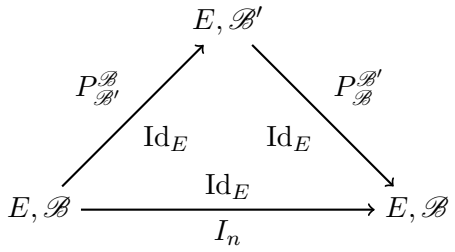


FIGURE XXIII.5 – Inverse d'une matrice de passage.

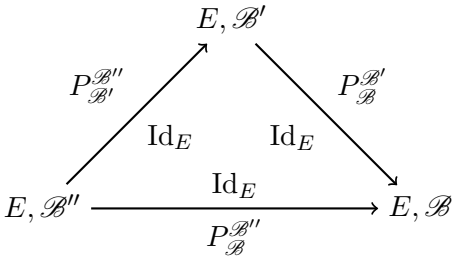


FIGURE XXIII.6 – Composition de changements de base.

Démonstration. 1. Notons $\mathscr{B} = (e_1, \ldots, e_n)$ et $\mathscr{B}' = (f_1, \ldots, f_n)$. On a

$$\begin{aligned} \mathrm{Mat}_{\mathscr{B}',\mathscr{B}}(\mathrm{Id}_E) &= \mathrm{Mat}_{\mathscr{B}}(\mathrm{Id}_E(f_1), \ldots, \mathrm{Id}_E(f_n)) \\ &= \mathrm{Mat}_{\mathscr{B}}(f_1, \ldots, f_n) \\ &= \mathrm{Mat}_{\mathscr{B}}(\mathscr{B}') \end{aligned}$$

2. $P = \mathrm{Mat}_{\mathscr{B}',\mathscr{B}}(\mathrm{Id}_E)$, or $\mathrm{Mat}_{\mathscr{B}',\mathscr{B}}(\mathrm{Id}_E).\mathrm{Mat}_{\mathscr{B},\mathscr{B}'}(\mathrm{Id}_E) = \mathrm{Mat}_{\mathscr{B},\mathscr{B}}(\mathrm{Id}_E \circ \mathrm{Id}_E) = \mathrm{Mat}_{\mathscr{B},\mathscr{B}}(\mathrm{Id}_E) = \mathrm{I}_n$, donc P est inversible et $P^{-1} = \mathrm{Mat}_{\mathscr{B},\mathscr{B}'}(\mathrm{Id}_E)$ d'après le corollaire 2.3.2, et donc $P^{-1} = \mathrm{Mat}_{\mathscr{B}'}(\mathscr{B})$ d'après le premier point.
3. On utilise à nouveau (i) : $\mathrm{Mat}_{\mathscr{B}}(\mathscr{B}').\mathrm{Mat}_{\mathscr{B}'}(\mathscr{B}'') = \mathrm{Mat}_{\mathscr{B}',\mathscr{B}}(\mathrm{Id}_E).\mathrm{Mat}_{\mathscr{B}'',\mathscr{B}'}(\mathrm{Id}_E) = \mathrm{Mat}_{\mathscr{B}'',\mathscr{B}}(\mathrm{Id}_E \circ \mathrm{Id}_E) = \mathrm{Mat}_{\mathscr{B}'',\mathscr{B}}(\mathrm{Id}_E) = \mathrm{Mat}_{\mathscr{B}}(\mathscr{B}'')$.

□

Le théorème suivant motive l'utilisation des matrices de passage.

Théorème 2.4.7 (Changement de base)**.**
Les matrices de passages permettent de relier

les matrices d'un même vecteur ou d'une même application relativement à des bases différentes :

Pour un vecteur Soit $x \in E$. On note $X = \mathrm{Mat}_{\mathscr{B}}(x)$ et $X' = \mathrm{Mat}_{\mathscr{B}'}(x)$, et $P = \mathrm{Mat}_{\mathscr{B}}(\mathscr{B}')$. Alors $X = PX'$.

Pour une application linéaire Avec les mêmes notations et en notant de plus F un $\mathbb{K}$-ev de dimension finie, $\mathscr{C}$ et $\mathscr{C}'$ deux bases de F, $u \in \mathscr{L}(E,F)$, et enfin $Q = \mathrm{Mat}_{\mathscr{C}}(\mathscr{C}')$. Alors $\mathrm{Mat}_{\mathscr{B}',\mathscr{C}'}(u) = Q^{-1}\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)P$.


La formule de changement de base pour un vecteur s'écrit $X = PX'$, et non $X' = PX$ (c'est une source d'erreur fréquente). Au moindre doute, n'hésitez pas à tracer le schéma correspondant.

Remarque 2.4.8.
Le premier point correspond au schéma de la figure **??**.

$$\begin{array}{ccc} x & & x \\ E,\mathscr{B} & \xleftarrow[P_{\mathscr{B}}^{\mathscr{B}'}]{\mathrm{Id}_E} & E,\mathscr{B}' \\ X & & X' \end{array}$$

FIGURE XXIII.7 – Illustration de la relation de changement de bases pour un vecteur.

Remarque 2.4.9.
Le second point correspond au schéma de la figure **??**.

Démonstration.Pour un vecteur il suffit de traduire l'égalité $x = \mathrm{Id}_E(x)$ dans les bonnes bases : x dans la base $\mathscr{B} = \mathrm{Id}(x$ dans la base $\mathscr{B}')$, soit : $X = \mathrm{Mat}_{\mathscr{B}',\mathscr{B}}(\mathrm{Id}_E)X' = PX'$.

Pour une application linéaire On traduit à nouveau $u(x) = u(x)$ dans les bonnes bases :

$$\begin{aligned} \mathrm{Mat}_{\mathscr{B}',\mathscr{C}'}(u) &= \mathrm{Mat}_{\mathscr{B}',\mathscr{C}'}(\mathrm{Id}_F \circ u \circ \mathrm{Id}_E) \\ &= \mathrm{Mat}_{\mathscr{C},\mathscr{C}'}(\mathrm{Id}_F)\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)\mathrm{Mat}_{\mathscr{B}',\mathscr{B}}(\mathrm{Id}_E) \\ &= Q^{-1}\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)P \end{aligned}$$

□

$$\begin{array}{ccc} E,\mathscr{B} & \xrightarrow[f]{\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(f)} & F,\mathscr{C} \\ \Big\uparrow P_{\mathscr{B}}^{\mathscr{B}'}\ \mathrm{Id}_E & & \mathrm{Id}_F\ \Big[P_{\mathscr{C}}^{\mathscr{C}'}\Big]^{-1} = P_{\mathscr{C}'}^{\mathscr{C}} \Big\downarrow \\ E,\mathscr{B}' & \xrightarrow[\mathrm{Mat}_{\mathscr{B}',\mathscr{C}'}(f)]{f} & F,\mathscr{C}' \end{array}$$

FIGURE XXIII.8 – Illustration de la relation de changement de bases pour une application linéaire.

Remarque 2.4.10.
Avec $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E et $f \in \mathscr{L}(E)$, on a $\mathrm{Mat}_{\mathscr{B}'}(f) = \left[P_{\mathscr{B}}^{\mathscr{B}'}\right]^{-1} \times \mathrm{Mat}_{\mathscr{B}}(f) \times P_{\mathscr{B}}^{\mathscr{B}'}$. On essaiera, pour chaque changement de base, de reproduire le schéma de la figure **??** pour se rappeler de cette formule.

$$\begin{array}{ccc} \mathscr{B} & \xrightarrow[f]{\mathrm{Mat}_{\mathscr{B}}(f)} & \mathscr{B} \\ \Big\uparrow P_{\mathscr{B}}^{\mathscr{B}'}\ \mathrm{Id} & & \mathrm{Id}\ \Big[P_{\mathscr{B}}^{\mathscr{B}'}\Big]^{-1} = P_{\mathscr{B}'}^{\mathscr{B}} \Big\downarrow \\ \mathscr{B}' & \xrightarrow[\mathrm{Mat}_{\mathscr{B}'}(f)]{f} & \mathscr{B}' \end{array}$$

FIGURE XXIII.9 – Illustration de la relation de changement de bases pour un endomorphisme.

Exemple 2.4.11.
Mêmes choses que dans l'exemple 2.4.2. $F = \mathbb{R}^3$, $\mathscr{C} = (e_1, e_2, e_3)$ (base canonique), $\mathscr{C}' = (h_1, h_2, h_3)$ avec $h_1 = e_1$, $h_2 = (1,1,0) = e_1 + e_2$, $h_3 = (-1,0,1) = -e_1 + e_3$.

On considère

$$u : \begin{cases} \mathbb{R}^2 & \longrightarrow & \mathbb{R}^3 \\ (x,y) & \longmapsto & (x-y, x, 2x+y). \end{cases}$$

1. Déterminer $\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)$.
2. Déterminer P et Q^{-1}, en déduire $\mathrm{Mat}_{\mathscr{B}',\mathscr{C}'}(u)$.
3. Vérifier en exprimant $u(g_i)$ en fonction des h_j.

Exemple 2.4.12.
On donne $\mathscr{C}$ = base canonique de $\mathbb{R}^3$ et $\mathscr{B}' = ((1,0,-1),(1,0,2),(0,1,-1)) = (v_1,v_2,v_3)$, et $x = 2v_1 + 2v_2 - v_3$. Exprimer x en fonction de e_1, e_2, e_3.

Remarque 2.4.13.
Ceci permet de voir que pour inverser une matrice, il suffit d'inverser la matrice de passage sous-jacente, et donc d'inverser un système linéaire.

Exemple 2.4.14.
Inverser $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 2 & -1 & 1 \end{pmatrix}$ en passant par des matrices de passage.

Remarque 2.4.15.
On appelle $P = \mathrm{Mat}_{\mathscr{B}}(\mathscr{B}')$ « matrice de passage de $\mathscr{B}$ dans $\mathscr{B}'$ » car elle permet de transformer une équation exprimée dans $\mathscr{B}$ en équation exprimée dans $\mathscr{B}'$. En effet, avec φ une forme linéaire et $L = \mathrm{Mat}_{\mathscr{B},1}(\varphi)$, l'équation cartésienne de $\mathrm{Ker}\,\varphi$ (c'est un hyperplan) s'écrit, dans la base $\mathscr{B}$, $LX = 0$. Dans la base $\mathscr{B}'$, cela s'écrit alors $LPX' = 0$. La ligne donnant l'équation dans la base $\mathscr{B}'$ est donc LP.

3 Matrices remarquables

3.1 Transposée

Définition 3.1.1.
Soit $A \in \mathscr{M}_{n,p}(\mathbb{K})$, $A = (a_{ij})$. On appelle *transposée de A* la matrice $(a_{ji}) \in \mathscr{M}_{p,n}(\mathbb{K})$, notée ${}^tA$ ou $A^\top$.

Exemple 3.1.2.
${}^t\begin{pmatrix} 4 & 2 \end{pmatrix} = \begin{pmatrix} 4 \\ 2 \end{pmatrix}$ et ${}^t\begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$. On a aussi ${}^tI_n = I_n$.

Proposition 3.1.3.
Soient $A, B \in \mathscr{M}_{n,p}(\mathbb{K})$, $\lambda \in \mathbb{K}$.

1. ${}^t(A + \lambda B) = {}^tA + \lambda\,{}^tB$, *i.e.* $A \mapsto {}^tA$ est linéaire.
2. Si $C \in \mathscr{M}_{p,q}(\mathbb{K})$, ${}^t(AC) = {}^tC\,{}^tA$.
3. ${}^t({}^tA)) = A$.
4. Si A est inversible, ${}^t(A^{-1}) = ({}^tA)^{-1}$.

Démonstration. 1. Élémentaire.

2. $A = (a_{ij})$, $C = (c_{ij})$, ${}^tA = (\alpha_{ij})$, ${}^tC = (\gamma_{ij})$, avec $\alpha_{ij} = a_{ji}$, $\gamma_{ij} = c_{ji}$, et on conclut par calcul direct.
3. Élémentaire.
4. On a $AA^{-1} = I_n$, donc en transposant ${}^t(A^{-1}) \times {}^tA = {}^tI_n = I_n$.

□

Remarque 3.1.4.
La transposition permet de transformer des résultats sur les colonnes en résultats sur les lignes, et inversement. Par exemple, une matrice est inversible si et seulement si ses lignes sont linéairement indépendantes.

Exemple 3.1.5.
$\begin{pmatrix} 5 & -6 & 3 \\ -3 & 4 & 8 \\ 7 & -8 & 14 \end{pmatrix}$ n'est pas inversible car $L_3 = 2L_1 + L_2$.

3.2 Matrices triangulaires

Définition 3.2.1.
Soit $A \in \mathscr{M}_n(\mathbb{K})$. On dit que A est *triangulaire supérieure (resp. inférieure)* si $\forall i,j \in [\![1,n]\!]$ tels que $i > j$ (resp. $i < j$), $a_{ij} = 0$.
On note $\tau_n^+(\mathbb{K})$ (resp. $\tau_n^-(\mathbb{K})$) l'ensemble des matrices triangulaires supérieures (resp. inférieures) d'ordre n.

Théorème 3.2.2.
$(\tau_n^{\pm}(\mathbb{K}), +, \times)$ est un anneau et $(\tau_n^{\pm}(\mathbb{K}), +, .)$ est un $\mathbb{K}$-ev de dimension $\dfrac{n(n+1)}{2}$.

Démonstration.
• $\mathbb{K}$-ev : élémentaire.
• Anneau : soient $A, B \in \tau_n^+(\mathbb{K})$. On note $AB = (\gamma_{ij})$. On suppose $i > j$, alors $\gamma_{ij} = \sum_{k=1}^{i-1} a_{ik}b_{kj} + \sum_{k=i}^{n} a_{ik}b_{kj}$, et tous les termes sont nuls.
• Dimension : les E_{ij} avec $i \leqslant j$ est une famille libre (déjà vu) et génératrice. Elle comporte $\dfrac{n(n+1)}{2}$ vecteurs. □

Remarque 3.2.3.
Avec cette démonstration on voit que $\gamma_{ii} = a_{ii}b_{ii}$.

Théorème 3.2.4.
Une matrice triangulaire est inversible si et seulement si elle n'a aucun zéro sur sa diagonale.

Démonstration.
Soit A triangulaire sup. d'ordre n. On note $(v_1, \dots, v_n)$ la famille de vecteurs telle que $A = \mathrm{Mat}_{\mathscr{B}}(v_1, \dots, v_n)$, avec $\mathscr{B}$ base canonique de $\mathbb{K}^n$.
• Si pas de zéro sur la diag. : on montre que $(v_1, \dots, v_n)$ est libre, avec $\lambda_1 v_1 + \dots + \lambda_n v_n = 0$, on pose le système, on résout : même pas besoin de faire de pivot de Gauss. Donc c'est une base, donc c'est inversible.
• S'il y a un zéro à la k^{e} position, alors $(v_1, \dots, v_k)$ ont tous des zéros après leur $(k-1)^{\text{e}}$ coordonnées, donc sont dans $\mathrm{Vect}(e_1, \dots, e_{k-1})$, ils sont donc liés. □

Lemme 3.2.5.
Soit E un espace vectoriel de dimension n et $\mathscr{B} = (e_1, \dots, e_n)$ une base de E. Pour $k \in [\![1, n]\!]$, on pose $E_k = \mathrm{Vect}(e_1, \dots, e_k)$. Soit $u \in \mathscr{L}(E)$ et $M = \mathrm{Mat}_{\mathscr{B}}(u)$.

Alors M est triangulaire supérieure si et seulement si pour tout $k \in [\![1, n]\!]$, E_k est stable par u.

Démonstration.
Soit $k \in [\![1, n]\!]$. Pour que E_k soit stable par u, il faut que $u(e_k) \in E_k$, c'est-à-dire que seuls les k premières lignes de la matrice colonne des coordonnées de $u(e_k)$ dans $\mathscr{B}$ soient non-nulles.

Or la matrice M de u est la matrice formée de ces colonnes. Pour que tous les E_k, pour $k \in [\![1, n]\!]$ soient stables par u, il est donc nécessaire qu'elle soit triangulaire supérieure.

Réciproquement, supposons que cette matrice soit triangulaire supérieure. Alors pour tout $k \in [\![1, n]\!]$ et tout $i \in [\![1, k]\!]$, on a $u(e_i) \in E_i \subset E_k$. Donc pour tout $k \in [\![1, k]\!]$, $u(E_k) \subset \mathrm{Vect}\, u(e_1), \dots, u(e_k) \subset E_k$. □

Remarque 3.2.6.
Ce résultat s'adapte aux matrices triangulaires inférieures, en posant $E_1 = \mathrm{Vect}(e_k)$, $E_2 = \mathrm{Vect}(e_{k-1}, e_k)$, ...

Théorème 3.2.7.
L'inverse d'une matrice triangulaire supérieure (resp. inférieure) inversible est également triangulaire supérieure (resp. inférieure).

Démonstration.
Nous donnons la démonstration pour les matrices triangulaires supérieures. Pour les matrices triangulaires inférieures, on peut exploiter la remarque ci-dessus ou utiliser les résultats sur la transposée en remarquant que la transposée d'une matrice triangulaire supérieure est triangulaire inférieure et vice-versa.

Soit $M \in \tau_n^+(\mathbb{K}) \cap \mathscr{GL}_n(\mathbb{K})$.

On choisit E un espace vectoriel de dimension n, $\mathscr{B} = (e_1, \dots, e_n)$ une base de E et on note u l'endomorphisme de E de matrice M relativement à $\mathscr{B}$.

M étant inversible, u est bijective.

D'après le lemme, tous les E_k sont stables par u. En appliquant le lemme, il suffit de montrer qu'ils sont stables par u^{-1} pour montrer que $\mathrm{Mat}_{\mathscr{B}}(u^{-1}) = M^{-1}$ est triangulaire supérieure.

Soit $k \in [\![1, n]\!]$. On a $u(E_k) \subset E_k$, donc $E_k \subset u^{-1}(E_k)$. Or $\dim u^{-1}(E_k) = \dim E_k$ (image d'un sous-espace vectoriel par un morphisme bijectif), donc $u^{-1}(E_k) = E_k$. On a donc l'inclusion souhaitée : u^{-1} est donc triangulaire supérieure. □

3.3 Matrices diagonales

Définition 3.3.1.
On appelle *matrice diagonale* toute matrice carrée $(a_{ij})_{1 \leqslant i,j \leqslant n}$ telle que pour tous $i, j \in [\![1, n]\!]$, $i \neq j \Rightarrow a_{i,j} = 0$.
On note $\mathscr{D}_n(\mathbb{K})$ l'ensemble des matrices diagonales d'ordre n.

Remarque 3.3.2.
• On note $\text{diag}(\lambda_1, \dots, \lambda_n)$ la matrice diagonale dont les termes diagonaux sont $(\lambda_1, \dots, \lambda_n)$.
• $\mathscr{D}_n(\mathbb{K}) = \tau_n^+(\mathbb{K}) \cap \tau_n^-(\mathbb{K})$.

Définition 3.3.3.
On appelle *matrice scalaire* toute matrice diagonale dont les coeffs de la diagonale sont tous égaux, *i.e.* de la forme $\lambda \mathrm{I}_n$.

Théorème 3.3.4.
$(\mathscr{D}_n(\mathbb{K}), +, \times)$ est un anneau et $(\mathscr{D}_n(\mathbb{K}), +, .)$ est un $\mathbb{K}$-ev de dimension n.

Démonstration.
Anneau et ev : immédiat avec $\mathscr{D}_n(\mathbb{K}) = \tau_n^+(\mathbb{K}) \cap \tau_n^-(\mathbb{K})$.
Dimension : $(E_{ii})_{1 \leqslant i \leqslant n}$ en forme une base. □

Remarque 3.3.5.
Une matrice diagonale est inversible si et seulement si tous ses coefficients diagonaux sont non-nuls. Et dans ce cas $\text{diag}(\lambda_1, \dots, \lambda_n)^{-1} = \text{diag}\left(\frac{1}{\lambda_1}, \dots, \frac{1}{\lambda_n}\right)$.
De plus, pour tout $p \in \mathbb{N}$, $(\text{diag}(\lambda_1, \dots, \lambda_n))^p = \text{diag}(\lambda_1^p, \dots, \lambda_n^p)$. Et si aucun coefficient diagonal n'est nul, cette relation est aussi valable pour $p \in \mathbb{Z}$.

3.4 Matrices symétriques et antisymétriques

Définition 3.4.1.
$A \in \mathscr{M}_n(\mathbb{K})$ est dite *symétrique (resp. antisymétrique)* si $A = {}^tA$ (resp. $A = -{}^tA$).

Remarque 3.4.2.
Une matrice symétrique ou antisymétrique est toujours carrée.

Exemple 3.4.3.
$\begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}$ est symétrique, pas $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$.

Exemple 3.4.4.
$\begin{pmatrix} 0 & -2 \\ 2 & 0 \end{pmatrix}$ est anti-symétrique, pas $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Proposition 3.4.5.
Les coefficients diagonaux d'une matrice antisymétrique sont nuls.

Démonstration.
Soit $i \in [\![1, n]\!]$, on a $a_{ii} = -a_{ii}$ donc $a_{ii} = 0$. □

Théorème 3.4.6.
L'ensemble des matrices symétriques (resp. antisymétriques) muni de $+$ et $\cdot$ est un $\mathbb{K}$-ev de dimension $\frac{n(n+1)}{2}$ (resp. $\frac{n(n-1)}{2}$).

Démonstration.
Ce sont respectivement les noyaux de $A \mapsto {}^tA - A$ et $A \mapsto {}^tA + A$, donc ce sont des sous-espaces vectoriels de $\mathscr{M}_n(\mathbb{K})$. □

 Ce ne sont pas des sous-anneau de $\mathscr{M}_n(\mathbb{K})$!

Exemple 3.4.7.
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$.
$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

4 Opérations élémentaires sur les matrices

Définition 4.0.1.
Il existe trois types d'opérations élémentaires sur les lignes et colonnes d'une matrice :

1. l'échange de deux lignes ou deux colonnes ;
2. la multiplication d'une ligne/colonne par un scalaire **non nul** ;

3. l'addition à une ligne/colonne d'une **autre** ligne/colonne multipliée par un scalaire.

Ces opérations sont notées respectivement :

1. $L_i \leftrightarrow L_j$ et $C_i \leftrightarrow C_j$;
2. $L_i \leftarrow \lambda L_i$ **avec** $\lambda \neq 0$ (*idem* avec des colonnes) ;
3. $L_i \leftarrow L_i + \lambda L_j$, avec $i \neq j$ (*idem* avec des colonnes).

Définition 4.0.2.
Soit $i, j \in [\![1, n]\!]$, $\lambda \in \mathbb{K}$.

1. On appelle matrice d'échange de coefficients i, j la matrice $\varepsilon_{ij} = \mathrm{I}_n - E_{ii} - E_{jj} + E_{ij} + E_{ji}$ (la dessiner).
2. On appelle matrice de dilatation de coefficient i et de rapport λ la matrice $D_i(\lambda) = \mathrm{I}_n + (\lambda - 1)E_{ii}$ (la dessiner).
3. On appelle matrice de transvection de coefficients i, j et de rapport λ la matrice $T_{ij}(\lambda) = \mathrm{I}_n + \lambda E_{ij}$ (la dessiner).

Remarquons que ces trois matrices sont inversibles.

Théorème 4.0.3.
Soit $A \in \mathscr{M}_n(\mathbb{K})$, et $i, j \in [\![1, n]\!]$.

1. L'opération $L_i \leftrightarrow L_j$ est équivalente à la multiplication de la matrice A à sa gauche par la matrice ε_{ij}.
2. L'opération $L_i \leftarrow \lambda L_i$ est équivalente à la multiplication de la matrice A à sa gauche par la matrice $\mathbb{D}_i(\lambda) = \mathrm{I}_n + (\lambda - 1)E_{ii}$.
3. L'opération $L_i \leftarrow L_i + \lambda L_j$ est équivalente à la multiplication de la matrice A à sa gauche par la matrice $T_{ij}(\lambda) = \mathrm{I}_n + \lambda E_{ij}$.
4. L'opération $C_i \leftrightarrow C_j$ est équivalente à la multiplication de la matrice A à sa droite par la matrice ε_{ij}.
5. L'opération $C_i \leftarrow \lambda C_i$ est équivalente à la multiplication de la matrice A à sa droite par la matrice $D_i(\lambda)$.
6. L'opération $C_i \leftarrow C_i + \lambda C_j$ est équivalente à la multiplication de la matrice A à sa droite par la matrice $T_{ji}(\lambda) = \mathrm{I}_n + \lambda E_{ij}$ (attention aux coefficients !).

Démonstration.
On appelle $L_1, \ldots, L_n$ les lignes de A. Tout est basé sur le fait que $E_{ij}A$ est la matrice nulle où on a rajouté L_j à la $i$ème ligne (le montrer). Et c'est tout.
Pour remarquer que les trois matrices $\varepsilon_{i,j}$, $D_i(\lambda)$ et $T_{i,j}(\lambda)$ sont inversibles, pour les deux dernières c'est simple : elles sont triangulaires sans 0 sur la diagonale. Pour la première, il suffit de voir qu'elle est sa propre inverse, car $\varepsilon_{ij}\varepsilon_{ij}$ est la matrice ε_{ij} où on a échangé les lignes i et j, donc c'est I_n. □

Exemple 4.0.4.
Calculer

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

On trouve $\begin{pmatrix} 7 & 3 & 2 \\ 32 & 12 & 10 \\ 25 & 9 & 8 \end{pmatrix}$.

5 Rang d'une matrice

5.1 Définitions

Remarque 5.1.1. 1. Soit E et F deux $\mathbb{K}$-espaces vectoriels et $\varphi : E \to F$ un isomorphisme de E sur F.

Soit $p \in \mathbb{N}$ et $(x_i)_{i \in [\![1,p]\!]}$ une famille d'éléments de E.

Alors φ réalise une bijection de $\mathrm{Vect}\,(x_1, \ldots, x_p)$ sur $\mathrm{Vect}\,(\varphi(x_1, \ldots, x_p))$, donc les familles $(x_i)_{i \in [\![1,p]\!]}$ et $(\varphi(x_i))_{i \in [\![1,p]\!]}$ ont même rang.

2. En particulier, soit n un entier et soit F un espace vectoriel de dimension finie n, muni

d'une base $\mathscr{B}$. L'application

$$\begin{array}{rccc} \varphi : & F & \to & \mathscr{M}_{n,1}(\mathbb{K}) \\ & x & \mapsto & \mathrm{Mat}_{\mathscr{B}}(x) \end{array}$$

est une bijection, donc pour toute famille $(x_i)_{i\in[\![1,p]\!]}$ d'éléments de F, $(\mathrm{Mat}_{\mathscr{B}}(x_i))_{i\in[\![1,p]\!]}$ est une famille de même rang.

3. Par ailleurs, soit E et F deux espaces vectoriels de dimensions finies respectives p et n et $(e_1,\dots,e_p)$ une base de E. Alors pour toute application linéaire u de E dans F, on a

$$\begin{aligned} \mathrm{Im}(u) &= u(\mathrm{Vect}(e_1,\dots,e_p)) \\ &= \mathrm{Vect}\left(u(e_1),\dots,u(e_p)\right) \end{aligned}$$

donc $\mathrm{rg}(u) = \mathrm{rg}\left(u(e_1),\dots,u(e_p)\right)$.

Définition 5.1.2.
Soit $A \in \mathscr{M}_{n,p}(\mathbb{K})$. Notons $C_1,\dots,C_p$ les colonnes de A. Alors on appelle *rang de* A et on note $\mathrm{rg}(A)$ l'entier $\mathrm{rg}\left(C_1,\dots,C_p\right)$.

Remarque 5.1.3.
Soit $A \in \mathscr{M}_{n,p}(\mathbb{K})$. Alors

1. Pour tout $r \in [\![0,p]\!]$ et tout choix de r colonnes C_1, …, C_r de A, la famille $(C_1,\dots,C_r)$ est de rang inférieur ou égal à $\mathrm{rg}\,A$. C'est une conséquence du fait que l'espace engendré par C_1,…, C_r est inclus dans $\mathrm{Im}\,A$.
2. Il existe un choix de $\mathrm{rg}(A)$ colonnes de A, C_1, …, $C_{\mathrm{rg}(A)}$ tel que $\mathrm{Vect}\left(C_1,\dots,C_{\mathrm{rg}(A)}\right) = \mathrm{Im}(A)$. En effet, la famille des colonnes de A est une famille génératrice d'un sous-espace vectoriel de $\mathbb{K}^n$ de dimension $\mathrm{rg}(A)$, on peut donc en extraire une base, qui comporte nécessairement $\mathrm{rg}(A)$ vecteurs colonnes.

Théorème 5.1.4.
Soit E et F deux espaces vectoriels de dimensions finies respectives p et n, de bases respectives $\mathscr{B}$ et $\mathscr{C}$, et $u \in \mathscr{L}(E,F)$. Alors $\mathrm{rg}(u) = \mathrm{rg}\left(\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)\right)$.

Démonstration.
En notant A la matrice $\mathrm{Mat}_{\mathscr{B},\mathscr{C}}$, C_1, …, C_p ses colonnes et e_1, …, e_p les vecteurs de $\mathscr{B}$, on a

$$\mathrm{rg}(A) = \mathrm{rg}(C_1,\dots,C_p) = \mathrm{rg}\left(u(e_1),\dots,u(e_p)\right) = \mathrm{rg}(u).$$

□

Théorème 5.1.5.
Soit F un $\mathbb{K}$-espace vectoriel de dimension finie de base $\mathscr{C}$, $(v_1,\dots,v_p)$ une famille de vecteurs de F. Alors $\mathrm{rg}\left(\mathrm{Mat}_{\mathscr{C}}(v_1,\dots,v_p)\right) = \mathrm{rg}\left(v_1,\dots,v_p\right)$.

Démonstration.
En notant A la matrice $\mathrm{Mat}_{\mathscr{C}}(v_1,\dots,v_p)$, et C_1, …, C_p ses colonnes, on a

$$\mathrm{rg}(A) = \mathrm{rg}(C_1,\dots,C_p) = \mathrm{rg}\left(v_1,\dots,v_p\right).$$

□

Théorème 5.1.6.
$A \in \mathscr{M}_n(\mathbb{K})$ est inversible si et seulement si $\mathrm{rg}\,A = n$.

Démonstration.
Soient $\mathscr{B} = (e_1,\dots,e_n)$ la base canonique de $\mathbb{K}^n$, et $(v_1,\dots,v_n)$ une famille de vecteurs de E telle que $A = \mathrm{Mat}_{\mathscr{B}}(v_1,\dots,v_n)$. Alors A inversible si et seulement si $(v_1,\dots,v_n)$ base si et seulement si $\mathrm{rg}(v_1,\dots,v_n) = n$ si et seulement si $\mathrm{rg}\,A = n$. □

Exercice 5.1.7.
Calculer les rangs suivants.

- $\mathrm{rg}\begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}$;
- $\mathrm{rg}(\mathrm{diag}(\lambda_1,\dots,\lambda_n))$;
- $\mathrm{rg}\begin{pmatrix} 1 & 2 & 3 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$.

Définition 5.1.8.
Soit n et p deux entiers. On dit qu'une matrice A de $\mathscr{M}_{n,p}(\mathbb{K})$ est *équivalente* à une autre matrice B de $\mathscr{M}_{n,p}(\mathbb{K})$ s'il existe deux matrices $P \in \mathscr{M}_n(\mathbb{K})$ et $Q \in \mathscr{M}_p(\mathbb{K})$ inversibles telles que $A = PBQ$.

Proposition 5.1.9.
La relation « être équivalente à » sur l'ensemble des matrices de $\mathscr{M}_{n,p}(\mathbb{K})$ est une relation d'équivalence.

Démonstration.
Cette relation est

Réflexive car pour toute $A \in \mathscr{M}_{n,p}(\mathbb{K})$, $A = \mathrm{I}_n A \mathrm{I}_p$ et I_n et I_p sont inversibles ;

Symétrique car pour tout $(A,B) \in (\mathscr{M}_{n,p}(\mathbb{K}))^2$ tel que A et B sont équivalentes, il existe deux matrices $P \in \mathscr{M}_n(\mathbb{K})$ et $Q \in \mathscr{M}_p(\mathbb{K})$ inversibles telles que $A = PBQ$, et on a alors $B = P^{-1}AQ^{-1}$ et P^{-1} et Q^{-1} sont inversibles ;

Transitive car pour tout $(A,B,C) \in (\mathscr{M}_{n,p}(\mathbb{K}))^3$ tel que A et B sont équivalentes et B et C sont équivalentes. Alors il existe $P \in \mathscr{M}_n(\mathbb{K})$, $Q \in \mathscr{M}_p(\mathbb{K})$, $R \in \mathscr{M}_n(\mathbb{K})$ et $S \in \mathscr{M}_p(\mathbb{K})$ inversibles, telles que $A = PBQ$ et $B = RCS$, donc $A = (PR)C(SQ)$ et PR et SQ sont inversibles.

Il s'agit donc bien d'une relation d'équivalence. □

Proposition 5.1.10. 1. Soit E et F deux espaces vectoriels de dimensions finies et $u \in \mathscr{L}(E,F)$. Soit $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E et $\mathscr{C}$ et $\mathscr{C}'$ deux bases de F. Alors $\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)$ et $\mathrm{Mat}_{\mathscr{B}',\mathscr{C}'}(u)$ sont des matrices équivalentes.

2. Soit E et F deux espaces vectoriels de dimensions finies, munies de bases respectives $\mathscr{B}$ et $\mathscr{C}$. Soit $u \in \mathscr{L}(E,F)$. Soit A une matrice équivalente à $\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)$. Alors il existe une base $\mathscr{B}'$ de E et une base $\mathscr{C}'$ de F telles que $\mathrm{Mat}_{\mathscr{B}',\mathscr{C}'}(u) = A$.

Démonstration. 1. D'après le théorème de changement de base, on a

$$\mathrm{Mat}_{\mathscr{B}',\mathscr{C}'}(u) = \mathrm{Mat}_{\mathscr{C}}(\mathscr{C}')^{-1}\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)\mathrm{Mat}_{\mathscr{B}}(\mathscr{B}')$$

et les matrices de changement de base sont inversibles, donc $\mathrm{Mat}_{\mathscr{B}',\mathscr{C}'}(u)$ et $\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)$ sont équivalentes.

2. Posons $M = \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)$. A est équivalente à M, donc on peut trouver $P \in \mathscr{M}_n(\mathbb{K})$ et $Q \in \mathscr{M}_p(\mathbb{K})$ inversibles telles que $A = PMQ$. Soit $f \in \mathscr{L}(F)$ et $g \in \mathscr{L}(E)$ les applications vérifiant $P^{-1} = \mathrm{Mat}_{\mathscr{C}}(f)$ et $Q = \mathrm{Mat}_{\mathscr{B}}(g)$. P et Q étant inversibles, f et g sont des automorphismes. Notons $\mathscr{B}'$ et $\mathscr{C}'$ les images respectives de $\mathscr{B}$ de $\mathscr{C}$ par g et f. Alors $\mathrm{Mat}_{\mathscr{B}}(\mathscr{B}') = Q$ et $\mathrm{Mat}_{\mathscr{C}}(\mathscr{C}') = P^{-1}$. Donc d'après le théorème de changement de base $\mathrm{Mat}_{\mathscr{B}',\mathscr{C}'}(u) = P\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)Q$. □

Théorème 5.1.11 (Théorème de réduction)**.**
Soit $A \in \mathscr{M}_{n,p}(\mathbb{K})$ une matrice de rang r.

1. Alors, $r \leqslant \min(n,p)$.
2. A est équivalente à la matrice $J_{n,p,r}$ définie par

$$J_{n,p,r} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & & \vdots \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots & \vdots & & \vdots \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} \mathrm{I}_r & 0_{r,p-r} \\ 0_{n-r,r} & 0_{n-r,p-r} \end{pmatrix}.$$

Démonstration. 1. On note $V_1, \ldots, V_p$ les colonnes de A. Il s'agit de p vecteurs de $\mathscr{M}_{n,1}(\mathbb{K})$, donc $\mathrm{rg}(V_1, \ldots, V_p) \leqslant p$ et de plus $\mathrm{rg}(V_1, \ldots, V_p) \leqslant \dim \mathscr{M}_{n,1}(\mathbb{K}) = n$.

2. Considérons $u : \mathscr{L}(\mathbb{K}^p, \mathbb{K}^n)$ canoniquement associée à la matrice A. u est de même rang que A.

   On sait qu'on peut trouver un supplémentaire S de $\mathrm{Ker}\, u$ tel que u réalise un isomorphisme de S sur $\mathrm{Im}\, u$. De plus $\dim S = \mathrm{rg}(u) = r$ et $\dim \mathrm{Ker}\, u = p - r$. Soit $(e_1, \ldots, e_r)$ une base de S, $(e_{r+1}, \ldots, e_p)$ une base de $\mathrm{Ker}\, u$. Posons $\mathscr{B} = (e_1, \ldots, e_p)$. $\mathscr{B}$ est une base de $\mathbb{K}^p$. Posons $f_i = u(e_i)$ pour $i \in [\![1, r]\!]$. Alors $(f_1, \ldots, f_r)$ est une base de $\mathrm{Im}\, u$, qu'on peut compléter en une base $\mathscr{C}$ de $\mathbb{K}^n$.

   Alors $\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u) = J_{n,p,r}$. Or u a pour matrice A dans les bases canoniques, donc A et $J_{n,p,r}$ sont équivalentes.

□

Remarque 5.1.12.
Nous venons de voir une interprétation géométrique de ce résultat. On peut aussi en donner une interprétation matricielle.

On applique l'algorithme du pivot de Gauss au système $AX = B$, avec $B \in \mathscr{M}_{n,1}(\mathbb{K})$ et $X \in \mathscr{M}_{p,1}(\mathbb{K})$. Après une phase de descente, on arrive à un système échelonné en lignes. Quitte à échanger quelques colonnes, A est donc équivalente à une

matrice de la forme

$$\begin{pmatrix} J & * \\ 0_{n-r,r} & 0_{n-r,p-r} \end{pmatrix} \text{ avec } J = \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}.$$

Remarquons qu'hormis ces échanges de colonnes, nous n'avons effectué que des opérations sur les lignes. Après la phase de remontée (opérations sur les lignes, toujours), on obtient que A est équivalente à une matrice de la forme

$$\begin{pmatrix} I_r & * \\ 0_{n-r,r} & 0_{n-r,p-r} \end{pmatrix}.$$

Il suffit donc d'effectuer quelques opérations élémentaires sur les colonnes de A pour obtenir que A est équivalente à $J_{n,p,r}$.

On remarquera donc que, en écrivant $A = PJ_{n,p,r}Q$, avec $P \in GL_n(\mathbb{R})$ et $Q \in GL_p(\mathbb{R})$, on lit dans P les opérations effectuées sur les lignes de A pendant l'algorithme du pivot de Gauss et dans Q celles effectuées sur les colonnes de A.

5.2 Opérations laissant le rang invariant

Théorème 5.2.1.
Multiplier une matrice par une matrice inversible (à droite ou à gauche) ne change pas son rang.

Démonstration.
Ce n'est que le point de vue matriciel du résultat analogue sur les applications linéaires. □

Tous les théorèmes suivants utiliseront ce résultat.

Théorème 5.2.2.
Deux matrices A et B sont équivalentes si et seulement si elles sont de même taille et de même rang.

Démonstration.
Dans un sens, utiliser le résultat précédent. Dans l'autre, utiliser le théorème de réduction. □

Théorème 5.2.3 (Invariance par transposition)**.**
Si $A \in \mathscr{M}_{n,p}(\mathbb{K})$, $\mathrm{rg}(A) = \mathrm{rg}({}^tA)$.

Démonstration.
C'est un corollaire du théorème de réduction : si $A = BJ_{n,p,r}C$, ${}^tA = {}^tC\,{}^tJ^t_{n,p,r}B = {}^tC J^t_{p,n,r}B$, qui est de rang r, car ${}^tB$ et ${}^tC$ sont inversibles et $J_{p,n,r}$ est de rang r. □

Corollaire 5.2.4.
Les résultats sur le rang applicables aux colonnes des matrices vus précédemment s'appliquent aussi aux lignes. Plus précisément :

1. Le rang d'une matrice est le rang de ses vecteurs lignes.
2. Le rang d'une famille de lignes d'une matrice est inférieur ou égal à celui de la matrice.
3. Pour tout matrice de rang r, il existe une famille de r lignes de cette matrice constituant une famille libre.

Exemple 5.2.5.
$\mathrm{rg}\begin{pmatrix} 1 & 2 & 3 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$ se calcule plus vite en passant à la transposée, *i.e.* en raisonnant sur les lignes au lieu des colonnes. On peut aussi faire un mix.

Théorème 5.2.6.
Les opérations élémentaires sur les lignes et colonnes préservent le rang.

Démonstration.
Facile car ces opérations reviennent à multiplier par des matrices inversibles. □

Théorème 5.2.7.
Supprimer une ligne ou une colonne de zéros dans une matrice ne change pas son rang.

Démonstration.
Pour les colonnes : analogue du résultat sur les vecteurs. Pour les lignes : passer à la transposée. □

5.3 Calculs pratiques

Remarque 5.3.1.
Calcul du rang et de l'inverse d'une matrice grâce au pivot de Gauss.

Pour le rang On peut appliquer la méthode du pivot à une matrice $M \in \mathscr{M}_{n,p}(\mathbb{K})$ non nécessairement carrée.

On peut mélanger les opérations sur les lignes et les colonnes.

On arrive au final à une matrice contenant des lignes non nulles $L_1, \ldots, L_k$, dont le premier élément est situé colonne c_1, $\ldots$, c_k avec $c_1 < \ldots < c_k$, puis $n-k$ lignes nulles. Alors $\operatorname{rg} M = \operatorname{rg}(\operatorname{Vect}(L_1, \ldots, L_k)) = k$ car les lignes L_1, $\ldots$, L_k forment une famille libre.

Pour le calcul du noyau d'une matrice non nécessairement carrée, on peut remarquer que les opérations sur les lignes le laissent invariant car multiplier à gauche une matrice par une matrice inversible ne change pas son noyau.

Pour le calcul de l'image d'une matrice non nécessairement carrée, on peut remarquer que les opérations sur les colonnes la laissent invariante car multiplier à droite une matrice par une matrice inversible ne change pas son image.

Pour le calcul de l'inverse d'une matrice carrée on peut travailler sur les lignes ou sur les colonnes mais **surtout pas sur les deux**. En effet, l'algorithme du calcul de l'inverse consiste à multiplier la matrice A par des matrices élémentaires jusqu'à obtenir l'identité, et à multiplier en parallèle la matrice identité par les mêmes matrices.

5.4 Matrices extraites

Définition 5.4.1.
Soit $M \in \mathscr{M}_{n,p}(\mathbb{K})$. On appelle matrice extraite de M toute matrice obtenue en supprimant h des lignes de M et k de ses colonnes avec $h \in [\![0, n-1]\!]$ et $k \in [\![0, p-1]\!]$.

Proposition 5.4.2.
Soit $M \in \mathscr{M}_{n,p}(\mathbb{K})$ et A une matrice extraite de M. Alors $\operatorname{rg}(A) \leqslant \operatorname{rg}(M)$.

Démonstration.
Posons $r = \operatorname{rg}(A)$. Alors on peut trouver r colonnes C_1, $\ldots$, C_r de A linéairement indépendantes. Notons C'_1, $\ldots$, C'_r les r colonnes de M correspondantes. Pour tout $i \in [\![1, r]\!]$, C_i est obtenue en supprimant certaines lignes de C'_i. Soit $(\lambda_1, \ldots, \lambda_r)$ r scalaires. Considérons les combinaisons linéaires $S' = \sum_{i=1}^{r} \lambda_i C'_i$ et $S = \sum_{i=1}^{r} \lambda_i C_i$. S est obtenue en rayant certaines lignes de S', donc si S' est nulle, S l'est également et tous les λ_i, sont alors nuls.

C'_1, $\ldots$, C'_r sont donc linéairement indépendantes, donc $\operatorname{rg}(M) \geqslant r$. □

Proposition 5.4.3.
Soit $M \in \mathscr{M}_{n,p}(\mathbb{K})$. Posons $r = \operatorname{rg}(M)$. Alors il existe une matrice A extraite de M, carrée, de taille r et inversible (donc de rang r).

Démonstration.
On peut trouver des colonnes C_1, $\ldots$, C_r de M telles que $\operatorname{rg}(C_1, \ldots, C_r) = r$. Ces colonnes permettent donc de former une matrice B de taille $n \times r$ de rang r. B possède n lignes. Comme elle est de rang r, il existe une r lignes L_1, $\ldots$, L_r de B telles que $\operatorname{rg}(B) = \operatorname{rg}(L_1, \ldots, L_r)$.

Or ces lignes L_1, $\ldots$, L_r permettent de former une matrice A, extraite de M. Cette matrice A est de taille $r \times r$ (donc carrée) et de rang r, donc inversible. □

6 Systèmes d'équations linéaires

6.1 Généralités

Définition 6.1.1.
On appelle *système linéaire à n équations et p inconnues* tout système de la forme :

$$\begin{cases} a_{11}x_1 & + & \dots & + & a_{1p}x_p & = & b_1 \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{n1}x_1 & + & \dots & + & a_{np}x_p & = & b_n \end{cases}$$

où les a_{ij} et les b_i sont dans $\mathbb{K}$, et les x_i sont les inconnues. Le *système homogène associé* correspond au cas où $b_1 = \cdots = b_n = 0$.

On dit que le système est *compatible* s'il admet une solution.

Interprétation matricielle En écrivant le système $AX = B$, on voit que (S) est compatible si et seulement si $B \in \operatorname{Im} A$.

Interprétation linéaire En choisissant un espace vectoriel E de dimension p et F de dimension n munis respectivement d'une base $\mathscr{B}$ et d'une base $\mathscr{C}$ et en notant u l'application linéaire de E dans F et b le vecteur de F tels que $A = \operatorname{Mat}_{\mathscr{C}}(u)$ et $B = \operatorname{Mat}_{\mathscr{C}}(b)$, on voit que (S) est compatible si et seulement si $b \in \operatorname{Im} u$.

Interprétation vectorielle En notant C_j les colonnes de A, on note que (S) est compatible si et seulement si $B \in \operatorname{Vect}(C_1, \dots, C_p)$.

Interprétation duale En notant L_i les lignes de A, et u_i les formes linéaires sur F telles que $L_i = \operatorname{Mat}_{\mathscr{C},\mathbb{K}}(u_i)$, on note que (S) est compatible si et seulement si les $u_i^{-1}(\{\, b_i \,\})$, pour $i \in [\![1, p]\!]$, contiennent au moins un vecteur en commun.

Interprétation géométrique Soit $i \in [\![1, n]\!]$. En supposant que $u_i^{-1}(\{\, b_i \,\})$ est non vide, alors il s'agit d'un hyperplan affine (*i.e.* il est de la forme $X_0 + H$ où $H = \operatorname{Ker} u_i$ est un hyperplan) si u_i n'est pas la forme linéaire nulle et il s'agit de F sinon. Donc l'ensemble des solutions est ou bien vide ou bien l'intersection d'un certain nombre d'hyperplans (autant que de lignes non nulles).

Exemple 6.1.2.
Écrire ces différents points de vue avec $\begin{pmatrix} 2 & -1 \\ 1 & 2 \\ 3 & -1 \end{pmatrix}$.

6.2 Solutions

Définition 6.2.1.
Soit (S) un système linéaire écrit sous forme matricielle $AX = B$. On appelle *rang du système* le rang de la matrice A. On le note $\operatorname{rg}(S)$.

Théorème 6.2.2.
Soit (S) un système linéaire de matrice associée $A \in \mathscr{M}_{n,p}(\mathbb{K})$.

1. L'ensemble des solutions du système homogène associé à (S) est un $\mathbb{K}$-ev de dimension $p - \operatorname{rg}(S)$ (p est le nombre d'inconnues).
2. L'ensemble des solutions de (S) est soit vide, soit un sous-espace affine de direction l'ensemble des solutions du système homogène associé à (S).

Démonstration. 1. Cet ensemble $\mathscr{S}_0$ de solutions est tout simplement $\operatorname{Ker} A$, et on utilise le théorème du rang.

2. On note $\mathscr{S}$ cet ensemble de solutions. Si (S) est compatible, soit $X_0 \in \mathscr{S}$ une solution. Soit X une autre solution. On montre alors facilement que $X - X_0$ est solution du système homogène, donc $X \in \mathscr{S}_0 + X_0$, et $\mathscr{S} \subset \mathscr{S}_0 + X_0$.
Réciproquement, soit $X \in \mathscr{S}_0 + X_0$. Il est facile de voir que $X \in \mathscr{S}$.

□

Définition 6.2.3.
Soit (S) un système linéaire écrit sous forme matricielle $AX = B$. Si A est inversible, on dit que (S) est un *système de Cramer*.

Théorème 6.2.4.
Tout système de Cramer a une unique solution, qui est $A^{-1}B$.

Démonstration.
Il est facile de voir que $A^{-1}B$ est une solution. C'est la seule car $\mathscr{S}$ est un sea dont la direction est de dimension $n-n=0$. □

7 Matrices semblables et trace

Dans toute cette partie, on ne considère que des matrices carrées.

7.1 Matrices semblables

a Changement de base pour un endomorphisme

Proposition 7.1.1.
Soit E un $\mathbb{K}$-ev de dimension finie, $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E et $u \in \mathscr{L}(E)$. Alors,

$$\mathrm{Mat}_{\mathscr{B}'}(u) = \mathrm{Mat}_{\mathscr{B}}(\mathscr{B}')^{-1}\mathrm{Mat}_{\mathscr{B}}(u)\mathrm{Mat}_{\mathscr{B}}(\mathscr{B}').$$

Démonstration.
C'est une conséquence immédiate de la formule de changement de base dans le cas où $F=E$, $\mathscr{C}=\mathscr{B}$ et $\mathscr{C}'=\mathscr{B}'$ (théorème 2.4.4). □

Définition 7.1.2.
Soit A et B deux matrices carrées de taille n. Deux matrices A et B sont dites semblables si et seulement s'il existe $P \in GL_n(\mathbb{K})$ vérifiant $A = P^{-1}BP$.

La relation « A est semblable à B » est appelée relation de *similitude*.

Proposition 7.1.3.
La relation de similitude est une relation d'équivalence sur $\mathscr{M}_n(\mathbb{K})$.

Démonstration.
Cette relation est

Réflexive car pour tout $A \in \mathscr{M}_n(\mathbb{K})$, on a $A = \mathrm{I}_n^{-1}A\mathrm{I}_n$.

Symétrique car pour tout $(A,B) \in \mathscr{M}_n(\mathbb{K})^2$ et tout $P \in GL_n(\mathbb{K})$ vérifiant $A = P^{-1}BP$, alors $P^{-1} \in GL_n(\mathbb{K})$ et $B = \left(P^{-1}\right)^{-1}AP^{-1}$.

Transitive car pour tout $(A,B,C) \in \mathscr{M}_n(\mathbb{K})^3$ et tout $(P,Q) \in GL_n(\mathbb{K})^2$ vérifiant $A = P^{-1}BP$ et $B = Q^{-1}CQ$, on a $A = P^{-1}Q^{-1}CQP = (QP)^{-1}C(QP)$.

□

Remarque 7.1.4.
Deux matrices semblables sont nécessairement équivalentes mais la réciproque n'est pas vraie. Par exemple, dans $\mathbb{R}^2$, I_2 et $17\mathrm{I}_2$ ont même rang (2) donc sont équivalentes mais ne sont pas semblables car pour tout matrice carrée P de taille 2 inversible, $P^{-1}(\mathrm{I}_2)P = \mathrm{I}_2 \neq 17\mathrm{I}_2$.

Proposition 7.1.5.
Soit A et B deux matrices carrées de taille n. A et B sont semblables si et seulement si ce sont les matrices d'un même endomorphisme u exprimées dans deux bases différentes.

Plus exactement, A et B sont semblables si et seulement s'il existe un espace vectoriel E de dimension n, deux bases $\mathscr{B}$ et $\mathscr{B}'$ et un endomorphisme u tel que $\mathrm{Mat}_{\mathscr{B}}(u) = A$ et $\mathrm{Mat}_{\mathscr{B}'}(u) = B$.

Démonstration.
Le sens indirect est une conséquence de la formule de changement de base pour un endomorphisme (proposition 7.1.1).

Montrons le sens direct. Supposons que A et B sont semblables, c'est-à-dire qu'il existe P tel que $A = P^{-1}BP$. Choisissons un espace vectoriel E de dimension n et une base $\mathscr{B} = (e_1, \ldots, e_n)$ de cet espace (on peut par exemple prendre $E = \mathbb{K}^n$ et $\mathscr{B}$ la base canonique de $\mathbb{K}^n$). Notons $e'_1, \ldots, e'_n$ les vecteurs de E dont les coordonnées dans la base $\mathscr{B}$ sont les colonnes de P. Alors $P = \mathrm{Mat}_{\mathscr{B}}(\mathscr{B}')$.

Notons enfin u l'endomorphisme de E vérifiant $\mathrm{Mat}_{\mathscr{B}}(u) = B$.

Alors,

$$\begin{aligned}\mathrm{Mat}_{\mathscr{B}'}(u) &= \mathrm{Mat}_{\mathscr{B}}(\mathscr{B}')^{-1}\mathrm{Mat}_{\mathscr{B}}(u)\mathrm{Mat}_{\mathscr{B}}(\mathscr{B}')\\ &= P^{-1}BP\\ &= A,\end{aligned}$$

donc A et B sont les deux matrices d'un même endomorphisme relativement aux bases respectives $\mathscr{B}'$ et $\mathscr{B}$. □

Proposition 7.1.6.
Considérons deux matrices A et B semblables de taille n. Alors pour tout $k \in \mathbb{N}$, A^k et B^k sont des matrices semblables.

Démonstration.
Ce résultat peut être démontré au moins des deux manières suivantes :

Par le calcul On montre par récurrence sur k que pour tout k, on a $A^k = P^{-1}B^kP$. Pour montrer que ce prédicat est héréditaire, il suffit de constater que pour tout $k \in \mathbb{N}$ tel que le prédicat est vérifié, on a également $A^{k+1} = A^kA = P^{-1}B^kPP^{-1}BP$.

Géométriquement A et B sont deux matrices d'un même endomorphisme u, donc A^k et B^k sont deux matrices de u^k.

□

7.2 Trace d'une matrice carrée

a Définition

Définition 7.2.1.
Soit A une matrice carrée de taille n. Alors la *trace de* A, notée $\mathrm{tr}\,(A)$ (ou $\mathrm{Tr}(A)$), est la somme des éléments diagonaux de A.

En notant $(a_{ij})_{(i,j)\in[\![1,n]\!]\times[\![1,n]\!]}$ les coefficients de A :

$$\mathrm{tr}\,(A) = \sum_{i=1}^{n} a_{ii}.$$

Remarque 7.2.2.
Pour tout $A \in \mathscr{M}_n(\mathbb{K})$, on a

$$\mathrm{tr}\,({}^tA) = \mathrm{tr}\,(A).$$

Démonstration.
Les matrices ${}^tA$ et A ont les mêmes éléments diagonaux. □

b Linéarité

Proposition 7.2.3.
Pour tout $n \in \mathbb{N}^*$, l'application trace est une forme linéaire sur $\mathscr{M}_n(\mathbb{K})$.

Démonstration.
Soit $(A, B) \in \mathscr{M}_n(\mathbb{K})^2$ et $\lambda \in \mathbb{K}$. Posons $C = \lambda A + B$ et montrons $\mathrm{tr}\,(\lambda A+B) = \lambda\mathrm{tr}\,(A)+\mathrm{tr}\,(B)$. Notons (a_{ij}), (b_{ij}) et c_{ij} les coefficients respectivement de A, de B et de C.

Alors, on a

$$\begin{aligned}\mathrm{tr}\,(C) &= \sum_{i=1}^{n} c_{ii}\\ &= \sum_{i=1}^{n} (\lambda a_{ii} b_{ii})\\ &= \lambda \sum_{i=1}^{n} a_{ii} + \sum_{i=1}^{n} b_{ii}\\ &= \lambda\mathrm{tr}\,(A) + \mathrm{tr}\,(B).\end{aligned}$$

□

c Propriété fondamentale de la trace

Proposition 7.2.4.
Soit $(A, B) \in \mathscr{M}_n(\mathbb{K})^2$, alors,

$$\mathrm{tr}\,(AB) = \mathrm{tr}\,(BA).$$

 $\mathrm{tr}\,(A \times B) \neq \mathrm{tr}\,A \times \mathrm{tr}\,B$; par exemple, dans $\mathscr{M}_2(\mathbb{K})$, $0 = \mathrm{tr}\,(E_{11} \times E_{22}) \neq 1 = \mathrm{tr}\,(E_{11}) \times \mathrm{tr}\,(E_{22})$.

Démonstration.
Posons $C = AB$ et $D = BA$. Notons (a_{ij}), (b_{ij}), (c_{ij}) et (d_{ij}) les coefficients respectifs de A, B, C et D.

On a, pour tout $(i, j) \in [\![1, n]\!]^2$:

$$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj},$$

$$d_{ij} = \sum_{k=1}^{n} b_{ik}a_{kj}.$$

D'où, pour tout $i \in [\![1, n]\!]$:

$$c_{ii} = \sum_{k=1}^{n} a_{ik}b_{ki},$$

$$d_{ii} = \sum_{k=1}^{n} b_{ik}a_{ki}.$$

D'où :

$$\mathrm{tr}\,(C) = \sum_{i=1}^{n}\sum_{k=1}^{n} a_{ik}b_{ki},$$

$$\mathrm{tr}\,(D) = \sum_{i=1}^{n}\sum_{k=1}^{n} a_{ki}b_{ik}.$$

Ainsi,

$$\operatorname{tr}(C) = \sum_{1\leqslant\alpha,\beta\leqslant n} a_{\alpha\beta}b_{\beta\alpha},$$
$$\operatorname{tr}(D) = \sum_{1\leqslant\alpha,\beta\leqslant n} a_{\alpha\beta}b_{\beta\alpha},$$

d'où l'égalité recherchée. □

Remarque 7.2.5. 1. On peut déduire de cette égalité que la trace d'un produit de matrices est invariant par permutations circulaires : pour toutes matrices $A_1, \ldots, A_k$ de taille n, on a

$$\begin{aligned}\operatorname{tr}(A_1A_2\ldots A_{k-1}A_k) &= \operatorname{tr}(A_2\ldots A_kA_1)\\ &= \operatorname{tr}(A_3\ldots A_kA_1A_2)\\ &\ldots\end{aligned}$$

2. En revanche, la trace d'un produit de matrice n'est **pas** invariant par n'importe quelle permutation. Par exemple, dans $\mathscr{M}_2(\mathbb{K})$, en notant (E_{ij}) les matrices de la base canonique :

$$\operatorname{tr}(E_{21}E_{11}E_{12}) = 1 \neq 0 = \operatorname{tr}(E_{11}E_{21}E_{12}).$$

d Invariance par similitude

Proposition 7.2.6.
Deux matrices semblables ont même trace (on dit que la trace est un *invariant de similitude*) : soit $A, B \in \mathscr{M}_n(\mathbb{K})$, deux matrices semblables. Alors $\operatorname{tr}(A) = \operatorname{tr}(B)$.

Démonstration.
Il existe $P \in GL_n(\mathbb{K})$ vérifiant $A = P^{-1}BP$. Alors on a

$$\begin{aligned}\operatorname{tr}(A) &= \operatorname{tr}\left(P^{-1}(BP)\right)\\ &= \operatorname{tr}\left((BP)P^{-1}\right)\\ &= \operatorname{tr}(B).\end{aligned}$$

□

 Ce résultat n'est pas valable pour des matrices équivalentes. Par exemple dans $\mathscr{M}_2(\mathbb{K})$, $\operatorname{tr}(\mathrm{I}_2.\mathrm{I}_2.(2\mathrm{I}_2)) \neq \operatorname{tr}\mathrm{I}_2$.

e Trace d'un endomorphisme en dimension finie

Définition 7.2.7.
Soit E un espace vectoriel de dimension finie et $u \in \mathscr{L}(E)$. La *trace de l'endomorphisme* u et on note $\operatorname{tr}(u)$ (ou $\operatorname{Tr}(u)$) est le scalaire défini par

$$\operatorname{tr}(u) = \operatorname{tr}(\operatorname{Mat}_{\mathscr{B}}(u)),$$

où $\mathscr{B}$ est une base quelconque de E. Cette valeur ne dépend pas du choix de la base $\mathscr{B}$.

Démonstration.
On a vu d'une part que deux matrices d'un même endomorphisme sont nécessairement semblables et d'autre part que la trace de matrices est un invariant de similitude. La valeur de $\operatorname{tr}(u)$ ne dépend donc pas du choix de la base $\mathscr{B}$. □

f Propriétés

Proposition 7.2.8.
Soit E un espace vectoriel de dimension finie. La trace est une forme linéaire sur $\mathscr{L}(E)$.

Démonstration.
Il suffit de choisir une base de $\mathscr{B}$ de E et constater que pour tous endomorphismes u et v, de matrices respectives A et B, et pour tout scalaire λ, on a

$$\begin{aligned}\operatorname{tr}(\lambda u + v) &= \operatorname{tr}(\lambda A + B)\\ &= \lambda\operatorname{tr}(A) + \operatorname{tr}(B)\\ &= \lambda\operatorname{tr}(u) + \operatorname{tr}(v).\end{aligned}$$

□

Proposition 7.2.9.
Soit E un espace vectoriel de dimension finie et v et u deux endomorphismes de E. Alors,

$$\operatorname{tr}(v \circ u) = \operatorname{tr}(u \circ v).$$

Démonstration.
Il suffit de choisir une base $\mathscr{B}$ de E. En notant A et B les matrices respectives de u et v, la matrice de $v \circ u$ est BA, celle de $u \circ v$ est AB et on sait que $\operatorname{tr}(AB) = \operatorname{tr}(BA)$, d'où le résultat. □

Exemple 7.2.10.
Vérifier ce résultat sur deux endomorphismes de $\mathbb{R}^3$.

g Trace d'un projecteur

Proposition 7.2.11.
Soit E un espace vectoriel de dimension finie et p un projecteur. Alors, la trace de p est la dimension de $\operatorname{Im} p$:

$$\operatorname{tr}(p) = \operatorname{rg} p.$$

Démonstration.
Notons n la dimension de E, q celle de $\operatorname{Im} p$. p étant un projecteur, on a $E = \operatorname{Im} p \oplus \operatorname{Ker} p$. Soit $(e_1, \dots, e_q)$ une base de $\operatorname{Im} p$. On a $\dim \operatorname{Ker} p = n - q$, donc on peut trouver une base $(e_{q+1}, \dots, e_n)$ de $\operatorname{Ker} p$. La famille $(e_1, \dots, e_n)$ est alors une base $\mathscr{B}$ de E et relativement à cette base, la matrice de p est une matrice diagonale dont les q premiers coefficients valent 1 et tous les autres sont nuls. Sa trace est donc q. □

Remarque 7.2.12.
Ce résultat est faux pour d'autres endomorphismes que les projecteurs. Considérer par exemple un endomorphisme de matrice E_{12}.

8 Matrices par blocs

Définition 8.0.1.
Soit $M \in \mathscr{M}_{n,p}(\mathbb{K})$. On peut écrire la matrice sous la forme

$$M = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1p} \\ m_{21} & m_{22} & \cdots & m_{2p} \\ \vdots & \vdots & & \vdots \\ m_{n1} & m_{n2} & \cdots & m_{np} \end{pmatrix}.$$

En traçant $q-1$ lignes horizontales distinctes et $r-1$ lignes verticales distinctes dans le tableau représentant M, on peut décomposer M en $q \times r$ matrices extraites M_{ij} pour $(i,j) \in [\![1,q]\!] \times [\![1,r]\!]$:

$$M = \begin{pmatrix} M_{11} & M_{12} & \cdots & M_{1r} \\ M_{21} & M_{22} & \cdots & M_{2r} \\ \vdots & \vdots & & \vdots \\ M_{q1} & M_{q2} & \cdots & M_{qr} \end{pmatrix}.$$

Cette décomposition est appelée *décomposition par blocs* de M en $q \times r$ blocs.

Formellement, une décomposition par bloc de M est la donnée de $q \times r$ matrices M_{ij} pour $(i,j) \in [\![1,q]\!] \times [\![1,r]\!]$ telles que

1. Pour tout $i \in [\![1,q]\!]$, les matrices M_{i1}, …, M_{ir} ont un même nombre de lignes n_i (toutes les matrices d'une même ligne ont même nombre de lignes).
2. Pour tout $j \in [\![1,r]\!]$, les matrices M_{1j}, …, M_{qj} ont un même nombre de colonnes p_j (toutes les matrices d'une même colonne ont même nombre de colonnes).
3. En notant a_{hk}^{ij} le coefficient de la ligne h, colonne k de la matrice M_{ij} pour $(i,j) \in [\![1,q]\!] \times [\![1,r]\!]$ et $(h,k) \in [\![1,n_i]\!] \times [\![1,p_j]\!]$, on a $a_{hk}^{ij} = m_{(s+h)(t+k)}$ où $s = n_1 + \ldots + n_{i-1}$ et $t = p_1 + \ldots + p_{j-1}$.

On dira que la décomposition précédente est *triangulaire supérieure par blocs* si $n = p$ et que :

1. pour tout $i \in [\![1,q]\!]$, M_{ii} est carrée ;
2. pour tout $(i,j) \in [\![1,q]\!]^2$ avec $i > j$, M_{ij} est nulle.

On définit de même les décompositions *triangulaires inférieures par blocs.*

Enfin, les décompositions *diagonales par blocs* sont celles dont tous les blocs M_{ij} tels $i \neq j$ sont nuls et tous les blocs M_{ii} sont carrés.

Exemple 8.0.2.
En posant

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 7 & 8 & 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 & 17 & 18 \\ 19 & 20 & 21 & 22 & 23 & 24 \\ 25 & 26 & 27 & 28 & 29 & 30 \\ 31 & 32 & 33 & 34 & 35 & 36 \end{pmatrix},$$

A peut se décomposer par bloc en

$$\begin{pmatrix} B & C & D \\ E & F & G \\ H & I & J \end{pmatrix},$$

où

$$B = \begin{pmatrix} 1 & 2 \\ 7 & 8 \end{pmatrix}, \qquad C = \begin{pmatrix} 3 \\ 9 \end{pmatrix},$$
$$D = \begin{pmatrix} 4 & 5 & 6 \\ 10 & 11 & 12 \end{pmatrix}, \quad E = \begin{pmatrix} 13 & 14 \end{pmatrix},$$
$$F = \begin{pmatrix} 15 \end{pmatrix}, \qquad G = \begin{pmatrix} 16 & 17 & 18 \end{pmatrix},$$
$$H = \begin{pmatrix} 19 & 20 \\ 25 & 26 \\ 31 & 32 \end{pmatrix}, \qquad I = \begin{pmatrix} 21 \\ 27 \\ 33 \end{pmatrix},$$
$$J = \begin{pmatrix} 22 & 23 & 24 \\ 28 & 29 & 30 \\ 34 & 35 & 36 \end{pmatrix}.$$

Remarque 8.0.3.

Lorsqu'on parle de décomposition triangulaire supérieure (resp. triangulaire inférieure, diagonale) par bloc, c'est bien la décomposition qui est triangulaire supérieure (resp. triangulaire inférieure, diagonale). Toute matrice carrée admet en effet une décomposition (triviale) triangulaire supérieure (resp. triangulaire inférieure, diagonale) par bloc.

Proposition 8.0.4 (Interprétation géométrique)**.**
On peut interpréter la décomposition par blocs de la façon suivante. Considérons la matrice $n \times p$ donnée dans la définition précédente :

$$M = \begin{pmatrix} M_{11} & M_{12} & \cdots & M_{1r} \\ M_{21} & M_{22} & \cdots & M_{2r} \\ \vdots & \vdots & & \vdots \\ M_{q1} & M_{q2} & \cdots & M_{qr} \end{pmatrix},$$

où pour tout $(i,j) \in [\![1,q]\!] \times [\![1,r]\!]$, M_{ij} est de taille $n_i \times p_j$. Soit E et F des espaces vectoriels respectivement de dimension p et n, $\mathscr{B} = (e_1, \ldots, e_p)$ une base de E, $\mathscr{C} = (f_1, \ldots, f_n)$ une base de F et $u \in \mathscr{L}(E,F)$ vérifiant $\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)$.

On note $\mathscr{B}_1$ la famille des p_1 premiers vecteurs de $\mathscr{B}$, $\mathscr{B}_2$ celle des p_2 suivants, ..., $\mathscr{B}_r$ celle des p_r derniers et $E_1 = \mathrm{Vect}(\mathscr{B}_1)$, ..., $E_r = \mathrm{Vect}(\mathscr{B}_r)$. Pour tout $j \in [\![1,r]\!]$, $\mathscr{B}_j$ est une base de E_j.

On note $\mathscr{C}_1$ la famille des n_1 premiers vecteurs de $\mathscr{C}$, $\mathscr{C}_2$ celle des n_2 suivants, ..., $\mathscr{C}_r$ celle des n_r derniers et $F_1 = \mathrm{Vect}(\mathscr{C}_1)$, ..., $F_q = \mathrm{Vect}(\mathscr{C}_q)$. Pour tout $i \in [\![1,q]\!]$, $\mathscr{C}_i$ est une base de F_i.

Alors

$$E = E_1 \oplus \ldots \oplus E_r,$$
$$F = F_1 \oplus \ldots \oplus F_q.$$

Tout $y \in F$ s'écrit de façon unique $\pi'_1(y) + \ldots + \pi'_q(y)$, où $\pi'_i(y) \in F_i$ pour tout $i \in [\![1,q]\!]$ (π'_i est alors la projection sur F_i parallèlement à la somme des F_k pour $k \neq i$).

De même notons, pour tout $j \in [\![1,r]\!]$, π_j la projection sur E_j parallèlement à la somme des E_k pour $k \neq j$.

Alors, pour tout $(i,j) \in [\![1,q]\!] \times [\![1,r]\!]$, on note

$$u_{ij} : \left\{ \begin{array}{ccc} E_j & \longrightarrow & F_i \\ x & \longmapsto & \pi'_i(u(x)) \end{array} \right. .$$

Ainsi, u_{ij} est obtenu en restreignant u au départ à E_j et, comme il n'est pas a priori possible de le restreindre à l'arrivée à F_i en le composant à gauche par la projection sur F_i (par rapport à la somme des F_k pour $k \neq i$) : $u_{ij} = \pi'_i \circ u_{|E_j}$.

On a alors, pour tout $x \in E$:

$$u(x) = \sum_{(i,j) \in [\![1,q]\!] \times [\![1,r]\!]} u_{ij}(\pi_j(x)).$$

De plus, pour tout $(i,j) \in [\![1,q]\!] \times [\![1,r]\!]$,

$$\mathrm{Mat}_{\mathscr{B}_j,\mathscr{C}_i}(u_{ij}) = M_{ij}.$$

Démonstration.

Remarquons tout d'abord que pour tout $x \in E$, on a

$$\begin{aligned} u(x) &= u\left(\sum_{j=1}^{r} \pi_j(x)\right) \\ &= \sum_{j=1}^{r} u(\pi_j(x)) \\ &= \sum_{j=1}^{r}\sum_{i=1}^{q} \pi_i'(u(\pi_j(x))) \\ &= \sum_{(i,j)\in[\![1,q]\!]\times[\![1,r]\!]} u_{ij}(\pi_j(x)). \end{aligned}$$

Soit $(i,j) \in [\![1,q]\!] \times [\![1,r]\!]$. On a

$$\begin{aligned} \mathscr{C}_i &= (f_{s+1}, f_{s+2}, \ldots, f_{s+n_i}), \\ \mathscr{B}_j &= (e_{t+1}, e_{t+2}, \ldots, e_{t+p_j}), \end{aligned}$$

où

$$\begin{aligned} s &= n_1 + \ldots + n_{i-1}, \\ t &= p_1 + \ldots + p_{j-1}. \end{aligned}$$

Soit $k \in [\![1,p_j]\!]$. En notant $(m_{ij})_{(i,j)\in[\![1,n]\!]\times[\![1,q]\!]}$ les coefficients de M, on a

$$\begin{aligned} u_{ij}(e_k) &= \pi_i'(u(e_{t+k})) \\ &= \pi_i'\left(\sum_{h=1}^{n} m_{h(t+k)} f_h\right) \\ &= \sum_{h=s+1}^{s+n_i} m_{h(t+k)} f_h \\ &= \sum_{h=1}^{n_i} m_{(s+h)(t+k)} f_{s+h}. \end{aligned}$$

On en déduit que la matrice de u_{ij} est la matrice des $\left(m_{(s+h),(t+k)}\right)_{(h,k)\in[\![1,n_i]\!]\times[\![1,p_j]\!]}$ qui est exactement la matrice M_{ij}. On a donc $\mathrm{Mat}_{\mathscr{B}_j,\mathscr{C}_i}(u_{ij}) = M_{ij}$. □

Proposition 8.0.5 (Addition par blocs)**.**
Soit $(A,B) \in \mathscr{M}_{n,p}(\mathbb{K})^2$, admettant des décompositions par blocs

$$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1r} \\ A_{21} & A_{22} & \cdots & A_{2r} \\ \vdots & \vdots & & \vdots \\ A_{q1} & A_{q2} & \cdots & A_{qr} \end{pmatrix},$$

$$B = \begin{pmatrix} B_{11} & B_{12} & \cdots & B_{1r} \\ B_{21} & B_{22} & \cdots & B_{2r} \\ \vdots & \vdots & & \vdots \\ B_{q1} & B_{q2} & \cdots & B_{qr} \end{pmatrix},$$

où pour tout $(i,j) \in [\![1,q]\!] \times [\![1,r]\!]$, A_{ij} et B_{ij} sont de même taille.

Alors $A+B$ vaut

$$\begin{pmatrix} A_{11}+B_{11} & A_{12}+B_{12} & \cdots & A_{1r}+B_{1r} \\ A_{21}+B_{21} & A_{22}+B_{22} & \cdots & A_{2r}+B_{2r} \\ \vdots & \vdots & & \vdots \\ A_{q1}+B_{q1} & A_{q2}+B_{q2} & \cdots & A_{qr}+B_{qr} \end{pmatrix}.$$

Démonstration.
Notons, pour tout $i \in [\![1,q]\!]$ (resp. pour tout $j \in [\![1,r]\!]$), n_i (resp. p_j) le nombre de lignes (resp. de colonnes) des matrices de la ligne i (resp. de la colonne j) de ces décompositions par bloc.

Posons $C = A+B$ et pour tout $(i,j) \in [\![1,q]\!] \times [\![1,r]\!]$, $C_{ij} = A_{ij} + B_{ij}$.

Notons a_{ij} pour $(i,j) \in [\![1,n]\!] \times [\![1,p]\!]$ les coefficients de la matrice A, b_{ij} ceux de B, c_{ij} ceux de C et pour tout $(i,j) \in [\![1,q]\!] \times [\![1,r]\!]$ et tout $(k,h) \in [\![1,n_i]\!] \times [\![1,p_j]\!]$, a_{hk}^{ij} (resp. b_{hk}^{ij}, resp. c_{hk}^{ij}) ceux de A_{ij} (resp. B_{ij}, resp. C_{ij}). On a alors, en posant $s = n_1 + \ldots + n_{i-1} + h$ et $t = p_1 + \ldots + p_{j-1} + k$.

$$c_{st} = a_{st} + b_{st} = a_{hk}^{ij} + b_{hk}^{ij} = c_{hk}^{ij}$$

On a donc

$$C = \begin{pmatrix} C_{11} & C_{12} & \cdots & C_{1r} \\ C_{21} & C_{22} & \cdots & C_{2r} \\ \vdots & \vdots & & \vdots \\ C_{q1} & C_{q2} & \cdots & C_{qr} \end{pmatrix}$$

D'où le résultat. □

Proposition 8.0.6 (Multiplication par blocs)**.**
Soit $A \in \mathscr{M}_{n,p}(\mathbb{K})$ et $B \in \mathscr{M}_{p,q}(\mathbb{K})$.

On considère des décompositions de A en $r \times s$ blocs et de B en $s \times t$ blocs,

$$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1s} \\ A_{21} & A_{22} & \cdots & A_{2s} \\ \vdots & \vdots & & \vdots \\ A_{r1} & A_{r2} & \cdots & A_{rs} \end{pmatrix},$$

$$B = \begin{pmatrix} B_{11} & B_{12} & \cdots & B_{1t} \\ B_{21} & B_{22} & \cdots & B_{2t} \\ \vdots & \vdots & & \vdots \\ B_{s1} & B_{s2} & \cdots & B_{st} \end{pmatrix},$$

telles que pour tout pour tout $(i,k,j) \in [\![1,r]\!] \times [\![1,s]\!] \times [\![1,t]\!]$, les matrices A_{ik} et B_{kj} aient des tailles compatibles par la multiplication.

Alors le produit $A \times B$ s'écrit par blocs :

$$C = \begin{pmatrix} C_{11} & C_{12} & \cdots & C_{1t} \\ C_{21} & C_{22} & \cdots & C_{2t} \\ \vdots & \vdots & & \vdots \\ C_{r1} & C_{r2} & \cdots & C_{rt} \end{pmatrix},$$

où pour tout $(i,j) \in [\![1,r]\!] \times [\![1,t]\!]$, on a

$$C_{ij} = \sum_{k=1}^{s} A_{ik} \times B_{kj}$$

Démonstration (non exigible)**.**
Nous donnons ici les grandes lignes de la démonstration, que nous traitons de façon géométrique.

Choisissons E, F, G trois espaces vectoriels de dimensions respectives q, p, n et trois bases respectives $\mathscr{B}$, $\mathscr{C}$ et $\mathscr{D}$ de ces espaces.

Notons $u \in \mathscr{L}(E,F)$ et $v \in \mathscr{L}(F,G)$ les applications linéaires vérifiant $\mathrm{Mat}_{(\mathscr{B},\mathscr{C})}(u) = B$ et $\mathrm{Mat}_{(\mathscr{C},\mathscr{D})}(v) = A$.

Comme précédemment, on peut, à partir de la base $\mathscr{B}$, décomposer E en une somme directe $E_1 \oplus \ldots \oplus E_t$ et construire des projections $\pi_1, \ldots, \pi_t$ sur ces sous-espaces respectifs, parallèlement à la somme des autres.

On fait de même pour décomposer F en $F_1 \oplus \ldots \oplus F_s$ et construire les projections $\pi'_1, \ldots, \pi'_s$ associées et pour décomposer G en $G_1 \oplus \ldots \oplus G_r$ et construire les projections $\pi''_1, \ldots, \pi''_r$ associées.

Posons $w = v \circ u$.

On peut construire comme précédemment des $u_{ij} \in \mathscr{L}(E_j, F_i)$ pour $(i,j) \in [\![1,s]\!] \times [\![1,t]\!]$ pour décomposer u, des $v_{ij} \in \mathscr{L}(F_j, G_i)$ pour $(i,j) \in [\![1,r]\!] \times [\![1,s]\!]$ pour décomposer v et des $w_{ij} \in \mathscr{L}(E_j, G_i)$ pour $(i,j) \in [\![1,r]\!] \times [\![1,t]\!]$ pour décomposer w.

En posant $C_{ij} = \mathrm{Mat}_{\mathscr{B},\mathscr{D}}(w_{ij})$ pour $(i,j) \in [\![1,r]\!] \times [\![1,t]\!]$, on obtient une décomposition par bloc de la matrice $\mathrm{Mat}_{\mathscr{B},\mathscr{D}}(w)$ qui n'est autre que $A \times B$.

Soit alors $(i,j) \in [\![1,r]\!] \times [\![1,s]\!]$ et $x \in E_j$. On a

$$\begin{aligned} w_{ij} &= \pi''_i \circ w_{|E_j} \\ &= \pi''_i \circ v \circ u_{|E_j} \\ &= \pi''_i \circ v \circ \left(\sum_{k=1}^{s} \pi'_k \right) \circ u_{|E_j} \\ &= \sum_{k=1}^{n} \pi''_i \circ v \circ \pi'_k \circ u_{|E_j} \\ &= \sum_{k=1}^{n} \pi''_i \circ v_{|F_k} \circ \pi'_k \circ u_{|E_j} \\ &= \sum_{k=1}^{n} v_{ik} \circ u_{kj}. \end{aligned}$$

On en déduit

$$\begin{aligned} C_{ij} &= \mathrm{Mat}_{\mathscr{B},\mathscr{D}}\left(\sum_{k=1}^{n} v_{ik} \circ u_{kj}\right) \\ &= \sum_{k=1}^{n} \mathrm{Mat}_{\mathscr{C},\mathscr{D}}(v_{ik}) \times \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u_{kj}) \\ &= \sum_{k=1}^{n} A_{ik} \times B_{kj}. \end{aligned}$$

□

Chapitre XXIV

Déterminants

Dans tout ce chapitre $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Les lettres n, p, q et r désignent des entiers naturels non nuls.

1 Groupe symétrique

Dans toute cette section, E désigne un ensemble.

1.1 Permutations

Définition 1.1.1.
On appelle ***permutation de*** E toute bijection de E dans E. On note S_E l'ensemble des permutations de E. Alors $(S_E, \circ)$ est un groupe appelé ***groupe des permutations de*** E.

Définition 1.1.2.
Si $E = [\![1, n]\!]$, on note S_n le groupe des pemutations de E, qui est un groupe fini de cardinal $n!$. Ce groupe s'appelle le ***groupe symétrique*** d'ordre n (ou de degré n). Une permutation σ de S_n se note $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$.

Exemple 1.1.3.
• La permutation σ de $[\![1, 5]\!]$ vérifiant $\sigma(1) = 2$, $\sigma(2) = 5$, $\sigma(3) = 1$, $\sigma(4) = 4$ et $\sigma(5) = 3$ se note $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}$. On vérifie bien que 1, 2, 3, 4 et 5 apparaissent une et une seule fois par ligne.
• Cette écriture permet de composer facilement des permutations :
$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$,
et de facilement calculer les antécédents.

1.2 Permutations particulières

Définition 1.2.1.
Soient $\sigma \in S_E$, et $x \in E$. On appelle ***orbite*** de x l'ensemble $\mathfrak{O}(x) = \{\sigma^k(x),\ k \in \mathbb{Z}\}$.

Exemple 1.2.2.
Si $E = [\![1, 6]\!]$ et $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 3 & 6 & 4 \end{pmatrix}$, alors $\mathfrak{O}(1) = \mathfrak{O}(2) = \{1, 2\}$ et $\mathfrak{O}(3) = \mathfrak{O}(4) = \mathfrak{O}(5) = \mathfrak{O}(6) = \{3, 4, 5, 6\}$.

Définition 1.2.3.
On appelle ***permutation circulaire*** toute permutation $\sigma \in S_E$ telle qu'il existe $x \in E$ vérifiant $\mathfrak{O}(x) = E$.

Exemple 1.2.4.
$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ est une permutation circulaire.

 Si une permutation a un point fixe et si card $(E) > 1$, alors la permutation n'est pas circulaire, mais la non existence de point fixe n'implique pas que la permutation est circulaire. Par exemple $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$ n'est pas circulaire.

Définition 1.2.5.
On dit qu'une permutation est un ***cycle*** s'il y a au plus une orbite non réduite à un élément. Cette orbite s'appelle alors le ***support*** de ce cycle, et son cardinal s'appelle la ***longueur*** du cycle.

Remarque 1.2.6.
Les éléments qui sont hors du support d'un cycle sont des points fixes de cette permutation.

Exemple 1.2.7.
$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}$ est un cycle de longueur 3 dont le support est $\{2, 3, 5\}$.

Remarque 1.2.8.
On note généralement les cycles de la manière suivante : $(x_1, x_2, \dots, x_p)$, où p est la longueur du cycle et $\{x_1, x_2, \dots, x_p\}$ son support, dans l'ordre, c'est-à-dire que x_1 est envoyé sur x_2, x_2 sur x_3,

..., x_{p-1} sur x_p et enfin x_p sur x_1. Les éléments de $[\![1,n]\!]$ autres que $x_1,\dots,x_p$ sont les points fixes du permutation. Le cycle de l'exemple 1.2.7 est ainsi tout simplement noté $(2,5,3)$. Remarquons qu'on peut aussi l'écrire $(5,3,2)$ ou $(3,2,5)$, car un cycle est une « boucle ».

Définition 1.2.9.
On appelle ***transposition*** tout cycle de longueur 2. Une transposition échange ainsi deux éléments de E. Si a et b sont deux éléments de E, la transposition qui échange a et b est notée τ_{ab}.

Exemple 1.2.10.
$\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}$ est une transposition, notée τ_{24}.

Remarque 1.2.11.
Toute transposition est une involution, *i.e.* est sa propre inverse.

1.3 Décomposition d'une permutation

Dans toute la suite de la section 1, $E=[\![1,n]\!]$. On se place donc dans S_n.

Lemme 1.3.1.
Deux cycles de supports disjoints commutent.

Démonstration.
Ceci est dû au fait que deux cycles de supports disjoints agissent sur des éléments distincts. Soient σ_1 et σ_2 deux cycles de supports respectifs I et J inclus dans $[\![1,n]\!]$ et tels que $I\cap J=\varnothing$. Soit $x\in I$, $y\in J$ et $z\in(I\cup J)^C$.

Alors $\sigma_1(x)\neq x$ et $\sigma_1(x)\in I$ donc $\sigma_1(x)\notin J$. Ainsi $\sigma_2(x)=x$ et $\sigma_2(\sigma_1(x))=\sigma_1(x)$. On en tire $\sigma_1\circ\sigma_2(x)=\sigma_1(x)=\sigma_2\circ\sigma_1(x)$.

De même, $\sigma_1(y)=y$ et $\sigma_2(y)\notin J$ donc $\sigma_1(\sigma_2(y))=\sigma_2(y)$, et il vient $\sigma_2\circ\sigma_1(y)=\sigma_2(y)=\sigma_1\circ\sigma_2(y)$.

Enfin, $\sigma_1(z)=z=\sigma_2(z)$ et donc $\sigma_1\circ\sigma_2(z)=z=\sigma_2\circ\sigma(1)(z)$.

Ainsi $\sigma_1\circ\sigma_2$ et $\sigma_2\circ\sigma_1$ coïncident en tous les éléments de $[\![1,n]\!]$, et sont bien égales. □

Exemple 1.3.2.
Pour vous en assurer, calculez pour $n=7$, $(1\ 4\ 3)\circ(2\ 5)$ et $(2\ 5)\circ(1\ 4\ 3)$.

Lemme 1.3.3.
Soit $\sigma\in S_n$. Tout point de $[\![1,n]\!]$ est dans une et une seule orbite de σ. L'ensemble des orbites de σ forme donc une partition de E (c'est-à-dire que la réunion de ces orbites est $[\![1,n]\!]$ mais ces orbites sont deux à deux disjointes).

Démonstration.
Tout point est dans au moins une orbite : la sienne. Si x est dans deux orbites distinctes, *i.e.* $x\in\mathfrak{O}(y)$ et $x\in\mathfrak{O}(z)$ avec $\mathfrak{O}(y)\neq\mathfrak{O}(z)$, alors il existe $k,\ell\in\mathbb{Z}$ tels que $x=\sigma^k(y)=\sigma^\ell(z)$. D'où $y=\sigma^{\ell-k}(z)$, et ainsi $y\in\mathfrak{O}(z)$. Il est alors facile de vérifier que $\mathfrak{O}(y)=\mathfrak{O}(z)$, ce qui est une contradiction. □

Théorème 1.3.4.
Toute permutation se décompose en produit de cycles de supports disjoints. À l'ordre près des facteurs, cette décomposition est unique.

Démonstration.
D'après le lemme 1.3.1, si cette décomposition existe on peut permuter l'ordre des facteurs.
Notons $\mathfrak{O}_1,\dots,\mathfrak{O}p$ les orbites de σ de cardinal au moins 2. Pour tout $i\in[\![1,p]\!]$ on définit la permutation C_i de la manière suivante :

(i) $\forall x\in\mathfrak{O}_i$, $C_i(x)=\sigma(x)$;
(ii) $\forall x\in[\![1,n]\!]\backslash\mathfrak{O}_i$, $C_i(x)=x$.

On vérifie que les C_i sont des cycles, que leurs supports sont deux à deux disjoints, et que $C_1\circ C_2\circ\ldots\circ C_p=\sigma$.

La démonstration de l'unicité n'est pas exigible, nous la donnons à but d'information. Soit $(C_1,\dots,C_p)$ des cycles à supports disjoints, vérifiant $\prod_{i=1}^{p}C_i=\sigma$. Soit $1\leqslant i\leqslant p$, soit x appartenant au support de C_i ($C_i(x)\neq x$ et si $j\neq i$, $C_j(x)=x$). Alors, comme les cycles C_j commutent, on a

$$\sigma(x)=\left(\prod_{j=1}^{p}C_j\right)(x)=C_i\left[\left(\prod_{j\neq i}C_j\right)(x)\right]=C_i(x).$$

Ainsi, l'orbite de x par C_i et par σ coïncident : l'orbite de x (par σ) est donc le support de C_i. Réciproquement, si $\sigma(x)\neq x$, alors il existe forcément un i tel que $C_i(x)\neq x$. Il y a donc exactement autant de cycles que d'orbites de σ non réduites à un élément, donc p est unique. De plus, chaque cycle a un support correspondant à une orbite de σ, non réduite à un point. Il suffit maintenant de voir que pour chaque orbite de σ de longueur $\ell>1$, il existe un unique cycle dont le support est exactement cette orbite : c'est, avec un élément x de cette orbite, $(x,\sigma(x),\dots,\sigma^{\ell-1}(x))$. □

Il faut savoir décomposer une permutation en produit de cycles de supports disjoints. Dans la pratique, voici comment l'on procède (le procédé est celui de la démonstration précédente). Soit $\sigma \in S_n$.
L'idée est la suivante : on part d'un élément de $[\![1, n]\!]$, et on regarde ses images successives par σ. On parcourt alors son orbite. Au bout d'un nombre fini d'étapes, on revient au point de départ. On a alors parcouru une boucle, ce qui correspond à un cycle C_1. Pour autant, tous les éléments de $[\![1, n]\!]$ n'ont pas forcément été rencontrés lors de cette boucle. On peut donc recommencer une autre promenade en partant d'un élément que nous n'avons pas encore rencontré. On fait alors une nouvelle boucle qui est une deuxième orbite, ce qui correspond à un second cycle C_2. En faisant cela pour toutes les orbites, on a construit autant de cycles que d'orbites. Ils ont tous des supports disjoints et leur composition donne σ. On remarque pour finir que puisque leurs supports sont disjoints, ils commutent. On peut donc composer ces cycles dans l'ordre que l'on veut. Un exemple pour illustrer tout cela :

Exemple 1.3.5.
Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 1 & 4 & 3 \end{pmatrix}$. Déterminons l'orbite de 1, par le schéma suivant, où une flèche va d'un élément à son image par σ : $1 \mapsto 5 \mapsto 4 \mapsto 1$, et la boucle est bouclée. L'orbite de 1 est donc, dans l'ordre, $\{1, 5, 4\}$. Prenons ensuite un élément qui n'est pas dans cette orbite, par exemple 2. On a alors : $2 \mapsto 2$, et la boucle est déjà bouclée, 2 est un point fixe de σ. Prenons un autre élément qui n'est dans aucune des deux orbites précédentes, par exemple 3 : $3 \mapsto 6 \mapsto 3$. L'orbite de 3 est donc $\{3, 6\}$. On s'arrête là car tous les éléments de $[\![1, 6]\!]$ ont été rencontrés. On peut donc écrire $\sigma = (1, 5, 4) \circ (2) \circ (3, 6)$. Comme (2) n'est en fait pas un cycle (c'est l'identité), on ne l'écrit pas. On n'écrit pas non plus les symboles $\circ$. On a donc $\sigma = (1, 5, 4)(3, 6)$, et on remarque que c'est aussi égal à $(3, 6)(1, 5, 4)$.

Cette écriture comme produit de cycles de supports disjoints est plus pratique que l'écriture sous forme de deux lignes : elle est plus courte et permet de repérer immédiatement les orbites. L'écriture à deux lignes s'en déduit très simplement.

De la décomposition précédente découle une autre, primordiale pour la suite du chapitre :

Théorème 1.3.6.
Toute permutation se décompose en produit de transpositions (on dit que S_n est engendré par ses transpositions).

Démonstration.
D'après le théorème précédent, il suffit de savoir décomposer un cycle en produit de transpositions. Soit $C = (x_1, \dots, x_p)$ un cycle. On montre alors que $C = (x_1, x_2)(x_2, x_3) \dots (x_{p-1}, x_p)$, et c'est fini.

Notons $T = (x_1, x_2)(x_2, x_3) \dots (x_{p-1}, x_p)$. Si $x \in [\![1, n]\!] \setminus \{x_1, \dots, x_p\}$, alors x est invariant par toutes les transpositions ainsi que par le cycle, donc $T(x) = C(x) = x$. Si $1 \leqslant i < p$, on a

$$\begin{aligned} T(x_i) &= \left(\prod_{j=1}^{p-1} (x_j, x_{j+1})\right)(x_i) \\ &= \left(\prod_{j=1}^{i-1} (x_j, x_{j+1})\right)(x_i, x_{i+1})(x_i) \\ &= \left(\prod_{j=1}^{i-1} (x_j, x_{j+1})\right)(x_{i+1}) \\ &= x_{i+1} \\ &= C(x_i). \end{aligned}$$

On conclut simplement en montrant que $T(x_p) = x_1 = C(x_p)$ par récurrence sur p.

□

 Cette décomposition n'est pas unique. Par exemple $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \tau_{12} \circ \tau_{23} \circ \tau_{34} = \tau_{41} \circ \tau_{12} \circ \tau_{23}$.
De plus, deux transpositions ne commutent en général pas : $\tau_{12} \circ \tau_{23} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \tau_{23} \circ \tau_{12}$.

1.4 Signature d'une permutation

Définition 1.4.1.
Soit $\sigma \in S_n$. On dit qu'un couple $(i,j) \in [\![1,n]\!]^2$ est une ***inversion*** de σ si $i<j$ et $\sigma(i)>\sigma(j)$. On note alors $I(\sigma)$ le nombre d'inversions de σ, et on définit la ***signature*** de σ, notée $\varepsilon(\sigma)$, comme étant l'entier $\varepsilon(\sigma)=(-1)^{I(\sigma)}$, qui vaut donc ± 1. Une permutation de signature 1 est dite ***paire***, ***impaire*** sinon.

Exemple 1.4.2.
Si $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 7 & 2 & 1 & 4 & 6 \end{pmatrix}$, alors $I(\sigma)=10$ et donc $\varepsilon(\sigma)=1$.

Proposition 1.4.3.
Toute transposition est impaire.

Démonstration.
Il suffit de voir que, si $1 \leqslant i < j \leqslant n$, $\tau i,j$ a pour inversions :
— le couple (i,j) ;
— les couples (i,x) et (x,j) pour $i<x<j$.
Il y a donc bien un nombre impair d'inversions pour une transposition. □

Lemme 1.4.4.
Si $\sigma \in S_n$, on a

$$\varepsilon(\sigma) = \prod_{1\leqslant i<j\leqslant n} \frac{\sigma(i)-\sigma(j)}{i-j}.$$

Démonstration.
En effet, $\displaystyle\prod_{1\leqslant i<j\leqslant n} \frac{\sigma(i)-\sigma(j)}{i-j} = \frac{\displaystyle\prod_{1\leqslant i<j\leqslant n} \sigma(i)-\sigma(j)}{\displaystyle\prod_{1\leqslant i<j\leqslant n} i-j}$. Or σ est une bijection, donc tout couple (i,j) tel que $i<j$ est égal à un unique couple de la forme $(\sigma(k),\sigma(\ell))$, avec nécessairement $k\neq\ell$. Cependant, si $i<j$ on ne sait pas si $k<\ell$ ou $k>\ell$. Réciproquement, pour tout couple (i,j) tel que $i<j$, $(\sigma(i),\sigma(j))$ est égal à un unique couple de la forme (k,ℓ), avec nécessairement $k\neq\ell$. Dans tous les cas, le numérateur et le dénominateur de la dernière fraction sont égaux au signe près. Donc $\displaystyle\prod_{1\leqslant i<j\leqslant n} \frac{\sigma(i)-\sigma(j)}{i-j} = \pm 1$.
Remarquons que si $i<j$, alors $\dfrac{\sigma(i)-\sigma(j)}{i-j}$ est négatif si et seulement si (i,j) est une inversion. Comme il y a $I(\sigma)$ inversions, ce produit vaut $(-1)^{I(\sigma)}$. □

Théorème 1.4.5.
L'application signature

$$\varepsilon \ : \ \left\{ \begin{array}{ccc} (S_n,\circ) & \to & (\{-1,1\},\times) \\ \sigma & \mapsto & \varepsilon(\sigma) \end{array} \right.$$

est un morphisme de groupes. Son noyau, noté $\mathfrak{A}_n = \{\sigma \in S_n |\ \varepsilon(\sigma)=+1\}$ est un sous-groupe de S_n appelé ***groupe alterné*** d'ordre n.

Démonstration (non exigible)**.**
On utilise directement le lemme 1.4.4 (qui n'est pas exigible lui non plus) : si $\sigma,\sigma' \in S_n$, on a :

$$\begin{aligned} &\varepsilon(\sigma\circ\sigma') \\ =& \prod_{1\leqslant i<j\leqslant n} \frac{\sigma(\sigma'(i))-\sigma(\sigma'(j))}{i-j} \\ =& \prod_{1\leqslant i<j\leqslant n} \frac{\sigma(\sigma'(i))-\sigma(\sigma'(j))}{\sigma'(i)-\sigma'(j)} \times \prod_{1\leqslant i<j\leqslant n} \frac{\sigma'(i)-\sigma'(j)}{i-j} \\ =& \prod_{1\leqslant I<J\leqslant n} \frac{\sigma(I)-\sigma(J)}{I-J} \times \prod_{1\leqslant i<j\leqslant n} \frac{\sigma'(i)-\sigma'(j)}{i-j} \\ =& \varepsilon(\sigma)\times\varepsilon(\sigma'). \end{aligned}$$

□

Corollaire 1.4.6.
Si σ est le produit de p transpositions, alors $\varepsilon(\sigma)=(-1)^p$.

Exemple 1.4.7.
Un cycle de longueur p est donc de signature $(-1)^{p+1}$.

Exemple 1.4.8.
Avec

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 1 & 4 & 3 \end{pmatrix} = (1,5,4)(3,6),$$

on a $\varepsilon(\sigma) = 1\times(-1) = -1$.

Remarque 1.4.9.
La signature d'une permutation est très souvent définie comme ceci, et il faut donc connaître cette caractérisation, qui est de plus très pratique pour le calcul de la signature. Si cette définition est choisie, il faut dans ce cas montrer que le nombre de transpositions de n'importe quelle décomposition en produit de transpositions a toujours la même parité.

Corollaire 1.4.10.
La signature est l'unique application ε de S_n dans $\{-1,1\}$ telle que $\varepsilon(\tau) = -1$ pour toute transposition τ et $\varepsilon(\sigma \circ \sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$ pour toutes permutations σ et σ'.

Démonstration.
Soit ε une telle application. Alors ε correspond avec la signature sur l'ensemble des transpositions, et puisque $\varepsilon(\sigma \circ \sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$ pour toutes permutations σ et σ', alors si σ est le produit de p transpositions, $\varepsilon(\sigma) = (-1)^p$, qui vaut donc la signature de σ. □

2 Applications multilinéaires

Désormais, E et F sont deux $\mathbb{K}$-espaces vectoriels.

2.1 Définition et exemples

Définition 2.1.1.
Soient $E_1, \dots, E_n$ et F des $\mathbb{K}$-espaces vectoriels et f une application de $E_1 \times \dots \times E_n$ dans F. On dit que f est ***n-linéaire*** si pour tout $k \in [\![1, n]\!]$, tout $(x_1, \dots, x_{k-1}, x_{k+1}, \dots, x_n) \in E_1 \times \dots \times E_{k-1} \times E_{k+1} \times \dots E_n$ l'application

$$\left\{ \begin{array}{ccc} E_k & \to & F \\ x & \mapsto & f(x_1, \dots, x_{k-1}, x, x_{k+1}, \dots, x_n) \end{array} \right.$$

est linéaire.

Si $n = 2$, on dit que f est ***bilinéaire*** et, si $F = \mathbb{K}$, on dit que f est une ***forme n-linéaire***.

L'ensemble des applications n-linéaires de $E_1 \times \dots \times E_n$ dans F est noté $\mathscr{L}(E_1, E_2, \dots, E_n; F)$. Si tous les E_i sont égaux et notés E, on utilise alors la notation $\mathscr{L}_n(E; F)$. Enfin l'ensemble des formes n-linéaires sur E^n est noté $\mathscr{L}_n(E)$ (c'est-à-dire si $F = \mathbb{K}$).

Remarque 2.1.2.
• On remarque facilement que tous ces ensembles d'applications multilinéaires sont des $\mathbb{K}$-ev.
• Une application linéaire est une application 1-linéaire.
• Toute application multilinéaire s'annule sur un vecteur dont une coordonnée est nulle, par linéarité par rapport à cette coordonnée.

Exemple 2.1.3.
Les applications suivantes sont bilinéaires :
• $\mathbb{K} \times E \to E$, $(\lambda, x) \mapsto \lambda \cdot x$, où E est un $\mathbb{K}$-ev.
• $\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$, $(u, v) \mapsto u \cdot v$.
• $\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$, $(u, v) \mapsto u \wedge v$.
• $\mathscr{M}_{n,p}(\mathbb{K}) \times \mathscr{M}_{p,q}(\mathbb{K}) \to \mathscr{M}_{n,q}(\mathbb{K})$, $(A, B) \mapsto AB$.
• $\mathscr{L}(E, E') \times \mathscr{L}(E', E'') \to \mathscr{L}(E, E'')$, $(f, g) \mapsto g \circ f$, où E, E', E'' sont trois $\mathbb{K}$-espaces vectoriels (la linéarité par rapport à g est vraie sans supposer que f et g sont linéaires ; pour la linéarité par rapport à f, g doit être linéaire).
• $\mathscr{C}^0([0,1])^2 \to \mathbb{R}$, $(f, g) \mapsto \displaystyle\int_0^1 f(t)g(t)\,\mathrm{d}t$.
• $(\mathbb{R}^2)^2 \to \mathbb{R}$, $(u, v) \mapsto \det(u, v)$.

2.2 Applications multilinéaires symétriques, antisymétriques et alternées

Définition 2.2.1.
Soit $f \in \mathscr{L}_n(E; F)$, et soit $\sigma \in S_n$. On définit l'application :
$$\sigma \star f \ : \ \left\{ \begin{array}{ccc} E^n & \to & F \\ (x_1, \dots, x_n) & \mapsto & f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \end{array} \right. .$$
On vérifie que $\sigma \star f$ est aussi une application n-linéaire.

Exemple 2.2.2.
Soit $f \in \mathscr{L}_3(\mathbb{R}; F)$, et $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in S_3$.

Alors $(\sigma \star f)(x_1, x_2, x_3) = f(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}) = f(x_3, x_1, x_2)$.

Proposition 2.2.3.
Soit $f \in \mathscr{L}_n(E;F)$ et soit $\sigma_1, \sigma_2 \in S_n$. Alors $\sigma_1 \star (\sigma_2 \star f) = (\sigma_1 \circ \sigma_2) \star f$.

Démonstration.
Soit $(x_1, \dots, x_n) \in E^n$. Alors, avec $(x_{\sigma_1(1)}, \dots, x_{\sigma_1(n)}) = (x'_1, \dots, x'_n)$,

$$\begin{aligned}[\sigma_1 \star (\sigma_2 \star f)](x_1, \dots, x_n) &= [\sigma_2 \star f](x_{\sigma_1(1)}, \dots, x_{\sigma_1(n)}) \\ &= [\sigma_2 \star f](x'_1, \dots, x'_n) \\ &= f(x'_{\sigma_2(1)}, \dots, x'_{\sigma_2(n)}) \\ &= f(x_{\sigma_1(\sigma_2(1))}, \dots, x_{\sigma_1(\sigma_2(n))}) \\ &= [(\sigma_1 \circ \sigma_2) \star f](x_1, \dots, x_n).\end{aligned}$$

□

Définition 2.2.4.
Une application n-linéaire f est dite ***symétrique*** si pour tout $\sigma \in S_n$, $\sigma \star f = f$. Elle est dite ***antisymétrique*** si pour tout $\sigma \in S_n$, $\sigma \star f = \varepsilon(\sigma) f$.

Remarque 2.2.5.
On remarque facilement que l'ensemble des applications symétriques est un $\mathbb{K}$-ev, et qu'il en est de même pour celui des applications antisymétriques.

 Les caractères « symétrique » et « antisymétrique » d'une application multilinéaire n'ont de sens que si les espaces vectoriels de départ sont tous égaux. Sinon, permuter des variables qui ne sont pas de même nature n'a pas de sens.

Exemple 2.2.6.
- Le produit de deux fonctions $\mathscr{C}^0(\mathbb{R})^2 \to \mathscr{C}^0(\mathbb{R})$, $(f,g) \mapsto fg$ est une application bilinéaire symétrique.
- Le produit vectoriel de $\mathbb{R}^3 \times \mathbb{R}^3$ dans $\mathbb{R}^3$ est une application bilinéaire antisymétrique.
- Le déterminant de $\mathbb{R}^2 \times \mathbb{R}^2$ dans $\mathbb{R}$ est bilinéaire, antisymétrique. En effet, il suffit de voir que $\det(v,u) = -\det(u,v)$.
- Le déterminant de $\mathbb{R}^3 \times \mathbb{R}^3 \times \mathbb{R}^3$ dans $\mathbb{R}$ est une application trilinéaire antisymétrique. En effet, remarquons que si $\sigma \in S_3$, alors il existe p transpositions $\tau_1, \dots, \tau_p$ telles que $\sigma = \tau_p \circ \dots \circ \tau_1$. Dans ce cas $\sigma \star \det = \tau_p \star (\tau_{p-1} \star (\dots \tau_2 \star (\tau_1 \star \det)))$. Mais pour toute transposition τ, $\tau \star \det = -\det$, car échanger deux vecteurs dans un déterminant change le signe de ce déterminant. Ainsi $\sigma \star \det = (-1)^p \det = \varepsilon(\sigma) \det$.

Remarquons d'abord que l'on peut caractériser le caractère symétrique ou antisymétrique d'une application multilinéaire par l'action des transpositions sur cette dernière.

Proposition 2.2.7.
Soit f une application n linéaire. Si pour toute transposition τ, on a $\tau \star f = f$ alors f est symétrique. De même si, pour toute transposition τ, on a $\tau \star f = -f$ alors f est antisymétrique.

Démonstration.
Facile, une fois que l'on sait décomposer une permutation en produit de transpositions, avec la propriété de morphisme de la signature ainsi que la proposition **? ?**. □

Proposition 2.2.8.
Soit $f \in \mathscr{L}_n(E;F)$ une application n-linéaire antisymétrique. Soit $(x_1, \dots, x_n) \in E^n$.

(i) Si τ est une transposition de S_n, alors $\tau \star f = -f$, *i.e.* f est changée en son opposé si l'on échange deux variables ;

(ii) S'il existe $i \neq j$ dans $[\![1, n]\!]$ tels que $x_i = x_j$, alors $f(x_1, \dots, x_n) = 0$;

(iii) On ne change pas la valeur de f si l'on ajoute à une variable une combinaison linéaire des autres ;

(iv) Si $(x_1, \dots, x_n)$ est liée, alors $f(x_1, \dots, x_n) = 0$.

Démonstration. (i) Direct car $\varepsilon(\tau) = -1$;

(ii) On note $X = (x_1, \dots, x_n)$ et $\widetilde{X} = \tau_{x_i x_j}(X)$, c'est-à-dire le vecteur obtenu à partir de X en échangeant les i^{e} et j^{e} coordonnées. Si $x_i = x_j$, on a $X = \widetilde{X}$,

d'où $\tau_{x_i x_j} \star f(X) = f(\widetilde{X}) = f(X)$. Or d'après (i), $\tau_{x_i x_j} \star f(X) = -f(X)$, d'où $f(X) = 0$;

(iii) Considérons par exemple que l'on rajoute à x_n la combinaison linéaire $\sum_{i=1}^{n-1} \lambda_i x_i$, avec $\lambda_i \in \mathbb{K}$. Les autres cas se traitent de la même manière. Alors, par linéarité par rapport à la dernière variable, on a :

$$f\left(x_1, \dots, x_{n-1}, x_n + \sum_{i=1}^{n-1} \lambda_i x_i\right) =$$

$$f(x_1, \dots, x_n) + \sum_{i=1}^{n-1} \lambda_i f(x_1, \dots, x_{n-1}, x_i).$$

Or d'après le point (ii), pour tout $i \in [\![1, n-1]\!]$, on a $f(x_1, \dots, x_{n-1}, x_i) = 0$, d'où

$$f(x_1, \dots, x_{n-1}, x_n + \sum_{i=1}^{n-1} \lambda_i x_i) = f(x_1, \dots, x_n).$$

(iv) Si $(x_1, \dots, x_n)$ est liée, alors on peut exprimer un des vecteurs de $x_1, \dots, x_n$ en fonction des autres. Par exemple (de même dans les autres cas), $x_n = \sum_{i=1}^{n-1} \lambda_i x_i$.
Alors d'après le point (iii), on a :

$$\begin{aligned} f(x_1, \dots, x_n) &= f(x_1, \dots, x_{n-1}, \sum_{i=1}^{n-1} \lambda_i x_i) \\ &= f(x_1, \dots, x_{n-1}, 0 + \sum_{i=1}^{n-1} \lambda_i x_i) \\ &= f(x_1, \dots, x_{n-1}, 0). \end{aligned}$$

Or, d'après la remarque 2.1.2, on a $f(x_1, \dots, x_{n-1}, 0) = 0$.

□

Définition 2.2.9.
Une application n-linéaire est dite ***alternée*** si elle s'annule sur tout n-uplet dont deux éléments au moins sont égaux.

Remarque 2.2.10.
Le point (ii) de la proposition 2.2.8 montre exactement que toute application antisymétrique est alternée. En fait, ces deux notions sont équivalentes, comme le montre le théorème suivant.

Théorème 2.2.11.
Si f est une application multilinéaire, f est antisymétrique si et seulement si elle est alternée.

Démonstration.
Il reste à montrer que si f est alternée, elle est antisymétrique. f va de E^n dans F. Soit τ_{ij} une transposition de S_n, avec $i, j \in [\![1, n]\!]$, $i < j$. Soit $X = (x_1, \dots, x_n) \in E^n$. On appelle X' le vecteur dont les i^{e} et j^{e} coordonnées valent toutes les deux $x_i + x_j$, et dont les autres coordonnées sont les mêmes que celles de X. Ou encore, $X' = (x_1, \dots, x_{i-1}, x_i + x_j, x_{i+1}, \dots, x_{j-1}, x_i + x_j, x_{j+1}, \dots, x_n)$. On en déduit que $f(X') = 0$. Or, par multilinéarité,

$$\begin{aligned} &f(X') \\ =&f(x_1, \dots, x_{i-1}, \underline{\mathbf{x_i} + \mathbf{x_j}}, x_{i+1}, \\ &\qquad \dots, x_{j-1}, \underline{\mathbf{x_i} + \mathbf{x_j}}, x_{j+1}, \dots, x_n) \\ =&f(x_1, \dots, x_{i-1}, \underline{\mathbf{x_i}}, x_{i+1}, \\ &\qquad \dots, x_{j-1}, \underline{\mathbf{x_i} + \mathbf{x_j}}, x_{j+1}, \dots, x_n) \\ &+ f(x_1, \dots, x_{i-1}, \underline{\mathbf{x_j}}, x_{i+1}, \\ &\qquad \dots, x_{j-1}, \underline{\mathbf{x_i} + \mathbf{x_j}}, x_{j+1}, \dots, x_n) \\ =&\underbrace{f(x_1, \dots, x_{i-1}, \underline{\mathbf{x_i}}, x_{i+1}, \dots, x_{j-1}, \underline{\mathbf{x_i}}, x_{j+1}, \dots, x_n)}_{=0} \\ &+ \underbrace{f(x_1, \dots, x_{i-1}, \underline{\mathbf{x_i}}, x_{i+1}, \dots, x_{j-1}, \underline{\mathbf{x_j}}, x_{j+1}, \dots, x_n)}_{=f(X)} \\ &+ \underbrace{f(x_1, \dots, x_{i-1}, \underline{\mathbf{x_j}}, x_{i+1}, \dots, x_{j-1}, \underline{\mathbf{x_i}}, x_{j+1}, \dots, x_n)}_{=f(\tau_{ij}(X))} \\ &+ \underbrace{f(x_1, \dots, x_{i-1}, \underline{\mathbf{x_j}}, x_{i+1}, \dots, x_{j-1}, \underline{\mathbf{x_j}}, x_{j+1}, \dots, x_n)}_{=0} \\ =&f(X) + f(\tau_{ij}(X)) \\ =&f(X) + \tau_{ij} \star f(X), \end{aligned}$$

d'où $\tau_{ij} \star f = -f$. On en déduit que pour toute transposition τ, et toute application multilinéaire f, $\tau \star f = -f$. Soit $\sigma \in S_n$. σ s'écrit comme le produit de p transpositions, $\sigma = \tau_1 \circ \dots \circ \tau_p$. D'après le point précédent on a $\sigma \star f = \tau_1 \star (\dots \star (\tau_p \star f) \dots) = -\tau_2 \star (\dots \star (\tau_p \star f) \dots) = (-1)^p f = \varepsilon(\sigma) f$, ce qui prouve bien le résultat voulu. □

En général on utilise plutôt le mot « alternée » qu'« antisymétrique ».

Exemple 2.2.12. — Le produit vectoriel entre deux vecteurs de $\mathbb{R}^3$ est une application alternée.
— L'application qui, à une famille de deux vecteurs de $\mathbb{R}^2$, associe son déterminant est une forme bilinéaire alternée. Il en est de

même pour le déterminant d'une famille de trois vecteurs de $\mathbb{R}^3$ (forme trilinéaire alternée).

3 Déterminant d'une famille de vecteurs

3.1 Définition en dimension finie.

Désormais, E est un $\mathbb{K}$-ev de dimension finie n. Notons $\mathscr{A}_n(E)$ l'ensemble des formes n-linéaires alternées sur E^n.

Exercice 3.1.1.
Si $n = 2$, soit $\mathscr{B} = (e_1, e_2)$ une base de E, soit $f \in \mathscr{A}_2(E)$ et soit les vecteurs $x = x_1e_1 + x_2e_2$ et $y = y_1e_1 + y_2e_2$.

Développer par linéarité $f(x, y)$ par rapport à sa première coordonnée, puis sa deuxième.

Faire de même en dimension 3.

Théorème 3.1.2.
Soit $\mathscr{B} = \{e_1, \dots, e_n\}$ une base de E. Pour $(X_1, \dots, X_n) \in E^n$ et $1 \leqslant j \leqslant n$, on note $(x_{ij})_{1\leqslant i\leqslant n}$ les coordonnées de X_j dans $\mathscr{B}$.

(i) $\mathscr{A}_n(E)$ est une droite vectorielle, *i.e.* est de dimension 1.

(ii) Considérons l'application

$$\det_{\mathscr{B}} \ : \ E^n \ \to \ \mathbb{K},$$

telle que pour tout $(X_1, \dots, X_n) \in E^n$,

$$\begin{aligned}\det_{\mathscr{B}}(X_1, \dots, X_n) &= \sum_{\sigma\in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} x_{i\sigma(i)} \\ &= \sum_{\sigma\in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} x_{\sigma(i)i}.\end{aligned}$$

C'est une forme n-linéaire alternée non nulle sur E^n, et c'est la seule vérifiant

$$\det_{\mathscr{B}}(\mathscr{B}) = \det_{\mathscr{B}}(e_1, \dots, e_n) = 1.$$

(iii) Si $f \in \mathscr{A}_n(E)$, on a $f = f(\mathscr{B}) \det_{\mathscr{B}}$ (avec $f(\mathscr{B}) = f(e_1, \dots, e_n)$) et donc $\mathscr{A}_n(E) = \text{Vect}(\det_{\mathscr{B}})$.

 Ici la dimension de E doit être égale à la puissance de E.

Démonstration (non exigible)**.**
Montrons déjà l'égalité des deux formes de la définition du déterminant. Soit $\sigma \in S_n$, comme σ est une permutation, on a

$$\prod_{i=1}^{n} x_{i,\sigma(i)} = \prod_{i=1}^{n} x_{\sigma^{-1}(i),i}.$$

On conclut en remarquant que comme $\sigma \circ \sigma^{-1} = \text{Id}$, alors $\varepsilon(\sigma) = \varepsilon(\sigma^{-1})$ et que $\sigma \mapsto \sigma^{-1}$ est une permutation de S_n.

(i) Ce point découlera directement du point (iii).

(ii) À vous de montrer que $\det_{\mathscr{B}}$ est n-linéaire.
Montrons déjà qu'elle est non nulle. Pour tout i, on peut écrire $e_i = \sum_{j=1}^{n} \delta_{i,j} e_j$ (δ étant le symbole de Kronecker), donc $\det_{\mathscr{B}}(\mathscr{B}) = \det_{\mathscr{B}}(e_1, \dots, e_n) = \sum_{\sigma\in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} \delta_{i,\sigma(i)}$.
Mais si $\sigma \neq \text{Id}$, il existe i tel que $i \neq \sigma(i)$, et ainsi $\delta_{i,\sigma(i)} = 0$. Par conséquent, $\det_{\mathscr{B}}(\mathscr{B}) = \varepsilon(\text{Id}) \prod_{i=1}^{n} \delta_{i,\text{Id}(i)} = 1$, ce qui montre d'ailleurs un autre point de (ii).
Montrons enfin qu'elle est alternée. Soit $(X_1, \dots, X_n) \in E^n$ tel qu'il existe $i, j \in [\![1, n]\!]$ avec $i < j$ et $X_i = X_j$. Alors :

$$\begin{aligned}\det_{\mathscr{B}}(X_1, \dots, X_n) &= \sum_{\sigma\in S_n} \varepsilon(\sigma) \prod_{k=1}^{n} x_{k\sigma(k)} \\ &= \sum_{\sigma\in \mathfrak{A}_n} \prod_{k=1}^{n} x_{k\sigma(k)} - \sum_{\sigma\in S_n\setminus\mathfrak{A}_n} \prod_{k=1}^{n} x_{k\sigma(k)}.\end{aligned}$$

On utilise alors l'idée suivante : si l'on note $\tau = \tau_{i,j}$, l'application $\mathfrak{A}_n \to S_n\setminus\mathfrak{A}_n$, $\sigma \mapsto \tau \circ \sigma$ est une bijection.
Ainsi,

$$\begin{aligned}\sum_{\sigma\in S_n\setminus\mathfrak{A}_n} \prod_{k=1}^{n} x_{k\sigma(k)} &= \sum_{\sigma\in \mathfrak{A}_n} \prod_{k=1}^{n} x_{k\tau\sigma(k)} \\ &= \sum_{\sigma\in \mathfrak{A}_n} \prod_{k=1}^{n} x_{k\sigma(k)},\end{aligned}$$

car $X_i = X_j$ et si $\sigma(k) \neq i$ et $\sigma(k) \neq j$, $\tau(\sigma(k)) = \sigma(k)$. On obtient donc bien $\det_{\mathscr{B}}(X_1, \dots, X_n) = 0$.
Le fait que $\det_{\mathscr{B}}$ soit la seule à vérifier $\det_{\mathscr{B}}(e_1, \dots, e_n) = 1$ découlera du point (iii).

(iii) Soient $f \in \mathscr{A}_n(E)$ et $(X_1, \dots, X_n) \in E^n$. On a :

$$
\begin{aligned}
& f(X_1,\dots,X_n)\\
= \;& f\left(\sum_{i_1=1}^{n} x_{i_1 1}e_{i_1},\dots,\sum_{i_n=1}^{n} x_{i_n n}e_{i_n}\right)\\
= \;& \sum_{i_1=1}^{n} x_{i_1 1} f\left(e_{i_1},\sum_{i_2=1}^{n} x_{i_2 2}e_{i_2},\dots,\sum_{i_n=1}^{n} x_{i_n n}e_{i_n}\right)\\
= \;& \sum_{i_1=1}^{n}\sum_{i_2=1}^{n}\cdots\sum_{i_n=1}^{n} x_{i_1 1}x_{i_2 2}\dots x_{i_n n} f(e_{i_1},\dots,e_{i_n})\\
= \;& \sum_{i_1,\dots,i_n\in[\![1,n]\!]} x_{i_1 1}\dots x_{i_n n} f(e_{i_1},\dots,e_{i_n})\\
= \;& \sum_{\substack{i_1,\dots,i_n\in[\![1,n]\!]\\ \text{tq. si } k\neq\ell \text{ alors } i_k\neq i_\ell}} x_{i_1 1}\dots x_{i_n n} f(e_{i_1},\dots,e_{i_n})\\
= \;& \sum_{\sigma\in S_n} x_{\sigma(1)1}\dots x_{\sigma(n)n} f(e_{\sigma(1)},\dots,e_{\sigma(n)})\\
= \;& \sum_{\sigma\in S_n}\left(\left(\prod_{i=1}^{n} x_{\sigma(i)i}\right)\varepsilon(\sigma) f(e_1,\dots,e_n)\right)\\
= \;& f(e_1,\dots,e_n)\sum_{\sigma\in S_n}\left(\varepsilon(\sigma)\prod_{i=1}^{n} x_{\sigma(i)i}\right)\\
= \;& f(\mathscr{B})\det_{\mathscr{B}}(X_1,\dots,X_n).
\end{aligned}
$$

□

Définition 3.1.3.
Cette fonction $\det_{\mathscr{B}}$ est appelée ***déterminant dans la base*** $\mathscr{B}$.

Exemple 3.1.4.
Si $n = 2$, remarquons que $S_n = \{\mathrm{Id}, \tau_{12}\}$. Si $\mathscr{B} = \{e_1, e_2\}$ est une base de E, et si $x, y \in E$ ont pour coordonnées (x_1, x_2) et (y_1, y_2) dans $\mathscr{B}$, on a : $\det_{\mathscr{B}}(x, y) = \varepsilon(Id)x_1y_2 + \varepsilon(\tau_{12})x_2y_1 = x_1y_2 - x_2y_1$, ce qui est la formule habituelle du déterminant en dimension 2.

De même, si $n = 3$, on remarque que $S_n = \{\mathrm{Id}, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$, ce qui donne :

$$\det_{\mathscr{B}}(x,y,z) = \underbrace{x_1y_2z_3}_{Id} + \underbrace{x_2y_3z_1}_{(1,2,3)} + \underbrace{x_3y_1z_2}_{(1,3,2)} - \underbrace{x_3y_2z_1}_{(1,3)} - \underbrace{x_2y_1z_3}_{(1,2)} - \underbrace{x_1y_3z_2}_{(2,3)}.$$

Remarque 3.1.5.
Dans l'exemple ci-dessus et $\mathscr{B}$ étant la base canonique, on peut remarquer que $\det_{\mathscr{B}}(x, y, z) = x \cdot (y \wedge z)$. Pouvez-vous former d'autres relations de ce type ?

 Attention, la valeur du déterminant varie suivant la base, comme le montre l'exemple suivant :

Exemple 3.1.6.
On pose $E = \mathbb{R}^2$, et $\mathscr{B} = \{(1,0),(0,1)\} = \{e_1, e_2\}$ et $\mathscr{B}' = \{(1,1),(2,0)\} = \{f_1, f_2\}$ deux bases de E. On pose $v = e_1 + e_2$ et $w = e_1 - e_2$. Alors $v = f_1$ et $w = -f_1 + f_2$. Alors $\det_{\mathscr{B}}(v, w) = -2$ et $\det_{\mathscr{B}'}(v, w) = 1$.

Théorème 3.1.7.
Soient $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E et $\mathscr{F}$ une famille de n vecteurs de E. On a alors :

(i) **Formule de changement de base :** $\det_{\mathscr{B}}(\mathscr{F}) = \det_{\mathscr{B}}(\mathscr{B}')\det_{\mathscr{B}'}(\mathscr{F})$.

(ii) $\mathscr{F}$ est une base ssi $\det_{\mathscr{B}}(\mathscr{F}) \neq 0$. Dans ce cas $\det_{\mathscr{F}}(\mathscr{B}) = \dfrac{1}{\det_{\mathscr{B}}(\mathscr{F})}$.

Démonstration.
Ces résultats découlent de résultats précédents :

(i) On utilise le point (iii) du théorème 3.1.1. Si on appelle f l'application $\det_{\mathscr{B}}$, f est n-linéaire alternée et donc $f = f(\mathscr{B}')\det_{\mathscr{B}'}$, ce qui exactement le résultat voulu.

(ii) On utilise le point (iv) de la proposition 2.2.8 : D'une part, si $\mathscr{F}$ est liée, on a $\det_{\mathscr{B}}(\mathscr{F}) = 0$, d'autre part, si $\mathscr{F}$ n'est pas liée, comme $\mathrm{card}(\mathscr{F}) = n$, $\mathscr{F}$ est alors une base, donc $\det_{\mathscr{F}}(\mathscr{F}) = 1$, et le point i précédent assure que $\det_{\mathscr{F}}(\mathscr{F}) = \det_{\mathscr{F}}(\mathscr{B})\det_{\mathscr{B}}(\mathscr{F})$.

□

Exemple 3.1.8.
En reprenant les bases $\mathscr{B}$ et $\mathscr{B}'$ de l'exemple précédent, on trouve bien $\det_{\mathscr{B}}(\mathscr{B}') = -2$ et $\det_{\mathscr{B}'}(\mathscr{B}) = -\dfrac{1}{2}$.

3.2 Interprétation en géométrie réelle.

 On considère ici le cas où le corps de base est $\mathbb{K} = \mathbb{R}$.

a Orientation d'un ev réel de dimension finie

Définition 3.2.1.
On dit que deux bases $\mathscr{B}$ et $\mathscr{B}'$ de E ont *la même orientation* si $\det_{\mathscr{B}}(\mathscr{B}') > 0$. La relation « avoir la même orientation » est une relation d'équivalence, et il y a exactement deux orientations possibles.

Démonstration.
Le fait qu'il s'agisse d'une relation d'équivalence ne pose aucune difficulté :
- *réflexivité* : $\det_{\mathscr{B}}(\mathscr{B}) = 1$.
- *symétrie* : $\det_{\mathscr{B}'}(\mathscr{B}) = \dfrac{1}{\det_{\mathscr{B}}(\mathscr{B}')}$, donc ces deux déterminants ont le même signe.
- *transitivité* : $\det_{\mathscr{B}}(\mathscr{B}'') = \det_{\mathscr{B}}(\mathscr{B}').\det_{\mathscr{B}'}(\mathscr{B}'')$.

Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base de E : elle définit une orientation. Soit $\mathscr{B}' = (-e_1, \dots, e_n)$ une seconde base. Puisque $\det_{\mathscr{B}}(\mathscr{B}') = -1$, $\mathscr{B}'$ définit une seconde orientation. Montrons qu'il n'y en pas d'autre : soit $\mathscr{B}''$ une troisième base. Puisque $\det_{\mathscr{B}}(\mathscr{B}'') = \det_{\mathscr{B}}(\mathscr{B}').\det_{\mathscr{B}'}(\mathscr{B}'')$, et $\det_{\mathscr{B}}(\mathscr{B}') < 0$, alors $\det_{\mathscr{B}}(\mathscr{B}'')$ et $\det_{\mathscr{B}'}(\mathscr{B}'')$ sont de signes opposés, donc l'un des deux est strictement positif, donc $\mathscr{B}''$ a la même orientation que $\mathscr{B}$ ou que $\mathscr{B}'$. □

Orienter E, c'est dire que l'une de ces deux orientations est *directe*. Les bases représentant l'autre orientation seront alors dites *indirectes*.

Exemple 3.2.2.
Pour tout $\theta \in \mathbb{R}$, les bases $(\overrightarrow{u}_\theta, \overrightarrow{v}_\theta)$ ont la même orientation que la base canonique dans $\mathbb{R}^2$.

b Déterminant et aire dans le plan.

On considère ici que $E = \mathbb{R}^2$, que l'on munit du produit scalaire usuel ainsi que de la norme euclidienne induite. Notons (e_1, e_2) la base canonique de $\mathbb{R}^2$.

On condidère que $\mathbb{R}^2$ est orienté par sa base canonique.

Proposition 3.2.3.
Soit (u, v) deux vecteurs de $\mathbb{R}^2$. Alors $\det_{(e_1,e_2)}(u, v)$ est l'aire algébrique du parallélogramme engendré par (u, v) (voir la figure XXIV.1). Elle est donc nulle si u et v sont colinéaires, strictement positive si (u, v) est orientée directement et strictement négative sinon.

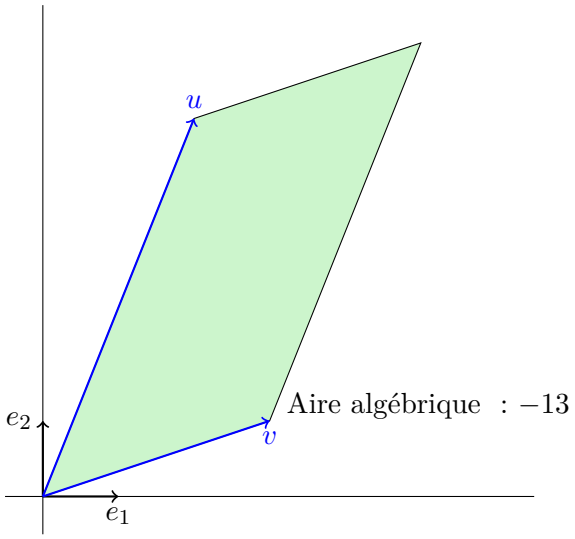


FIGURE XXIV.1 – Aire du parallélogramme engendré par (u, v), avec $u = (2, 5)$ et $v = (3, 1)$.

Démonstration.
Posons $u = (u_1, u_2)$ et $v = (v_1, v_2)$ (voir la figure XXIV.2). Quitte à échanger u et v, on peut supposer que (u, v) est directe, l'aire algébrique du parallélogramme est donc positive.

On peut aussi supposer que $u \neq (0, 0)$. Rappelons que l'aire d'un parallélogramme est le produit de la longueur d'un de ses côtés par la hauteur correpondante. Avec $u' = (-u_2, u_1)$, on remarque que $u \cdot u' = 0$ donc que u et u' sont orthogonaux, ainsi que $\|u\| = \|u'\|$,. La hauteur correspondant à u est donc $h = \left|\dfrac{u'}{\|u'\|} \cdot v\right|$ et l'aire du parallélogramme est donc $h\,\|u\| = |u' \cdot v| = |u_1 v_2 - u_2 v_1|$. □

Remarque 3.2.4.
Ce résultat est vrai en considérant le déterminant pris dans une base orthonormée directe quelconque, et non juste dans la base canonique.

Exemple 3.2.5.
Si u est un vecteur non nul de $\mathbb{R}^2$ et $\mathscr{B}$ est la base canonique de $\mathbb{R}^2$, on obtient directement une représentation cartésienne de la droite engendrée

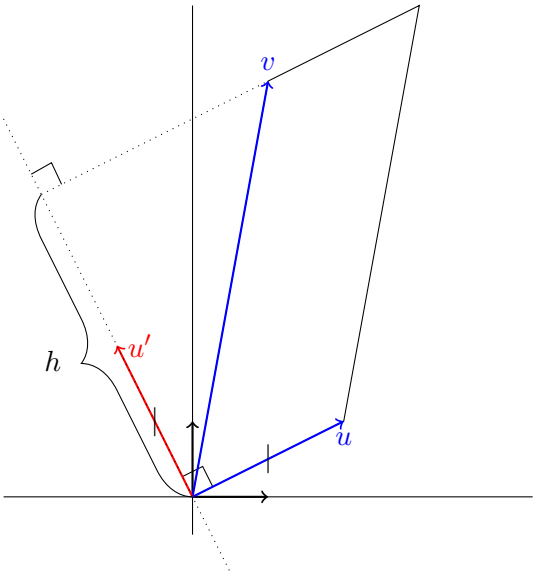


FIGURE XXIV.2 – Illustration du lien entre l'aire d'un parallélogramme et le déterminant.

par u par :

$$\forall x \in \mathbb{R}^2,\ x \in \operatorname{Vect} u \Leftrightarrow \det_{\mathscr{B}}(x,u) = 0.$$

c Déterminant et volume dans l'espace.

On considère ici que $E = \mathbb{R}^3$, que l'on munit du produit scalaire usuel ainsi que de la norme euclidienne induite. Notons (e_1, e_2, e_3) la base canonique de $\mathbb{R}^3$.

On considère que $\mathbb{R}^3$ est orienté par sa base canonique.

Proposition 3.2.6.
Soit (u, v, w) trois vecteurs de $\mathbb{R}^3$. Alors $\det_{(e_1,e_2,e_3)}(u, v, w)$ est le volume algébrique du pavé engendré par (u, v, w) (voir la figure XXIV.3). Elle est donc nulle si (u, v, w) sont coplanaires, strictement positive si (u, v, w) est orientée directement et strictement négative sinon.

Démonstration.
Cette preuve est laissée aux soins du lecteur : pensez à utiliser le produit vectoriel ! □

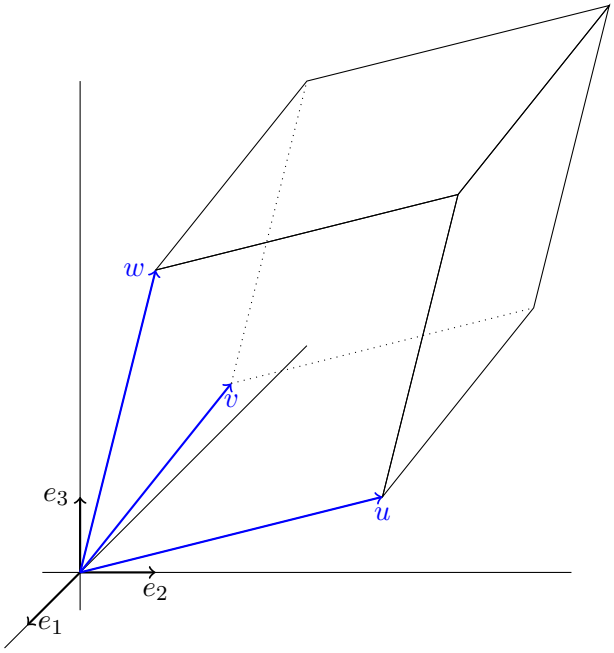


FIGURE XXIV.3 – Représentation du pavé engendré par (u, v, w).

Remarque 3.2.7.
Ce résultat est vrai en considérant le déterminant pris dans une base orthonormée directe quelconque, et non juste dans la base canonique.

Exemple 3.2.8.
Si u et v sont des vecteurs non colinéaires de $\mathbb{R}^3$ et $\mathscr{B}$ est la base canonique de $\mathbb{R}^3$, on obtient directement une représentation cartésienne du plan engendré par u et v par :

$$\forall x \in \mathbb{R}^3,\ x \in \operatorname{Vect}(u,v) \Leftrightarrow \det_{\mathscr{B}}(x,u,v) = 0.$$

4 Déterminant d'un endomorphisme

E est un $\mathbb{K}$-ev- de dimension n, dont une base est $\mathscr{B} = (e_1, \dots, e_n)$. Soit $f \in \mathscr{L}(E)$.

Remarque 4.0.1.
Pour $\mathscr{F} = (x_1, \dots, x_n) \in E^n$, on commettra le (léger) abus de notation suivant :

$$f(\mathscr{F}) = (f(x_1), \dots, f(x_n)).$$

Définition 4.0.2.
On appelle *déterminant* de f le scalaire noté $\det f$ tel que

$$\det f = \det_{\mathscr{B}}(f(\mathscr{B})) = \det_{\mathscr{B}}(f(e_1), \dots, f(e_n)).$$

Ce scalaire ne dépend pas de la base $\mathscr{B}$ choisie.

Remarque 4.0.3.
Pour pouvoir calculer ce déterminant, il faut que pour tout i, $f(e_i) \in E$, donc que f soit un endomorphisme.

Démonstration.
On introduit l'application
$\varphi : \left\{ \begin{array}{ccc} E^n & \to & \mathbb{K} \\ (v_1, \dots, v_n) & \mapsto & \det_{\mathscr{B}}(f(v_1), \dots, f(v_n)) \end{array} \right.$.
On montre que φ est n-linéaire (à vous de le faire) et alternée :
supposons qu'il existe $i, j \in [\![1, n]\!]$ tels que $i \neq j$ et $v_i = v_j$. Il faut montrer que $\varphi(v_1, \dots, v_n) = 0$. On a $\varphi(v_1, \dots, v_n) = \det_{\mathscr{B}}(f(v_1), \dots, f(v_n))$. Mais $f(v_i) = f(v_j)$ donc $\det_{\mathscr{B}}(f(v_1), \dots, f(v_n)) = 0$, car $\det_{\mathscr{B}}$ est alterné.
Il existe donc $\lambda \in \mathbb{K}$ tel que $\varphi = \lambda \det_{\mathscr{B}}$, et on a vu que $\lambda = \varphi(\mathscr{B})$.
Soit $\mathscr{B}'$ une seconde base de E.
Alors :

$$\begin{aligned} \det_{\mathscr{B}'}(f(\mathscr{B}')) &= \det_{\mathscr{B}'}(\mathscr{B}).\det_{\mathscr{B}} f(\mathscr{B}') \\ &= \det_{\mathscr{B}'}(\mathscr{B}).\varphi(\mathscr{B}') \\ &= \det_{\mathscr{B}'}(\mathscr{B}).\varphi(\mathscr{B}).\det_{\mathscr{B}}(\mathscr{B}') \\ &= \varphi(\mathscr{B}) \\ &= \det_{\mathscr{B}}(f(\mathscr{B})). \end{aligned}$$

□

Exemple 4.0.4.
Soit $g : \mathbb{R}^2 \to \mathbb{R}^2$ une application linéaire tel que $g(e_1) = e_1$ et $g(e_2) = 0$. Alors $\det g = \begin{vmatrix} 1 & 0 \\ 0 & 0 \end{vmatrix} = 0$.
Et d'autre part $\det(g + \mathrm{Id}_{\mathbb{R}^2}) = \begin{vmatrix} 2 & 0 \\ 0 & 1 \end{vmatrix} = 2$.

Si l'on prend la base $\mathscr{B}' = \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right) = (f_1, f_2)$, alors on trouve $g(f_1) = e_1 = \frac{1}{2}(f_1 + f_2)$ et $g(f_2) = e_1 = \frac{1}{2}(f_1 + f_2)$, d'où en effet $\det g = \det_{\mathscr{B}'}(g(\mathscr{B}')) = \begin{vmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{vmatrix} = 0$ et $\det(g + \mathrm{Id}_{\mathbb{R}^2}) = \begin{vmatrix} 3/2 & 1/2 \\ 1/2 & 3/2 \end{vmatrix} = 9/4 - 1/4 = 2$.

Proposition 4.0.5.
Soit $\mathscr{F}$ une famille de n vecteurs de E.

1. $\det_{\mathscr{B}}(f(\mathscr{F})) = \det f \times \det_{\mathscr{B}}(\mathscr{F})$;
2. si $g \in \mathscr{L}(E)$, $\det(g \circ f) = \det f \times \det g$;
3. $\det(\mathrm{Id}_E) = 1$;
4. f est un automorphisme de E ssi $\det f \neq 0$;
5. Si $\det f \neq 0$, alors $\det\left(f^{-1}\right) = \dfrac{1}{\det f}$.
6. $\det(\lambda f) = \lambda^n \det f$.

Démonstration.
1. En utilisant la démonstration précédente, on a : $\det_{\mathscr{B}}(f(\mathscr{F})) = \varphi(\mathscr{F}) = \varphi(\mathscr{B}) \times \det_{\mathscr{B}}(\mathscr{F})$, et on a montré que $\varphi(\mathscr{B}) = \det f$.
2.
$$\begin{aligned} \det(g \circ f) &= \det_{\mathscr{B}}(g(f(e_1)), \dots, g(f(e_n)) \\ &= \det_{\mathscr{B}} g(\underbrace{f(e_1), \dots, f(e_n)}_{=\mathscr{F}}) \\ &= \det_{\mathscr{B}} g(\mathscr{F}) = \det g \times \det_{\mathscr{B}} \mathscr{F} \\ &= \det g \times \det f. \end{aligned}$$
3. $\det(\mathrm{Id}_E) = \det_{\mathscr{B}}(\mathrm{Id}_E(\mathscr{B})) = \det_{\mathscr{B}}(\mathscr{B}) = 1$.
4. ($\Rightarrow$) : f^{-1} existe et donc $\det(f \circ f^{-1}) = \det \mathrm{Id}_E = 1$. Or d'après le point 2, $\det(f \circ f^{-1}) = \det f \times \det(f^{-1})$, donc on obtient $\det f \neq 0$, et aussi $\det f^{-1} = \dfrac{1}{\det f}$ (ce qui par ailleurs prouve le point 4).
($\Leftarrow$) : On suppose que $\det f \neq 0$. Donc $\det_{\mathscr{B}}(f(\mathscr{B})) \neq 0$, d'où $f(\mathscr{B})$ est une base de E, et ainsi f est un automorphisme.
5. Par multilinéarité du déterminant, $\det(\lambda f) = \det_{\mathscr{B}}(\lambda f(e_1), \dots, \lambda f(e_n)) = \lambda^n \det_{\mathscr{B}}(f(e_1), \dots, f(e_n)) = \lambda^n \det f$.

□

Exemple 4.0.6.
$\det(2\mathrm{Id}_{\mathbb{R}^2}) = 2^2 \det \mathrm{Id}_{\mathbb{R}^2} = 4$, mais $\det(2\mathrm{Id}_{\mathbb{R}^3}) = 2^3 \det \mathrm{Id}_{\mathbb{R}^3} = 8$.

 De manière générale, $\det(f + g) \neq \det(f) + \det(g)$.

5 Déterminant d'une matrice carrée

5.1 Définitions et propriétés

Définition 5.1.1.
Soit $A \in \mathscr{M}_n(\mathbb{K})$ et $\mathscr{C} = (e_1, \dots, e_n)$ la base canonique de $\mathbb{K}^n$. Alors, il existe une unique $f \in \mathscr{L}(\mathbb{K}^n)$ telle que $A = \mathrm{Mat}_{\mathscr{C}}(f)$. On définit alors le déterminant de A comme étant le scalaire $\det f$.

Ainsi, si $A = (a_{i,j})_{1 \leqslant i,j \leqslant n}$, en notant $(C_1, \dots, C_n)$ les colonnes de A, on a

$$\det A = \det_{\mathscr{C}}(C_1, \dots, C_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

On retrouve les mêmes propriétés que pour le déterminant d'une application linéaire :

Théorème 5.1.2.
Soit E un $\mathbb{K}$-ev et $f \in \mathscr{L}(E)$, et soit $\mathscr{B}$ une base quelconque de E. Alors,

$$\det(f) = \det(\mathrm{Mat}_{\mathscr{B}}(f)).$$

De même, si $\mathscr{F}$ est une famille de n vecteurs de E, $\det_{\mathscr{B}}(\mathscr{F}) = \det(\mathrm{Mat}_{\mathscr{B}}(\mathscr{F}))$.

Démonstration.
Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base de E. Avec $A = (a_{i,j}) = \mathrm{Mat}_{\mathscr{B}}(f)$, on a, d'une part,

$$\det A = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}.$$

De plus,

$$\begin{aligned} \det(f) = \det_{\mathscr{B}}(f(\mathscr{B})) &= \det_{\mathscr{B}} \left(\sum_{i=1}^{n} a_{i,j} e_i \right)_{j=1}^{n} \\ &= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)} \\ &= \det A \end{aligned}$$

On procède de même pour une famille de vecteurs. □

Proposition 5.1.3.
Soit $A, B \in \mathscr{M}_n(\mathbb{K})$.

1. $\det(A \times B) = \det A \times \det B$.
2. $\det \mathrm{I}_n = 1$.
3. A est inversible si et seulement si $\det A \neq 0$. Si $\det A \neq 0$, on a $\det A^{-1} = \dfrac{1}{\det A}$.
4. $\det {}^tA = \det A$.
5. Si $\lambda \in \mathbb{K}$, $\det(\lambda A) = \lambda^n \det(A)$.

Démonstration. 1. , 2., 3. et 5. immédiats d'après les propriétés du déterminant d'une application linéaire.

5. si $A = (a_{ij})$, on note ${}^tA = (b_{ij})$ avec $b_{ij} = a_{ji}$. Alors :

$$\begin{aligned} \det {}^tA &= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} b_{i,\sigma(i)} \\ &= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i} \\ &\underset{\text{déjà vu}}{=} \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)} \\ &= \det A. \end{aligned}$$

□

Exercice 5.1.4.
Montrer de deux manières différentes que deux matrices semblables ont même déterminant.

5.2 Matrices triangulaires et triangulaires par blocs

Lemme 5.2.1.
Soit $\sigma \in S_n$ tel que pour tout $i \in [\![1, n]\!]$, $i \leqslant \sigma(i)$. Alors $\sigma = \mathrm{Id}$.

Démonstration.
Posons l'hypothèse de récurrence (H_i) : pour tout k de $n - i$ à n, $\sigma(k) = k$.

→ Initialisation : par hypothèse on a $\sigma(n) \geqslant n$. Mais $\sigma(n) \in [\![1, n]\!]$, donc nécessairement $\sigma(n) = n$. (H_0) est donc vraie.

→ Hérédité : supposons (H_i) vraie pour $i \in [\![0, n-1]\!]$. Alors pour tout $k \geqslant n - i$, $\sigma(k) = k$. Par injectivité de σ il vient donc : pour tout $k < n - i$, $\sigma(k) < n - i$. En particulier $\leqslant n - i - 1 \leqslant \sigma(n - i - 1) < n - i$, et donc forcément $\sigma(n - i - 1) = n - i - 1$, et (H_{i+1}) est vérifiée.

On a donc bien $\sigma = \mathrm{Id}$. □

Théorème 5.2.2 (Déterminant d'une matrice triangulaire)**.**
Soit $A = (a_{i,j})$ une matrice triangulaire. Alors,

$$\det A = \prod_{i=1}^{n} a_{i,i}.$$

Démonstration.
Supposons A triangulaire supérieure. Alors pour tous $i, j \in [\![1, n]\!]$, $i > j \Rightarrow a_{i,j} = 0$. On sait que

$$\det A = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

Soit $\sigma \in S_n$ tel que $\sigma \neq \mathrm{Id}$. Alors d'après le lemme 5.2.1, il existe i_0 tel que $\sigma(i_0) < i_0$. Alors $a_{i_0\sigma(i_0)} = 0$ donc $\prod_{i=1}^{n} a_{i,\sigma(i)} = 0$. Ainsi, dans la somme $\sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$, seule le terme pour $\sigma = \mathrm{Id}$ est non nul, et donc

$$\det A = \prod_{i=1}^{n} a_{i,\mathrm{Id}(i)} = \prod_{i=1}^{n} a_{i,i}.$$

On a évidemment le même résultat pour les matrices triangulaires inférieures. □

Exemple 5.2.3.
Une matrice A dont les coefficients sont écrits entre barres verticales signifie $\det A$.

$$\begin{vmatrix} 1 & 0 & 0 \\ 2 & 3 & 0 \\ -51 & -4 & 2 \end{vmatrix} = \begin{vmatrix} 3 & 1 & -16 \\ 0 & 1 & 15 \\ 0 & 0 & 2 \end{vmatrix} = 6.$$

Remarque 5.2.4.
Avec ce résultat on retrouve facilement qu'une matrice triangulaire est inversible si et seulement si elle n'a pas de zéro sur la diagonale.

Proposition 5.2.5.
Soit $M = \begin{pmatrix} A & B \\ 0 & \mathrm{I}_p \end{pmatrix}$ une matrice par blocs de $\mathscr{M}_{n+p}(\mathbb{K})$, avec $A \in \mathscr{M}_n(\mathbb{K})$ et $B \in \mathscr{M}_{n,p}(\mathbb{K})$. Alors

$$\det M = \det A.$$

Démonstration.
Considérons l'application $f : (\mathscr{M}_{n,1}(\mathbb{K}))^n \to \mathbb{K}$ telle que $f(x_1, \ldots, x_n) = \det M$, avec $M = \begin{pmatrix} A & B \\ 0_n & \mathrm{Id}_p \end{pmatrix}$ et B fixée, où A est la matrice de $(x_1, \ldots, x_n)$ dans la base canonique. Avec un léger abus de notation, on notera ceci $f(A)$. Cette application est n-linéaire alternée, donc il existe $k \in \mathbb{K}$ telle que pour tout $A \in \mathscr{M}_n(\mathbb{K})$, $f(A) = k \det A$. Or pour $A = \mathrm{I}_p$, M est une matrice triangulaire de déterminant 1, donc $k = 1$, et le résultat est démontré. □

Remarque 5.2.6.
Nous avons bien sûr de la même manière $\det \begin{pmatrix} \mathrm{I}_n & B \\ 0 & C \end{pmatrix} = \det C$.

Théorème 5.2.7.
[Déterminant d'une matrice triangulaire par blocs]
Soit $M = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ une matrice triangulaire par blocs. Alors,

$$\det M = \det A \times \det C.$$

Démonstration.
Il suffit d'écrire

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix} = \begin{pmatrix} \mathrm{I}_n & 0 \\ 0 & C \end{pmatrix} \begin{pmatrix} A & B \\ 0 & \mathrm{I}_p \end{pmatrix}.$$

□

Remarque 5.2.8.
Le résultat s'adapte évidemment dans le cas des matrices triangulaire inférieures par blocs, ainsi que dans le cas de matrices triangulaires par blocs avec plus de deux blocs sur la diagonale.

 La formule ne se généralise pas aux matrices par blocs non triangulaires. Ainsi,

$$\begin{vmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} \neq \begin{vmatrix} 0 & 0 \\ 0 & 1 \end{vmatrix} \cdot \begin{vmatrix} 0 & 0 \\ 0 & 1 \end{vmatrix} - \begin{vmatrix} 1 & 0 \\ 0 & 0 \end{vmatrix} \cdot \begin{vmatrix} 1 & 0 \\ 0 & 0 \end{vmatrix}.$$

5.3 Opérations élémentaires et pivot de Gauss

La méthode présentée ci-après est la méthode de base : elle fonctionne toujours, et est la plus rapide dans la grande majorité des cas.

On fixe $A \in \mathscr{M}_n(\mathbb{K})$.

Théorème 5.3.1. 1. Ajouter à une ligne ou une colonne de A une combinaison linéaire des autres lignes ou colonnes ne change pas le déterminant de A.

2. Multiplier une ligne ou une colonne de A par une constante $\lambda \in \mathbb{K}$, change le déterminant de A en $\lambda \det A$.

3. Échanger deux lignes ou deux colonnes de A change le déterminant de A en $-\det A$.

Démonstration.
C'est direct, car le déterminant est une fonction n-linéaire alternée de ses lignes, ainsi que de ses colonnes.

On peut aussi en donner une preuve matricielle. Effectuer chacune de ces opérations élémentaires revient à multiplier A par une certaine matrice inversible M, déjà vue dans le chapitre XXII. Ainsi le déterminant de A est changé en $\det M \times \det A$. Il suffit donc de calculer le déterminant de M, ce qui ne pose aucun problème dans les deux premiers cas, car alors M est triangulaire. Dans le cas 3, remarquons (par exemple pour les lignes) que $L_i \leftrightarrow L_j$ est équivalente à la suite d'opérations suivantes :

Ligne n$^\text{o}$ i	Ligne n$^\text{o}$ j	Opération effectuée
L_i	L_j	
$L_i + L_j$	L_j	$L_i \leftarrow L_i + L_j$
$L_i + L_j$	$-L_i$	$L_j \leftarrow L_j - L_i$
L_j	$-L_i$	$L_i \leftarrow L_i + L_j$
L_j	L_i	$L_i \leftarrow -L_i$

Il suffit donc de multiplier $\det A$ par le produit des déterminants de ces opérations successives, qui sont tous 1, sauf le dernier qui vaut -1 : ce produit vaut bien -1. □

Remarque 5.3.2.
À l'instar d'un calcul de rang, il est possible de mélanger des opérations sur les lignes et sur les colonnes pour calculer un déterminant de matrice.

Exemple 5.3.3.
Avec l'opération $C_2 \leftarrow 2C_2 - 3C_1$, on a

$$\begin{vmatrix} 2 & 3 \\ 5 & 7 \end{vmatrix} = \frac{1}{2}\begin{vmatrix} 2 & 0 \\ 5 & -1 \end{vmatrix} \underset{\text{triang.}}{=} -1.$$

Exemple 5.3.4.
Avec les opérations $C_2 \leftarrow 2C_2 - 3C_1$ et $C_3 \leftarrow 2C_3 - 5C_1$, on a

$$\begin{aligned}\begin{vmatrix} 2 & 3 & 5 \\ 4 & 3 & -1 \\ 3 & -1 & 2 \end{vmatrix} &= \frac{1}{2^2}\begin{vmatrix} 2 & 0 & 0 \\ 4 & -6 & -22 \\ 3 & -11 & -13 \end{vmatrix} \\ &= \frac{1}{4} \times 2 \times \begin{vmatrix} -6 & -22 \\ -11 & -11 \end{vmatrix} \\ &= -88.\end{aligned}$$

5.4 Développement par rapport à une ligne ou une colonne

Définition 5.4.1.
Soit $A = (a_{i,j}) \in \mathscr{M}_n(\mathbb{K})$.

1. On appelle *mineur d'ordre* (i,j) de A le scalaire $\Delta_{i,j} = \det A_{i,j}$ où $A_{i,j}$ est la matrice de $\mathscr{M}_{n-1}(\mathbb{K})$ obtenue à partir de A en supprimant la i^e ligne et la j^e colonne.
2. On appelle *cofacteur d'ordre* (i,j) de A le scalaire $(-1)^{i+j}\Delta_{i,j}$.
3. On appelle *comatrice de* A notée $\operatorname{com}(A)$ la matrice des cofacteurs *i.e.* $\operatorname{com}(A) = ((-1)^{i+j}\Delta_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathscr{M}_n(\mathbb{K})$.

Exemple 5.4.2.
Soit $A = \begin{pmatrix} 1 & 2 & 0 \\ 3 & 2 & 0 \\ 0 & 1 & -2 \end{pmatrix}$. On a alors $\operatorname{com} A = \begin{pmatrix} -4 & 6 & 3 \\ 4 & -2 & -1 \\ 0 & 0 & -4 \end{pmatrix}$.

Théorème 5.4.3 (Développement par rapport à une ligne ou une colonne)**.**
Soit $A \in \mathscr{M}_n(\mathbb{K})$, $A = (a_{i,j})$, soit $i, j \in [\![1, n]\!]$.

1. Développement par rapport à la i^e ligne :

$$\det A = \sum_{k=1}^{n} (-1)^{i+k} a_{i,k} \Delta_{i,k}.$$

2. Développement par rapport à la j^{e} colonne :

$$\det A = \sum_{k=1}^{n} (-1)^{k+j} a_{k,j} \Delta_{k,j}.$$

Démonstration.
On ne démontre que le développement par rapport à la première ligne :

$$\begin{aligned}
&\det A \\
&= |a_{ij}| = \begin{vmatrix} L_1 \\ M \end{vmatrix} \\
&= \begin{vmatrix} a_{11} & 0 & \dots & 0 \\ & M & & \end{vmatrix} + \begin{vmatrix} 0 & a_{12} & 0 & \dots & 0 \\ & & M & & \end{vmatrix} \\
&\quad + \dots + \begin{vmatrix} 0 & \dots & 0 & a_{1n} \\ & & M & \end{vmatrix} \\
&= a_{11} \underbrace{\begin{vmatrix} 1 & 0 & \dots & 0 \\ & M & & \end{vmatrix}}_{=\delta_1} + a_{12} \underbrace{\begin{vmatrix} 0 & 1 & 0 & \dots & 0 \\ & & M & & \end{vmatrix}}_{=\delta_2} \\
&\quad + \dots + a_{1n} \underbrace{\begin{vmatrix} 0 & \dots & 0 & 1 \\ & & M & \end{vmatrix}}_{=\delta_n} \\
&= \sum_{j=1}^{n} a_{1j} \delta_j.
\end{aligned}$$

Calculons δ_j. Pour cela on note $C_1, \dots, C_n$ les n colonnes de la matrice $M = \begin{pmatrix} a_{21} & \dots & a_{2n} \\ \dots & & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$:

$$\begin{aligned}
\delta_j &= \begin{vmatrix} 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ C_1 & \dots & C_{j-1} & C_j & C_{j+1} & \dots & C_n \end{vmatrix} \\
&= (-1)^{j-1} \begin{vmatrix} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ C_j & C_1 & \dots & C_{j-1} & C_{j+1} & \dots & C_n \end{vmatrix} \\
&= \begin{vmatrix} C_1 & \dots & C_{j-1} & C_{j+1} & \dots & C_n \end{vmatrix},
\end{aligned}$$

car c'est une matrice triangulaire par blocs.
Or $\begin{pmatrix} C_1 & \dots & C_{j-1} & C_{j+1} & \dots & C_n \end{pmatrix} = A_{1j}$, d'où $\delta_j = (-1)^{j+1} \Delta_{1j}$ et on a le résultat voulu.

On peut aussi observer ce résultat directement dans la définition du déterminant :

$$\begin{aligned}
\det(A) &= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{k=1}^{n} a_{k,\sigma(k)} \\
&= \sum_{j=1}^{n} \sum_{\sigma \in S_n,\ \sigma(i)=j} \varepsilon(\sigma) \prod_{k=1}^{n} a_{k,\sigma(k)} \\
&= \sum_{j=1}^{n} a_{i,j} \sum_{\sigma \in S_n,\ \sigma(i)=j} \varepsilon(\sigma) \prod_{\substack{k=1 \\ k \neq j}}^{n} a_{k,\sigma(k)}
\end{aligned}$$

Il suffit ensuite de remarquer que, pour chaque $1 \leqslant j \leqslant n$, il y a bien $(n-1)!$ permutations σ vérifiant $\sigma(i) = j$ puis que le terme

$$\sum_{\sigma \in S_n,\ \sigma(i)=j} \varepsilon(\sigma) \prod_{\substack{k=1 \\ k \neq j}}^{n} a_{k,\sigma(k)}$$

correspond bien au cofacteur d'ordre i, j de A. Nous laissons le lecteur intéressé montrer cela. □

Remarque 5.4.4.
Dans $\mathbb{R}^3$ et la base canonique $\mathscr{B}$, on retrouve les relations observées en début de chapitre : $\det_{\mathscr{B}}(x, y, z) = x \cdot (y \wedge z)$ *etc.*

Remarque 5.4.5.
• Cette méthode n'est à utiliser que lorsqu'il y a une ligne ou une colonne contenant un ou deux coefficients non nuls seulement, sinon elle beaucoup plus longue que la méthode du pivot de Gauss. N'oubliez pas non plus que si l'on veut développer par rapport à une ligne ou une colonne, il existe d'autres lignes ou colonnes que les premières !
• Pour démontrer le théorème 5.4.3, nous avons utilisé le résultat 5.2.7. Il est possible de démontrer ces deux résultats dans l'autre sens, mais attention à ne pas utiliser un résultat dans sa propre démonstration.

Exemple 5.4.6.
Comparer le calcul de $\begin{vmatrix} 1 & 3 & 4 \\ 2 & -1 & 2 \\ -5 & 1 & 7 \end{vmatrix}$ avec les deux méthodes (développement ou pivot de Gauss).

Corollaire 5.4.7.
Soit $A \in \mathscr{M}_n(\mathbb{K})$. Alors $A \times {}^t\mathrm{com}\, A = {}^t\mathrm{com}\, A \times$

$A = (\det A)\cdot \mathrm{I}_n$. En particulier, si A est inversible, alors $A^{-1} = \dfrac{1}{\det A}\cdot {}^t\mathrm{com}\, A$.

Remarque 5.4.8.
Ce résultat est inutilisable en pratique pour calculer des inverses de matrices. Si $n = 2$, ça va (on retrouve la formule de l'inverse d'une matrice 2×2), pour $n = 3$, c'est trop long, et pour $n \geqslant 4$ c'est un cauchemar. Essayez !

Démonstration.
On note $A = (a_{ij})$ et ${}^t\mathrm{com}\, A = (b_{ij})$ avec $b_{ij} = (-1)^{i+j}\Delta_{ji}$. On note également A. ${}^t\mathrm{com}\, A = (C_{ij})_{i,j}$, donc

$$C_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} = \sum_{k=1}^{n}(-1)^{k+j}a_{ik}\Delta_{jk}.$$

$\to$ si $i = j$: grâce à la formule de développement par rapport à la j^{e} ligne, on trouve $C_{ij} = \det A$.
$\to$ si $i \neq j$: on note Δ la matrice obtenue à partir de A en remplaçant la j^{e} ligne par la i^{e} ligne : cette matrice à deux lignes égales, donc $\det\Delta = 0$. On développe $\det\Delta$ par rapport à la j^{e} ligne, et on a :

$$0 = \det\Delta = \sum_{k=1}^{n}(-1)^{k+j}a_{ik}\Delta_{jk} = C_{ij},$$

d'où le résultat.

On procède de la même manière pour calculer ${}^t\mathrm{com}\, A\times A$. □

Proposition 5.4.9 (Déterminant de Vandermonde)**.**
Soit $n \in \mathbb{N}^*$ et $x_0, \ldots, x_n$ $n+1$ scalaires. On définit le *déterminant de Vandermonde* par :

$$V(x_0, x_1, \ldots, x_n) = \begin{vmatrix} 1 & x_0 & x_0^2 & \ldots & x_0^n \\ 1 & x_1 & x_1^2 & \ldots & x_1^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^n \end{vmatrix}.$$

Alors,

$$V(x_0, \ldots, x_n) = \prod_{0\leqslant i<j\leqslant n}(x_j - x_i).$$

Démonstration.
Ce déterminant est un classique parmi les classiques. Il est possible de le calculer directement par pivot de Gauss. Ici, on le démontre par récurrence.

Les cas $n = 0$ ou $n = 1$ sont évidents : $V(x_0) = 1$ et $V(x_0, x_1) = x_1 - x_0$.

Soit $n \in \mathbb{N}$ tel que le résultat soit vrai au rang n. Considérons le polynôme $V(x_0, \ldots, x_n, X)$. En le développant par rapport à la dernière ligne, on voit qu'il est de degré au plus $n+1$, et que le terme en X^{n+1} a pour coefficient $V(x_0, \ldots, x_n)$. Or il est aisé de voir qu'il a pour racines $x_0, \ldots, x_n$. Il existe donc un scalaire $k \in \mathbb{K}$ tel que

$$V(x_0, \ldots, x_n, X) = k\prod_{i=0}^{n}(X - x_i).$$

Ce scalaire k est le coefficient dominant de $V(x_0, \ldots, x_n, X)$, c'est donc en développant sur la dernière ligne : $V(x_0, \ldots, x_n)$. Ainsi, en évaluant ce polynôme en x_{n+1}, il vient :

$$V(x_0, \ldots, x_n, x_{n+1}) = V(x_0, \ldots, x_n)\prod_{i=0}^{n}(x_{n+1} - x_i)$$

ce qui, en utilisant l'hypothèse de récurrence, est bien le résultat recherché. □

Remarque 5.4.10.
On peut utiliser le déterminant de Vandermonde pour montrer que la famille des polynômes d'interpolation de Lagrange est libre.

Chapitre XXV

Espaces euclidiens et préhilbertiens réels

Le corps de base est $\mathbb{R}$. n, p, q, r et s désignent des entiers naturels non nuls. E désigne un espace vectoriel.

1 Produit scalaire, norme et distance

Définition 1.0.1.
On appelle *produit scalaire sur E* toute application $\varphi : E \times E \to \mathbb{R}$ bilinéaire symétrique et telle que pour tout $x \in E$, on ait d'une part $\varphi(x,x) \geqslant 0$ et d'autre part $\varphi(x,x) = 0$ si et seulement si $x = 0$. Un espace vectoriel réel muni d'un produit scalaire est dit *préhilbertien*. Si de plus il est de dimension finie, il est dit *euclidien*.

Remarque 1.0.2.
— Différentes notations sont utilisées couramment pour le produit scalaire de x et y : $(x|y), \langle x \,|\, y\rangle, (x,y), \langle x,y\rangle, x \cdot y$.
— Par bilinéarité, si x ou $y = 0$, $\langle x \,|\, y\rangle = 0$.
— La symétrie et la linéarité par rapport à une variable suffisent à montrer la bilinéarité.
— Jusqu'à maintenant on définissait le produit scalaire à partir d'angles. En fait c'est l'inverse que l'on fait lorsque l'on théorise tout cela.

Exemple 1.0.3.
— Les produits scalaires usuels vus en début d'année sur $\mathbb{R}^2$ et $\mathbb{R}^3$ sont bien évidemment des produits scalaires.
— Il existe de nombreux produits scalaires sur $\mathbb{R}^2$; par exemple $((x_1,y_1),(x_2,y_2)) \mapsto x_1x_2 - y_1x_2 + 2y_1y_2 - x_1y_2$.
— Il existe également sur $\mathbb{R}^n$ un produit scalaire canonique ; $(x_1,\dots,x_n).(y_1,\dots,y_n) = \sum_{k=1}^{n} x_iy_i$.
— Par extension, tout $\mathbb{R}$-ev de dimension n, étant isomorphe à $\mathbb{R}^n$, est muni d'un produit scalaire. Ainsi, sur $\mathbb{R}_n[X]$ le produit scalaire usuel est $\left(\sum_{k=0}^{n} a_kX^k\right).\left(\sum_{k=0}^{n} b_kX^k\right) = \left(\sum_{k=0}^{n} a_kb_k\right)$.
— Soit a et b deux réels avec $a < b$. Sur $\mathscr{C}([a,b],\mathbb{R})$, l'application $(f,g) \mapsto \int_a^b fg$ est un produit scalaire (attention : cet espace est de dimension infinie, donc n'est pas euclidien, mais préhilbertien réel).

Exercice 1.0.4.
L'espérance munit-elle l'ensemble des variables aléatoires réelles sur un espace probabilisé fini d'un produit scalaire (via $\langle X,Y\rangle = \mathrm{E}(XY)$) ?
Proposer une solution à ce « problème ».

Définition 1.0.5 (Distance)**.**
Soit E un ensemble (quelconque, pas nécessairement un espace vectoriel). On appelle *distance sur E* toute application $\mathrm{d} : E^2 \to \mathbb{R}^+$ vérifiant les trois conditions suivantes :
(i) $\forall (x,y) \in E^2 \quad \mathrm{d}(x,y) = 0 \iff x = y$;
(ii) $\forall (x,y) \in E^2 \quad \mathrm{d}(x,y) = \mathrm{d}(y,x)$ (symétrie) ;
(iii) $\forall (x,y,z) \in E^3 \quad \mathrm{d}(x,z) \leqslant \mathrm{d}(x,y) + \mathrm{d}(y,z)$ (inégalité triangulaire).
Un ensemble muni d'une distance est appelé *espace métrique*.

Exemple 1.0.6.
— La distance usuelle dans le plan est une distance.
— La distance de deux points sur un graphe connexe, comptée comme le nombre d'arêtes à parcourir sur ce graphe.

Remarque 1.0.7.
Soit E un ensemble muni d'une distance d. Soit $(x,y,z) \in E^3$. Alors, on a

$$|\,\mathrm{d}(x,y) - \mathrm{d}(x,z)| \leqslant \mathrm{d}(y,z).$$

Démonstration.
On a $\mathrm{d}(x,z) \leqslant \mathrm{d}(x,y) + \mathrm{d}(y,z)$, donc $\mathrm{d}(x,z) - \mathrm{d}(x,y) \leqslant \mathrm{d}(y,z)$. De même, $\mathrm{d}(x,y) \leqslant \mathrm{d}(x,z) + \mathrm{d}(z,y)$, donc $\mathrm{d}(x,y) - \mathrm{d}(x,z) \leqslant \mathrm{d}(y,z)$. Or $|\,\mathrm{d}(x,y) - \mathrm{d}(x,z)| = \max(\,\mathrm{d}(x,z) - \mathrm{d}(x,y), \mathrm{d}(x,y) - \mathrm{d}(x,z))$, d'où le résultat. □

Définition 1.0.8 (Norme)**.**
Soit E un $\mathbb{R}$-espace vectoriel. On appelle norme sur E toute application $\|.\| : E \to \mathbb{R}^+$ vérifiant les trois conditions suivantes :

(i) $\forall x \in E \qquad \|x\| = 0 \iff x = 0$;

(ii) $\forall \lambda \in \mathbb{R},\ \forall x \in E \qquad \|\lambda x\| = |\lambda|\,\|x\|$ (homogénéité) ;

(iii) $\forall (x, y) \in E \qquad \|x + y\| \leqslant \|x\| + \|y\|$ (inégalité triangulaire).

Exemple 1.0.9.
Sur $\mathbb{R}^n$ et pour $p \in [1, +\infty[$, les applications

$$\|\cdot\|_p \ : \ (x_1, \dots, x_n) \mapsto \left(\sum_{k=1}^{n} |x_k|^p \right)^{1/p}$$

et

$$\|\cdot\|_\infty \ : \ (x_1, \dots, x_n) \mapsto \max_{k \in [\![1,n]\!]} |x_k|$$

sont des normes.

Remarque 1.0.10.
Soit E un $\mathbb{R}$-espace vectoriel muni d'une norme $\|.\|$. Alors pour tout $(x, y) \in E^2$, on a

$$|\|x\| - \|y\|| \leqslant \|x - y\| .$$

Démonstration.
Soit $(x, y) \in E^2$. Remarquons qu'on a $\|x\| = \|x + y - y\| \leqslant \|x + y\| + \|y\|$ par l'inégalité triangulaire, d'où l'on déduit $\|x\| - \|y\| \leqslant \|x + y\|$. Symétriquement, on remarque qu'on a $\|y\| - \|x\| \leqslant \|x + y\|$. Or $|\|x\| - \|y\|| = \max(\|x\| - \|y\|, \|y\| - \|x\|)$. On en déduit le résultat. □

Définition 1.0.11 (Distance associée à une norme)**.**
Soit E un $\mathbb{R}$-espace vectoriel muni d'une norme $\|.\|$. On appelle *distance associée à la norme* $\|.\|$ l'application $(x, y) \mapsto \|x - y\|$.

Proposition 1.0.12.
Cette application est bien une distance.

Exemple 1.0.13.
La distance associée à $\|\cdot\|_1$ est parfois appelée *distance de Manhattan*. Dans Manhattan, les rues forment un damier « orthogonal », on ne peut donc que se déplacer parallèlement à ces axes. La distance parcourue entre deux points n'est donc pas la distance « euclidienne » usuelle ...

Exercice 1.0.14.
Pour une norme $\|\cdot\|$, on appelle boule centrée en $a \in E$ et de rayon $r \geqslant 0$ l'ensemble

$$B(a, r) = \{\, x \in E \mid \|a - x\| \leqslant r \,\} .$$

Tracer les boules centrée en 0 et de rayon 1 pour les normes $\|\cdot\|_1$, $\|\cdot\|_2$ et $\|\cdot\|_\infty$ sur $\mathbb{R}^2$.

Démonstration.
Soit d la distance associée à une norme $\|.\|$ sur un $\mathbb{R}$-espace vectoriel E. On a clairement $\forall (x, y) \in E^2 \quad \mathrm{d}(x, y) \geqslant 0$, donc d est bien une application de E^2 dans $\mathbb{R}^+$. On vérifie aisément les trois conditions de la définition d'une distance :

(i) Soit $(x, y) \in E^2$. On a $\mathrm{d}(x, y) = \|x - y\|$. Or $\|x - y\| = 0 \iff x - y = 0$. Donc $\mathrm{d}(x, y) = 0 \iff x = y$.

(ii) Soit $(x, y) \in E^2$. On a $\mathrm{d}(y, x) = \|y - x\| = \|-(x - y)\| = |-1|\,\|x - y\| = \mathrm{d}(x, y)$.

(iii) Soit $(x, y, z) \in E^3$. On a $\mathrm{d}(x, z) = \|x - y + y - z\| \leqslant \|x - y\| + \|y - z\| = \mathrm{d}(x, y) + \mathrm{d}(y, z)$.

□

Définition 1.0.15 (Norme associée à un produit scalaire)**.**
Soit $(E, \langle\,|\,\rangle)$ un espace préhilbertien. On appelle *norme associée au produit scalaire* $\langle\,|\,\rangle$ l'application $x \mapsto \sqrt{\langle x \,|\, x \rangle}$.

Remarque 1.0.16.

1. Il est clair, par positivité du produit scalaire, que cette application est bien définie. La racine carrée étant à valeurs dans $\mathbb{R}^+$, elle est de plus à valeurs dans $\mathbb{R}^+$. Il reste à voir si cette application est bien une norme.
2. La norme associée à un produit scalaire dépend évidemment du produit scalaire. Par exemple sur $\mathbb{R}^2$, les normes associées respectivement au produit scalaire usuel et au produit scalaire $((x, y), (x', y')) \mapsto \frac{1}{2}xx' + 2yy'$

sont différentes (regarder par exemple les valeurs pour les vecteurs $(1,0)$ et $(0,1)$).

3. On a directement que pour une famille $(x_1,\dots,x_n)$ de vecteurs,

$$\left\|\sum_{i=1}^{n} x_i\right\|^2 = \sum_{1\leqslant i,j\leqslant n} \langle x_i \,|\, x_j\rangle$$
$$= \sum_{i=1}^{n} \|x_i\|^2 + 2\sum_{1\leqslant i<j\leqslant n} \langle x_i \,|\, x_j\rangle .$$

Pour deux vecteurs, on retrouve $\|x\pm y\|^2 = \|x\|^2 \pm 2\langle x \,|\, y\rangle + \|y\|^2$.

Dans tout ce qui suit, sauf mention expresse du contraire, $(E,\langle\,|\,\rangle)$ désigne un espace vectoriel préhilbertien, et $\|.\|$ la norme associée à son produit scalaire.

Proposition 1.0.17.
Soit $(E,\langle\,|\,\rangle)$ un espace préhilbertien et $\|.\|$ la norme associée. On a

1. $\forall x\in E \quad \|x\|=0 \iff x=0$;
2. $\forall \lambda\in\mathbb{R} \quad \forall x\in E \qquad \|\lambda x\| = |\lambda|\cdot\|x\|$.

Démonstration. 1. Soit $x\in E$. On a $\|x\|=0 \iff \langle x \,|\, x\rangle = 0$. $\langle\,|\,\rangle$ étant un produit scalaire, on a donc $\|x\|=0 \iff x=0$.

2. Soit $\lambda\in\mathbb{R}$ et $x\in E$. On a $\|\lambda x\| = \sqrt{\langle \lambda x \,|\, \lambda x\rangle} = \sqrt{\lambda^2\langle x \,|\, x\rangle} = |\lambda|\sqrt{\langle x \,|\, x\rangle}$.

□

Avec ce qui précède, il suffit maintenant de démontrer que $\|.\|$ vérifie l'inégalité triangulaire pour démontrer qu'il s'agit bien d'une norme. Pour cela, on démontre tout d'abord le théorème suivant.

Théorème 1.0.18 (Inégalité de Cauchy-Schwarz)**.**
Soit $(E,\langle\,|\,\rangle)$ un espace préhilbertien et $\|.\|$ la norme associée. Alors pour tout $(x,y)\in E^2$, on a

$$|\langle x,y\rangle| \leqslant \|x\|\cdot\|y\| .$$

L'égalité a lieu si et seulement si x et y sont colinéaires.

Démonstration.
Soient $x,y\in E$. Pour $y=0$ le résultat est évident. Sinon, on peut donner deux démonstrations

Géométrique Posons $u = \frac{1}{\|y\|}y$. On vérifie aisément $\|u\|=1$. Posons alors $x' = \langle x \,|\, u\rangle\, u$ et $x'' = x - x'$ (faire un dessin). On a alors

$$\langle x' \,|\, x''\rangle = \langle x' \,|\, x\rangle - \langle x' \,|\, x'\rangle = \langle x \,|\, u\rangle^2 - \langle x \,|\, u\rangle^2 = 0.$$

On en déduit

$$\|x\|^2 = \|x'\|^2 + 2\langle x' \,|\, x''\rangle + \|x''\|^2$$
$$= \|x'\|^2 + \|x''\|^2$$
$$\geqslant \|x'\|^2 .$$

On en déduit $\|x\|\,.\,\|y\| \geqslant \|x'\|\,.\,\|y\|$. Or on a :

$$\|x'\|\,.\,\|y\| = |\langle x \,|\, u\rangle|\,.\,\|y\|$$
$$= |\langle x \,|\, y\rangle|.$$

D'où le résultat.

Algébrique pour tout $t\in\mathbb{R}$, on a : $\|x+ty\|^2 = \|x\|^2 + 2t\langle x \,|\, y\rangle + t^2\|y\|^2$. C'est un polynôme toujours positif, donc son discriminant est négatif ou nul.

Il y a égalité dans l'inégalité de Cauchy-Schwarz si et seulement si ce discriminant est nul, donc si et seulement si ce polynôme a une racine réelle, donc si et seulement si il existe t tel que [à vous de l'écrire], donc si et seulement si x et y sont colinéaires.

Une idée calculatoire astucieuse Si $x=0$ ou $y=0$, le résultat est évident. Sinon, on remarque que $\left\|\frac{x}{\|x\|}\right\| = 1$ et l'on écrit ($\pm$ signifie qu'on le fait pour $+$ puis pour $-$) :

$$0 \leqslant \left\|\frac{x}{\|x\|} \pm \frac{y}{\|y\|}\right\|^2 = \left\|\frac{x}{\|x\|}\right\|^2 + \left\|\frac{y}{\|y\|}\right\|^2 \pm 2\frac{\langle x \,|\, y\rangle}{\|x\|\,\|y\|}$$

ce qui donne

$$0 \leqslant 1 \pm \frac{\langle x \,|\, y\rangle}{\|x\|\,\|y\|}$$

et c'est fini !

□

Proposition 1.0.19 (Inégalité triangulaire)**.**
Soit $(E,\langle\,|\,\rangle)$ un espace préhilbertien, $x,y\in E$. Alors,

$$\|x+y\| \leqslant \|x\| + \|y\| .$$

De plus, on a l'égalité si et seulement si x et y sont colinéaires et de même sens.

Démonstration.
On a $\|x+y\|^2 = \langle x+y \,|\, x+y\rangle = \|x\|^2 + 2\langle x \,|\, y\rangle + \|y\|^2$. Or $(\|x\|+\|y\|)^2 = \|x\|^2 + 2\|x\|.\|y\| + \|y\|^2$ et $\langle x \,|\, y\rangle \leqslant \|x\|.\|y\|$, donc $\|x+y\|^2 \leqslant (\|x\|+\|y\|)^2$. $\|x+y\|$ et $\|x\|+\|y\|$ étant positifs, on en déduit le résultat.

L'égalité a lieu si et seulement si $\langle x \,|\, y\rangle = \|x\|.\|y\|$. Pour cela, il est nécessaire d'avoir $\langle x \,|\, y\rangle \geqslant 0$ (car le produit de deux normes est positif ou nul) et x et y colinéaires (cas d'égalité de Cauchy-Schwarz), donc il est nécessaire que x et y soient colinéaires — l'un s'écrit comme produit de l'autre par un scalaire — et de même sens — ce scalaire est positif ou nul. Cette condition est clairement suffisante. □

Théorème 1.0.20.
Soit $(E, \langle\,|\,\rangle)$ un espace préhilbertien, $x, y \in E$.

1. Identité du parallélogramme :
$$\|x+y\|^2 + \|x-y\|^2 = 2(\|x\|^2 + \|y\|^2).$$
2. Identité de polarisation :
$$\begin{aligned}\langle x \,|\, y\rangle &= \frac{1}{2}(\|x+y\|^2 - \|x\|^2 - \|y\|^2)\\ &= \frac{1}{4}(\|x+y\|^2 - \|x-y\|^2).\end{aligned}$$

Remarque 1.0.21.
Faire le dessin d'un parallélogramme, on utilise le théorème d'Al-Kashi deux fois (une par hypothénuse).

Démonstration.
Il suffit de développer les normes. □

Remarque 1.0.22.
Ces identités permettent de retrouver l'expression du produit scalaire quand on ne connaît que la norme.

Exemple 1.0.23.
Existe-t-il un produit scalaire donnant la norme $\|(x,y)\|^2 = (x+y)^2 + x^2$?

2 Orthogonalité

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

2.1 Premières définitions

Définition 2.1.1.
Soient $x, y \in E$. On dit que x est *unitaire* (ou *normé*) si $\|x\| = 1$. On dit que x et y sont *orthogonaux* et l'on note $x \perp y$ si $\langle x \,|\, y\rangle = 0$.

Remarque 2.1.2.
Si $x \neq 0_E$, il y a exactement deux vecteurs unitaires colinéaires à x.

Exemple 2.1.3.
• Tout vecteur est toujours orthogonal au vecteur nul.
• Dans $\mathbb{R}^2$ muni du produit scalaire usuel, $(1,3)$ et $(-6,2)$ sont orthogonaux.
• Dans $\mathbb{R}^2$ muni du produit scalaire $(x,y)\cdot(x',y') = 2xx' - xy' - x'y + 3yy'$, les vecteurs $(1,1)$ et $(2,-1)$ sont orthogonaux.

2.2 Familles orthogonales

Définition 2.2.1.
Une famille de vecteurs est dite *orthogonale* s'ils sont 2 à 2 orthogonaux. Si les vecteurs sont de plus unitaires, la famille est dite *orthonormale* (ou *orthonormée*).

Exemple 2.2.2.
Les $f_n : x \mapsto \cos(nx)$, $n \in \mathbb{N}$, forment une famille orthogonale pour le produit scalaire usuel de $\mathscr{C}([0,2\pi],\mathbb{R})$.

Théorème 2.2.3 (Pythagore)**.**
Soit $(v_1,\dots,v_n)$ une famille orthogonale de n vecteurs. Alors $\left\|\sum_{k=1}^{n} v_k\right\|^2 = \sum_{k=1}^{n} \|v_k\|^2$.

Démonstration.
On développe le produit scalaire : $\|\sum_{k=1}^{n} v_k\|^2 = \sum_{i=1}^{n}\sum_{j=1}^{n}\langle v_i \,|\, v_j\rangle$. □

Exemple 2.2.4.
Dans $\mathbb{R}^3$ muni du produit scalaire usuel, on pose $v_1 = (1,2,3)$, $v_2 = (-5,1,1)$ et $v_3 = (-1,-16,11)$. Vérifier que la famille (v_1,v_2,v_3) est orthogonale et s'assurer que l'égalité donnée par le théorème de Pythagore est vérifiée.

Théorème 2.2.5.
Toute famille orthogonale ne comportant **aucun vecteur nul** est libre.

Démonstration.
Soient λ_k tels que $\sum_{k=1}^{n} \lambda_k v_k = 0$. Alors pour tout i, $\left\langle \sum_{k=1}^{n} \lambda_k v_k \,\middle|\, v_i \right\rangle = 0$ or quand on développe la somme on a $\lambda_i \langle v_i \,|\, v_i\rangle$. □

Remarque 2.2.6.
Toute famille orthonormale est une famille orthogonale ne comportant aucun vecteur nul.

Corollaire 2.2.7.
Toute famille orthogonale ne comportant **aucun vecteur nul** et de cardinal $\dim E$ est une base de E.

Exemple 2.2.8.
$\begin{pmatrix}0\\1\\2\end{pmatrix}, \begin{pmatrix}1\\-2\\1\end{pmatrix}$ et $\begin{pmatrix}5\\2\\-1\end{pmatrix}$ forment une famille orthogonale, et donc une base de $\mathbb{R}^3$.

Théorème 2.2.9 (orthonormalisation de Gram–Schmidt)**.**
On suppose E euclidien de dim n. Soit $(u_1,\dots,u_n)$ une base de E. Alors il existe une base $(v_1,\dots,v_n)$ de E telle que :

1. $(v_1,\dots,v_n)$ est orthonormale ;
2. $\forall k \in [\![1,n]\!]$, $\mathrm{Vect}(u_1,\dots u_k) = \mathrm{Vect}(v_1,\dots v_k)$.

Les v_k sont uniques au signe près et on peut choisir : $v_k = \dfrac{u_k - \sum_{i=1}^{k-1} \langle u_k \,|\, v_i\rangle\, v_i}{\left\| u_k - \sum_{i=1}^{k-1} \langle u_k \,|\, v_i\rangle\, v_i \right\|}$.

Démonstration.
Explication pour le choix de v_1.
• Analyse : on suppose la famille construite jusqu'au rang k. Construisons le $k+1^{\text{e}}$ vecteur.
Il faut choisir v_{k+1} dans $\mathrm{Vect}(u_1,\dots,u_k,u_{k+1}) = \mathrm{Vect}(v_1,\dots,v_k,u_{k+1})$: $v_{k+1} = \lambda_1 v_1 + \dots \lambda_k v_k + \mu u_{k+1}$. $\langle v_{k+1} \,|\, v_j\rangle = 0$ donne $\lambda_j + \mu \langle u_{k+1} \,|\, v_j\rangle = 0$, donc $v_{k+1} = \mu\left(-\sum_{i=1}^{k} \langle u_{k+1} \,|\, v_i\rangle\, v_i + u_{k+1} \right)$. Reste à choisir μ pour avoir $\|v_{k+1}\| = 1$ (2 choix possibles).
• Synthèse : on a vu unicité au signe près. On vérifie que les vecteurs trouvés conviennent bien. □

Exemple 2.2.10.
Orthonormaliser $(1,X,X^2)$ pour le produit scalaire de $\mathbb{R}_2[X]$, $\langle P \,|\, Q\rangle = \int_0^1 P(t)Q(t)\,\mathrm{d}t$. On trouve (P_1,P_2,P_3), où

$$\begin{aligned} P_1 &= 1, \\ P_2 = \frac{X - 1/2}{1/(2\sqrt{3})} &= \sqrt{3}(2X-1), \\ P_2 = \frac{X^2 - X + 1/6}{\|\dots\|} &= \sqrt{5}(6X^2 - 6X + 1). \end{aligned}$$

Corollaire 2.2.11.
Tout espace euclidien a une base orthonormale. Toute famille orthonormale peut être complétée en une base orthonormale.

Proposition 2.2.12 (Coordonnées dans une base orthonormale)**.**
E euclidien, $(v_1,\dots,v_n)$ base orthonormale de E. Alors, pour tout $x \in E$, $x = \sum_{k=1}^{n} \langle x \,|\, v_k\rangle\, v_k$.

Démonstration.
On écrit $x = \sum_{k=1}^{n} \lambda_k v_k$, puis $\langle x \,|\, v_k\rangle = \langle v_k \,|\, v_k\rangle = \lambda_k$ en développant. □

Exemple 2.2.13.
Trouver les coordonnées de $(1,-3)$ dans la base $\left(\frac{1}{\sqrt{2}}(1,1), \frac{1}{\sqrt{2}}(1,-1)\right)$ (pour le produit scalaire usuel).

Proposition 2.2.14 (Expression du produit scalaire dans une base orthonormale)**.**
Soit E euclidien, $(v_1,\dots,v_n)$ une base orthonormale de E. x et y de coordonnées (x_i) et (y_i) dans la base $(v_1,\dots,v_n)$. Alors $\langle x \,|\, y\rangle = \sum_{k=1}^{n} x_k y_k$.

Remarque 2.2.15.
Tous les produits scalaires ont la même expression «usuelle» *à condition de se placer dans une base orthonormale* ***pour ce produit scalaire.***

2.3 Sous-espaces vectoriels orthogonaux

Définition 2.3.1.
Soit F et G deux sous-espaces vectoriels de E. On dit que F et G sont des sous-espaces orthogonaux et on écrit $F \perp G$ si

$$\forall x \in F \quad \forall y \in G \qquad x \perp y.$$

Exemple 2.3.2.
Dans $\mathbb{R}^3$ avec le produit scalaire usuel, $\mathrm{Vect}(1,-1,0) \perp \mathrm{Vect}((1,1,0),(0,0,1))$.

Remarque 2.3.3.
Si F et G sont orthogonaux, alors ils sont en somme directe. En effet, soit alors $x \in F \cap G$. On a alors $x \perp x$, donc $\langle x \,|\, x\rangle = 0$, donc $x = 0$. Donc $F \cap G \subset \{\,0\,\}$, d'où on déduit le résultat.

Théorème 2.3.4.
Soient F et G deux sev de dimension finies de E. On note $(f_1,\dots,f_q)$ une famille génératrice de F et $(g_1,\dots,g_p)$ une famille génératrice de G. Alors

$F \perp G$ si et seulement si pour tout $i \in [\![1,q]\!]$ et $j \in [\![1,p]\!]$ on a $\langle f_i \,|\, g_j\rangle = 0$.

Démonstration.
($\Rightarrow$) par définition de $F \perp G$.
($\Leftarrow$) soient $f = \sum \lambda_i f_i$ et $g = \sum \mu_j g_j$. Alors $\langle f \,|\, g\rangle = \sum_i \sum_j \lambda_i \mu_j \langle f_i \,|\, g_j\rangle = 0$. □

Définition 2.3.5.
Soit X une partie (quelconque) de E. On appelle *orthogonal* de X et on noté $X^\perp$ (ou X^o) l'ensemble $\{\, y \in E \mid \forall x \in X \;\; \langle x \,|\, y\rangle = 0 \,\}$.

Proposition 2.3.6.
Soit X une partie de E. Alors

1. $X^\perp$ est un sev de E ;
2. Pour toute partie Y de E telle que $X \subset Y$, on a $Y^\perp \subset X^\perp$;
3. $X \subset \left(X^\perp\right)^\perp$.

Démonstration.
1. On a $0 \in X^\perp$ car 0 est orthogonal à tout vecteur, donc à tout vecteur de X ; de plus toute combinaison linéaire de vecteurs orthogonaux à tout vecteur de X est orthogonale à tout vecteur de X.
   Sinon, il suffit de voir que
   $$X^\perp = \bigcap_{x \in X} \mathrm{Ker}\, \langle x \,|\, \cdot \rangle\,.$$
2. Tout élément de $Y^\perp$ est orthogonal à tout vecteur de Y, donc a fortiori à tout vecteur de X.
3. Soit x un vecteur de X. Tout vecteur de $X^\perp$ est orthogonal à tout vecteur de X, donc en particulier à x. Donc x est orthogonal à tout vecteur de $X^\perp$, donc appartient à $\left(X^\perp\right)^\perp$.

□

Remarque 2.3.7.
Il n'y a pas forcément égalité dans le dernier point. Par exemple, avec $X = \varnothing$, $(X^\perp)^\perp = \{0\}$.

Théorème 2.3.8.
Soit F un sev de E. Alors $F^\perp$ est le plus grand sous-espace vectoriel orthogonal à F (et F et $F^\perp$ sont de plus en somme directe).

Si de plus E est euclidien, alors $E = F \oplus F^\perp$ et $F^\perp$ est l'unique sous-espace vectoriel G vérifiant $E = F \oplus G$ et $F \perp G$. C'est pourquoi on appelle $F^\perp$ ***le*** supplémentaire orthogonal de F dans E.

De plus, dans le cas euclidien, on a $F = (F^\perp)^\perp$.

Démonstration.
On sait déjà que $F^\perp$ est un sous-espace vectoriel. F et $F^\perp$ sont clairement orthogonaux (donc en somme directe) et de plus pour tout sous-espace vectoriel G tel que F et G sont orthogonaux, tout élément x de G est orthogonal à tout élément de F, donc appartient à $F^\perp$, donc $G \subset F^\perp$.

Supposons de plus que E est euclidien. Alors le sous-espace vectoriel F est aussi un espace vectoriel euclidien, donc possède une base orthonormale $(f_1, \dots, f_q)$. Cette base est une famille orthonormale de E, qu'on peut compléter en une base orthonormale $(f_1, \dots, f_q, g_1, \dots, g_p)$ de E. Posons $G = \text{Vect}(g_1, \dots, g_p)$. On a alors $\dim E = p+q = \dim F + \dim G$. De plus pour tout $i \in [\![1, q]\!]$ et tout $j \in [\![1, p]\!]$, on a $f_i \perp g_j$, donc $F \perp G$, donc $G \subset F^\perp$. Donc $\dim E \leqslant \dim F + \dim F^\perp$. Or F et $F^\perp$ sont en somme directe, donc $\dim(F \oplus F^\perp) \leqslant \dim E$, donc $G = F^\perp$ et $E = F \oplus F^\perp$ (et de plus, $F^\perp = \text{Vect}\,(g_1, \dots, g_p)$).

On en déduit, $\dim(F^\perp)^\perp = \dim E - \dim F^\perp = \dim F$. Or on sait qu'on a $F \subset (F^\perp)^\perp$, donc $F = (F^\perp)^\perp$. □

Remarque 2.3.9 (Important)**.**
Le résultat ne se généralise pas à des espaces préhilbertiens E qui ne sont pas de dimension finie. Dans ce cas (non-euclidien), on peut trouver des sous-espaces vectoriels F tels que F et $F^\perp$ ne soient pas supplémentaires et tels que $\left(F^\perp\right)^\perp \neq F$ (on peut même trouver F tel que $F \neq E$ et $F^\perp = \{\,0\,\}$). On verra ce résultat en exercice dans le cas de $\mathbb{R}[X]$.

Remarque 2.3.10 (Culturelle)**.**
En revanche, pour toute partie X d'un espace préhilbertien, on a toujours $\left(\left(X^\perp\right)^\perp\right)^\perp = X^\perp$ (une inclusion est la conséquence du fait que $\left(X^\perp\right)^\perp$ contient X et qu'en conséquence leurs orthogonaux sont inclus dans l'autre sens ; l'autre inclusion vient du fait que le biorthogonal de $X^\perp$ contient $X^\perp$).

Exemple 2.3.11.
On pose, pour tout couple (P, Q) d'éléments de $\mathbb{R}_2[X]$, $\langle P \,|\, Q\rangle = P'(1)Q'(1) + P(-1)Q(-1) + P(0)Q(0)$. Vérifier qu'il s'agit d'un produit scalaire et trouver $\mathbb{R}_1[X]^\perp$ dans $\mathbb{R}_2[X]$.

Exercice 2.3.12.
On considère dans $\mathbb{R}[X]$ le sev $F = \text{Vect}(1+X, 1+X^2, \dots, 1+X^n, \dots)$. On rappelle qu'un hyperplan est un sev admettant un supplémentaire de dimension 1.
On munit $\mathbb{R}[X]$ du produit scalaire

$$\left(\sum_{k=0}^{+\infty} a_k X^k, \sum_{k=0}^{+\infty} b_k X^k\right) = \sum_{k=0}^{+\infty} a_k b_k.$$

1. Montrer que F est un hyperplan de $\mathbb{R}[X]$.
2. Déterminer $F^\perp$ pour le produit scalaire usuel de $\mathbb{R}[X]$.
3. Quel résultat vrai en dimension finie est ici mis en défaut ?

DANS TOUTE LA SUITE, $(E, \langle\,|\,\rangle)$ EST UN ESPACE VECTORIEL EUCLIDIEN DE DIMENSION n.

2.4 Formes linéaires d'un espace euclidien

Théorème 2.4.1 (Théorème de représentation de Riesz-Fréchet)**.**
Soit $(E, \langle\,|\,\rangle)$ euclidien. Soit $f \in \mathscr{L}(E, \mathbb{R})$. Alors il existe un unique $v_f \in E$ vérifiant $\forall x \in E\ f(x) = \langle v_f \,|\, x\rangle$ ou encore $f = \langle v_f \,|\, .\rangle$.

Remarque 2.4.2.
Explication géométrique : f est définie par son noyau (hyperplan H) et la valeur prise sur un vecteur qui n'est pas dans le noyau.
De même, $(\text{Vect}\, v_f)^\perp$ est de dimension $n-1$, donc c'est un hyperplan. Si on choisit v_f vecteur normal à H, alors f et $\langle v_f \,|\, .\rangle$ ont le même noyau. La norme de v_f est alors choisie de sorte qu'elle corresponde avec la valeur précédente de f sur un vecteur qui n'est pas dans le noyau.

Démonstration.
On considère l'application $\varphi : \left\{ \begin{array}{ccc} E & \longrightarrow & \mathscr{L}(E, \mathbb{R}) \\ v & \longmapsto & (x \mapsto \langle v \,|\, x\rangle) \end{array} \right.$.

Alors, φ est linéaire. De plus, si $\varphi(v_1) = \varphi(v_2)$, alors pour tout $x \in E$, $\langle v_1 \,|\, x\rangle = \langle v_2 \,|\, x\rangle$, ie pour tout x, $\langle v_1 - v_2 \,|\, x\rangle = 0$, donc $v_1 - v_2 \in E^\perp$ Or $E^\perp = \{\, 0 \,\}$ car pour tout $x \in E^\perp$, $\langle x \,|\, x\rangle = 0$. Donc $v_1 = v_2$ et φ est injective. Mais comme $\dim E = \dim \mathscr{L}(E, \mathbb{R})$, alors φ est un isomorphisme. D'où le résultat. □

Exemple 2.4.3.
Soit $f \in \mathscr{L}(\mathbb{R}^n, \mathbb{R})$. f est de la forme $f(x_1, \ldots, x_n) = a_1x_1 + \ldots + a_nx_n$, ie $\langle (a_1, \ldots, a_n) \,|\, (x_1, \ldots, x_n)\rangle$.

2.5 Écriture matricielle du produit scalaire

Soit $e = (e_1, \ldots, e_n)$ base orthonormale de E, x et y des vecteurs de matrices (dans e) X et Y. Alors $\langle x \,|\, y\rangle = {}^tX.Y$.
Dans le cadre d'application du théorème de Riesz-Fréchet, on a $f(x) = {}^tV_f.X$, et ainsi $\mathrm{Mat}_e(f) = {}^t\mathrm{Mat}_e(v_f)$. Les points de vue se rejoignent.

2.6 Symétries et projecteurs orthogonaux

Définition 2.6.1.
On appelle *projection orthogonale* (resp. *symétrie orthogonale*) toute projection (resp. symétrie) sur un (resp. par rapport à un) sev F parallèlement à $F^\perp$.

Proposition 2.6.2.
Un projecteur p est orthogonal si et seulement si $\mathrm{Im}\, p \perp \mathrm{Ker}\, p$. Une symétrie s est orthogonale si et seulement si $\mathrm{Ker}(s - \mathrm{Id}) \perp \mathrm{Ker}(s + \mathrm{Id})$.

Démonstration.
Direct. □

Théorème 2.6.3 (expression d'un projecteur orthogonal dans une base orthonormée)**.**
Soit F sev d'un ev euclidien E. Soit $(f_1, \ldots, f_p)$ une base orthonormale de F. Soit $x \in E$. Le projeté orthogonal de x sur F est $p(x) = \sum_{i=1}^{p} \langle x \,|\, f_i\rangle\, f_i$.

Démonstration.
On complète $(f_1, \ldots, f_p)$ en une base orthonormale de E notée $(f_1, \ldots, f_n)$. Alors $(f_{p+1}, \ldots, f_n)$ est une base de $F^\perp$ ($\perp$ + dimension). Donc $x = \sum_{i=1}^{n} \langle x \,|\, f_i\rangle\, f_i$, donc somme d'un élément de F et d'un élément de $F^\perp$: cet élément de F est le projeté de x sur F. □

Exemple 2.6.4.
Déterminer la projection orthogonale (et la symétrie orthogonale) de $(2, 1-1)$ sur $\mathrm{Vect}(-1, 2, 4)$, ainsi que sur son supplémentaire orthogonal, pour le produit scalaire $((x_1, y_1)|(x_2, y_2)) = 3x_1x_2 + 2y_1x_2 + 2x_1y_2 + y_1y_2$.

Remarque 2.6.5.
On peut ré-écrire le procédé d'orthonormalisation de Gram-Schmidt comme suit.

Avec $F_k = \mathrm{Vect}(e_1, \ldots, e_k)$, en notant p_k le projeté de e_{k+1} sur F_k, on procède comme suit.

- On renormalise e_1 pour obtenir v_1.
- Pour chaque $1 \leqslant k \leqslant p-1$, on remarque que $e_{k+1} - p_k \in F_k^\perp$. On renormalise donc $e_k - p_k$ pour obtenir v_{k+1}.

2.7 Distance à un sous ev

Définition 2.7.1 (distance d'un point à une partie d'un espace euclidien)**.**
Soit A une partie de E et $x \in E$. On appelle distance de x à A et on note $\mathrm{d}(x, A)$ le réel $\inf_{a \in A} \mathrm{d}(x, a)$.

Théorème 2.7.2.
Soit F un sev de E. Alors la distance de x à F est atteinte en un seul point, qui est la projection orthogonale de x. De plus : $\mathrm{d}(x, F)^2 = \|x\|^2 - \|p(x)\|^2$. En particulier $\mathrm{d}(x, F) = 0$ si et seulement si $x \in F$.

Démonstration.
Soit $f \in F$. $x - f = x - p(x) + p(x) - f$, décomposition dans $F^\perp \oplus F$. On applique Pythagore. □

Exemple 2.7.3.
Le minimum de la fonction

$$f : \left\{ \begin{array}{ccc} \mathbb{R}^3 & \to & \mathbb{R} \\ (a,b) & \mapsto & \displaystyle\int_0^1 (-a - bx + x^2)^2 \,\mathrm{d}x \end{array} \right.$$

est atteint pour $a = -1/6$ et $b = 1$ et vaut $1/180$.

2.8 Hyperplans affines d'un espace euclidien

Définition 2.8.1.
On appelle hyperplan affine d'un espace vectoriel (non nécessairement euclidien) tout sous-espace affine de la forme $a + H$ où a est un élément de l'espace vectoriel et H est un hyperplan de cet espace.

Définition 2.8.2.
Soit $\mathscr{H}$ un hyperplan affine d'un espace euclidien E. Notons H la direction de $\mathscr{H}$. On appelle vecteur normal à $\mathscr{H}$ tout vecteur normal à H. L'ensemble des vecteurs normaux à $\mathscr{H}$ est une droite vectorielle.

Démonstration.
L'espace étant euclidien, $H^\perp$ est le supplémentaire orthogonal de H. H étant un hyperplan, $H^\perp$ est une droite vectorielle. □

Remarque 2.8.3.
Étant donné un vecteur non-nul $\overrightarrow{n}$ de E, il existe un unique hyperplan vectoriel admettant $\overrightarrow{n}$ pour vecteur normal : $\{ \overrightarrow{n} \}^\perp$ (En effet, d'une part $\{ \overrightarrow{n} \}^\perp = (\mathrm{Vect}(\overrightarrow{n}))^\perp$) est un hyperplan et $\overrightarrow{n}$ est normal à cet hyperplan, d'autre part tout hyperplan normal à $\overrightarrow{n}$ est nécessairement inclus dans $\{ \overrightarrow{n} \}^\perp$ dont égal par égalité des dimensions.)

Étant donné de plus un point A de E, il existe un unique hyperplan affine admettant $\overrightarrow{n}$ pour vecteur normal et passant par A : $A + \{ \overrightarrow{n} \}^\perp$. (En effet, s'il existe sa direction est nécessairement $\{ \overrightarrow{n} \}^\perp$ donc il ne peut s'agit que de $A + \{ \overrightarrow{n} \}^\perp$ et il est clair que ce sous-espace affine répond à la question.)

Définition 2.8.4.
Soit $f : E \to \mathbb{R}$. Les sous-ensembles de E de la forme

$$\{ x \in E \mid f(x) = k \},$$

pour $k \in \mathbb{R}$, sont appelés les lignes de niveau de l'application f.

Proposition 2.8.5.
Soit A un point de E.

Un sous ensemble de E est un hyperplan affine si et seulement si c'est une ligne de niveau d'une application de la forme

$$\begin{array}{ccc} E & \to & \mathbb{R} \\ M & \mapsto & \langle \overrightarrow{n} | \overrightarrow{AM} \rangle \end{array}$$

où $\overrightarrow{n}$ est un vecteur non nul.

Dans ce cas, $\overrightarrow{n}$ est un vecteur normal à l'hyperplan.

Démonstration.
Soit $\mathscr{H}$ un hyperplan affine de E. $\mathscr{H}$ s'écrit $B + H$ où $B \in \mathscr{H}$ et H est un hyperplan vectoriel. H est donc le noyau d'une forme linéaire non-nulle φ. Or E est un espace euclidien, donc d'après le théorème de Riesz, φ s'écrit sous la forme $x \mapsto \langle x | \overrightarrow{n} \rangle$ pour un certain $\overrightarrow{n} \in E$, avec $\overrightarrow{n}$ non-nul (sinon φ serait nulle). Donc on a pour tout $M \in E$:

$$\begin{aligned} M \in \mathscr{H} &\iff M - B \in H \\ &\iff \overrightarrow{BM} \in H \\ &\iff \varphi(\overrightarrow{BM}) = 0 \\ &\iff \varphi(\overrightarrow{AB}) + \varphi(\overrightarrow{BM}) = \varphi(\overrightarrow{AB}) \\ &\iff \varphi(\overrightarrow{AM}) = \varphi(\overrightarrow{AB}) \\ &\iff \langle \overrightarrow{n} | \overrightarrow{AM} \rangle = \varphi(\overrightarrow{AB}). \end{aligned}$$

Donc $\mathscr{H} = \left\{ M \in E \;\middle|\; \langle \overrightarrow{n} | \overrightarrow{AM} \rangle = \varphi(\overrightarrow{AB}) \right\}$. L'hyperplan affine $\mathscr{H}$ est donc bien une ligne de niveau de l'application

$$\begin{array}{ccc} E & \to & \mathbb{R} \\ M & \mapsto & \langle \overrightarrow{n} | \overrightarrow{AM} \rangle \end{array}$$

où $\overrightarrow{n}$ est un vecteur non nul.

Réciproquement, soit k un réel et $\overrightarrow{n}$ un vecteur non-nul. Notons $\mathscr{H} = \left\{ M \in E \;\middle|\; \langle \overrightarrow{n} | \overrightarrow{AM} \rangle = k \right\}$. Montrons que $\mathscr{H}$ est un hyperplan affine.

Notons $\varphi : x \mapsto \langle x | \overrightarrow{n} \rangle$. Alors φ est une forme linéaire non-nulle de noyau un hyperplan vectoriel H. De plus, $\operatorname{Im}\varphi$ n'est pas réduite à $\{0\}$, donc est de dimension au moins 1 donc est égale à $\mathbb{R}$. Donc φ est surjective. Soit x un antécédent de k par φ. Posons $B = A + x$. Alors $\varphi(\overrightarrow{AB}) = \varphi(x) = k$, donc $B \in \mathscr{H}$.

Soit alors $M \in E$. On a :

$$\begin{aligned} M \in \mathscr{H} &\iff \langle \overrightarrow{n} | \overrightarrow{AM} \rangle = k \\ &\iff \varphi(\overrightarrow{AM}) - \varphi(\overrightarrow{AB}) = 0 \\ &\iff \varphi(\overrightarrow{AM} - \overrightarrow{AB}) = 0 \\ &\iff \varphi(\overrightarrow{BM}) = 0 \\ &\iff \overrightarrow{BM} \in H \\ &\iff M \in B + H. \end{aligned}$$

Donc $\mathscr{H} = B + H$.

De plus pour tout $x \in H$, $\langle x | \overrightarrow{n} \rangle = \varphi(x) = 0$ donc $\overrightarrow{n}$ est normal à H, donc à $\mathscr{H}$. □

Corollaire 2.8.6.
Choisissons une base orthonormale de E.

Soit alors $\mathscr{H}$ un hyperplan affine. Alors pour tout vecteur $\overrightarrow{n}$ normal à $\mathscr{H}$, de coordonnées $(a_1, \ldots, a_n)$, $\mathscr{H}$ admet une équation de la forme

$$a_1 x_1 + \ldots + a_n x_n = k$$

où $(x_1, \ldots, x_n)$ sont les coordonnées du point considéré dans la base et k un réel fixé.

Réciproquement, pour tout n-uplet $(a_1, \ldots, a_n)$ de réels non tous nuls et tout réel k l'équation

$$a_1 x_1 + \ldots + a_n x_n = k$$

est celle d'un hyperplan affine admettant pour vecteur normal le vecteur de coordonnées $(a_1, \ldots, a_n)$.

Démonstration.
C'est une simple traduction de la proposition, en prenant pour A le vecteur nul. □

Remarque 2.8.7.
Regarder ce que cela donne pour $n = 2$ et $n = 3$.

Proposition 2.8.8.
Soit $\mathscr{H}$ un hyperplan affine, A un point de $\mathscr{H}$ et $\overrightarrow{n}$ un vecteur normal à $\mathscr{H}$ **unitaire**.

Alors, pour tout point M, on a

$$\mathrm{d}(M, \mathscr{H}) = \left| \langle \overrightarrow{AM} | \overrightarrow{n} \rangle \right|.$$

Démonstration.
Notons p la projection orthogonale sur H. Alors la distance de M à $\mathscr{H}$ n'est autre que la distance de $\overrightarrow{AM}$ à H. En effet :

$$\begin{aligned} \mathrm{d}(M, \mathscr{H}) &= \inf_{B \in \mathscr{H}} \mathrm{d}(M, B) \\ &= \inf_{B \in \mathscr{H}} \left\| \overrightarrow{BM} \right\| \\ &= \inf_{B \in \mathscr{H}} \|M - B\| \\ &= \inf_{x \in H} \|M - (A + x)\| \\ &= \inf_{x \in H} \left\| \overrightarrow{AM} - x \right\| \\ &= \mathrm{d}(\overrightarrow{AM}, H). \end{aligned}$$

On en déduit que $\mathrm{d}(M, \mathscr{H})$ vaut $\left\| \overrightarrow{AM} - p(\overrightarrow{AM}) \right\|$. Or $\overrightarrow{AM} - p(\overrightarrow{AM})$ est orthogonal à H et $H^\perp$ n'est autre que $\operatorname{Vect} \overrightarrow{n}$. Donc $\overrightarrow{AM} - p(\overrightarrow{AM})$ s'écrit sous la forme $\lambda \overrightarrow{n}$. On a alors :

$$\begin{aligned} \mathrm{d}(M, \mathscr{H}) &= \|\lambda \overrightarrow{n}\| \\ &= |\lambda| \, \|\overrightarrow{n}\| \\ &= |\lambda|, \end{aligned}$$

car $\overrightarrow{n}$ est unitaire.

De plus,

$$\begin{aligned} \langle \overrightarrow{AM} | \overrightarrow{n} \rangle &= \langle \overrightarrow{AM} - p(\overrightarrow{AM}) | \overrightarrow{n} \rangle + \langle p(\overrightarrow{AM}) | \overrightarrow{n} \rangle \\ &= \lambda \langle \overrightarrow{n} | \overrightarrow{n} \rangle + 0, \end{aligned}$$

d'où

$$\mathrm{d}(M, \mathscr{H}) = \left| \langle \overrightarrow{AM} | \overrightarrow{n} \rangle \right|.$$

□

Corollaire 2.8.9.
Donnons-nous une base orthonormale de E.

Soit $\mathscr{H}$ un hyperplan affine d'équation

$$a_1 x_1 + \ldots + a_n x_n = k$$

dans cette base, où $a_1, \ldots, a_n$ sont des scalaires non tous nuls et k un scalaire.

Alors pour tout point M de E, de coordonnées $(x_1, \ldots, x_n)$, on a

$$\mathrm{d}(M, \mathscr{H}) = \frac{|a_1x_1 + \ldots + a_nx_n - k|}{\sqrt{a_1^2 + \ldots + a_n^2}}.$$

Démonstration.
Notons $\overrightarrow{u}$ le vecteur de coordonnées a_1, …, a_n et $A(y_1, \ldots, y_n)$ un point de $\mathscr{H}$. On sait que $\overrightarrow{u}$ est un vecteur non-nul normal à $\mathscr{H}$. Posons alors $\overrightarrow{n} = \frac{1}{\|\overrightarrow{u}\|}\overrightarrow{u}$.

Soit M un point de E, de coordonnées $(x_1, \ldots, x_n)$, D'après la proposition, on a

$$\begin{aligned}\mathrm{d}(M, \mathscr{H}) &= \left|\langle\overrightarrow{AM}|\overrightarrow{n}\rangle\right| \\ &= \frac{1}{\|\overrightarrow{u}\|}\left|\langle\overrightarrow{AM}|\overrightarrow{u}\rangle\right| \\ &= \frac{1}{\|\overrightarrow{u}\|}\left|\langle\overrightarrow{OM}|\overrightarrow{u}\rangle - \langle\overrightarrow{OA}|\overrightarrow{u}\rangle\right|.\end{aligned}$$

Or $\langle\overrightarrow{OA}|\overrightarrow{u}\rangle = k$ car $A \in \mathscr{H}$, donc

$$\mathrm{d}(M, \mathscr{H}) = \frac{|a_1x_1 + \ldots + a_nx_n - k|}{\sqrt{a_1^2 + \ldots + a_n^2}}.$$

□

Remarque 2.8.10.
Voir ce que cela donne en dimension 2 et en dimension 3.

Définition 2.8.11.
Soit H un hyperplan de E. Tout choix d'une orientation de E et d'un vecteur u normal à H et non-nul induit une orientation sur H de la façon suivante :

On dira qu'une base $(e_1, \ldots, e_{n-1})$ de H est directe (resp. indirecte) si et seulement si $(e_1, \ldots, e_{n-1}, u)$ l'est aussi.

Remarque 2.8.12.
Regarder ce que cela donne en dimension 3.

Cette définition paraît simple mais il y a tout de même deux points à justifier. Tout d'abord le fait que pour toute base $(e_1, \ldots, e_{n-1})$ de H, $(e_1, \ldots, e_{n-1}, u)$ est une base de H. Cela résulte du fait que H et $\mathrm{Vect}(u)$ sont supplémentaires.

Ensuite, il convient de remarquer que définir une orientation pour l'espace vectoriel H, n'est pas juste partionner en deux l'ensemble des bases mais de le partitionner de façon que toutes les bases appelées directes (resp. indirectes) soient de même orientation.

Soit donc $\mathscr{B}_H = (e_1, \ldots, e_{n-1})$ et $\mathscr{B}'_H = (e'_1, \ldots, e'_{n-1})$ deux bases de H. Montrons qu'elles ont la même orientation si et seulement si $\mathscr{B}_E = (e_1, \ldots, e_{n-1}, u)$ et $\mathscr{B}'_E = (e'_1, \ldots, e'_{n-1}, u)$ ont la même orientation.

Notons M la matrice de passage de $\mathscr{B}_H$ à $\mathscr{B}'_H$. Elle est de déterminant positif si et seulement si les deux sont de même orientation.

La matrice M' de passage de $\mathscr{B}_E$ à $\mathscr{B}'_E$ s'écrit alors par blocs :

$$M' = \begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix}$$

Donc, en développant par rapport à la dernière ligne ou à la dernière colonne : $\det M' = \det M$. On en déduit que $\mathscr{B}_H$ et $\mathscr{B}'_H$ ont la même orientation si et seulement si $\mathscr{B}_E$ et $\mathscr{B}'_E$ aussi.

3 Automorphismes orthogonaux

Soit E un espace vectoriel euclidien ***orienté***, de dimension n. Soit $f \in \mathscr{L}(E)$.

3.1 Définitions générales

Définition 3.1.1.
On appelle *endomorphisme orthogonal* toute application $f \in \mathscr{L}(E)$ telle que pour tous $x, y \in E$, $\langle f(x) \,|\, f(y)\rangle = \langle x \,|\, y\rangle$. On dit qu'un tel endomorphisme *préserve le produit scalaire*.

On a le théorème fondamental suivant :

Théorème 3.1.2. (i) Un endomorphisme f est orthogonal si et seulement s'il préserve les normes, *i.e.* pour tout $x \in E$, $\|f(x)\| = \|x\|$. Un endomorphisme orthogonal est donc une isométrie.

(ii) Toute isométrie vectorielle est une bijection. Un endomorphisme orthogonal est donc un automorphisme.

Démonstration. (i) ($\Rightarrow$) : évident puisque $\|f(x)\|^2 = \langle f(x) \,|\, f(x)\rangle = \langle x \,|\, x\rangle = \|x\|^2$.
($\Leftarrow$) : on utilise l'identité de polarisation : $\langle f(x) \,|\, f(y)\rangle = \frac{1}{2}(\|f(x)+f(y)\|^2 - \|f(x)\|^2 - \|f(y)\|^2)$
$= \frac{1}{2}(\|f(x+y)\|^2 - \|f(x)\|^2 - \|f(y)\|^2) = \frac{1}{2}(\|x+y\|^2 - \|x\|^2 - \|y\|^2) = \langle x \,|\, y\rangle$.

(ii) Déjà fait en début d'année : si on a $x, y \in E$, $\|f(x) - f(y)\| = \|f(x-y)\| = \|x-y\|$.

□

Exercice 3.1.3.
Dans la démonstration précédente, utilise t-on la linéarité de f ? Et si c'est le cas, où ?

Proposition 3.1.4.
Tout endomorphisme orthogonal change une base orthonormale en une base orthonormale.

Démonstration.
Soit $(e_1, \dots, e_n)$ une b.o.n. Ceci est équivalent à : $\forall i, j$, $\langle e_i \,|\, e_j\rangle = \delta_{ij}$, où δ désigne le symbole de Kronecker.
Donc $\forall i, j$, $\langle f(e_i) \,|\, f(e_j)\rangle = \langle e_i \,|\, e_j\rangle = \delta_{ij}$, et donc $(f(e_1), \dots, f(e_n))$ est également une b.o.n. □

Proposition 3.1.5.
Toute application (sans la supposer linéaire) de E dans E qui préserve le produit scalaire est nécessairement linéaire.

Démonstration.
Soit $(e_1, \dots, e_n)$ une base orthonormale de E. Pour montrer que f est linéaire, il suffit de montrer que pour tout $\lambda_1, \dots, \lambda_n \in \mathbb{R}$, $f(\sum_{k=1}^{n} \lambda_k e_k) = \sum_{k=1}^{n} \lambda_k f(e_k)$. On pose $x = \sum_{k=1}^{n} \lambda_k e_k$. Mais on a déjà vu que les coordonnées de x dans la base $(e_1, \dots, e_n)$ sont $\langle x \,|\, e_1\rangle, \dots, \langle x \,|\, e_n\rangle$ donc pour tout k, $\lambda_k = \langle x \,|\, e_k\rangle$.
Mais $(f(e_1), \dots, f(e_n))$ est aussi une base orthonormale de E car f est orthogonale. On a alors

$$\begin{aligned} f(x) &= \sum_{k=1}^{n} \langle f(x) \,|\, f(e_k)\rangle \, f(e_k) \\ &\qquad \text{car } (f(e_1), \dots, f(e_n)) \text{ est une base orthonormale} \\ &= \sum_{k=1}^{n} \langle x \,|\, e_k\rangle \, f(e_k) \\ &\qquad \text{car } f \text{ préserve le produit scalaire} \\ &= \sum_{k=1}^{n} \lambda_k f(e_k) \end{aligned}$$

et donc la linéarité de f est bien prouvée. □

Remarque 3.1.6.
Il y a en revanche des applications non linéaires qui préservent la norme sans préserver le produit scalaire. Par exemple, sur $\mathbb{R}$ muni du produit scalaire $(x, y) \mapsto xy$, la norme associée au produit scalaire est la valeur absolue et l'application qui à tout rationnel associe lui-même et à tout irrationnel associe son opposé préserve la norme. En revanche, elle ne préserve pas le produit scalaire (regarder par exemple l'effet sur 1 et $\sqrt{2}$, ou raisonner par l'absurde en utilisant la remarque précédente).

Exemple 3.1.7.
On considère le plan complexe (vu comme $\mathbb{R}$-ev), muni de sa structure euclidienne usuelle : $\langle z_1, z_2\rangle = \mathrm{Re}(z_1 \bar{z_2})$. La base canonique de $\mathbb{C}$, $(1, i)$, est orthonormée.

Les similitudes complexes de rapport 1 sont des isométries. Nous l'avons montré en début d'année ! Ce sont donc des endomorphismes orthogonaux de $\mathbb{C}$.

Rappelons que ce sont les applications de la forme $\rho_\theta : z \mapsto e^{i\theta} z$ et $s_\theta : z \mapsto e^{i\theta} \bar{z}$, avec $\theta \in \mathbb{R}$.

Remarquons que ρ_θ est la rotation d'angle θ, que s_0 est la symétrie orthogonale d'axe $\mathbb{R}$ et s_π est la symétrie orthogonale d'axe $i\mathbb{R}$.

Remarquons aussi que l'image de $(1, i)$ par ρ_θ est la base notée (u_θ, v_θ), qui est orthonormée directe.

Exemple 3.1.8.
Une symétrie orthogonale est un endomorphisme orthogonal. Ce n'est pas le cas des projecteurs orthogonaux.

Voyons maintenant les propriétés des endomorphismes orthogonaux.

Définition 3.1.9.
On note $\mathscr{O}(E)$, appelé *groupe orthogonal*, l'ensemble des endomorphismes orthogonaux.

Proposition 3.1.10. (i) $\mathscr{O}(E)$ est un sous-groupe de $\mathscr{GL}(E)$.

(ii) Un endomorphisme est orthogonal si et seulement s'il change une base orthonormale en une base orthonormale (auquel cas, il change toute base orthonormale en une base orthonormale).

(iii) Soient $\mathscr{B}$ une base orthonormale de E, $f \in \mathscr{L}(E)$ et $M = \mathrm{Mat}_{\mathscr{B}}(f)$. Alors $f \in \mathscr{O}(E)$ si et seulement si $M\,{}^tM = {}^tMM = I_n$.

(iv) Si $f \in \mathscr{O}(E)$, alors $\det f = \pm 1$.

(v) Si F est un sev de E stable par f, $F^\perp$ est aussi stable par f.

Démonstration. (i) On a déjà vu que tout endomorphisme orthogonal est une bijection, donc $\mathscr{O}(E)$ est une partie de $\mathscr{GL}(E)$. De plus $\mathrm{Id}_E \in \mathscr{O}(E)$, donc cette partie est non vide.

En outre, si $f, g \in \mathscr{O}(E)$ on a pour tout $(x, y) \in E^2$: $\langle (f\circ g)(x) \,|\, (f\circ g)(y)\rangle = \langle g(x) \,|\, g(y)\rangle$ car f est orthogonale, et puisque g l'est aussi on a $\langle g(x) \,|\, g(y)\rangle = \langle x \,|\, y\rangle$. Par conséquent, $f \circ g \in \mathscr{O}(E)$. Donc $\mathscr{O}(E)$ est stable par composition.

Enfin, soit $f \in \mathscr{O}(E)$. On a f bijective et pour tout $(x, y) \in E^2$, on a : $\langle x \,|\, y\rangle = \left\langle f(f^{-1}(x)) \,\middle|\, f(f^{-1}(y))\right\rangle = \left\langle f^{-1}(x) \,\middle|\, f^{-1}(y)\right\rangle$. Donc f^{-1} préserve le produit scalaire. $\mathscr{O}(E)$ est donc stable par passage à l'inverse.

(ii) On a déjà démontré le sens direct de cette proposition. Démontrons l'autre sens :

Soit f un endomorphisme changeant une b.o.n. en une b.o.n. Soit $(e_1, \dots, e_n)$ une b.o.n. Pour montrer que f est orthogonal, on va montrer que f préserve la norme. Soit $x = \sum_{k=1}^{n} x_k e_k$. Puisque $(e_1, \dots, e_n)$ est une b.o.n, alors $\|x\|^2 = \sum_{k=1}^{n} x_k^2$. Mais $f(x) = \sum_{k=1}^{n} x_k f(e_k)$ et $(f(e_1), \dots, f(e_n))$ est une b.o.n, donc $\|f(x)\|^2 = \sum_{k=1}^{n} x_k^2 = \|x\|^2$.

(iii) Notons $(e_1, \dots, e_n)$ les vecteurs de $\mathscr{B}$ et $C_1, \dots, C_n$ les vecteurs colonnes de M. On a donc, pour tout j : $C_i = (m_{ij})_{i\in[\![1,n]\!]}$. Le coefficient $a_{i,j}$ de la matrice ${}^tMM$ a pour expression $\sum_{k=1}^{n} m_{ki}m_{kj}$, et on remarque qu'il s'agit exactement du produit scalaire $\langle f(e_1) \,|\, f(e_j)\rangle$.

Notons $\mathscr{B}'$ la famille $(f(e_1), \dots, f(e_n))$. ${}^tMM = I_n$ si et seulement si pour tout (i, j), $a_{i,j} = \delta_{i,j}$, c'est-à-dire si et seulement si pour tout (i, j), $\langle f(e_i) \,|\, f(e_j)\rangle = \delta_{i,j}$, c'est-à-dire si et seulement si $\mathscr{B}'$ est une base orthonormale.

Or $\mathscr{B}'$ est l'image d'une base orthonormale par l'endomorphisme f. Donc d'après le point ii il s'agit d'une base orthonormale si et seulement si f est orthogonal. On en déduit $f \in \mathscr{O}(E) \iff {}^tMM = I_n$.

(iv) Soient $\mathscr{B}$ une base orthonormale de E, on note $M = \mathrm{Mat}_{\mathscr{B}}(f)$. Alors $\det f = \det M$. Or $\det M = \det {}^tM$, et donc $1 = \det I_n = \det({}^tMM) = \det {}^tM . \det M = (\det M)^2 = (\det f)^2$. Donc $\det f = \pm 1$.

(v) On suppose F stable par f. Montrons d'abord que $f(F) = F$, et non pas seulement $f(F) \subset F$. Puisque $f(F) \subset F$, alors $f|_F$ est un endomorphisme de F. Mais puisque f est injective, $f|_F$ l'est aussi est ainsi $f|_F$ est une bijection de F dans lui-même, d'où le résultat.

Soit $x \in F^\perp$. Il s'agit de montrer que $f(x) \in F^\perp$, *i.e.* pour tout $y \in F$, $\langle f(x) \,|\, y\rangle = 0$. Fixons $y \in F$. Puisque $f(F) = F$, alors il existe $z \in F$ tel que $y = f(z)$. Ainsi $\langle f(x) \,|\, y\rangle = (\langle f(x) \,|\, f(z)\rangle = \langle x \,|\, z\rangle$ car f est orthogonal. Mais $x \in F^\perp$ et $z \in F$, donc $\langle x \,|\, z\rangle = 0$ et ainsi $\langle f(x) \,|\, y\rangle = 0$. Par conséquent $f(x) \in F^\perp$.

□

Définition 3.1.11.
L'ensemble des endomorphismes orthogonaux de déterminant 1 est noté $\mathscr{SO}(E)$ ou $\mathscr{O}^+(E)$, et appelé le *groupe spécial orthogonal*. Les éléments de $\mathscr{SO}(E)$ sont dits *positifs*, on dit aussi que ce sont des *rotations*.

L'ensemble des endomorphismes orthogonaux de déterminant -1, soit $\mathscr{O}(E)\backslash\mathscr{SO}(E)$, est noté $\mathscr{O}^-(E)$. Les éléments de $\mathscr{O}^-(E)$ sont dits *négatifs*,.

Proposition 3.1.12. (i) $\mathscr{SO}(E)$ est un sous-groupe de $\mathscr{O}(E)$.

(ii) Soit $f \in \mathscr{O}(E)$, f est positif si et seulement s'il change une base orthonormale directe en une base orthonormale directe.

Démonstration. (i) L'application det est un morphisme de $\mathscr{O}(E)$ dans $(\{-1,1\},\times)$ puisque pour tous endomorphismes f et g, $\det(f\circ g)=\det f.\det g$. Or $\mathscr{SO}(E)$ est son noyau, donc il s'agit d'un sous-groupe de $\mathscr{O}(E)$.

(ii) Soit $\mathscr{B}$ une b.o.n.d. f étant orthogonal, $f(\mathscr{B})$ est une base orthonormale. Or $\det_{\mathscr{B}}(\mathscr{B})=1$ et $\det f=\pm1$ et $\det_{\mathscr{B}}(f(\mathscr{B}))=\det f.\det_{\mathscr{B}}\mathscr{B}$, donc $f(\mathscr{B})$ est directe si et seulement si $\det f=1$, c'est-à-dire si et seulement si $f\in\mathscr{SO}(E)$.

□

3.2 Matrices orthogonales

Définition 3.2.1.
Soit $M\in\mathscr{M}_n(\mathbb{R})$. On dit que M est **orthogonale** si ${}^tM.M=M.{}^tM=I_n$, *i.e.* M est inversible d'inverse ${}^tM$.

Remarque 3.2.2.
Il suffit de montrer que ${}^tM.M=I_n$ ou $M.{}^tM=I_n$.

Exercice 3.2.3.
$M=\frac{1}{\sqrt{6}}\begin{pmatrix}\sqrt{2}&0&2\\ \sqrt{2}&\sqrt{3}&-1\\ -\sqrt{2}&\sqrt{3}&1\end{pmatrix}$ est-elle orthogonale ?

Théorème 3.2.4.
Soit $\mathscr{B}$ une base orthonormale de E et $f\in\mathscr{L}(E)$. Alors f est orthogonal si et seulement si $\mathrm{Mat}_{\mathscr{B}}(f)$ est orthogonale.

Démonstration.
Déjà vu en iii □

Définition 3.2.5.
L'ensemble des matrices orthogonales d'ordre n est appelé appelé *groupe orthogonal de degré n* et noté $\mathscr{O}(n)$ ou $O_n(\mathbb{R})$.

L'ensemble des matrices orthogonales de déterminant 1 est appelé le *groupe spécial orthogonal de degré n* et est noté $\mathscr{SO}(n)$, $SO_n(\mathbb{R})$ ou $\mathscr{O}^+(n)$. Les matrices de $\mathscr{SO}(n)$ sont dites *positives*.

L'ensemble $\mathscr{O}(n)\backslash\mathscr{SO}(n)$ est noté $\mathscr{O}^-(n)$ ou $O_n^-(\mathbb{R})$, ses matrices sont dites *négatives*.

Proposition 3.2.6.
Soit M une matrice orthogonale.

(i) ${}^tM$ est orthogonale.

(ii) $O_n(\mathbb{R})$ est un sous-groupe de $(\mathscr{GL}_n(\mathbb{R}),\times)$.

(iii) La famille des colonnes de M forme une base orthonormale de $\mathbb{R}^n$.

(iv) La famille des lignes de M forme une base orthonormale de $\mathbb{R}^n$.

(v) $\det M=\pm1$.

(vi) $SO_n(\mathbb{R})$ est un sous-groupe de $O_n(\mathbb{R})$.

(vii) Si $f\in\mathscr{L}(E)$ et $\mathscr{B}$ est une base orthonormale de E, $f\in\mathscr{SO}(E)$ si et seulement si $\mathrm{Mat}_{\mathscr{B}}(f)\in\mathscr{SO}(n)$.

Démonstration.
On ne fait que redire ce qui a été vu avant. □

Théorème 3.2.7.
Le déterminant d'une famille de vecteurs ne dépend pas de la b.o.n. directe choisie, c'est-à-dire : soient $\mathscr{C}$ et $\mathscr{B}$ deux bases orthonormales directes de E, et $\mathscr{F}$ une famille de n vecteurs de E. Alors $\det_{\mathscr{C}}(\mathscr{F})=\det_{\mathscr{B}}(\mathscr{F})$.

Démonstration.
On a $\det_{\mathscr{C}}(\mathscr{F})=\det\mathscr{M}_{\mathscr{C}}(\mathscr{F})$, et $\det_{\mathscr{B}}(\mathscr{F})=\det\mathscr{M}_{\mathscr{B}}(\mathscr{F})$. Si on note $P=\mathscr{M}_{\mathscr{C}}(\mathscr{B})$, alors P est la matrice de l'endomorphisme transformant $\mathscr{B}$ en $\mathscr{C}$, qui est orthogonal direct

puisque $\mathscr{B}$ et $\mathscr{C}$ sont des b.o.n.d., donc $P \in \mathscr{SO}(n)$, donc $\det P = 1$. Or P est également la matrice de passage de $\mathscr{C}$ dans $\mathscr{B}$, donc $\mathscr{M}_{\mathscr{C}}(\mathscr{F}) = P\mathscr{M}_{\mathscr{B}}(\mathscr{F})$. Or $\det P = 1$, on a donc le résultat voulu. □

Remarque 3.2.8.
De la même manière on montrerait que si $\mathscr{B}$ est une b.o.n.d. et $\mathscr{C}$ est une b.o.n. indirecte, alors $\det_{\mathscr{C}}(\mathscr{F}) = -\det_{\mathscr{B}}(\mathscr{F})$.

3.3 Produit mixte

Soit $(E, \langle\,|\,\rangle)$ un espace vectoriel euclidien orienté de dimension n.

Définition 3.3.1.
Soit $x_1, \ldots, x_n$ n vecteurs de E. On appelle *produit mixte* de ces vecteurs et on note $[x_1, \ldots, x_n]$ le déterminant de cette famille de vecteurs pris dans une base orthonormale directe $\mathscr{B}$:

$$[x_1, \ldots, x_n] = \det_{\mathscr{B}}(x_1, \ldots, x_n).$$

Remarque 3.3.2.
Pour justifier cette définition, il est essentiel de remarquer :

1. d'une part qu'il existe au moins toujours une base orthonormale directe (il suffit de prendre n'importe quelle base othonormale et, si elle n'est pas directe, de changer l'un de ses vecteurs en son opposé) ;
2. d'autre part que la valeur de $\det_{\mathscr{B}}(x_1, \ldots, x_n)$ est la même dans toutes les bases orthonormales directes.

Remarque 3.3.3. 1. Le produit mixte de x_1, $\ldots$, x_n s'interprète géométriquement comme le volume orienté d'un parallélépipède donc un sommet est l'origine et dont les arêtes partant de l'origine sont $[OM_1]$, $\ldots$, $[OM_n]$, où $\overrightarrow{OM_i} = x_i$ pour $i = 1, \ldots, n$.

2. (hors-programme) Étant donné $n-1$ vecteurs $x_1, \ldots, x_{n-1}$, l'application $\varphi : y \mapsto [x_1, \ldots, x_n, y]$ est une forme linéaire. D'après le théorème de Riesz, il existe un unique vecteur x tel que pour tout y, $\varphi(y) = \langle x\,|\,y\rangle$. Ce vecteur est appelé produit vectoriel de $x_1, \ldots, x_{n-1}$ et est noté $x_1 \wedge x_2 \wedge \ldots \wedge x_{n-1}$. On a donc, par définition du produit vectoriel, pour tout y : $[x_1, \ldots, x_{n-1}, y] = < x_1 \wedge x_2 \wedge \ldots \wedge x_{n-1} | y >$. On peut remarquer que $x_1 \wedge \ldots x_{n-1}$ est orthogonal à x_i pour $i = 1, \ldots, n-1$, que le produit vectoriel est une application $(n-1)$ linéaire alternée et enfin que pour $n = 3$ on retrouve la définition connue du produit vectoriel de deux vecteurs dans l'espace.

Proposition 3.3.4.
Soit $f \in \mathscr{L}(E)$. Alors pour tout n-uplet $(x_1, \ldots, x_n)$ de vecteurs de E, on a

$$[f(x_1), \ldots, f(x_n)] = \det f \times [x_1, \ldots, x_n].$$

On savait déjà qu'une application linéaire f transforme un parallélépipède en un parallélépipède. Ce résultat nous dit de plus que f multiplie les volumes orientés par $\det f$, donc les volumes par $|\det f|$.

Démonstration.
Soit $\mathscr{B}$ une base orthonormale directe de E. Alors

$$\begin{aligned}[f(x_1), \ldots, f(x_n)] &= \det_{\mathscr{B}}(f(x_1), \ldots, f(x_n)) \\ &= \det f \times \det_{\mathscr{B}}(x_1, \ldots, x_n) \\ &= \det f \times [x_1, \ldots, x_n].\end{aligned}$$

□

3.4 Automorphismes orthogonaux du plan

Dans cette partie, E est un ev euclidien **orienté** de dimension 2.

Nous allons retrouver dans cette partie les résultats obtenus dans le premier chapitre sur les isométries vectorielles de $\mathbb{C}$. On le généralise ici à tout ev euclidien de dimension 2.

Théorème 3.4.1. 1. Soit $M \in \mathscr{SO}(2)$. Alors il existe $\theta \in \mathbb{R}$ tel que

$$M = R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

De plus l'application

$$\varphi \ : \ \left\{ \begin{array}{ccc} (\mathbb{R},+) & \to & (\mathscr{SO}(2),\times) \\ \theta & \mapsto & R(\theta) \end{array} \right.$$

est un morphisme de groupe surjectif, de noyau $2\pi\mathbb{Z}$. En particulier $\mathscr{SO}(2)$ est un groupe abélien.

2. Si $M \in \mathscr{O}(2)\backslash\mathscr{SO}(2)$, alors il existe $\theta \in \mathbb{R}$ tel que $M = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$.
3. L'application

$$\begin{array}{rccc} \psi : & \mathbb{U} & \to & \mathscr{SO}(2) \\ & z & \mapsto & \begin{pmatrix} \mathrm{Re}(z) & \mathrm{Re}(iz) \\ \mathrm{Im}(z) & \mathrm{Im}(iz) \end{pmatrix} \end{array}$$

est un isomorphisme de groupes ($\mathbb{U}$ est l'ensemble des complexes de module 1).

Démonstration. 1. Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathscr{O}(2)$. Alors les vecteurs colonnes de M forment une b.o.n, donc :

$$\left\{ \begin{array}{rcl} ab + cd & = & 0 \\ a^2 + c^2 & = & 1 \\ b^2 + d^2 & = & 1 \end{array} \right. .$$

Ainsi, il existe $\theta, \rho \in \mathbb{R}$ tels que $a = \cos\theta, c = \sin\theta, b = \cos\rho, d = \sin\rho$. Alors, $\cos\theta\cos\rho + \sin\theta\sin\rho = 0$ *i.e.* $\cos(\theta-\rho) = 0$, *i.e.* $\theta = \rho + \frac{\pi}{2}[\pi]$. Ainsi,

$$\left\{ \begin{array}{rcl} \cos\theta & = & \sin\rho \\ \sin\theta & = & -\cos\rho \end{array} \right.$$

ou

$$\left\{ \begin{array}{rcl} \cos\theta & = & -\sin\rho \\ \sin\theta & = & \cos\rho \end{array} \right. .$$

Le premier cas n'est possible que si $M \in \mathscr{SO}(2)$, le second que si $M \in \mathscr{O}(2)\backslash\mathscr{SO}(2)$.
Pour finir de montrer **??**, on a, pour tous $\theta, \rho \in \mathbb{R}$, $\varphi(\theta+\rho) = R(\theta+\rho) = R(\theta) \times R(\rho)$ après un calcul faisant intervenir la formule de trigonométrie $\cos(\theta+\rho) = \cos\theta\cos\rho - \sin\theta\sin\rho$. L'application φ est donc bien un morphisme de groupes. Sa surjectivité est évidente d'après la première partie de cette démonstration. Son noyau est l'ensemble des réels θ tels que $\cos\theta = 1$ et $\sin\theta = 0$: c'est donc bien $2\pi\mathbb{Z}$. Et enfin, on a évidemment $R(\theta) \times R(\rho) = \varphi(\theta+\rho) = \varphi(\rho+\theta) = R(\rho) \times R(\theta)$, donc $\mathscr{SO}(2)$ est abélien.

2. Même démonstration.
3. Il s'agit de montrer qu'il s'agit bien d'une application à valeurs dans $\mathscr{SO}(2)$, ce qui est assez facile dès qu'on remarque que tout complexe z s'écrit sous la forme $e^{i\theta}$ et que $\mathrm{Re}(z) = \cos\theta$, $\mathrm{Im}(z) = \sin\theta$, $\mathrm{Re}(iz) = -\sin\theta$, $\mathrm{Im}(iz) = \cos\theta$. Par un calcul direct (en utilisant le fait que $|z| = 1$) ou d'après le point précédent, on montre qu'il s'agit d'un morphisme de groupes. Enfin, ce morphisme est injectif car si $z \in \mathrm{Ker}\,\psi$, on a nécessairement $\mathrm{Re}(z) = 1$ et $\mathrm{Im}(z) = 0$, donc $z = 1$. Il est surjectif car toute $M \in \mathscr{SO}(2)$ s'écrit sous la forme $R(\theta)$, qui a pour antécédent $e^{i\theta}$.

□

Théorème 3.4.2.
Soit f une isométrie vectorielle directe de E (*i.e.* un automorphisme orthogonal positif). Alors :

(i) Il existe un unique θ (modulo 2π) tel que la matrice de f dans n'importe quelle b.o.n. **directe** soit $R(\theta)$.
On dit alors que f est la *rotation vectorielle d'angle* θ et que θ est une *mesure* de l'angle de f.

(ii) Si f n'est pas l'identité, l'ensemble des points fixes de f (*i.e.* $\mathrm{Ker}(f-\mathrm{Id})$) est réduit à $\{0\}$.

Démonstration. (i) Soient $\mathscr{B}$ et $\mathscr{B}'$ deux b.o.n. directes de E. Alors $\mathrm{Mat}_{\mathscr{B}}(f) \in \mathscr{SO}(2)$, donc d'après le théorème 3.4.1, il existe $\theta \in \mathbb{R}$ tel que $\mathrm{Mat}_{\mathscr{B}}(f) = R(\theta)$. Alors $\mathrm{Mat}_{\mathscr{B}'}(f) = PR(\theta)P^{-1}$, où P est la matrice de passage $\mathrm{Mat}_{\mathscr{B}'}(\mathscr{B})$. Mais comme $\mathscr{B}$ et $\mathscr{B}'$ sont deux b.o.n. directes, $P \in \mathscr{SO}(2)$, et donc il existe $\rho \in \mathbb{R}$ tel que $P = R(\rho)$. On a ainsi : $\mathrm{Mat}_{\mathscr{B}'}(f) = R(\rho)R(\theta)R(-\rho) = R(\rho+\theta-\rho) = R(\theta)$.
Il faut démontrer l'unicité de θ : mais pour tout $\theta_1, \theta_2 \in \mathbb{R}$, on a $R(\theta_1) = R(\theta_2)$ ssi $R(\theta_1-\theta_2) = \mathrm{Id}$ ssi $(\theta_1-\theta_2) \in \mathrm{Ker}\,\varphi$ ssi $(\theta_1-\theta_2) \in 2\pi\mathbb{Z}$ ssi $\theta_1 = \theta_2$ $[2\pi]$.

(ii) Si $f = \mathrm{Id}$, on a immédiatement $\mathrm{Ker}(f-\mathrm{Id}) = E$.
Sinon, on a $\mathrm{Mat}_{\mathscr{B}}(f - \mathrm{Id}) = R(\theta) - \mathrm{Id} = \begin{pmatrix} \cos\theta - 1 & -\sin\theta \\ \sin\theta & \cos\theta - 1 \end{pmatrix}$. Cette matrice a pour déterminant $(\cos\theta-1)^2 + \sin^2\theta = 2(1-\cos\theta)$. Or $f \neq \mathrm{Id}$,

donc $\theta \notin 2\pi\mathbb{Z}$, *i.e.* $\cos\theta \neq 1$. Le déterminant précédent est donc non nul, c'est-à-dire que $(f - \mathrm{Id})$ est un automorphisme, donc son noyau est réduit à $\{0\}$. □

Remarque 3.4.3.
Géométriquement, une rotation vectorielle d'angle non nul modulo 2π n'a qu'un point fixe : son centre.

Remarque 3.4.4.
On parle de « rotation d'angle de mesure θ » dans le point (i) du théorème 3.4.2 sans avoir jamais défini auparavant les mots « angle » et « mesure ».

Bien que toute construction rigoureuse de la notion d'angle orienté soit hors programme, on peut cependant résumer la définition d'un angle orienté de la manière suivante : pour tous vecteurs non nuls u et v de $\mathbb{R}^2$, avec $u' = \|u\|^{-1} u$ et $v' = \|v\|^{-1} v$, il existe une unique rotation r telle que $r(u') = v'$, et c'est cette rotation que l'on peut appeler *angle orienté* de (u, v). Tout réel θ pour lequel r admet $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ pour matrice dans une base orthonormale directe est alors appelé **UNE** *mesure* de l'angle (u, v) et est généralement notée elle aussi (u, v). La notation usuelle $(u, v) = \theta\ [2\pi]$ se trouve ainsi justifiée.

Attention, il est indispensable que la base utilisée pour déterminer θ via la matrice de r soit **DIRECTE**, sinon une mesure de l'angle obtenue est en fait l'opposée d'une mesure de l'angle (u, v), modulo 2π.

Théorème 3.4.5 (Détermination d'une mesure de l'angle d'une rotation)**.**
Soient f une rotation vectorielle de E, θ une mesure de son angle et u un vecteur **unitaire**. Soit $\mathscr{C}$ une b.o.n. directe de E. Alors $\cos\theta = \langle u \,|\, f(u)\rangle$ et $\sin\theta = \det_{\mathscr{C}}(u, f(u))$.

Démonstration.
Soit v un vecteur tel que (u, v) soit une b.o.n.d. $\mathscr{B}$ de E. Alors $\mathrm{Mat}_{\mathscr{B}}(f) = R(\theta)$. Donc $f(u) = \cos\theta u + \sin\theta v$, d'où $\langle u \,|\, f(u)\rangle = \cos\theta$, et $\det_{\mathscr{C}}(u, f(u)) = \det_{\mathscr{B}}(u, f(u)) = \begin{vmatrix} 1 & \cos\theta \\ 0 & \sin\theta \end{vmatrix} = \sin\theta$. □

Remarque 3.4.6.
Si u n'est pas unitaire, $\det(u, f(u)) = \|u\|^2 \sin\theta$ et $\langle u \,|\, f(u)\rangle = \|u\|^2 \cos\theta$.

Remarque 3.4.7.
On remarque que dans une b.o.n.d., la trace d'une rotation est $2\cos\theta$. La trace ne dépendant pas de la base choisie, si l'on connaît la matrice M d'une rotation dans une base quelconque, alors une mesure θ de son angle vérifie $2\cos\theta = \mathrm{tr}\, M$.

Théorème 3.4.8.
Une application orthogonale négative (*i.e.* qui n'est pas une rotation) est une *réflexion*, c'est-à-dire une symétrie orthogonale par rapport à une droite.

Remarque 3.4.9.
En dimension quelconque, une réflexion est une symétrie orthogonale par rapport à un hyperplan.

Démonstration.
Soit $f \in \mathscr{O}^-(E)$. Soit $\mathscr{B}$ une b.o.n.d. de E et $\theta \in \mathbb{R}$ tel que $\mathrm{Mat}_{\mathscr{B}}(f) = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix} = A(\theta)$. On note $\mathscr{B} = (e_1, e_2)$. On introduit le vecteur $u = \cos\dfrac{\theta}{2} e_1 + \sin\dfrac{\theta}{2} e_2$. On le complète en une b.o.n.d. avec $v = -\sin\dfrac{\theta}{2} e_1 + \cos\dfrac{\theta}{2} e_2$. On calcule $f(u) = A(\theta).\begin{pmatrix} \cos\dfrac{\theta}{2} \\ \sin\dfrac{\theta}{2} \end{pmatrix} = u$ et $f(v) = A(\theta).\begin{pmatrix} -\sin\dfrac{\theta}{2} \\ \cos\dfrac{\theta}{2} \end{pmatrix} = -v$. Par conséquent $\mathrm{Mat}_{(u,v)}(f) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, qui est bien la matrice d'une réflexion. □

Théorème 3.4.10.
Tout automorphisme de E est un produit de réflexions.

Démonstration.
Pour tout $\theta \in \mathbb{R}$, $R(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Or dans ce produit de matrices, la première matrice est celle d'une réflexion d'après le théorème précédent, et la seconde également. □

Ce produit de matrices et le théorème 3.4.8 donnent la décomposition géométrique d'une rotation (attention : ce produit ne commute pas !).

Chapitre XXVI

Séries numériques

Dans tout ce chapitre, $\mathbb{K}$ désigne le corps $\mathbb{R}$ ou $\mathbb{C}$, et $(u_n)_{n\in\mathbb{N}}$, $(v_n)_{n\in\mathbb{N}}$ et $(w_n)_{n\in\mathbb{N}}$ sont des suites à valeurs dans $\mathbb{K}$.

1 Prolégomènes

Définition 1.1.
À toute suite $(u_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ on associe la suite $(S_n)_{n\in\mathbb{N}}$ définie par

$$\forall n \in \mathbb{N},\ S_n = \sum_{k=0}^{n} u_k.$$

— Cette suite (S_n) est appelée *série de terme général* u_n. On la note $\sum u_n$ ou $\sum_{n\geqslant 0} u_n$. L'indice n est bien entendu muet.
— Lorsque la suite (u_n) n'est définie qu'à partir d'un certain rang n_0, la série de terme général u_n est définie par la suite $S_n = \sum_{k=n_0}^{n} u_k$, pour tout $n \geqslant n_0$. Elle est notée $\sum_{n\geqslant n_0} u_n$.
— Le terme d'indice n de la suite (S_n) s'appelle la *somme partielle d'indice (ou d'ordre)* n, ou n^e *somme partielle* de la série $\sum u_n$.
— On dit que la série $\sum u_n$ *converge* si la suite (S_n) converge. Dans ce cas la limite de (S_n) est appelée *somme de la série* $\sum u_n$ et notée $\sum_{n=0}^{+\infty} u_n$.
Dans le cas contraire on dit que la série *diverge*.
— La *nature* d'une série est sa convergence ou sa divergence. Deux séries sont dites *de même nature* si elles sont toutes les deux convergentes ou toutes les deux divergentes.

Remarque 1.2.
Une série n'est donc qu'une suite, et on peut donc lui appliquer tous les résultats connus sur les suites. Réciproquement, toute suite est une série (*cf.* 1.8).

Remarque 1.3.
Si (u_n) est complexe, notons (a_n) sa partie réelle et (b_n) sa partie imaginaire. Alors, en vertu du cours sur les suites, $\sum u_n$ converge si et seulement si $\sum a_n$ et $\sum b_n$ convergent, et dans le cas de convergence, $\sum_{n=0}^{+\infty} u_n = \sum_{n=0}^{+\infty} a_n + i\sum_{n=0}^{+\infty} b_n$.

Exemple 1.4 (Séries arithmétiques)**.**
Les séries de la forme $\sum na$, avec $a \in \mathbb{C}$, ne sont convergentes que si $a = 0$.

Dans tous les cas la somme partielle S_n vaut $a\dfrac{n(n+1)}{2}$.

Définition 1.5.
Soit $\sum_{n\geqslant 0} u_n$ une série convergente, alors pour tout $n \in \mathbb{N}$, la série $\sum_{k\geqslant n} u_k$ converge également. Sa somme $R_n = \sum_{k=n+1}^{+\infty} u_k$ est appelée *reste d'ordre (ou d'indice)* n de la série $\sum u_n$.

De plus, pour tout $n \in \mathbb{N}$, on a

$$\sum_{k=0}^{n} u_k + \sum_{k=n+1}^{+\infty} u_k = \sum_{k=0}^{+\infty} u_k,$$

soit, en notant S_n la somme partielle d'ordre n et R_n le reste d'ordre n,

$$S_n + R_n = \sum_{k=0}^{+\infty} u_k.$$

Démonstration.
Soit $n \in \mathbb{N}$ et $N \geqslant n$. Alors,

$$\sum_{k=n+1}^{N} u_k = \sum_{k=0}^{N} u_k - \sum_{k=0}^{n} u_k = S_N - S_n.$$

Comme (S_N) converge vers $\sum_{k=0}^{+\infty} u_k$, alors $\sum_{k\geqslant n+1} u_k$ converge et sa somme est donc

$$\sum_{k=n+1}^{+\infty} u_k = \sum_{k=0}^{+\infty} u_k - S_n.$$

□

Exemple 1.6 (Séries géométriques)**.**
Les séries de la forme $\sum z^n$, avec $z \in \mathbb{C}$, sont convergentes si et seulement si $|z| < 1$. Dans tous les cas la somme partielle S_n vaut $\dfrac{1-z^{n+1}}{1-z}$ si $z \neq 1$, et $n+1$ si $z = 1$.

Si $|z| < 1$, alors la somme de la série est

$$\sum_{n=0}^{+\infty} z^n = \frac{1}{1-z}.$$

Le reste de la série est

$$R_n = \sum_{k=n+1}^{+\infty} z^k = \frac{z^{n+1}}{1-z}.$$

Remarque 1.7.
Soit $\sum u_n$ une série convergente, dont on note S_n et R_n les restes à l'ordre n.

Alors $\displaystyle\sum_{n=0}^{+\infty} u_n = S_n + R_n$ et $R_n \xrightarrow[n\to+\infty]{} 0$.

En particulier, si $|R_n| < \varepsilon$, on peut dire que S_n est une approximation de $\displaystyle\sum_{n=0}^{+\infty} u_n$ à ε près.

Proposition 1.8.
Deux séries dont les termes généraux sont égaux à partir d'un certain rang ont même nature.

Démonstration.
Soient (u_n) et (v_n) deux suites égales à partir du rang N.
On note $S_n = \displaystyle\sum_{k=0}^{n} u_k$ et $S'_n = \sum_{k=0}^{n} v_k$.

Alors pour tout $n \geqslant N$, $S_n = S'_n + (S_N - S'_N)$. □

Proposition 1.9 (Lien suite-série)**.**
L'application

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{K}^{\mathbb{N}} & \longrightarrow & \mathbb{K}^{\mathbb{N}} \\ u & \longmapsto & S = \left(\displaystyle\sum_{k=0}^{n} u_k \right)_{n\in\mathbb{N}} \end{array} \right.$$

est un automorphisme d'espaces vectoriels.

Sa réciproque est l'application $\varphi^{-1} : \mathbb{K}^{\mathbb{N}} \to \mathbb{K}^{\mathbb{N}}$, où pour tout $S \in \mathbb{K}^{\mathbb{N}}$, $u = \varphi^{-1}(S)$ est la suite définie par

$$u_0 = S_0 \text{ et } \forall n \in \mathbb{N}^*,\ u_n = S_n - S_{n-1}.$$

Démonstration.
La linéarité de φ est facile à vérifier. Il est également aisé de montrer que $\varphi \circ \psi = \psi \circ \varphi = \mathrm{Id}$. □

Remarque 1.10.
En posant $S_{-1} = 0$, on peut écrire que, pour tout $n \in \mathbb{N}$,

$$S_n = \sum_{k=0}^{n} u_k = \sum_{k=0}^{n} S_k - S_{k-1}.$$

Toute série peut donc être vue comme une série télescopique.

Proposition 1.11 (Séries télescopiques)**.**
La suite (u_n) et la série $\sum(u_{n+1} - u_n)$ ont même nature.

Dans le cas de convergence,

$$u_n - u_0 \xrightarrow[n\to+\infty]{} \sum_{n=0}^{+\infty} u_{n+1} - u_n.$$

Démonstration.
Nous savons déjà que les suites $(u_n)_{n\in\mathbb{N}}$ et $(u_{n+1})_{n\in\mathbb{N}}$ ont même nature.

De plus la somme partielle d'indice n de la série $\sum(u_{n+1} - u_n)$ vaut $u_{n+1} - u_0$ par sommation télescopique. Elle est donc égale au terme u_{n+1}, à une constante près, et a donc la même nature que la suite $(u_{n+1})_{n\in\mathbb{N}}$.

Dans le cas de convergence, il reste à passer à la limite dans la relation $\displaystyle\sum_{n=0}^{N}(u_{n+1} - u_n) = u_{N+1} - u_0$. □

Exemple 1.12.
La série $\displaystyle\sum_{n>0} \frac{1}{n(n+1)}$ converge. En effet pour tout $n \in \mathbb{N}^*$, $\dfrac{1}{n(n+1)} = \dfrac{1}{n} - \dfrac{1}{n+1}$, et la suite $\left(\dfrac{1}{n}\right)_{n>0}$ converge.

Nous pouvons même aller plus loin : $\displaystyle\sum_{k=1}^{n} \frac{1}{k(k+1)} = 1 - \frac{1}{n+1}$ donc $\displaystyle\sum_{n=1}^{+\infty} \frac{1}{n(n+1)} = 1$.

On voit aussi que le reste d'ordre n vaut $\dfrac{1}{n+1}$.

Exercice 1.13.
En simplifiant $\dfrac{(n+1)-n}{1+n(n+1)}$, montrer que $\sum \arctan \dfrac{1}{1+n+n^2}$ converge et calculer sa somme.

Proposition 1.14 (Linéarité de la somme)**.**
L'ensemble des suites dont la série est convergente, muni des lois + et ·, forme un $\mathbb{K}$-espace vectoriel et l'application qui à une telle suite associe la somme de sa série est linéaire.

Démonstration.
Élémentaire, d'après les résultats sur les suites. □

Finissons par le résultat principal de cette première partie :

Théorème 1.15 (Divergence grossière)**.** (i) Si la série $\sum u_n$ converge, alors $u_n \xrightarrow[n\to+\infty]{} 0$.

(ii) Si la suite (u_n) ne tend pas vers 0, on dit que la série $\sum u_n$ *diverge grossièrement.*

Démonstration. (i) Supposons que la série $\sum u_n$ converge. Puisque pour tout $n > 0$, $u_n = S_n - S_{n-1}$, alors u_n est la différence des termes généraux de deux suites convergeant vers la même limite. La suite (u_n) tend donc vers 0.

(ii) C'est la contraposée du premier point.

□

Exemple 1.16.
La série $\sum \cos n$ diverge grossièrement. En effet, en supposant que $\cos n \xrightarrow[n\to+\infty]{} 0$, la relation $\cos(2n) = 2\cos^2 n - 1$ donne une contradiction.

 La réciproque du premier point du théorème 1.13 est fausse. On peut citer en exemple la série harmonique $\displaystyle\sum_{n\geqslant 1} \frac{1}{n}$, qui sera revue plus tard.

Donnons également l'exemple de la suite $u_n = \ln(n+2) - \ln(n+1) = \ln\left(1 + \dfrac{1}{n+1}\right)$. Évidemment, $u_n \xrightarrow[n\to+\infty]{} 0$.

Mais $\displaystyle\sum_{k=0}^{n} u_k = \ln(n+2)$, par sommation télescopique. La série $\sum u_n$ diverge donc.

2 Séries à termes réels positifs

Étudions maintenant le cas particulier où tous les termes d'une série sont des réels positifs ou nuls. La propriété fondamentale est dans ce cas la suivante.

Proposition 2.1.
Soit (u_n) une suite à valeurs positives et $S_n = \displaystyle\sum_{k=0}^{n} u_k$. Alors la suite (S_n) est croissante.

Démonstration.
Tout simplement, $S_{n+1} - S_n = u_{n+1} \geqslant 0$. □

Remarque 2.2.
Attention, une série peut ne pas être à terme positifs mais avoir toutes ses sommes partielles positives, comme la série $\displaystyle\sum_{n\geqslant 0} (-1)^n$.

Proposition 2.3.
Une série à termes positifs converge si et seulement si la suite de ses sommes partielles est majorée.

Démonstration.
La suite des sommes partielles est croissante. Elle est donc convergente si et seulement si elle est majorée, comme conséquence directe du théorème de la limite monotone.
□

Proposition 2.4.
Soient (u_n) et (v_n) deux suites réelles telles que pour tout $n \in \mathbb{N}$, $0 \leqslant u_n \leqslant v_n$.

(i) Si $\sum v_n$ converge, alors $\sum u_n$ également et $0 \leqslant \displaystyle\sum_{n=0}^{+\infty} u_n \leqslant \sum_{n=0}^{+\infty} v_n$.

(ii) Si $\sum u_n$ diverge, alors $\sum v_n$ également.

Démonstration.
Il suffit de remarquer que si (S_n) est la suite des sommes partielles de $\sum u_n$ et (S'_n) celle de $\sum v_n$, alors $0 \leqslant S_n \leqslant S'_n$.

(i) (S'_n) converge, donc est majorée, donc (S_n) est également majorée, et comme elle est croissante, elle converge également. Il reste alors à passer à la limite dans la relation $0 \leqslant S_n \leqslant S'_n$.

(ii) c'est le théorème de minoration.

□

Remarque 2.5.
Si la relation $0 \leqslant u_n \leqslant v_n$ n'est vérifiée qu'à partir d'un certain rang, le résultat du théorème 2.4 est valable, à ceci près que dans le point (i) on ne peut pas conclure que $0 \leqslant \sum_{n=0}^{+\infty} u_n \leqslant \sum_{n=0}^{+\infty} v_n$, mais seulement $0 \leqslant \sum_{n=N}^{+\infty} u_n \leqslant \sum_{n=N}^{+\infty} v_n$.

Exemple 2.6.
$\sum \frac{1}{(n+1)^2}$ converge et

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

En effet, pour tout $n > 0$, $0 < \frac{1}{(n+1)^2} < \frac{1}{n(n+1)}$, donc $0 < \sum_{n=1}^{+\infty} \frac{1}{(n+1)^2} < 1$ car $\sum_{n=1}^{+\infty} \frac{1}{n(n+1)} = 1$. Puisque pour $n = 0$, $\frac{1}{(n+1)^2} = 1$, il vient le résultat.

Corollaire 2.7.
Soient (u_n) et (v_n) deux suites réelles positives, (v_n) ne s'annulant pas à partir d'un certain rang.

(i) Si $u_n = O(v_n)$, alors la convergence de $\sum v_n$ entraîne celle de $\sum u_n$.

(ii) Si $u_n = o(v_n)$, alors la convergence de $\sum v_n$ entraîne celle de $\sum u_n$.

(iii) Si $u_n \sim v_n$ (donc (u_n) ne s'annule pas à partir d'un certain rang), alors $\sum v_n$ et $\sum u_n$ sont de même nature.

Démonstration. (i) $\frac{u_n}{v_n}$ est bornée par un certain réel $M > 0$, donc à partir d'un certain rang, $0 \leqslant u_n \leqslant M v_n$ car (u_n) et (v_n) sont positives. On conclut donc avec 2.4.

(ii) si $u_n = o(v_n)$, alors en particulier $u_n = O(v_n)$.

(iii) si $u_n \sim v_n$, alors $u_n = O(v_n)$ et $v_n = O(u_n)$.

□

Exemple 2.8.
Puisque $\sin\left(\frac{1}{2^n}\right) \sim \frac{1}{2^n}$, d'après le résultat sur les séries géométriques, $\sum \sin\left(\frac{1}{2^n}\right)$ converge.

Pour pouvoir utiliser le dernier corollaire, nous avons besoin de « séries étalon », dont la nature est bien connue, et auxquelles on compare les séries à étudier. Les quelques exemples déjà étudiés font partie de ces séries de référence standard, mais la famille de séries la plus utilisée est celle des *séries de Riemann*, dont font partie la série harmonique et la série $\sum \frac{1}{(n+1)^2}$.

Théorème 2.9.
Soit $\alpha \in \mathbb{R}$. La série $\sum_{n \geqslant 1} \frac{1}{n^\alpha}$ converge si et seulement si $\alpha > 1$.

Démonstration.
Si $\alpha = 1$, remarquons que $\frac{1}{n} \sim \ln(n+1) - \ln n$. Donc $\sum_{n \geqslant 1} \frac{1}{n^\alpha}$ est de même nature que $\sum_{n \geqslant 1} (\ln(n+1) - \ln n)$, qui elle-même est de même nature que la suite $(\ln n)$ d'après 1.9, d'où la divergence.

Si $\alpha \neq 1$, $\frac{1}{n^\alpha} \sim \frac{1}{\alpha - 1}\left(\frac{1}{n^{\alpha-1}} - \frac{1}{(n+1)^{\alpha-1}}\right)$ (effectuer un développement asymptotique de $\frac{1}{n^{\alpha-1}} - \frac{1}{(n+1)^{\alpha-1}}$ ou appliquer l'inégalité des accroissements finis à $x \mapsto x^{1-\alpha}$). La série de terme général $\frac{1}{n^{\alpha-1}} - \frac{1}{(n+1)^{\alpha-1}}$ est de même nature que la suite $\left(\frac{1}{n^{\alpha-1}}\right)$, d'où le résultat.

On peut aussi remarquer que si $\alpha \leqslant 0$, la divergence est grossière, et si $0 < \alpha < 1$, la série diverge car $\frac{1}{n^\alpha} > \frac{1}{n}$. □

Le résultat classique suivant est une application directe de 2.7 et 2.9 :

Corollaire 2.10 (Règle $n^\alpha u_n$)**.**
Soient (u_n) une suite réelle positive et $\alpha \in \mathbb{R}$.

(i) S'il existe $\alpha > 1$ telle que $n^\alpha u_n \xrightarrow[n\to+\infty]{} 0$, alors $\sum u_n$ converge.

(ii) S'il existe $\alpha \leqslant 1$ telle que $n^\alpha u_n \xrightarrow[n\to+\infty]{} +\infty$, alors $\sum u_n$ diverge.

(iii) Si la suite $(n^\alpha u_n)$ converge vers une limite non nulle, la série $\sum u_n$ converge si et seulement si $\alpha > 1$.

Démonstration. (i) si $n^\alpha u_n \xrightarrow[n\to+\infty]{} 0$ alors $u_n = o\left(\frac{1}{n^\alpha}\right)$, et $\sum \frac{1}{n^\alpha}$ converge.

(ii) si $n^\alpha u_n \xrightarrow[n\to+\infty]{} +\infty$ alors $\frac{1}{n^\alpha} = o(u_n)$, et $\sum \frac{1}{n^\alpha}$ diverge.

(iii) si la suite $n^\alpha u_n \xrightarrow[n\to+\infty]{} \ell$ avec $\ell \in \mathbb{R}_+^*$, $\sum u_n$ et $\sum \frac{1}{n^\alpha}$ ont même nature.

□

Exemple 2.11 (Séries de Bertrand)**.**
Soient α, $\beta \in \mathbb{R}$. On considère la série $\sum_{n\geqslant 2} \frac{1}{(\ln n)^\beta n^\alpha}$.

• Si $\alpha > 1$: il existe $\gamma \in]1, \alpha[$ et $n^\gamma \frac{1}{(\ln n)^\beta n^\alpha} \xrightarrow[n\to+\infty]{} 0$ par croissances comparées, car $\alpha - \gamma > 0$. Ainsi la série converge.

• Si $\alpha < 1$: il existe $\gamma \in]\alpha, 1[$ et $n^\gamma \frac{1}{(\ln n)^\beta n^\alpha} \xrightarrow[n\to+\infty]{} +\infty$ par croissances comparées, car $\alpha - \gamma < 0$. Ainsi la série diverge.

• Si $\alpha = 1$: si $\beta \leqslant 0$, le terme général est plus grand que $\frac{1}{n}$, donc la série diverge. Nous traiterons le cas $\beta > 0$ en 3.3.

3 Comparaison série-intégrale

Proposition 3.1.
Soit $f : \mathbb{R}_+ \to \mathbb{R}_+$ une fonction continue par morceaux et décroissante.
Alors la série $\sum f(n)$ converge si et seulement si la suite $\left(\int_0^n f(t)\,\mathrm{d}t\right)$ est convergente.
De plus la suite définie par $u_n = \sum_{k=0}^{n} f(k) - \int_0^n f(t)\,\mathrm{d}t$ converge.

Démonstration.
Soit $k \in \mathbb{N}$. Par décroissance de f, on a :

$$\forall t \in [k, k+1],\ 0 \leqslant f(k+1) \leqslant f(t) \leqslant f(k).$$

Puis, par intégration de cet encadrement sur $[k, k+1]$:

$$0 \leqslant f(k+1) \leqslant \int_k^{k+1} f(t)\,\mathrm{d}t \leqslant f(k) \qquad \text{(XXVI.1)}$$

et par sommation, pour $n \geqslant 1$:

$$0 \leqslant \sum_{k=0}^{n-1} f(k+1) \leqslant \int_0^n f(t)\,\mathrm{d}t \leqslant \sum_{k=0}^{n-1} f(k)$$

ou encore

$$0 \leqslant \sum_{k=0}^{n} f(k) - f(0) \leqslant \int_0^n f(t)\,\mathrm{d}t \leqslant \sum_{k=0}^{n} f(k) - f(n). \qquad \text{(XXVI.2)}$$

Les suites $\sum_{k=0}^{n} f(k)$ et $\int_0^n f(t)\,\mathrm{d}t$ ont donc la même nature.

De plus, il vient $0 \leqslant f(n) \leqslant \sum_{k=0}^{n} f(k) - \int_0^n f(t)\,\mathrm{d}t$, soit $0 \leqslant u_n$. Ainsi (u_n) est minorée. Enfin, on a

$$u_{n+1} - u_n = f(n+1) - \int_n^{n+1} f(t)\,\mathrm{d}t \leqslant 0.$$

La suite (u_n) est donc décroissante et minorée et converge donc. □

Remarque 3.2.
L'encadrement XXVI.1 est à rapprocher de la méthode des rectangles, vue dans le chapitre sur l'intégration.

Exemple 3.3.
Achevons l'étude des séries de Bertrand commencée en 2.11.

Si $\beta > 0$, considérons l'application $f : t \mapsto \frac{1}{t(\ln t)^\beta}$. Elle est continue et décroissante sur $[2, +\infty[$.

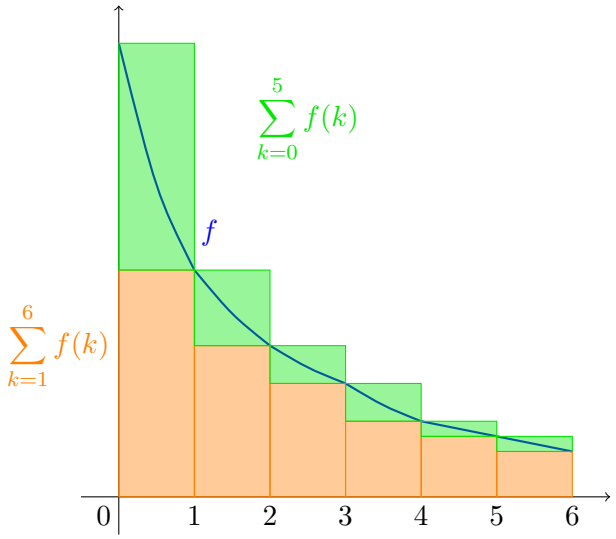


FIGURE XXVI.1 – Exemple de comparaison série-intégrale pour une fonction f décroissante, positive.

Si $\beta = 1$, une primitive de f est $F : t \mapsto \ln(\ln t)$ et $\displaystyle\int_2^n f(t)\,\mathrm{d}t = F(n) - F(2)$. Or $F(n) \xrightarrow[n\to+\infty]{} +\infty$ donc la série diverge.

Par comparaison, la série diverge également si $0 \leqslant \beta < 1$.

Si $\beta > 1$, une primitive de f est $F : t \mapsto \dfrac{(\ln t)^{1-\beta}}{1-\beta}$ et $\displaystyle\int_2^n f(t)\,\mathrm{d}t = F(n) - F(2)$. Or $F(n) \xrightarrow[n\to+\infty]{} 0$ car $1-\beta < 0$, donc la série converge.

Exercice 3.4.
Redémontrer le résultat 2.9 en utilisant 3.1.

Exemple 3.5.
On pose $f : x \mapsto \dfrac{1}{1+x}$. On sait alors que la suite de terme général $u_n = \displaystyle\sum_{k=0}^{n} f(k) - \int_0^n f(t)\,\mathrm{d}t = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} - \ln n$ converge, vers une limite notée γ et nommée *constante d'Euler*.

Exemple 3.6.
L'encadrement (XXVI.2) permet d'avoir une estimation du reste d'une série convergente de la forme $\sum f(n)$ avec f décroissante.
Par exemple, soit $f : x \mapsto \dfrac{1}{x^2}$. Alors

$$\frac{1}{n+1} - \frac{1}{N} = \int_{n+1}^{N} \frac{\mathrm{d}t}{t^2} \leqslant \sum_{n+1}^{N} \frac{1}{n^2} \leqslant \int_n^{N-1} \frac{\mathrm{d}t}{t^2} \leqslant \frac{1}{n} - \frac{1}{N-1}$$

et en passant à la limite quand $N \xrightarrow[n\to+\infty]{} +\infty$,

$$\frac{1}{n+1} \leqslant \sum_{n+1}^{+\infty} \frac{1}{n^2} \leqslant \frac{1}{n}.$$

Si l'on veut une approximation de $\displaystyle\sum_{n=1}^{+\infty} \frac{1}{n^2}$ à 10^{-3} près, il suffit donc de choisir $n = 1000$ et de calculer $\displaystyle\sum_{n=1}^{1000} \frac{1}{n^2}$.

Exercice 3.7.
On peut obtenir une approximation de cette somme en calculant seulement la somme d'une trentaine de termes. Comment ?

4 Séries absolument convergentes

Revenons à des séries à termes quelconques dans $\mathbb{K}$. Nous allons étudier une convergence plus restreinte que la convergence définie en 1.1 : la *convergence absolue*.

Définition 4.1.
On dit que la série $\sum u_n$ est *absolument convergente* si la série à termes positifs $\sum |u_n|$ converge.

Proposition 4.2.
Toute série absolument convergente est convergente.

Démonstration.
Commençons par établir le résultat pour des suites à valeurs réelles. Pour cela, définissons pour une suite (u_n) les deux suites (u_n^-) et (u_n^+) définies par : $u_n^+ = \max(u_n, 0)$ et $u_n^- = \max(-u_n, 0)$. Nous avons alors :

$$u_n^+ = \begin{cases} 0 & \text{si } u_n < 0 \\ |u_n| & \text{si } u_n \geqslant 0 \end{cases}$$

$$u_n^- = \begin{cases} 0 & \text{si } u_n > 0 \\ |u_n| & \text{si } u_n \leqslant 0 \end{cases}$$

$$0 \leqslant u_n^+ \leqslant |u_n| \qquad \text{(XXVI.3)}$$

$$0 \leqslant u_n^- \leqslant |u_n| \qquad \text{(XXVI.4)}$$

$$u_n = u_n^+ - u_n^- \qquad \text{(XXVI.5)}$$

$$|u_n| = u_n^+ + u_n^-.$$

De (XXVI.3) et (XXVI.4) on tire que $\sum u_n^+$ et $\sum u_n^-$ sont convergentes car $\sum |u_n|$ est convergente.
De (XXVI.5) on tire que $\sum u_n$ est convergente.

Étendons maintenant ce résultat au cas d'une suite (u_n) à valeurs complexes absolument convergente. Pour tout n, on a $0 \leqslant |\operatorname{Re} u_n| \leqslant |u_n|$, or la série $\sum |u_n|$ converge, donc la série $\sum |\operatorname{Re} u_n|$ est convergente, donc $\sum \operatorname{Re} u_n$ est absolument convergente, donc convergente d'après le premier point. De même $\sum \operatorname{Im} u_n$ converge. Donc $\sum u_n$ converge. □

 La réciproque est fausse. Soit par exemple la suite de terme général $u_n = \dfrac{(-1)^n}{n} - \dfrac{(-1)^{n+1}}{n+1} = v_n - v_{n+1}$, avec $v_n = \dfrac{(-1)^n}{n}$. La série $\sum u_n$ est donc de même nature que la suite (v_n), elle converge donc.
Mais $|u_n| = \dfrac{1}{n} + \dfrac{1}{n+1} \sim \dfrac{2}{n}$, donc $\sum u_n$ n'est pas absolument convergente. On dit qu'une telle suite, convergente mais pas absolument, est *semi-convergente*. L'étude de telles suites est souvent délicate !

Corollaire 4.3.
Soit (u_n) une suite complexe et (v_n) une suite à termes positifs telles que $|u_n| = O(v_n)$. Alors si $\sum v_n$ converge, $\sum u_n$ également.

Démonstration.
Par comparaison de séries à termes positifs, $\sum u_n$ converge absolument, donc converge. □

Remarque 4.4.
Une série à termes de signe constant converge absolument si et seulement si elle converge.

Proposition 4.5.
L'ensemble des séries absolument convergentes est un sous-espace vectoriel de l'ensemble des séries convergentes.

Démonstration.
Élémentaire par l'inégalité triangulaire. □

Proposition 4.6.
Soit $\sum u_n$ une série absolument convergente. Alors

$$\left|\sum_{n=0}^{+\infty} u_n\right| \leqslant \sum_{n=0}^{+\infty} |u_n|.$$

Démonstration.
Soit $N \in \mathbb{N}$, alors, par l'inégalité triangulaire,

$$\left|\sum_{n=0}^{N} u_n\right| \leqslant \sum_{n=0}^{N} |u_n| \leqslant \sum_{n=0}^{+\infty} |u_n|.$$

On conclut par passage à la limite en N. □

5 Représentation décimale des réels

Notons $\mathbb{D}$ l'ensembles des *décimaux*, c'est-à-dire l'ensemble

$$\{\, x \in \mathbb{R} \mid \exists n \in \mathbb{N},\ 10^n x \in \mathbb{Z} \,\} = \left\{ \frac{k}{10^n} \;\middle|\; k \in \mathbb{Z},\ n \in \mathbb{N} \right\}.$$

Rappelons le résultat suivant, démontré dans le chapitre sur les réels : si $x \in \mathbb{R}$, on pose pour tout $n \in \mathbb{N}$, $r_n = \dfrac{\lfloor 10^n x \rfloor}{10^n}$ appelé *approximation décimale par défaut de x à 10^{-n} près*. La suite (r_n) est alors une suite de décimaux inférieurs à x, et elle a x pour limite.
Nous pouvons alors donner le théorème suivant :

Théorème 5.1.
Pour tout $y \in [0,1[$:
• Si $y \notin \mathbb{D}$, il existe une unique suite $(y_n)_{n\in\mathbb{N}^*}$ d'éléments de $[\![0,9]\!]$ telle que $y = \sum_{n=1}^{+\infty} y_n 10^{-n}$.
• Si $y \in \mathbb{D}$, il y a existence de deux telles suites : l'une finissant par une infinité de 0, l'autre par une infinité de 9. Ainsi, $0,1 = 1.10^{-1} + \sum_{n=2}^{+\infty} 0.10^{-n} = 0.10^{-1} + \sum_{n=2}^{+\infty} 9.10^{-n}$.

Dans tous les cas, il existe une unique suite $(y_n)_{n\in\mathbb{N}^*}$ d'éléments de $[\![0,9]\!]$ telle que $y = \sum_{n=1}^{+\infty} y_n 10^{-n}$, et tel que pour tout $n_0 \in \mathbb{N}$, il existe $n \geqslant n_0$ tel que $a_n \neq 9$: la série $\sum_{n\geqslant 1} y_n 10^{-n}$ est alors appelée le *développement décimal propre* de y.

Démonstration.
Prouvons l'existence. Considérons la suite de terme général $r_n = \dfrac{\lfloor 10^n y \rfloor}{10^n}$ (approximation décimale par défaut de y), et posons $y_0 = \lfloor y \rfloor = 0$, et pour tout $n \geqslant 1$: $y_n = 10^n(r_n - r_{n-1}) = \lfloor 10^n y \rfloor - 10 \lfloor 10^{n-1} y \rfloor$.
Les y_n sont donc bien des entiers de $[\![0,9]\!]$.
De plus, : $\sum_{n=1}^{N} y_n 10^{-n} = \sum_{n=1}^{N} (r_n - r_{n-1}) = r_N - r_0 = r_N$.
Puisque (r_n) a pour limite y, alors $y = \sum_{n=1}^{+\infty} y_n 10^{-n}$.
Si la suite (y_n) ne converge pas vers 9, il s'agit bien du développement propre.
Sinon, la suite est stationnaire. Il existe un rang n_0 qui est le maximum de l'ensemble $\{n \in \mathbb{N},\ y_n \neq 9\}$. Le développement propre est alors obtenu en changeant y_{n_0} en $y_{n_0} + 1$, et en changeant tous les termes suivants en 0.
Nous avons toujours $y = \sum_{n=1}^{+\infty} y_n 10^{-n}$ car $\sum_{n=n_0+1}^{+\infty} 9.10^{-n} = 9.10^{-n_0-1}.\dfrac{1}{1-\frac{1}{10}} = 10^{-n_0}$.
Prouvons enfin l'unicité du développement propre. Supposons que y admette deux développements propres distincts : $y = \sum_{n=1}^{+\infty} y_n 10^{-n} = \sum_{n=1}^{+\infty} z_n 10^{-n}$. Notons N le plus petit indice tel que $y_N \neq z_N$, et N' le plus petit indice strictement supérieur à N tel que $y_{N'} \neq 9$. Pour fixer les idées, supposons que $y_N < z_N$.
Alors :

$$\begin{aligned}
y &= \sum_{n=1}^{N-1} y_n 10^{-n} + y_N 10^{-N} + \sum_{n=N+1}^{N'-1} y_n 10^{-n} \\
&\quad + y_{N'} 10^{-N'} + \sum_{n=N'+1}^{+\infty} y_n 10^{-n} \\
&< \sum_{n=1}^{N-1} y_n 10^{-n} + y_N 10^{-N} + \sum_{n=N+1}^{+\infty} 9.10^{-n} \\
&< \sum_{n=1}^{N-1} z_n 10^{-n} + y_N 10^{-N} + 10^{-N} \\
&< \sum_{n=1}^{N-1} z_n 10^{-n} + (y_N + 1) 10^{-N} \\
&< \sum_{n=1}^{N-1} z_n 10^{-n} + z_N 10^{-N} \\
&< y
\end{aligned}$$

ce qui est bien sûr absurde. □

6 Compléments

Voici deux critères de convergence qui peuvent être utiles.

Proposition 6.1 (Test de comparaison logarithmique)**.**
Soient (u_n) et (v_n) deux suites à termes réels strictement positifs telles que pour tout $n \in \mathbb{N}$, $\dfrac{u_{n+1}}{u_n} \leqslant \dfrac{v_{n+1}}{v_n}$.
Alors :

(i) si $\sum v_n$ converge, il en est de même de $\sum u_n$;

(ii) si $\sum u_n$ diverge, il en est de même de $\sum v_n$.

Démonstration.
Nous avons pour tout n, $\dfrac{u_{n+1}}{v_{n+1}} \leqslant \dfrac{u_n}{v_n}$, et donc par récurrence : $\dfrac{u_n}{v_n} \leqslant \dfrac{u_0}{v_0}$. En posant $\mu = \dfrac{u_0}{v_0}$, il vient donc : $u_n \leqslant \mu v_n$. Le résultat découle alors directement de 2.4. □

Proposition 6.2 (Règle de d'Alembert)**.**
Soit (u_n) une suite à termes réels strictement positifs.

(i) S'il existe $q \in]0,1[$ tel que pour tout $n \in \mathbb{N}$, $\dfrac{u_{n+1}}{u_n} \leqslant q$, alors la série $\sum u_n$ est convergente.

(ii) S'il existe $q \in [1,+\infty[$ tel que pour tout $n \in \mathbb{N}$, $\dfrac{u_{n+1}}{u_n} \geqslant q$, alors la série $\sum u_n$ est divergente.

(iii) en particulier, si $\lim\limits_{n\to+\infty} \dfrac{u_{n+1}}{u_n} = \ell \in \overline{\mathbb{R}}$:
- si $\ell \in [0,1[$, la série $\sum u_n$ est convergente ;
- si $\ell > 1$, la série $\sum u_n$ est divergente ;
- si $\ell = 1$, on ne peut rien dire, sauf dans le cas $u_n \leqslant u_{n+1}$ à partir d'un certain rang, où il y a divergence grossière.

Démonstration. (i) Posons $v_n = q^n$. Alors $\sum v_n$ converge, et pour tout n, $\dfrac{u_{n+1}}{u_n} \leqslant \dfrac{v_{n+1}}{v_n}$. Le critère de comparaison logarithmique 6.1 permet alors de conclure.

(ii) Même démonstration (ou même divergence grossière).

(iii) Découle des deux points précédents.

□

Exemple 6.3.

• Soient $x \in \mathbb{R}^*$ et $u_n = \dfrac{x^n}{n!}$. Alors $\dfrac{u_{n+1}}{u_n} \xrightarrow[n\to+\infty]{} 0$, donc $\sum u_n$ converge, et de plus on en tire que $u_n \xrightarrow[n\to+\infty]{} 0$.

• Soient $\alpha \in \mathbb{R}$ et $u_n = n^\alpha$. Alors $\dfrac{u_{n+1}}{u_n} \xrightarrow[n\to+\infty]{} 1$, et pourtant, suivant la valeur de α, $\sum u_n$ peut aussi bien diverger que converger.